UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

ADQUIRIR, INSTALAR, CONFIGURAR Y PUESTA EN CORRECTO FUNCIONAMIENTO DE COMPONENTES QUE PERMITAN DAR CONTINUIDAD Y MEJORAMIENTO A LA SEGURIDAD INFORMÁTICA DEL PARQUE INFORMÁTICO PROPIEDAD DE LA UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS, CONFORMADOS POR: COMPONENTE UNO: DETECCIÓN, PREVENCIÓN Y RESPUESTA DE RED (NDR) Y COMPONENTES DOS: SOFTWARE DE SEGURIDAD ANTIVIRUS.

Tabla de contenido

1. OBJETO

Adquirir, instalar, configurar y puesta en correcto funcionamiento de componentes que permitan dar continuidad y mejoramiento a la seguridad informática del parque informático propiedad de la Universidad Distrital Francisco José de Caldas, conformados por: componente uno: detección, prevención y respuesta de red (NDR) y componentes dos: Software de seguridad antivirus.

Componente 1:

Adquirir, instalar, configurar y puesta en correcto funcionamiento de una solución tecnológica para equipos servidores físicos y virtuales, pc, portátiles y máquinas virtuales propiedad de la Universidad Distrital Francisco José de Caldas, que permita la detección, prevención y respuesta de red contra ciberamenazas, incluyendo soporte técnico 7x24 y actualizaciones (update y upgrade)

Componente 2:

Adquirir, instalar, configurar y puesta en correcto funcionamiento de una solución de seguridad antivirus para equipos servidores físicos y virtuales, pc, portátiles y máquinas virtuales propiedad de la Universidad Distrital Francisco José de Caldas, incluyendo soporte técnico 7x24 y actualizaciones (update y upgrade)

2. ANTECEDENTES

La Universidad Distrital dispone de un parque informático conformado por equipos de cómputo (portátiles y escritorio) y equipos servidores, los cuales cuentan el software de seguridad Kaspersky® instalado y en funcionamiento, el cual protege los dispositivos de ataques tipo 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 2020 adquiriendo con este: 3400 licencias del software de seguridad para endpoints, 200 licencias para la solución de virtualización de Citrix que la universidad adquirió para la prestación de los servicios de nube privada en Aplicaciones y Escritorios Virtuales; y 30 licencias para equipos servidores, distribuidas de la siguiente manera:

Ítem	Dispositivo	Cantidad
1	Citrix XenApp y XenDesktop (Escritorios y aplicaciones Virtuales)	200
2	Equipos Servidores UDNET	20
3	Equipos Servidores Biblioteca	10

Tabla 1 - Licenciamiento escritorios virtuales y servidores

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.

3. ALCANCE

Para el cumplimiento del objeto del contrato, el oferente ganador del presente proceso debe realizar:

Para el **Componente 1** se formulan los siguientes objetivos específicos:

- **3.1.** Adquirir e instalar la plataforma de detección, prevención y respuesta de red contra ciberamenazas.
- **3.2.** Adquisición de 200 licencias para endpoints sobre la plataforma de detección, prevención y respuesta de red contra ciberamenazas con una cobertura de un (1) año cada una.
- **3.3.** Adquirir soporte de partner en esquema 7x24 por un (1) año para toda la solución de detección, prevención y respuesta de red contra ciberamenazas incluyendo actualizaciones (update y upgrade).
- **3.4.** Instalación, configuración y puesta en correcto funcionamiento de la plataforma de detección, prevención y respuesta de red contra ciberamenazas, así como la integración con los dispositivos licenciados.

Para el **Componente 2** se formulan los siguientes objetivos específicos:

- **3.5.** Adquirir 3000 licencias de software de seguridad antivirus para dispositivos de usuario final, con una cobertura de dos (2) años cada una.
- **3.6.** Adquirir 2841 licencias de agente EDR del software de seguridad para dispositivos de usuario final, con una cobertura de dos (2) años cada una.
- **3.7.** Adquirir 200 licencias de software de seguridad antivirus para ambientes virtuales compatibles con XenDesktop 7.15 con una cobertura de dos (2) años cada una.
- **3.8.** Adquirir 30 licencias de software de seguridad antivirus para dispositivos servidores, con una cobertura de dos (2) años cada una.
- **3.9.** Adquirir soporte de partner en esquema 7x24 por dos (2) años para toda la solución de software de seguridad antivirus incluyendo actualizaciones (update y upgrade).
- **3.10.** Instalación, configuración y puesta en correcto funcionamiento de la solución de software de seguridad antivirus.

4. JUSTIFICACIÓN

La Universidad Distrital dispone de un parque informático conformado por equipos de cómputo (portátiles y escritorio) y equipos servidores, los cuales cuentan con el software de seguridad Kaspersky® instalado y en funcionamiento, el cual protege los dispositivos de ataques tipo backdoor, rootkits, troyanos, keyloggers, spyware, virus y otros malware manteniendo la confidencialidad, disponibilidad e integridad de la información almacenada en los dispositivos previamente mencionados.

Los equipos servidores, PC, portátiles y escritorios 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 tools, jokes, exploits, entre otros.

De acuerdo con lo anterior, se requiere la adquisición del licenciamiento del software de seguridad antivirus, así como la adquisición de la plataforma de detección, prevención y respuesta de red contra ciberamenazas, el soporte por parte de la empresa proveedora.

5. CONDICIONES GENERALES

A continuación, se presentan las condiciones generales:

- **a)** El proponente por el simple hecho de presentar su propuesta económica acepta la totalidad de los términos y condiciones establecidas en el presente documento. Por lo tanto, ninguno de estos términos y condiciones establecidas puede generar costos adicionales a la Universidad, a los asignados al presente proceso. Es decir, costos no previstos por el proponente en su propuesta técnica y comercial.
- **b)** En caso de que de la propuesta comercial entregada por el proponente tenga términos y condiciones, estos no podrán contradecir los presentes términos técnicos, teniendo en cuenta que son de obligatorio cumplimiento. En consecuencia, la Universidad Distrital Francisco José de Caldas excluye los términos y condiciones técnicas establecidas por el proponente en su propuesta comercial y únicamente tendrá en cuenta los valores de la oferta económica para la evaluación. En caso de que los términos establecidos contemplen alguna situación o condición no contemplada por la Universidad en los presentes términos técnicos, se revisarán entre las partes para aprobación por parte de la Universidad.
- **c)** El proponente deberá ofertar la totalidad de cada componente con soluciones del mismo fabricante.
- **d)** El proponente o los proponentes de los dos componentes deberán hacer la integración de los mismos durante la instalación, configuración y puesta en correcto funcionamiento de cada componente. Lo anterior sin generar costos adicionales a la Universidad, a los asignados al presente proceso.
- **e)** El software contratado debe corresponder a las últimas versiones funcionales liberadas en el mercado.
- **f)** Para la instalación, configuración, puesta en funcionamiento y carga de las nuevas licencias del software de seguridad (Antivirus), el proponente designará personal experto certificado en el software de seguridad.
- **g)** Para la instalación, configuración, puesta en funcionamiento de la plataforma de detección, prevención y respuesta de red contra ciberamenazas, el proponente designará personal experto certificado en el software.
- **h)** Los productos del software de seguridad (Antivirus) para usuario final de los sistemas Windows deben contar con Idioma español.
- **i)** Se debe tener administración centralizada desde las consolas, que permita realizar instalación del software antivirus en los diferentes equipos y donde se creen las políticas de protección y actualización.
- **j)** En caso de que el proponente ofrezca un software de seguridad antivirus distinto al actualmente instalado, el proponente deberá realizar la desinstalación del antivirus actual de cada equipo e instalar posteriormente el nuevo software sin generar un tiempo de no protección por equipo superior a una hora. Lo anterior deberá ser realizado por sus propios medios sin generar costos adicionales a la Universidad, a los asignados al presente proceso.
- **k)** El proponente 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, así como de la plataforma de detección, prevención y respuesta de red contra ciberamenazas. Los temas y cronograma se coordinarán con el supervisor y personal técnico de UDNET al inicio de la ejecución del contrato.
- **l)** 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 proponente estará en la obligación de hacer la gestión necesaria con la casa matriz logrando que se mantenga el nivel de funcionalidad de los aplicativos descritos en el numeral de Especificaciones Técnicas.
- **m)** El proponente se compromete a mantener a la universidad informada de las diferentes noticias o sucesos de seguridad informática que surjan o sucedan en el ámbito nacional e internacional mediante boletines mensuales y charlas cada dos (2) meses para fomentar a la comunidad universitaria una cultura de seguridad con los datos

personales y empresariales. La programación de estos boletines o charlas serán concertadas entre las dos partes y se adiciona al acta de inicio del contrato.

n) El proponente 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 la duración del contrato.

o) El proponente acordará con el supervisor y la Red de Datos UDNET el cronograma de actividades que incluya, entre otros. Este cronograma hará parte del acta de inicio.

p) El proponente debe cumplir con las obligaciones, términos y condiciones establecidas en el presente proceso incluyendo anexos, atendiendo las instrucciones que el supervisor realice durante la ejecución del contrato.

q) El plazo para la ejecución del contrato consiste en la entrega del licenciamiento total a nombre de la Universidad Distrital, la carga en los equipos servidores de las licencias y la transferencia de conocimiento de la solución.

r) La vigencia del licenciamiento del software de seguridad Antivirus será de dos (2) años, periodo durante el cual el proveedor prestará los servicios de soporte y actualizaciones.

s) La vigencia del licenciamiento del software de detección, prevención y respuesta de red contra ciberamenazas será de un (1) año, periodo durante el cual el proveedor prestará los servicios de soporte y actualizaciones.

t) El partner debe contar con certificación expedida por la casa matriz donde se indica que es canal Partner GOLD o superior del producto para el software de seguridad antivirus.

u) El partner debe contar con certificación expedida por la casa matriz donde se indica que es canal Partner GOLD o superior para plataforma de detección, prevención y respuesta de red contra ciberamenazas.

v) Los proponentes deben estar inscritos en el Sistema Único de Registro de Personas y Banco de Proveedores AGORA de la Universidad Distrital. (https://funcionarios.portaloas.udistrital.edu.co/agora/)

6. CONFIDENCIALIDAD

El proponente respetará el carácter confidencial de toda la información obtenida dentro del marco de la ejecución del contrato y no deberá divulgarse a terceros, sin acuerdo previo y por escrito de la Universidad Distrital Francisco José de Caldas. La información relativa al análisis, aclaración, evaluación y comparación de las propuestas y las recomendaciones para la adjudicación del contrato podrán ser solicitadas a la Universidad Distrital.

7. ESPECIFICACIONES TÉCNICAS MÍNIMAS

Características técnicas - Solución de detección, prevención y respuesta de red.		
Ítem	**Descripción**	**Ficha técnica o link página web fabricante** **Ubicación en la propuesta (Folio N°)** **Diligencia Proponente**
1	**Servidor de Correlación y Consola Administrativa**	
1.01	La solución debe disponer de una consola de gestión centralizada e integral 100% Web	
1.02	La solución deberá poder realizar una inspección de red basado en los siguientes protocolos: HTTP, HTTPS, FTP, SMB, DNS; así como también la capacidad de auditar tráfico TCP y UDP.	
1.03	Debe actuar en tiempo real, ejecutando un análisis profundo y completo de las amenazas; y generando información catalogada a nivel de usuario, IP, nombre de la amenaza, severidad, cantidad de infecciones y cantidad de callbacks. Así como también información detallada del comportamiento de la amenaza entre las que se encuentran:	

Características técnicas - Solución de detección, prevención y respuesta de red.		
Ítem	**Descripción**	**Ficha técnica o link página web fabricante** **Ubicación en la propuesta (Folio N°)** **Diligencia Proponente**
	• **Capacidades nocivas de la amenaza:** comportamiento malicioso, cambios realizados al sistema operativo, identificación de comandos raw asociados al software malicioso. • **Información mínima de cada equipo afectado:** cantidad, tipo, nombre, severidad, dirección IP del servidor de Comando y control, fecha y hora de detección, puertos usados. • Punto de acceso que genero la infección. • En caso de malware desconocido, debe proporcionar la siguiente información: SHA-256/MD5, tipo de archivo, protocolo usado, cantidad de ocurrencias, ejecutable del malware.	
1.04	Contar con funcionalidad que emita reportes de al menos: • Reportes sobre las Alertas (actividad actual o histórica) • Reportes en un rango de fechas y rango de direcciones IP. • Reportes detallados de llamadas a servidores remotos, identificando cuando sea posible la geolocalización de la dirección IP.	
1.05	Los eventos y alertas deben ser notificados al servidor central de gestión y podrán ser enviados a una solución de tipo SIEM.	
1.06	La solución debe contar con un API bidireccional para la integración con otras plataformas y herramientas.	
1.07	La solución debe tener la posibilidad de exportar todos los eventos a formatos como Excel, entre otros.	
1.08	El motor de correlación centralizado debe permitir la validación de certificados.	
1.09	Construcción automática del patrón del comportamiento de la red y de los endpoints en un periodo no superior a dos semanas.	
1.10	Identificación de variación en el patrón de comportamiento de usuarios y procesos en endpoints.	
1.11	Identificación de variación en el patrón de comportamiento relacionado al acceso a dominios sospechosos.	
1.12	El resultado del análisis debe indicar qué modulo detectó la amenaza: motor de AV, reputación de archivos, Sandbox, etc.	
1.13	La solución ofertada debe analizar las imágenes almacenadas en los equipos, independientemente si cuentan con firma digital.	
1.14	Debe contar con un motor de antivirus basado en firmas, heurística, emulación y soporte de una red privada de inteligencia	
1.15	La solución debe contemplar el resguardo del tráfico de red para un posterior análisis forense del mismo.	
1.16	La solución debe poder analizar y procesar trazas externas de datos del tipo .pcap con el objetivo de detectar indicios de amenazas.	
1.17	La tecnología de detección debe identificar indicadores de ataques en tiempo real basándose en patrones de comportamiento de red producto de las descargas, interacciones u otros tipos de aprovechamiento de vulnerabilidades de red hacia internet.	
1.18	Debe correlacionar los ataques combinados que llegan a través de vectores de amenazas vía navegación y correo electrónico.	
1.19	Debe ser capaz de recibir la información de amenazas avanzadas desde una fuente colaborativa externa y distribuirla al resto de componentes de la solución.	
1.20	La solución debe permitir la identificación de las direcciones IP de origen de los ataques, así como su geolocalización en caso de direcciones IP Públicas.	
1.21	La solución deberá tener también la capacidad de detectar amenazas avanzadas que se aprovecha de vulnerabilidades conocidas y/o sitios web maliciosos sin necesidad de acudir a la nube del proveedor.	

Características técnicas - Solución de detección, prevención y respuesta de red.		
Ítem	**Descripción**	**Ficha técnica o link página web fabricante Ubicación en la propuesta (Folio N°) Diligencia Proponente**
1.22	La solución debe proporcionar detección contra ataques originados en la web, como descargas de archivos maliciosos y acciones de devolución de llamada (callback) de malware.	
1.23	La solución debe detectar técnicas de evasión de tráfico TOR networks, Ultrasurf and malicious SSL.	
2	**Análisis de Amenazas de tipo Sandboxing**	
2.01	La solución debe contar con técnicas de detección de evasión de máquinas virtuales.	
2.02	Debe contar con tecnología propietaria de Sandbox. Debe permitir verificar el envío y recepción de información desde y hacia internet sin comprometer la seguridad de la entidad.	
2.03	El proceso de detección de malware del entorno virtual deberá ser capaz de: • Análisis dinámico de comportamiento • Análisis de patrones y firmas • Poder detectar malware de tipo día cero. • Identificar comunicaciones que pudieran ser relacionadas con llamadas de comando y control.	
2.04	La solución debe registrar toda la actividad que un objeto malicioso trate de ejecutar, acción ejecutada en ambientes de máquinas virtuales, presentando las modificaciones sobre el sistema operativo o aplicación que logre modificar, tales como: • Registro de la aplicación • Registro de procesos • Registro de archivos • Registro de comportamiento • Registro de comunicaciones	
2.05	Capacidad para evaluar y analizar, mediante máquinas virtuales o técnicas de emulación, amenazas sobre los sistemas operativos preconfigurados con: Windows 7 Y Windows 10.	
2.06	En el entorno virtual de análisis, el malware deberá ser inspeccionado y examinado en máquinas virtuales correspondientes a varios sistemas operativos, aplicaciones, navegadores y complemento de navegadores.	
2.07	La solución debe ser capaz de ejecutar todo el código sospechoso, URL y diversos tipos de archivos en un entorno virtual propietario de inspección.	
2.08	Capacidad de identificación de extensiones de archivos que han sido modificados	
2.09	La plataforma de Sandbox debe soportar malware de 32-Bit y 64-Bit en modo usuario y kernel.	
2.10	Debe soportar la ejecución e inspección de los siguientes tipos de archivos: documentos de la suite MS Office (en todas sus versiones), documentos PDF, archivos ejecutables, archivos compuestos (Ejemplo Zip, Rar) y archivos multimedia en el entorno de Sandbox.	
2.11	La plataforma de Sandbox debe incluir las licencias de nivel de sistemas operativos y de software instalado.	
2.12	La plataforma de Sandbox debe ser capaz de monitorizar el tráfico generado por la muestra analizada	
2.13	La plataforma de Sandbox facilitará la descarga de dumps de memoria para la realización de análisis forenses.	
2.14	La plataforma de Sandbox proporcionara información en detalle de la actividad de una muestra dentro de la máquina virtual.	
2.15	Debe contar con análisis de AV, reputación de archivos, reputación de URL y categoría de aplicaciones	
2.16	La solución debe ser capaz de ejecutar el código sospechoso, acceso URL y diversos tipos de archivos en un entorno virtual de inspección dentro del mismo dispositivo. Para ello realizará tanto análisis estático (basado en reglas) como dinámico (basado en comportamiento).	

Características técnicas - Solución de detección, prevención y respuesta de red.		
Ítem	**Descripción**	**Ficha técnica o link página web fabricante Ubicación en la propuesta (Folio N°) Diligencia Proponente**
2.17	La solución debe detectar la amenaza sin necesidad de conocer la firma, es decir, a través del comportamiento de la propia amenaza.	
2.18	La solución debe proporcionar detección en las comunicaciones desde y hacia los servicios de internet, contra los ataques de malware de día cero, exploits, botnets y Ataques dirigidos.	
2.19	La solución deberá proporcionar la siguiente información como mínimo por cada una de las amenazas detectadas por malware en entorno de Sandbox: • Fecha y hora del ataque • Hash MD5/SHA-256 de los binarios maliciosos • Tipo de archivo malicioso detectado • URL/IP de infección • Capacidades nocivas de la amenaza: capacidades de robo de información, comportamiento malicioso, cambios al sistema operativo	
2.20	La solución debe registrar y almacenar evidencia de la ejecución de malware moderno y ataques dirigidos en el entorno virtual de inspección, tales como: direcciones IP, protocolos empleados.	
2.21	La solución debe ser capaz de analizar archivos adjuntos incluidos en los correos electrónicos, así como direcciones URL que se encuentren en el cuerpo del correo.	
2.22	La solución debe analizar archivos adjuntos en los mensajes de correo electrónico, que estén comprimidos.	
2.23	El entorno de Sandbox debe poder procesar hasta 30.000 archivos al día.	
3	**Solución de detección, prevención y respuesta de red**	
3.1	**Arquitectura y Diseño**	
3.1.1	La solución debe poder ejecutarse en entornos virtualizados con soporte a hipervisor de VMWare	
3.2	**Requerimientos Funcionales**	
3.2.1	La solución deberá ser capaz de detectar malwares Zero-Day y APT.	
3.2.2	La solución deberá ser capaz de detectar las tres etapas del ciclo de vida de ataque del malware moderno: Exploit, Dropper y Data Exfiltration	
3.2.3	La solución debe proporcionar detección en tiempo casi real de malware desconocido.	
3.2.4	Soporte de archivos comprimidos de múltiples niveles	
3.2.5	Los datos forenses deben ser en tiempo real, mostrando el nivel de compromiso y permitiendo a los administradores tomar decisiones	
4	**Solución de Detección y Respuesta de Endpoint (EDR)**	
4.1	**Requerimientos Funcionales**	
4.1.01	La solución debe incluir protección para sistemas operativos Mac, Linux, Windows (la última versión liberada por Microsoft Windows 10, 11 Windows Server 2008 R2, Windows Server 2012, 2016 y 2019), así como la integración con tecnologías de virtualización como XenDesktop versión 7.15 y posteriores, entre otros.	
4.1.02	La solución debe ser capaz de identificar con precisión los archivos maliciosos, que incluyen, entre otros, cualquier extensión de archivo, archivo (incluidos archivos protegidos con contraseña).	
4.1.03	La solución debe poder analizar cualquier tipo de archivo mediante el uso de múltiples aplicaciones y múltiples versiones, que incluyen, entre otros: exe, dll, pdf, doc, docx, xls, xlsx, gif, jpeg, png, tiff, swf, mov, qt, mp4, jpg, mp3, asf, ico, htm, url, rm, com, vcf, ppt, rtf, chm, hlp y otros.	
4.1.04	La solución debe tener la capacidad de realizar análisis malware, así como exploits de vulnerabilidades	
4.1.05	La solución debe tener la capacidad de verificar / ejecutar un análisis en todos los hosts para cualquier nombre de archivo, extensión de archivo, archivo MD5 / SHA1.	

Características técnicas - Solución de detección, prevención y respuesta de red.		
Ítem	**Descripción**	**Ficha técnica o link página web fabricante Ubicación en la propuesta (Folio N°) Diligencia Proponente**
4.1.06	La solución debe defenderse contra ataques avanzados persistentes / de día cero, que incluyen, pero no se limitan a: • Malware general. • Ataques de día cero. • Explotar la vulnerabilidad de software existente. • Ransomware. • Inyección SQL. • Hacktivismo. • Clickjacking. • Spyware. • Amenazas persistentes avanzadas / Ataques dirigidos • Ataques de botnet. • Rootkits. • Amenazas polimórficas. • Amenazas combinadas. • malware ofuscado, malware desconocido y ataques de día cero. • Scripts maliciosos que aprovechan: PowerShell, Visual Basic, Perl, Python, Java / JAR. • Ataques residentes en la memoria y otros ataques sin malware. • Ataques basados en documentos (archivos PDF y macros). • Ataques de inicio de sesión remoto y el uso malicioso de software legítimo. • Malware conocido y variantes que incluyen ransomware basado en malware.	
4.1.07	La solución debe detectar malware sin depender de firmas o listas estáticas que requieren actualización constante.	
4.1.08	La solución debe ser capaz de detectar amenazas localmente, sin depender de un servicio en la nube.	
4.1.09	La solución debe tener la capacidad de detectar conexiones de Comando y Control (C&C) entrantes o salientes.	
4.1.10	La solución debe ser capaz de proporcionar datos forenses detallados del objeto malicioso adjunto detectado en los correos electrónicos. Los datos forenses deben incluir, entre otros: • Binarios de Malware Asociado Actual • Capturas de pantalla de VM durante la ejecución • Cualquier cambio en el sistema operativo host. • Cualquier cambio a la memoria. • Cualquier cambio en el sistema de archivos. • Cualquier cambio a la puesta en marcha del sistema.	
4.1.11	La solución debe proporcionar visibilidad, monitoreo y registro de eventos de endpoint, archivos afectados, procesos iniciados, cambios en el registro del sistema y actividad de la red.	
4.1.12	La solución debe proporcionar amenazas de detección desde cualquier fuente, incluidas, entre otras, las siguientes: • A través de descargas web. • A través del contenido copiado de dispositivos de almacenamiento, enlaces o archivos adjuntos en correos electrónicos. • Infección entregada a través de contenido encriptado.	
4.1.13	La solución debe establecer la capacidad y configurar una lista de acciones de forma manual o automáticas contra cada detección (bloquear, poner en cuarentena o eliminar) la amenaza.	
4.1.14	Eliminar malware o archivos temporales en los dispositivos que se detecte infección o ataque.	

Características técnicas - Solución de detección, prevención y respuesta de red.		
Ítem	**Descripción**	**Ficha técnica o link página web fabricante Ubicación en la propuesta (Folio N°) Diligencia Proponente**
4.2	**Administración y Reportes**	
4.2.1	La solución debe tener políticas unificadas, informes centralizados y análisis forenses procesables dentro de una consola única para la administración centralizada.	
4.2.2	La solución debe proporcionar análisis, visualizaciones y capacidades de análisis de enlaces para detectar y combatir amenazas avanzadas internas / externas.	
4.2.3	La solución debe proporcionar un registro de todos los programas maliciosos detectados.	
4.2.4	La solución debe proporcionar herramientas para realizar análisis de causa raíz.	
4.2.5	La plataforma debe poder tomar acciones inmediatas a partir de la alerta de incidentes.	
4.2.6	Visibilidad para rastrear y analizar malware.	
4.2.7	Debe tener la capacidad de crear y exportar informes y reportes relacionados con los incidentes detectados.	
4.2.8	La solución debe ser capaz de integrarse con SIEM para la administración de logs.	
4.2.9	La solución debe poder enviar notificaciones por correo electrónico.	
4.2.10	La solución debe poder crear usuarios por roles controladas por privilegios y funciones (Administrador, Revisor, Investigador, etc.).	
4.2.11	Debe soportar integración con fuentes de amenazas de terceros y propias que brinde inteligencia de amenazas para identificar ataque de terceros.	

Tabla 2 - Características técnicas - Solución de detección, prevención y respuesta de red

Características técnicas - Solución de Seguridad Antivirus		
Ítem	**Descripción**	**Ficha técnica o link página web fabricante Ubicación en la propuesta (Folio N°) Diligencia Proponente**
1	La solución debe contar con una consola de administración on-premise o en la nube que permita tener un sistema de administración, distribución y actualización centralizada de los endpoint, así como la configuración de las características ofrecidas por el producto.	
2	La solución de seguridad antivirus debe ser desarrollada e integrada por un único fabricante de forma tal que tanto el soporte de la solución como sus funcionalidades se integran y administran a través de la consola de administración.	
3	La solución debe proveer un inventario de hardware y software que permita al administrador conocer el software que ha sido instalado en el endpoint.	
4	La solución debe incluir seguridad para dispositivos de usuario final (antivirus, antimalware, antispyware, IPS/IDS, firewall personal, filtro de contenido web, control de aplicaciones, protección anti-ransomware, análisis de vulnerabilidades, protección con contraseña, antivirus para correo, control de phishing - pharming, cifrado de datos y dispositivos).	
5	La solución debe contar con una tarea que permita la desinstalación remota de las aplicaciones.	
6	La solución debe permitir que el administrador defina una Lista Blanca de dispositivos permitidos como Solo lectura o Acceso completo.	
7	El módulo de control de aplicaciones para dispositivos de usuario final y equipos servidores debe contar como mínimo con las siguientes características: Comprobación en la ejecución, verificación de	

Características técnicas - Solución de Seguridad Antivirus		
Ítem	**Descripción**	**Ficha técnica o link página web fabricante** **Ubicación en la propuesta (Folio N°)** **Diligencia Proponente**
	aplicaciones mediante escaneo programado, definición de mensajes personalizados para los usuarios finales, incluye detección de aplicaciones ofreciendo protección automática sobre las nuevas versiones del listado de aplicaciones establecido, permitir crear listas negras y blancas de aplicaciones basadas en categorías, certificados, Metadatos, hashes, condiciones personalizadas y portables.	
8	Módulo de filtrado de contenido web debe permitir crear reglas de bloqueo de recursos web basado en categorías, url específica, tipos de datos, debe tener la capacidad de poder ser asignado a usuarios del directorio activo, así como la asignación de horarios para la aplicación de diferentes reglas de control.	
9	El filtrado de contenido web, debe tener la capacidad de bloqueo para conexiones realizadas bajo HTTP o HTTPS indistintamente.	
10	La solución debe incluir protección para sistemas operativos Mac, Linux, Windows (la última versión liberada por Microsoft, Windows 10, 11, Windows Server 2008 R2, Windows Server 2012, 2016 y 2019). La solución ofertada no debe interferir con el desempeño normal de los equipos y aplicativos instalados en los equipos.	
11	La solución debe permitir crear grupos y generar políticas a los mismos.	
12	La solución debe contar con un módulo de generación de reportes y notificaciones, como mínimo debe exportar las mismas en formatos XML, PDF o HTML.	
13	La solución debe ser administrable desde una única consola de administración centralizada y debe tener la capacidad de ser consultada mediante navegador web desde cualquier estación de trabajo.	
14	La solución debe permitir la configuración granular de permisos de acceso a la consola de administración permitiendo al administrador crear diferentes perfiles de acuerdo con la labor que se asigne.	
15	La consola de administración debe tener la capacidad de notificar los intentos de infección de virus de acuerdo con parámetros definidos.	
16	Debe poseer un módulo de protección de antivirus basado en firmas, las cuales se deben poder programar en un día y hora específica para ser descargadas.	
17	Desde la consola de administración de la herramienta se debe poder hacer limitación del ancho de banda que va a ser utilizado por las actualizaciones de firmas para no generar carga en la red.	
18	Permitir características de administración proactiva para brindar a los administradores información y recomendaciones de políticas antes de la generación de patrones de virus. Políticas contra epidemias de virus.	
19	Permitir una estructura jerárquica la cual ofrezca determinación en el control de acceso, como permisos y roles sobre la solución de seguridad.	
20	Permitir la limpieza de daños en tiempo real para eliminar remanentes de virus, troyanos, spyware y entradas en el registro del sistema.	
21	Realizar actualizaciones automáticas de las listas de definiciones de virus a partir de una ubicación centralizada, así mismo debe permitir un modo de actualización local y en la nube en caso de no estar disponible el repositorio local.	
22	Controlar modificaciones del endpoint contra la remoción no autorizada del agente por parte del cliente a través de una contraseña.	
23	Todos los módulos de la solución deben ser de un único proveedor y desplegados mediante un único agente.	
24	La solución debe permitir el cambio de la configuración de los antivirus en los clientes de forma remota y a través de reglas aplicables a un grupo de máquinas.	
25	La solución debe permitir la creación de tareas de actualización de firmas, verificación de virus y actualización del producto.	
26	La solución debe generar registros (logs) del escaneo localmente con envío posterior de su contenido al administrador.	

Características técnicas - Solución de Seguridad Antivirus		
Ítem	**Descripción**	**Ficha técnica o link página web fabricante** **Ubicación en la propuesta (Folio N°)** **Diligencia Proponente**
27	La solución debe permitir la visualización de forma rápida y sencilla del estado y estadísticas de las infecciones generadas y permitir también visualizar las endpoint y servidores donde ocurrió la detección o infección.	
28	Visualizar mediante un Dashboard en tiempo real de la incidencia de virus, estado de la actualización de las máquinas y cualquier aviso o errores que puedan ocurrir.	
29	Permitir el aprendizaje automático para detectar amenazas desconocidas que generen riesgos de seguridad en los procesos o archivos sospechosos originados desde medios de almacenamiento externos, internos, servicios web o canales de correo.	
30	Permitir manualmente registrar excepciones de archivos que ya fueron analizados y descartados de acciones maliciosas ya sea por ser procesos permitidos o aplicaciones de uso interno.	
31	La solución debe contar con una herramienta de despliegue remoto que permita la instalación remota de la solución, así como la instalación de software de terceros o que no pertenecen al fabricante, pero cuentan con un archivo ejecutable o msi para su distribución. Así mismo permitir la instalación silenciosa a través de políticas de Directorio Activo, script de logon, etc.	
32	La solución debe contar con un sistema de cifrado integral de archivos, carpetas, unidades de almacenamiento, discos duros la cual debe manejar como mínimo un algoritmo de cifrado AES 256 con el fin de elevar el nivel de seguridad de la información almacenada en caso de robo o pérdida de algunos de los dispositivos	
33	La solución debe incluir una herramienta de soporte remoto que permita a los integrantes de soporte la posibilidad de interactuar con el equipo de manera remota y que a su vez se registren las operaciones realizadas por la persona que realizo la conexión	
34	La solución debe contar con una herramienta de conexión remota que permita la manipulación local del equipo de usuario final guardando un registro de las acciones realizadas con los archivos en la conexión.	
35	La solución debe contar con un módulo de detección y respuesta (EDR) que esté integrado con la solución antivirus ofertado.	
36	La solución debe incorporar un módulo que permita realizar el análisis de una amenaza o ataque para identificar el tipo de daño que pueda causar.	
37	La solución debe contar con la opción de emplear respuestas automatizadas para erradicar la amenaza del sistema.	
38	La solución debe brindar una interfaz y funciones sencillas que permitan dar alcance de manera rápida a un incidente.	
39	La solución debe descubrir las conexiones de una amenaza y su historial mediante la visualización de la ruta de expansión del ataque.	
40	La solución debe permitir crear tareas automatizadas a partir del manejo de indicadores de compromiso así como permitir la importación de estos a la plataforma de protección.	
41	La solución debe entregar un informe en el que se pueda visualizar el alcance del ataque y la afectación a usuarios, procesos, archivos y registro del sistema que pudieron ser comprometidos	
42	La solución debe permitir el aislamiento de los equipos de manera automática y/o manual al encontrar un evento asociado a una amenaza de propagación rápida.	
43	La solución debe evitar que el archivo malicioso se ejecute y se propague por toda la red durante la investigación.	
44	La solución de EDR debe ser completamente administrable e integrada con la solución ofertada, no se aceptan consolas de manejo independientes.	
45	La solución de protección de correo electrónico debe verificar los mensajes en busca de virus, malware, macros, objetos cifrados y archivos comprimidos.	

Características técnicas - Solución de Seguridad Antivirus		
Ítem	**Descripción**	**Ficha técnica o link página web fabricante Ubicación en la propuesta (Folio N°) Diligencia Proponente**
46	La solución de protección de correo electrónico debe ejecutar un análisis anti-phishing de los mensajes, analizar mensajes en busca de enlaces de anuncios o enlaces maliciosos y los relacionados a software legítimo.	
47	La solución de protección de correo electrónico debe permitir verificar los mensajes en busca de spam, posible spam y correo masivo.	
48	La solución de protección de correo electrónico debe permitir crear y configurar reglas para procesar los mensajes.	
49	La solución de protección de correo electrónico debe contener un panel con widgets para supervisar la aplicación.	
50	La solución de protección de correo electrónico debe permitir crear listas de usuarios personalizadas de direcciones admitidas y rechazadas.	
51	La solución debe proporcionar sobre los eventos detectados en el tráfico de correo electrónico y eventos de la aplicación detectados durante el funcionamiento de la aplicación.	
52	La solución de protección de correo electrónico debe permitir crear informes sobre el funcionamiento de la aplicación y enviarlos por correo electrónico.	

Tabla 3 - Características técnicas - Solución de Seguridad Antivirus

8. LICENCIAMIENTO Y SOPORTE.

El licenciamiento y servicio de soporte para el primer componente (Solución de detección, prevención y respuesta de red) será por un (1) año.

El licenciamiento y servicio de soporte para el segundo componente (Solución de seguridad Antivirus) será por dos (2) años.

Para los dos componentes:

El servicio de soporte de partner debe ser en esquema 7x24: todos los días de la semana en cualquier hora. Periodo durante el cual el contratista debe realizar las actualizaciones, las cuales se clasifican en:

- 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.

El servicio de soporte adquirido durante la vigencia contratada, debe ser vía telefónica, vía correo electrónico o mediante sistema de tickets. El contratista deberá entrega la respectiva matriz de escalamiento.

El soporte técnico tiene la responsabilidad 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 (update, upgrade) 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, previamente aprobados por el personal técnico asignado por parte de la Universidad.

El soporte técnico debe realizar las instalaciones, configuraciones, revisión y afinamiento de configuraciones de todos los componentes técnicos descritos en el presente documento, durante el tiempo del licenciamiento, cuantas veces lo requiera la Universidad, asegurando que el servicio de soporte se preste por personal certificado en el software ya sea en sitio, remoto, telefónico o correo electrónico de acuerdo con la matriz de escalamiento.

9. CRONOGRAMA

El contratista presentará el cronograma a seguir durante la ejecución del contrato, el cual debe ser verificado y aprobado por el supervisor delegado por parte de la Universidad, con la asesoría de la Red de Datos UDNET. Dicho documento hará parte del acta de inicio y debe incluir la entrega de licenciamiento, recursos a utilizar y actividades que se ejecutarán para dar cumplimiento al contrato; también debe incluir las fechas de presentación de los informes periódicos los cuales deben ser validados y firmados tanto por el contratista.

10. DOCUMENTACIÓN DE CARÁCTER TECNICO.

Durante la presentación de la propuesta el oferente debe cumplir y entregar los siguientes documentos:

- SERVICIO Y DISTRIBUCIÓN AUTORIZADA: Dicho certificado debe estar vigente durante la validez de la propuesta, de igual manera durante la ejecución del contrato.
- El proveedor debe presentar certificación expedida por la casa matriz donde se indica que es canal Partner GOLD o superior del producto para la solución de antivirus, teniendo en cuenta que el orden ascendente de los niveles de certificación es: Silver, Gold, Platinum. Las diferencias entre los tipos de certificación del partner, se presenta en el tipo de soporte que fábrica brinda. La empresa Certificada en Gold o Platinum debe tener como mínimo dos personas certificadas en el manejo de la herramienta y así puedan dar mayor soporte sobre la solución adquirida, y con respecto con la silver dan es apoyo mas no un soporte completo. Las ventajas de los niveles gold y platinum es la atención a sucesos en la universidad por parte de personal certificado por fabrica en la solución y así garantizar la respuesta más acertadas y cumplir las necesidades de seguridad que la universidad posee.
- El proveedor debe presentar certificación expedida por la casa matriz donde se indica que es canal Partner GOLD o superior para la plataforma de detección de ataques dirigidos y avanzados.
- Anexo 1. Carta de presentación de propuesta firmada por el representante legal.
- Anexo 2. Certificaciones de experiencia.
- Anexo 3 y 4. Propuesta Económica.

11. EVALUACIÓN TÉCNICA DE LAS PROPUESTAS

Se llevará a cabo por parte de la Oficina de la Red de datos UDNET de la Universidad Distrital y se tendrá en cuenta el cumplimiento de los requerimientos solicitados en las presentes especificaciones técnicas. A esta evaluación no se le asignará puntaje, su resultado será “CUMPLE TECNICAMENTE” O “NO CUMPLE TECNICAMENTE”.

Los criterios por evaluar serán los siguientes

FACTORES DE EVALUACIÓN/ CALIFICACIÓN	RESULTADO
Evaluación Técnica	Cumple / No cumple

Tabla 4 - Criterios de evaluación

12. CALIFICACION

Las ofertas que hayan sido evaluadas como "ADMISIBLE" en la evaluación jurídica, financiera y técnica, serán calificadas de acuerdo con la siguiente tabla:

TABLA CALIFICACION		
Ítem	**Factor**	**Puntaje (Máximo)**
1	Económica	800
2	Licencias adicionales para endpoint solución de detección, prevención y respuesta de red. (Componente 1)	100
3	Licencias adicionales para endpoint software de seguridad antivirus. (Componente 2)	100
CALIFICACION TOTAL		**1000**

Tabla 5 – *Calificación*

13. LICENCIAS ADICIONALES

Para este factor, se asignará una calificación de hasta doscientos (200) puntos, para el oferente que ofrezca características técnicas adicionales descritas en la tabla 6 "*Tabla 6 - Licencias Adicionales*"

TABLAS LICENCIAS ADICIONALES		
Ítem	**Calificación**	**Puntaje (Máximo)**
1	Licencias adicionales para endpoint solución de detección, prevención y respuesta de red. (Componente 1)	100
2	Licencias adicionales para endpoint software de seguridad antivirus. (Componente 2)	100
CALIFICACION TOTAL		**200**

Tabla 6 - *Licencias Adicionales*

Dependiendo de las características técnicas adicionales que el proponente oferte deberá diligenciar el Anexo 17.5 "*ANEXO N° 5 - OFRECIMIENTOS ADICIONALES*".

13.1. Licencias Adicionales solución de detección, prevención y respuesta de red.

Se le asignará cien (100) puntos al proponente que ofrezca licencias adicionales para la solución de detección, prevención y respuesta de red teniendo en cuenta las condiciones establecidas en el presente pliego de condiciones. Este puntaje se asignará a los oferentes, una vez estén habilitados jurídico, financiera y que hayan cumplido técnicamente, la calificación se hará de acuerdo con la siguiente tabla:

TABLA LICENCIAS ADICIONALES SOLUCIÓN DE DETECCIÓN, PREVENCIÓN Y RESPUESTA DE RED			
Ítem	**Descripción**	**Asignación de Puntos**	**Total**
1	Licencias adicionales para endpoint de la solución de detección, prevención y respuesta de red durante un (1) año. Dicho licenciamiento debe cumplir con los requisitos que se indican en el numeral 7. Especificaciones técnicas mínimas	1 punto por cada 2 licencias adicionales	Hasta 100 puntos

Tabla 7 – *Licencias adicionales solución de detección, prevención y respuesta de red*

13.2. Licencias Adicionales Software de seguridad antivirus.

Se le asignará cien (100) puntos al proponente que ofrezca licencias adicionales para endpoint del software de seguridad antivirus teniendo en cuenta las condiciones establecidas en el presente pliego de condiciones. Este puntaje se asignará a los oferentes, una vez estén habilitados jurídico, financiera y que hayan cumplido técnicamente, la calificación se hará de acuerdo con la siguiente tabla:

TABLA LICENCIAS ADICIONALES SOLUCIÓN DE DETECCIÓN, PREVENCIÓN Y RESPUESTA DE RED			
Ítem	**Descripción**	**Asignación de Puntos**	**Total**
1	Licencias adicionales para endpoint del software de seguridad antivirus durante dos (2) años. Dicho licenciamiento debe cumplir con los requisitos que se indican en el numeral 7. Especificaciones técnicas mínimas	1 punto por cada 5 licencias adicionales	Hasta 100 puntos

Tabla 8 *– Licencias adicionales software de seguridad antivirus*

14. FORMA DE PAGO

1. El valor del contrato será hasta por la suma de la oferta ganadora del presente proceso de selección, el cual incluirá el IVA correspondiente y demás impuestos nacionales y distritales. La Universidad Distrital sólo pagará al contratista,

previa presentación de la documentación requerida, y bajo ningún motivo o circunstancia, aceptará o hará pagos a terceros sin previa autorización expresa a la Universidad.

2. La Universidad pagará al contratista el valor del contrato en un solo contado, previamente a la presentación y aprobación por parte de la supervisión de:

   a) Entrega de documento generado por el fabricante en donde se presente una descripción completa del tipo de contrato de soporte:
      - ✓ Nombre del distribuidor (mayorista).
      - ✓ Nombre de usuario final, a nombre de la Universidad Distrital
      - ✓ Fecha de inicio, fecha de finalización de los licenciamientos
      - ✓ Referencia de producto
      - ✓ Cantidad de licencias adquiridas
      - ✓ Código de activación (en caso de que aplique)

   b) Entrega de documento generado por el partner en donde se presenta una descripción completa del licenciamiento y tipo de contrato de soporte, el cual no debe contradecir lo establecido en la presente ficha técnica y en donde también se deberán relacionar todos los equipos con su respectivo serial.
   c) Informe de ejecución firmado por el personal técnico delegado por el contratista y por la universidad que debe incluir como mínimo: actividades desarrolladas, relación de equipos donde se instaló el software, versiones de software instalado, anexar protocolos de instalación aplicados, identificación donde se alojen archivos backup (cuando aplique).
   d) Factura incluido IVA discriminado, con un periodo de vencimiento no inferior a cuarenta y cinco (45) días. En caso de ser factura electrónica se deberá
   e) Acta de inicio firmada por el contratista y el supervisor del contrato por parte de la Universidad Distrital.
   f) Acta de recibo a satisfacción por parte de la Supervisión.
   g) Documentos referidos en la circular No 001 y 002 de 2016 de la División de Recursos Financieros.
   h) Mecanismo que permita a la Universidad Distrital Francisco José de Caldas verificar de manera directa con el fabricante el soporte que ampara a los equipos, por un periodo mínimo de un (1) año.
   i) Certificación de cumplimiento del pago de seguridad social y parafiscales del periodo en que se apruebe la factura, suscrita por el representante legal o el revisor fiscal, según sea el caso.
   j) Documento anexo a la factura en el cual se relacionen los siguientes campos:
      - ✓ Ítem
      - ✓ Referencia.
      - ✓ Descripción.
      - ✓ Marca.
      - ✓ Costo unitario sin IVA
      - ✓ IVA aplicado (%)
      - ✓ Costo total con IVA
   k) Demás documentos exigidos por la Universidad.

El pago se efectuará dentro de los cuarenta y cinco (45) días siguientes a la aprobación de la respectiva factura, previa certificación de cumplimiento expedida por el Supervisor del contrato, y una vez se realicen los trámites legales, fiscales y presupuestales a que haya lugar.

Nota 1: Para el **componente 1** se tiene un presupuesto de QUINIENTO CINCUENTA Y CUATRO MILLONES OCHOCIENTOS OCHENTA Y SEIS MIL SEISCIENTOS SESENTA Y CINCO DE PESOS Incluyendo Iva ($554.000.000 M/CTE)

Nota 2: Para el **componente 2** se tiene un presupuesto de TRESCIENTOS VEINTIÚN MILLONES DE PESOS Incluyendo Iva ($321.000.000 M/CTE)

15. EXPERIENCIA

El oferente deberá acreditar su experiencia mediante la información contenida en el RUP. El oferente deberá acreditar que ha celebrado, ejecutado y liquidado (siempre y cuando el régimen de contratación exija esta liquidación), totalmente, cuatro (4) contratos en los últimos cinco (5) años, contados retroactivamente desde la fecha del cierre del presente proceso de selección, cumpliendo con las siguientes condiciones:

1. El objeto de estos contratos deberá consistir o estar relacionado con el objeto del presente proceso de selección.
2. La sumatoria de los contratos deberá ser, como mínimo, igual o superior a una (1) vez el valor del presupuesto oficial establecido en los presentes Pliegos de Condiciones.
3. Cuando las experiencias registradas en el RUP o en las certificaciones expresen su valor en dólares, se tendrá en cuenta la TRM a la fecha en que se celebró el contrato.
4. Cada experiencia aportada mediante el RUP se analizará por separado. En caso de tratarse de contratos adicionados, el valor de las adiciones se convertirá a salarios mínimos mensuales legales vigentes (SMMLV) a la fecha de firma de la adición y se sumará al valor del contrato principal (si fuere el caso).
5. Cuando se presente el RUP para verificar en éste la experiencia requerida, los contratos indicados por el oferente deberán cumplir con al menos uno (1) de los códigos del Clasificador de las Naciones Unidas en el tercer nivel, para cada uno de los componentes a los que se presente, y que se señalan a continuación:

CLASIFICACIÓN UNSPSC	DESCRIPCIÓN
432332	Software de seguridad y protección
432337	Software de administración de sistemas
81111508	Servicios de implementación de aplicaciones
81111800	Servicios de sistemas y administración de componentes de sistemas
81111801	Seguridad de los computadores, redes o internet
81111809	Servicio de instalación de sistemas
81112200	Mantenimiento y soporte de software
81112202	Actualizaciones o parches de software

Tabla 9 - Clasificación UNSPSC

La actualización a "*pesos de hoy*" del valor de los contratos ejecutados se calculará en relación con el valor del salario mínimo del año de la fecha de terminación, es decir, el valor de los ítems se expresará en salarios mínimos correspondientes al año de terminación. Para efectos del cálculo correspondiente, se anexa la siguiente tabla sobre los valores del SMLMV de los últimos años:

PERIODO	MONTO
Enero 1 de 2017 a Dic. 31 de 2017	$ 737.717
Enero 1 de 2018 a Dic. 31 de 2018	$ 781.242
Enero 1 de 2019 a Dic. 31 de 2019	$ 828.116
Enero 1 de 2020 a Dic. 31 de 2020	$ 877.803
Enero 1 de 2021 a Dic. 31 de 2021	$ 908.526
Enero 1 de 2022 a Dic. 31 de 2022	$ 1.000.000
Enero 1 de 2023 a la fecha	$ 1.160.000

Tabla 10 - SMLMV de los últimos años

NOTA: TENIENDO EN CUENTA QUE EL REGISTRO ÚNICO DE PROPONENTES –RUP- NO CONSIGNA EL TIEMPO DE EJECUCIÓN DE LOS CONTRATOS Y PORCENTAJES DE PARTICIPACIÓN, CUANDO EL PROPONENTE FUERE PLURAL, ÉSTE DEBERÁ ACREDITAR LA EXPERIENCIA CONSIGNADA EN EL RUP, ADJUNTANDO LAS CERTIFICACIONES Y/O COPIA DE LOS CONTRATOS EN LOS CUALES SE PUEDA EVIDENCIAR DICHOS ASPECTOS.

NOTA: En dicho documento (RUP) se verificará que el oferente esté inscrito antes de la fecha de cierre en la clasificación que se establece en el anterior cuadro.

- **A.** Para el caso de experiencias que sean presentadas como integrante de consorcio, unión temporal o promesa de sociedad futura, se tendrá en cuenta únicamente el valor correspondiente al porcentaje de su participación, por tanto, la certificación lo debe señalar.
- **B.** Cuando el proponente incluya valores que no correspondan a la experiencia general o especifica aquí señaladas, este valor será descontado del valor total del contrato certificado respectivo.
- **C.** Los proponentes que se presenten en Consorcio, Unión Temporal o Promesa de Sociedad Futura deberán cumplir en conjunto con la experiencia requerida, lo cual significa que deberá ser acreditada por todos, algunos o uno de los integrantes.
- **D.** En caso de requerirlo, la Universidad podrá solicitar la copia del contrato, así como del o de los OTROSI que se hubieran firmado.
- **E.** La Universidad se reserva el derecho de verificar toda la información y documentación que los proponentes presenten en su propuesta. De presentarse inconsistencias, la propuesta será rechazada.
- **F.** EN CUANTO A PERSONAS NATURALES EXTRANJERAS DOMICILIADAS EN COLOMBIA Y PERSONAS JURÍDICAS EXTRANJERAS CON SUCURSAL EN EL PAÍS, deberán acreditar este requerimiento como lo haría una persona jurídica de origen nacional. En cuanto a personas naturales y persona jurídicas privadas extranjeras no inscritas en el RUP, por no tener domicilio o sucursal en el país, el requisito exigido es el mismo, pero deberá ser aportado mediante contratos, certificaciones de contratos o documentos equivalentes.

Sin embargo, es necesario tener en cuenta que todos los documentos otorgados en el exterior para acreditar lo dispuesto en este numeral, deberán presentarse legalizados en la forma prevista en el Código General del Proceso y el Artículo 480 del Código de Comercio. Si se tratare de documentos expedidos por autoridades de países miembros del Convenio de La Haya de 1961, se requerirá únicamente de la Apostille.

G. Las certificaciones o contratos para las personas naturales y jurídicas extranjeras no domiciliadas en Colombia, deben tener como mínimo la siguiente información:

a. Nombre o razón social de la entidad que certifica
b. Valor del contrato
c. Objeto del contrato y alcance del mismo, de ser el caso
d. Fecha de suscripción e iniciación
e. Fecha de terminación: Estos contratos deberán estar terminados y, de ser el caso, liquidados, antes de la fecha de cierre del presente proceso
f. Porcentaje de participación, en tratándose de consorcio, unión temporal o promesa de sociedad futura
g. Nombre Completo, cargo, dirección y número de Teléfono de la Persona que expide la Certificación.

NOTA: Aquella experiencia que sea calificada en el cumplimiento del contrato como "*malo*", "*regular*" o expresiones similares, que demuestren o que indiquen, que durante su ejecución fueron sujetas a multas o sanciones debidamente impuestas por la administración, no se aceptarán por la Universidad.

16. GLOSARIO

- **Endpoint:** Equipo de dispositivo final ya sea equipo de escritorio o portátil en el cual se instalará el software de seguridad.
- **7x24:** 5 días hábiles de la semana de 8:00 am a 5:00 pm, con remplazo de hardware al siguiente día hábil.
- **Spam:** se refiere a cualquier forma de comunicación no solicitada que se envía de forma masiva.
- **Spyware:** es el software diseñado para recopilar datos de un dispositivo y reenviarlos a un tercero sin el conocimiento del usuario.
- **Adware:** son programas diseñados para mostrar publicidad, redirigir solicitudes de búsqueda a sitios web de publicidad y recopilar datos comerciales acerca del usuario para mostrar avisos personalizados.
- **Phising:** es una técnica de ingeniería social que usan los ciberdelincuentes para robar información personal o corporativa a través del correo.
- **Ransomware:** es un tipo de malware o código malicioso que impide la utilización de los equipos o sistemas que infecta y que tiene como objetivo encriptar y/o secuestrar la información.
- **Backdoor:** es un tipo de virus diseñado para dar acceso a usuarios maliciosos al control de un equipo infectado de manera remota.
- **Riskware:** se refiere a programas legítimos potencialmente peligrosos debido a incompatibilidad de software.
- **Rootkits:** es un paquete de software malicioso diseñado para permitir el acceso no autorizado a un equipo o a otro software.
- **Troyanos:** es un software que instala otros programas, a menudo malware, en el ordenador infectado sin el consentimiento del usuario.
- **Keyloggers:** es un software que realiza seguimiento y registra cada tecla que se pulsa en un dispositivo, a menudo sin el permiso ni el conocimiento del usuario.
- **Dialers:** es un programa que usa el módem del ordenador para realizar llamadas de tarificación adicional mediante una conexión de marcación sobre Internet.
- **Hacking tools:** son herramientas que usan los ciberdelincuentes para acceder a otros sistemas.
- **Exploits:** es un programa o código que se aprovecha de una vulnerabilidad o fallo de seguridad en una aplicación o sistema, de forma que un atacante podría aprovechar ese fallo en su beneficio.
- **NDR:** Network Detection and Response, o en español, detección y respuesta de red es un grupo variado de tecnologías complementarias de seguridad de la red que buscan supervisar, detectar, analizar y responder automáticamente a las ciberamenazas.
- **IPS:** sistema de prevención de intrusiones (IPS) permite identificar el tráfico malicioso y bloquea de manera proactiva el ingreso de dicho tráfico a la red.
- **IDS:** sistema de detección de intrusiones (IDS) es una aplicación que detecta accesos no autorizados a un ordenador o a una red.
- **Pharming:** es una estafa en línea similar al phishing, en la que se manipula el tráfico de un sitio web y se roba información confidencial.

17. ANEXOS

17.1. ANEXO 1 - CARTA DE PRESENTACIÓN DE PROPUESTA

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

ANEXO N° 1

CARTA DE PRESENTACIÓN DE PROPUESTA

Bogotá, D. C., ___de____de 2023

Señores

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

Ciudad

Nosotros los suscritos: _____ de acuerdo con el presente proceso de contratación presentamos propuesta formal para su evaluación y en caso de que nos sea aceptada por la UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS nos comprometemos a firmar el contrato correspondiente, a cumplir con las obligaciones derivadas de él, así mismo, con las especificaciones técnicas que son parte integral de este.

Adicionalmente declaramos:

- Que conocemos la información general y demás documentos del proceso y aceptamos los requisitos en ellos contenidos.
- Que nos comprometemos a ejecutar totalmente el contrato, en el plazo establecido.
- Que ninguna persona o entidad distinta de las aquí nombradas tienen intereses en esta propuesta, en el contrato que como consecuencia de ella llegare a celebrarse y que, por consiguiente, sólo compromete a los firmantes.
- Que, si se nos adjudica el contrato, nos comprometemos a constituir las garantías requeridas y a suscribir éstas y aquél dentro de los términos señalados para ello.
- Que aceptamos todos y cada uno de los requerimientos técnicos exigidos en el presente proceso.

Así mismo, declaramos BAJO LA GRAVEDAD DEL JURAMENTO, sujeto a las sanciones establecidas en el Código Penal:

1. Que la información contenida en la propuesta es verídica y que asumimos total responsabilidad frente a la UNIVERSIDAD cuando los datos suministrados sean falsos o contrarios a la realidad, sin perjuicio de lo dispuesto en el Código Penal y demás normas concordantes.
2. Que no nos hallamos incursos en causal alguna de inhabilidad e incompatibilidad de las señaladas en la Constitución y en la Ley y no nos encontramos en ninguno de los eventos de prohibiciones especiales para contratar. En especial, manifestamos que no nos hallamos reportados en el Boletín de responsables Fiscales vigente, publicado por la Contraloría General de la República, de acuerdo con lo previsto en el numeral 4 del Artículo 38 de la Ley 734 de 2002 (Código Disciplinario Único), en concordancia con el Artículo 60 de la Ley 610 de 2000. (Se recuerda al proponente que, si está incurso en alguna causal de inhabilidad o incompatibilidad, no puede participar en el proceso de selección de contratistas y debe abstenerse de formular propuesta.), así como el origen lícito de los recursos destinados al proyecto o a la ejecución del contrato.
3. Que no hemos sido sancionados por ninguna Entidad Oficial por incumplimiento de contratos estatales ni se nos ha hecho efectivo ninguno de los amparos de la garantía única, mediante providencia ejecutoriada dentro de los últimos DOS (2) años anteriores a la fecha de cierre de esta Convocatoria , ni hemos sido sancionados dentro de dicho término por incumplimiento de

nuestras obligaciones contractuales por ningún contratante particular ni por autoridades administrativas en condición de terceros. (NOTA: Si el proponente es un consorcio o una unión temporal, para estos efectos, deberá tener en cuenta a cada uno de sus miembros individualmente considerados. Si durante dicho período el proponente ha sido objeto de sanciones contractuales (multas y/o cláusula penal) o se le ha hecho efectivo cualquiera de los amparos de la Garantía Única, por parte de cualquier entidad estatal, en lugar de hacer este juramento debe indicar aquí que ha tenido las sanciones y/o que le han sido hechos efectivos los amparos.

Por ello, ACEPTAMOS CON LA SUSCRIPCIÓN DE LA CARTA DE PRESENTACIÓN DE LA PROPUESTA, TODOS Y CADA UNO DE LOS REQUERIMIENTOS TÉCNICOS EXIGIDOS PARA **"ADQUIRIR, INSTALAR, CONFIGURAR Y PUESTA EN CORRECTO FUNCIONAMIENTO DE ELEMENTOS QUE PERMITAN DAR CONTINUIDAD Y MEJORAMIENTO A LA SEGURIDAD INFORMÁTICA DEL PARQUE INFORMÁTICO PROPIEDAD DE LA UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS, MEDIANTE DOS COMPONENTES: DETECCIÓN, PREVENCIÓN Y RESPUESTA DE RED (NDR) Y SOFTWARE DE SEGURIDAD ANTIVIRUS."**

Atentamente,

Nombre o Razón Social del Proponente: _____

NIT: _____

Nombre del Representante Legal: _____

C. C. No.: _____ De: _____

Dirección: _____

Correo electrónico: _____

Teléfonos: _____ Fax: _____

Ciudad: _____

FIRMA: _____

17.2. ANEXO 2 - CERTIFICACIONES DE EXPERIENCIA

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

ANEXO N° 2

CERTIFICACIONES DE EXPERIENCIA

Ítem	Año	Objeto del contrato	Valor	Entidad y/o empresa	Numero consecutivo del reporte del contrato ejecutado en el RUP	Folio en donde se encuentra la certificación
1						
2						
3						
4						

Tabla - Relación de certificaciones de experiencia.

Nota: Se debe diligenciar la tabla anterior "*Relación de certificaciones de experiencia*" y adjuntar las certificaciones y/o copia de los contratos en los cuales se pueda evidenciar dichos aspectos. Adicionalmente se debe tener en cuenta las condiciones establecidas en el numeral 13 "EXPERIENCIA" de las especificaciones técnicas.

Atentamente,

Nombre o Razón Social del Proponente: _____

NIT: _____

Nombre del Representante Legal: _____

C. C. No.: _____ De: _____

FIRMA: _____

17.3. ANEXO 3 - PROPUESTA ECONÓMICA – PRIMER COMPONENTE - SOLUCIÓN DETECCIÓN, PREVENCIÓN Y RESPUESTA DE RED

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

ANEXO N° 3

PROPUESTA ECONÓMICA – PRIMER COMPONENTE - SOLUCIÓN DETECCIÓN, PREVENCIÓN Y RESPUESTA DE RED

Bogotá, D. C., ___de____de 2023

Señores

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

Ciudad

El suscrito _____, obrando en nombre y representación de _____, por medio del presente, oferto en firme, irrevocablemente y como precio fijo, con destino a la celebración del contrato objeto de este proceso, y en consecuencia, ofrezco proveer los bienes correspondientes relacionados en el pliego de condiciones, bajo las características técnicas establecidas para tales bienes relacionados en las especificaciones técnicas y conforme a las condiciones y cantidades, previstos para tal efecto, precio que se discrimina así:

Componente 1 – Software de detección, prevención y respuesta de red					
Ítem	**Descripción**	**Referencias y/o números de parte**	**Cantidad**	**Valor Unitario (Antes de IVA)**	**Valor Subtotal (Antes de IVA)**
1	Adquisición de licenciamiento por un (1) año para la solución de detección, prevención y respuesta de red.		1		
2	Adquisición de licencias para endpoints por un (1) año sobre la solución de detección, prevención y respuesta de red.		200		
3	Soporte de partner en esquema 7x24 por un (1) año para toda la solución de detección, prevención y respuesta de red incluyendo actualizaciones (update y upgrade).		1		
4	Instalación, configuración y puesta en correcto funcionamiento de la solución de detección, prevención y respuesta de red, así como la integración con los dispositivos licenciados.		1		
Total, Antes de IVA:					
Total, IVA 19%:					
Total, IVA incluido					

Nota 1: Al momento de diligenciar la propuesta comercial, no deje de cotizar ningún ítem. Si usted no cotiza algún elemento la propuesta será rechazada. Recuerde, la propuesta se evaluará económicamente sobre el valor total incluido IVA.

Nota 2: Estarán a cargo del proponente todos los costos asociados a la preparación, elaboración y presentación de la propuesta. Por lo tanto, la UNIVERSIDAD DISTRITAL no reconocerá ningún reembolso por este concepto.

Nota 3: Debe ser diligenciado en su totalidad, debe ser clara y precisa en sus referencias y/o números de partes ya que hace parte de la evaluación técnica y económica, por tal razón no se tendrán en cuenta propuestas que tengan faltantes en esta información, que modifiquen dicha información, que entre en contradicción con lo requerido por la Universidad o que no permita la evaluación objetiva de la misma. Para todos los casos, si un ítem corresponde a costo cero (0) se debe indicar de manera explícita diligenciando la celda correspondiente.

NOTA: LA OFERTA TOTAL DEBE REALIZARSE EN PESOS COLOMBIANOS

Antes de diligenciar este anexo tenga en cuenta que:

NOTA: SI EL PROPONENTE NO DISCRIMINA EL IMPUESTO AL VALOR AGREGADO (IVA) Y EL BIEN CAUSA DICHO IMPUESTO, LA UNIVERSIDAD LO CONSIDERARA INCLUIDO EN EL VALOR TOTAL DE LA PROPUESTA Y ASÍ LO ACEPTARA EL PROPONENTE.

Atentamente,

Nombre o Razón Social del Proponente: _____

NIT: _____

Nombre del Representante Legal: _____

C. C. No. : _____ De: _____

FIRMA: _____

17.4. ANEXO 4 - PROPUESTA ECONÓMICA – SEGUNDO COMPONENTE – SOLUCION DE SEGURIDAD ANTIVIRUS

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

ANEXO N° 4

PROPUESTA ECONÓMICA – SEGUNDO COMPONENTE – SOLUCION DE SEGURIDAD ANTIVIRUS

Bogotá, D. C., ___de____de 2023

Señores

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

Ciudad

El suscrito _____, obrando en nombre y representación de _____, por medio del presente, oferto en firme, irrevocablemente y como precio fijo, con destino a la celebración del contrato objeto de este proceso, y en consecuencia, ofrezco proveer los bienes correspondientes relacionados en el pliego de condiciones, bajo las características técnicas establecidas para tales bienes relacionados en las especificaciones técnicas y conforme a las condiciones y cantidades, previstos para tal efecto, precio que se discrimina así:

COMPONENTE 2 – SOFTWARE DE SEGURIDAD ANTIVIRUS					
Ítem	**Descripción**	**Referencias y/o números de parte**	**Cantidad**	**Valor Unitario (Antes de IVA)**	**Valor Subtotal (Antes de IVA)**
1	* Adquisición de licenciamiento por dos (2) años para el software de seguridad para dispositivos de usuario final.		3000		
2	* Adquisición de licenciamiento por dos (2) años del agente EDR del software de antivirus para dispositivos de usuario final.		2841		
3	* Adquisición de licenciamiento por dos (2) años para la solución seguridad antivirus para ambientes virtuales compatibles con XenDesktop 7.15.		200		
4	* Adquisición de licenciamiento por dos (2) años para la solución seguridad antivirus para servidores virtuales.		30		
5	Soporte de partner en esquema 7x24 por dos (2) años para la solución de seguridad antivirus incluyendo actualizaciones (update y upgrade).		1		
6	** Instalación, configuración y puesta en correcto funcionamiento de la solución de seguridad antivirus sobre los equipos de la universidad.		1		
Total, Antes de IVA:					
Total, IVA 19%:					
Total, IVA incluido					

Nota 1: * En caso de que el oferente contemple una solución de software de seguridad antivirus Kaspersky®, deberá realizar la renovación del licenciamiento actual. En caso contrario, deberá realizar la adquisición.

Nota 2: ** La instalación configuración y puesta en correcto funcionamiento solo aplica para soluciones de software de seguridad antivirus distintas a Kaspersky®.

Nota 3: Al momento de diligenciar la propuesta comercial, no deje de cotizar ningún ítem. Si usted no cotiza algún elemento la propuesta será rechazada. Recuerde, la propuesta se evaluará económicamente sobre el valor total incluido IVA.

Nota 4: Estarán a cargo del proponente todos los costos asociados a la preparación, elaboración y presentación de la propuesta. Por lo tanto, la UNIVERSIDAD DISTRITAL no reconocerá ningún reembolso por este concepto.

Nota 5: Debe ser diligenciado en su totalidad, debe ser clara y precisa en sus referencias y/o números de partes ya que hace parte de la evaluación técnica y económica, por tal razón no se tendrán en cuenta propuestas que tengan faltantes en esta información, que modifiquen dicha información, que entre en contradicción con lo requerido por la Universidad o que no permita la evaluación objetiva de la misma. Para todos los casos, si un ítem corresponde a costo cero (0) se debe indicar de manera explícita diligenciando la celda correspondiente.

NOTA: LA OFERTA TOTAL DEBE REALIZARSE EN PESOS COLOMBIANOS

Antes de diligenciar este anexo tenga en cuenta que:

NOTA: SI EL PROPONENTE NO DISCRIMINA EL IMPUESTO AL VALOR AGREGADO (IVA) Y EL BIEN CAUSA DICHO IMPUESTO, LA UNIVERSIDAD LO CONSIDERARA INCLUIDO EN EL VALOR TOTAL DE LA PROPUESTA Y ASÍ LO ACEPTARA EL PROPONENTE.

Atentamente,

Nombre o Razón Social del Proponente: _____

NIT: _____

Nombre del Representante Legal: _____

C. C. No. : _____ De: _____

FIRMA: _____

17.5. ANEXO 5 – OFRECIMIENTOS ADICIONALES

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

ANEXO N° 5

OFRECIMIENTOS ADICIONALES

Ítem	Descripción	Referencia(s) o número de parte	Cantidad Ofrecida	Ficha técnica o link página web fabricante Ubicación en la propuesta (Folio N°)
1	Licencias adicionales para endpoint solución de detección, prevención y respuesta de red (Componente 1)			
2	Licencias adicionales para endpoint software de seguridad antivirus. (Componente 2)			