ESPECIFICACIONES TECNICAS

TABLA DE CONTENIDO:

1. OBJETO

Contratar la adquisición, instalación y puesta en correcto funcionamiento de equipos, licencias y componentes que permitan la actualización y reforzamiento de la infraestructura de telecomunicaciones y de la seguridad perimetral de la Universidad Distrital Francisco José de Caldas mediante dos componentes: Sistema de seguridad perimetral y Equipos enrutadores.

Componente 1:

Contratar la adquisición de hardware y software en conjunto con los servicios de licenciamiento, configuración, instalación, migración y puesta en correcto funcionamiento del sistema de seguridad perimetral en alta disponibilidad para la Universidad Distrital Francisco José de Caldas.

Componente 2:

Adquirir equipos enrutadores y componentes de telecomunicaciones para la actualización y reforzamiento de la infraestructura la red WAN de la Universidad según los términos de referencia.

2. ANTECEDENTES

Componente 1:

Actualmente el sistema de seguridad perimetral de la Universidad Distrital Francisco José de Caldas está basado en el conjunto de hardware: servidor de propósito general con sistema operativo Linux y el software: Netfilter Iptables. Este componente de la infraestructura que ofrece conexión controlada desde y hacia internet a la entidad ha prestado su funcionalidad desde hace más de una década, tiempo durante el cual ha mitigado los riesgos y vulnerabilidades que involucran la conexión a Internet.

Por otro lado, cuando se requiere mitigar riesgos informáticos e identificar las vulnerabilidades y amenazas en las que pueden estar comprometidos todos los usuarios de la comunidad universitaria, es necesaria la descarga de los Logs del sistema a un segundo equipo para analizarlos e identificar los patrones de la brecha de seguridad.

La Universidad Distrital Francisco José Caldas debe contar con estrategias para el cumplimiento de la legislación y normatividad vigente, entre la que se encuentran la Ley 599 de 2000 Capítulo VII, Directiva No. 005 de 2005 de la alcaldía Mayor de Bogotá, Ley 1266 de 2008, Ley 1273 de 2009, Ley 1581 de 2012, Ley 1712 de 2014, Decreto 103 de 2015, Conpes 3854 de 2016, entre otros. Esto con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información, garantizando su buen uso por parte de la comunidad universitaria que se compone de aproximadamente 26.000 Estudiantes y 1500 Docentes y 3000 administrativos.

Continuando con el cumplimiento de lineamientos para entidades estatales, la Universidad Distrital debe hacer adopción al protocolo IPv6 a más tardar el 31 de diciembre del año 2020 según Resolución 2710 de 2017 del Ministerio de Tecnologías de la Información y las Comunicaciones. Esto implica levantar el inventario de equipos

en red, entre ellos el sistema de seguridad perimetral, en cada uno de los equipos verificar la compatibilidad con el protocolo IPv6 y determinar las acciones que deben ser tomadas para lograr la transición hacia este protocolo, asegurando que exista una conexión a Internet de forma segura y continúa.

La infraestructura de telecomunicaciones de la Universidad Distrital conecta 18 sedes con el nodo Central, que se encuentra en el edificio Sabio Caldas, a través de enlaces de datos contratados con el Proveedor de Servicios de Internet, actualmente ETB, con el cual se tiene un acceso a internet dedicado de 2000 Mbps sobre el que se debe mejorar los niveles de seguridad con el fin de aumentar la confiabilidad, integridad y disponibilidad de la información de la entidad

Componente 2:

Por la distribución geográfica de las sedes, la Universidad Distrital Francisco José de Caldas cuenta con enlaces de datos dedicados (enlaces WAN MPLS) desde la sede Calle 40, donde se cuenta con la salida a internet, hacia las diferentes sedes. Para conectar las sedes hacia la Calle 40, se utilizan equipos de enrutamiento los cuales se encargan de manejar tanto el tráfico interno de la sede, así como el trafico destinado hacia otras sedes o internet.
Dado que los servicios prestados a través de la infraestructura de telecomunicaciones requieren mayores recursos de ancho de banda, se han venido aumentando progresivamente la capacidad de los enlaces dedicados en las sedes, lo que requiere equipos enrutadores con mayor rendimiento para utilizar la capacidad de los enlaces proyectados.

3. JUSTIFICACIÓN

Componente 1:

Con el fin de mejorar los niveles de la seguridad de la información, mejorar el nivel de protección frente amenazas informáticas desde y hacia internet, mitigar riesgos informáticos, implementar las condiciones que permitan la transición al protocolo IPv6 en los equipos de cómputo y mejorar el servicio de conectividad a Internet, la Universidad Distrital a través de la Red de Datos UDNET requiere el mejoramiento del sistema de seguridad perimetral por lo cual busca adelantar el proceso de contratación para la adquisición de hardware y software en conjunto con los servicios de licenciamiento, configuración, instalación, migración y puesta en correcto funcionamiento del sistema de seguridad perimetral en alta disponibilidad, que ofrezca mayor protección frente amenazas informáticas y además aumente la confidencialidad, integridad, disponibilidad de los activos de información.

Componente 2:

Con el presente proceso se busca continuar modernizando la plataforma de telecomunicaciones, reemplazando equipos que tienen rendimiento limitado, e incorporando equipos con mayores capacidades tanto en hardware como en software los cuales cuentan con mayor desempeño y mejoras tecnológicas.

La adquisición de estos equipos permite disponer de hardware para soportar el remplazo de equipos que ya están próximos a cumplir su ciclo de vida y garantizar la disponibilidad y calidad de los servicios actuales y aquellos que proyecte la universidad a un futuro próximo a través de la plataforma de telecomunicaciones.

El presente proyecto busca garantizar la continua disponibilidad de los recursos y servicios de las tecnologías de la información y las comunicaciones existentes, en beneficio de la comunidad académica y administrativa, optimizando los recursos.

4. ALCANCE

Componente 1:

- Adquisición, instalación, configuración y migración del Sistema de Seguridad Perimetral (HA) compuesto por hardware, software y licenciamiento. El sistema adquirido será puesto en marcha en las instalaciones de la Universidad Distrital Francisco José de Caldas.

- Mejorar el nivel de protección de la comunidad académico administrativa de la Universidad, frente amenazas informáticas de las sedes conectadas al nodo central desde y hacia internet.

- Adelantar el proceso contractual que permita seleccionar la mejor propuesta a partir de la recepción de ofertas del Sistema de Seguridad Perimetral (HA), según las especificaciones técnicas descritas en el presente documento con el fin de evaluarlas Jurídica, Financiera y Técnicamente.

Componente 2:

- Instalar seis (6) equipos Router con mayores capacidades de hardware y software, en las sedes ASAB, Calle 34, Macarena A, Macarena B, Tecnológica y Vivero, y de esta manera optimizar el uso del enlace de datos, mejorando el acceso a los servicios y recursos de la comunidad académica a través de la infraestructura de telecomunicaciones. Los equipos contaran con servicio de soporte, con reemplazo de partes, por tres (3) años, en esquema de atención 8X5XNBD, de acuerdo a las condiciones solicitadas en la “Tabla 13. Propuesta Comercial componente 2”.

5. 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

- Calidad del bien y/o servicio objeto del contrato.
- Devoluciones o cambio por incumplimiento de las especificaciones técnicas y/o calidad de los bienes.
- Pérdida de los productos por hurto, atentados o deterioro, como consecuencia del transporte de la misma entre el proveedor y/o en las instalaciones del contratista.
- Incumplimiento de lo establecido en los términos de referencia y/o en la oferta presentada al cierre del proceso de selección.
- No tener en cuenta los criterios ambientales aplicables a este tipo de contratación.
- 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.
- Retrasos o incumplimiento en los tiempos planteados y aprobados en el cronograma para la ejecución del contrato.
- Fallas en el soporte y en el cumplimiento de los tiempos o en cuanto al personal para brindar el soporte de los equipos o los medios para atender y realizar el soporte.
- Que se divulgue información que se conozca en virtud del cumplimiento de obligaciones y que no era susceptible de ser difundida.
- La no toma de las medidas de seguridad industrial apropiadas por el contratista ganador del presente proceso de selección, a favor de la conservación de las condiciones físicas y mentales de sus trabajadores, la comunidad universitaria, así como de terceras personas que activa o pasivamente tengan alguna relación.
- Que el proveedor no cuente en inventario con componentes y/o piezas, durante un periodo de soporte mínimo de tres (3) años, para su cumplimiento.
- La variación de los precios de mercado como resultado del impacto de la TRM, impactando cualquier actividad relacionada con la ejecución previa y posterior del contrato.
- Atraso y sobre costos en la entrega de los bienes y/o servicios requeridos.
- Que se afecten o desmejoren las condiciones de funcionamiento actuales de los espacios y/o equipos donde se realice la instalación.

Riesgos previsibles a cargo de la Universidad Distrital

- Incumplimiento de las obligaciones establecidas.
- El no pago del contrato, en la forma establecida, cualquiera sea la modalidad de esta contratación.
- Descripción equivocada de características para la adquisición de bienes y/o servicio.

- No establecimiento de requisitos técnicos necesarios en los estudios de conveniencia y en el pliego de condiciones.
- Que se suministre información errada o desactualizada al contratista para cualquiera de las actividades de su objeto contractual.
- La no ejecución del contrato en la forma debida y establecida en los Términos de referencia.
- La no comunicación permanente por parte del supervisor del contrato con el oferente(s) ganador (es) del proceso de selección que ocasione, demoras y tropiezos en el desarrollo del contrato que se firmare.
- Cambiar las condiciones técnicas establecidas, sin comunicación y consulta previas con el contratista y debidamente autorizadas por la Universidad.

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:

Componente 1:

- En caso de no adquirir el sistema de seguridad perimetral (HA) propuesto, la Universidad deberá continuar con el sistema de seguridad perimetral actualmente en funcionamiento lo cual presenta altos riesgos.
- Los equipos servidores, computadores de mesa, portátiles y plataformas virtuales de la Universidad estarían expuestos a amenazas desde Internet tales como: ransomware, botnet, hacking tools, explotación de vulnerabilidades, entre otros, permitiendo el aprovechamiento de vulnerabilidades informáticas por parte de personas inescrupulosas y comprometiendo la confidencialidad, disponibilidad e integridad de la información de la Universidad almacenada en los mismos.
- La adopción del protocolo IPv6 en la Universidad no se podría lograr con los niveles de seguridad de la información adecuados.

- No se tendría trazabilidad en tiempo real de los eventos críticos como son navegación web y ataques informáticos generados por los usuarios desde y hacia la conexión a Internet con la que cuenta la Universidad.

Componente 2:

- No se podría ampliar el ancho de banda de los enlaces de datos de las sedes que lo requieren por la saturación presentada en los mismos.
- No se podría asegurar la continuidad del servicio en las sedes en caso de falla de los equipos actuales.
- No se contaría con equipos de mayores capacidades de hardware para optimizar el uso de los enlaces en las sedes.

6. PRESUPUESTO

El presupuesto total estimado para el presente proceso es hasta por la suma de **SETECIENTOS SETENTA MILLONES DE PESOS MONEDA CORRIENTE ($770.000.000)** incluidos IVA y demás impuestos aplicables. Este presupuesto se distribuirá para los componentes de la siguiente forma:

- ✓ Componente 1: **QUINIENTOS MILLONES QUINIENTOS MIL PESOS MONEDA CORRIENTE ($500.000.000,00 M/Cte.)**,, incluidos IVA y demás Impuestos Nacionales y Distritales, según Certificado de Disponibilidad Presupuestal No. xxx del, xx de xxx de 2018 con cargo al rubro “Sistema integral de la información”, expedido por el Jefe de la Sección de Presupuesto de la Universidad Distrital.

- ✓ Componente 2: **DOSCIENTOS SETENTA MILLONES DE PESOS MONEDA CORRIENTE ($270.000.000 M/Cte.),** incluidos IVA y demás Impuestos Nacionales y Distritales, según Certificados de Disponibilidad Presupuestal No. xxx del, xx de xxx de 2018, con cargo al rubro “Sistema integral de la información”. expedidos 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 divulgar a terceros, sin acuerdo previo y por escrito de la Universidad Distrital Francisco José de Caldas.

8. FIN DE VENTA Y SOPORTE

El contratista debe entregar certificación expedida por el fabricante donde se garantiza que los equipos y sus componentes ofertados no se encuentran en periodo de fin de venta.

9. ESPECIFICACIONES TÉCNICAS

8.1. ESPECIFICACIONES TÉCNICAS COMPONENTE 1:

Los factores que deben ser ofertados en el momento de responder el pliego de condiciones deben cumplir en su totalidad con las características técnicas mínimas de carácter obligatorio. De no cumplir con estas características la propuesta no será aceptada por no permitir la escogencia objetiva del contratista.

La evaluación de orden técnico se hará a partir de la tabla 1 “Características mínimas de carácter obligatorio” y por lo tanto el proponente debe diligenciar cada uno de los ítem en la celda correspondiente a la columna con título: “Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)” debe ser confirmada mediante documentación oficial y pública del fabricante (guías de administración, manuales y/o guías técnicas) en medio físico y digital, en el cual se debe referenciar para cada característica un link a página WEB oficial donde se encuentre la documentación y número de página del documento encontrado en el link, donde se puede validar el cumplimiento de la especificación técnica. En el caso de las certificaciones y servicios solicitados se debe relacionar el número de página (folio) de la propuesta entregada.

8.1.1 CARACTERÍSTICAS TÉCNICAS MÍNIMAS DE CARÁCTER OBLIGATORIO

	ÍTEM	CARACTERÍSTICA	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)
GENERALIDADES	1	El Sistema de Seguridad Perimetral (HA) debe estar compuesto por todo el hardware, software y licenciamiento necesarios para su funcionamiento incluyendo alta disponibilidad HA.	
	2	El sistema debe contar con máximo dos equipos con el fin de minimizar los puntos de falla, optimizar el espacio en el data center, optimizar el uso de las conexiones de red y facilitar la administración incluyendo el sistema de monitoreo y reportes. Estos deben trabajar de forma redundante entre sí en Alta disponibilidad (HA) soportando todos los servicios que presta el sistema de seguridad perimetral HA.	
	3	El hardware y software que ejecuten las funcionalidades del sistema deben ser de tipo appliance. No serán aceptados equipamientos servidores y sistema operativo de uso genérico	
	4	Los equipos ofrecidos deben ser adecuados para montaje en rack 19”. Cada equipo puede ocupar máximo 3 unidades de Rack.	
	5	El software del sistema deberá ser ofertado en la última versión estable y recomendada por el fabricante.	
	6	El sistema debe tener la capacidad de identificar al usuario de red con integración a Microsoft Active Directory, sin la necesidad de instalación de agente en el Controlador de dominio, ni en las estaciones de los usuarios.	

	7	Los equipos deben estar certificados para IPv6 en Firewall por USGv6 o IPv6 Ready	
	8	El sistema debe incluir actualización automática de firmas de prevención de intrusos (IPS), bloqueo de archivos maliciosos (Antivirus y Antispyware), Filtrado WEB por categorías e identificación de aplicaciones	
	9	Motor de procesamiento en paralelo: el módulo de hardware del plano de control y el módulo de hardware del plano de datos deben estar separados y deben estar embebidos en cada equipo.	
	10	Los equipos ofertados NO deben estar en anuncio de fin de vida (end-of-life) y fin de venta (end-of-sale) por parte del fabricante	
	11	Debe permitir el control de políticas por identificación de País.	
	12	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)	
ALTA DISPONIBILIDAD	13	Soporta configuración de alta disponibilidad (HA) en los modos Activo/Pasivo y Activo/Activo en modo transparente y en layer 3	
	14	El HA (modo de Alta-Disponibilidad) debe permitir monitoreo de fallo de link.	
CAPACIDAD Y CANTIDADES	15	Throughput para cada equipo de mínimo 8 Gbps con la funcionalidad de control de aplicaciones habilitada y logs habilitados para todas las firmas (actualizaciones) que el fabricante disponga.	
	16	Throughput para cada equipo de mínimo 4 Gbps con las siguientes funcionalidades habilitadas simultáneamente para todas firmas (actualizaciones) que el sistema disponga debidamente activadas y actuando con logs habilitados para: control de aplicaciones, IPS, Antivirus y Antispyware.	
	17	Cada equipo debe tener la Capacidad de procesar mínimo 3 millones de conexiones de red simultáneas (concurrentes)	
	18	Cada equipo debe tener la Capacidad de procesar mínimo 135.000 nuevas conexiones en red por segundo.	
	19	Cada equipo debe tener Fuente 120V AC, redundante y hot-swappable (dos fuente en redundancia)	
	20	Cada equipo debe incluir Disco de Estado Sólido (SSD) de mínimo 240 GB para almacenamiento del sistema y logs	
	21	Mínimo 8 Interfaces Ethernet base-TX 10/100/1000 de tráfico de red para cada equipo (No debe incluir interfaces para alta disponibilidad, ni administración)	

	22	Mínimo 4 Interfaces 10Gbps SFP/SFP+ de tráfico de red para cada equipo (No debe incluir interfaces para alta disponibilidad, ni administración) incluyendo Mínimo 2 optical transceiver SFP+ 10-Gigabit multi-mode	
	23	Mínimo 1 Interfaz para alta disponibilidad a 1 Gbps (No deben estar incluidas en las interfaces para tráfico de Red, ni administración)	
	24	Mínimo 1 Interfaz adicional para alta disponibilidad a 10 Gbps SFP+ (No deben estar incluidas en las interfaces para tráfico de Red, ni administración)	
	25	Interfaz dedicada para administración 10/100/1000 para cada equipo	
	26	1 interfaz de tipo consola	
	27	Capacidad de mínimo 60 zonas de seguridad	
SERVICIOS Y PROTOCOLOS DE RED	28	Soporte de mínimo 1024 VLAN Tags 802.1q	
	29	Soporte de Agregación de links 802.3ad	
	30	Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2) Para IPv4	
	31	Debe soportar enrutamiento estático y dinámico (OSPFv3) Para IPv6	
	32	Capacidad de balancear varios enlaces de internet sin el uso de políticas específicas	
	33	Las funcionalidades de control de aplicaciones, VPN IPSec y SSL, QoS y SSL Decryption y protocolos de enrutamiento dinámico deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no hay contrato de licenciamiento con el fabricante.	
CONTROL POR POLÍTICA DE FIREWALL	34	Soportar controles por zona de seguridad	
	35	Controles de políticas por puerto y protocolo.	
	36	Control de políticas por aplicaciones, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones.	
	37	Control de políticas por usuarios, grupos de usuarios, IPs, redes y zonas de seguridad.	
	38	Soportar objetos y Reglas multicast.	
	39	Soportar los atributos de agendamiento de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.	
CONTRO	40	El sistema deberá tener la capacidad de reconocer aplicaciones, independiente del puerto y protocolo	

	41	Debe ser posible la liberación y bloqueo solamente de aplicaciones sin la necesidad de liberación de puertos y protocolos.	
	42	Detectar y limitar el ancho de banda (download/upload) usado por aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos del LDAP/AD	
	43	Para mantener la seguridad de la red, debe soportar el control sobre aplicaciones desconocidas y no solamente sobre aplicaciones conocidas	
PREVENCIÓN DE AMENAZAS	44	Para seguridad del ambiente contra ataques informáticos, el sistema de seguridad debe poseer módulo de IPS, Antivirus y Anti-Spyware integrados en los equipos que componen el sistema	
	45	El sistema debe soportar granularidad en las políticas de IPS Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos esos ítems.	
	46	Debe incluir seguridad contra ataques de denegación de servicios.	
	47	Debe permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3	
	48	Soportar bloqueo de archivos por tipo	
	49	Debe ser posible la configuración de diferentes políticas de control de amenazas y ataques basados en políticas del firewall donde cada política pueda incluir como mínimo Usuarios, Grupos de usuarios, origen, destino, zonas de seguridad	
	50	El sistema debe ofrecer funcionalidades para análisis de Malware no conocidos incluidas en la propia herramienta.	
	51	El sistema debe ser capaz de enviar archivos sospechosos transferidos de forma automática para análisis "In Cloud" o local, donde el archivo será ejecutado y simulado en un ambiente controlado.	
FILTRO URL	52	Debe ser posible crear políticas por usuario, grupo de usuario, IPs, redes y zonas de seguridad	
	53	Deberá incluir la capacidad de creación de políticas basadas en la visibilidad y control de quién está utilizando URLs a través de la integración con servicios de directorio, autentificación vía LDAP, Active Directory, E-Directory y base de datos local	
	54	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría URL	
	55	Debe permitir al menos 60 categorías de URLs	

	56	Debe soportar la creación de categorías URL custom	
	57	Debe soportar la exclusión de URLs del bloqueo por categoría	
IDENTIFICACIÓN DE USUARIOS	58	Debe permitir integración con Radius, ldap, Active Directory, E-directory y base de datos local, para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.	
	59	Debe soportar la recepción de eventos de autenticación de controladoras Wireless, dispositivos 802.1x y soluciones NAC via syslog, para la identificación de direcciones IP y usuarios	
	60	Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en ambientes Citrix y Microsoft Terminal Server, permitiendo visibilidad y control granular por usuario sobre el uso de las aplicaciones que tienen estos servicios	
	61	Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en servidores accedidos remotamente, incluso que no sean servidores Windows.	
CALIDAD DE SERVICIO	62	Como la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube, ustream, etc.) y tener un alto consumo de ancho de banda, el sistema debe controlarlas por políticas de máximo ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones.	
	63	Soportar la creación de políticas de QoS por: - Dirección de origen - Dirección de destino - Por usuario y grupo de LDAP/AD - Por aplicaciones - Por puerto	
	64	El QoS debe permitir la definición de clases por: - Ancho de Banda garantizado - Ancho de Banda Máximo - Cola de prioridad.	
	65	Soportar priorización RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.	
	66	Soportar marcación de paquetes Diffserv	
FILTRO DE DATOS	67	Permitir identificar y opcionalmente prevenir la transferencia de informaciones sensibles, incluyendo, mas no limitando al número de tarjetas de crédito, permitiendo la creación de nuevos tipos de datos via expresión regular	
	68	Permitir la detección de portales de phishing estableciendo políticas que eviten el envío de credenciales válidas de usuarios a sitios no autorizados	

VPN	69	Debe soportar VPN IPSec Nativa Client-To-Site y Site-to-Site (Incluyendo conexión Site-to-Site con infraestructuras en la nube mínimo con: Amazon, Microsoft Azure)	
	70	La VPN IPSEc debe soportar mínimo: - 3DES; - Autenticación MD5 y SHA-1; - Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; - Algoritmo Internet Key Exchange (IKEv1 & IKEv2); - AES 128 y AES 256 (Advanced Encryption Standard) - Autenticación vía certificado IKE PKI.	
	71	Debe poseer interoperabilidad VPN IPSec mínimo con los siguientes fabricantes: Cisco, Checkpoint, Juniper, Palo Alto Networks, Fortinet, Sonic Wall	
	72	Permitir que el usuario realice la conexión por medio de cliente instalado en el sistema operativo del equipo cliente o por medio de interfaz WEB	
	73	Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local	
	74	Permite establecer un túnel VPN client-to-site del cliente al sistema de seguridad, proveyendo una solución de single-sign-on a los usuarios, integrándose como las herramientas de Windows-logon	
	75	Debe permitir que las conexiones VPN SSL o VPN IPSec sean establecidas de las siguientes formas: - Antes o durante la autenticación del usuario en la estación - Después de la autenticación del usuario en la estación - Manualmente por el usuario	
	76	El cliente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10	
	77	Capacidad de soportar mínimo 2000 clientes de VPN SSL simultáneos sin uso de licenciamiento o licenciado a perpetuidad	
	78	Capacidad de soportar mínimo 1000 túneles de VPN IPSEC simultáneos sin uso de licenciamiento o licenciado a perpetuidad	
CONSOLA DE ADMINISTRACIÓN y MONITOREO	79	El sistema debe incluir consola de administración y monitoreo, incluyendo el licenciamiento de software necesario para las dos funcionalidades, como también el hardware dedicado para el funcionamiento de las mismas	
	80	La consola de administración y monitoreo puede residir en el mismo appliance de seguridad de red, desde que posea recurso de CPU, memoria, interfaz de red y sistema operacional dedicados para esta función.	

	81	La administración del sistema debe soportar acceso via SSH, cliente WEB (HTTPS) y API abierta	
	82	La administración en la consola debe permitir/hacer: - Creación y administración de políticas de firewall y control de aplicaciones - Creación y administración de políticas de IPS y Anti-Spyware - Creación y administración de políticas de filtro de URL - Monitoreo de logs - Herramientas de investigación de logs - Debugging - Captura de paquetes	
	83	Debe permitir la validación de las políticas, avisando cuando haya Reglas que ofusquen o tengan conflicto con otras (shadowing)	
	84	Debe posibilitar la visualización y comparación de configuraciones actuales, la configuración anterior y configuraciones más antiguas	
	85	Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizó y el horario del cambio	
	86	Debe permitir la generación de mapas geográficos en tiempo real para la visualización de orígenes y destinos del tráfico generado en la Universidad	
	87	Debe proveer resúmenes con la vista correlacionada de aplicaciones, amenazas (IPS, Anti Spyware) URLs y filtro de archivos, para un mejor diagnóstico y respuesta a incidentes	
	88	Debe ser posible acceder remotamente al sistema a aplicar configuraciones durante momentos donde el tráfico sea muy alto y la CPU y memoria del equipamiento este siendo totalmente utilizada.	
	89	Debe tener presentaciones de las siguientes informaciones, de forma histórica y en tiempo real (actualizado de forma automática y continua cada 1 minuto): - Debe mostrar la situación del dispositivo y del clúster - Debe poder mostrar las principales aplicaciones - Debe poder mostrar las principales aplicaciones por riesgo - Debe poder mostrar los administradores autenticados en la plataforma de seguridad - Debe poder mostrar el número de sesiones simultáneas - Debe poder mostrar el estado de las interfaces - Debe poder mostrar el uso de CPU	

SERVICIOS	90	Soporte y cambio de partes 7x24 durante 3 años: El proveedor debe prestar el Soporte técnico de todos los componentes del sistema durante los 3 años contratados, con servicio en sitio, remoto, telefónico o a través correo electrónico, por personal certificado en la marca. Cuando el diagnóstico sobre los equipos o partes determine falla total o parcial, el contratista deberá realizar el proceso de RMA. El equipo entregado o partes por RMA debe contar con iguales o superiores características y capacidades tanto en hardware como en software que el equipo o parte reemplazada. La atención de soporte será en esquema 7x24xNBD: 7 días de la semana las 24 horas del día, con reemplazo de hardware al siguiente día hábil, el tiempo de atención no puede superar las 4 horas. Estos servicios hacen parte de la oferta incluyendo todos costos asociados para su cumplimiento (fletes, impuestos, transporte, importación, entre otros).	
	91	Instalación, configuración, migración, puesta en funcionamiento y optimización del sistema: hardware, software, licenciamiento y todas las funcionalidades adquiridas, incluyendo todos los cables, accesorios y demás elementos necesarios.	
	92	Licenciamiento en HA durante 3 años incluyendo todas las funcionalidades descritas en este documento	
	93	Transferencia de conocimiento certificada por el fabricante para dos personas del equipo técnico de la Red de Datos UDNET	

Tabla 1. "Características mínimas de carácter obligatorio"

8.1.1 CARACTERÍSTICAS TÉCNICAS ADICIONALES

Se le asignará máximo trescientos (300) puntos al proponente que ofrezca características técnicas adicionales según la tabla 2. Este puntaje se asignará entre todos los oferentes, una vez estén habilitados jurídico, técnico y financieramente.

La calificación se hará de acuerdo a la siguiente tabla:

Ítem	Descripción	Asignación de Puntos	Puntaje Máximo
1	Interfaces adicionales Ethernet base-TX 10/100/1000 de tráfico de red para cada equipo (No debe incluir interfaces para alta disponibilidad, ni administración)	10 puntos por cada Interfaz	40
2	Interfaces adicionales 10 Gbps SFP/SFP+ de tráfico de red para cada equipo (No debe incluir interfaces para alta disponibilidad, ni administración)	25 puntos por cada Interfaz	50
3	Optical transceiver adicionales SFP+ 10-Gigabit multi-mode para cada equipo. (El número total de transceiver de este tipo no puede exceder el número total de interfaces ofertadas en ítem 2 de esta tabla.)	25 puntos por cada optical transceiver	50

4	Interfaces adicionales 40 Gbps QSFP+ de tráfico de red Para cada equipo (No debe incluir interfaces para alta disponibilidad, ni administración).	30 puntos por cada Interfaz	60
5	Optical transceiver adicionales QSFP+ 40-Gigabit multi-mode para cada equipo. (El número total de transceiver de este tipo no puede exceder el número total de interfaces ofertadas en ítem 4 de esta tabla.)	25 puntos por cada optical transceiver.	50
6	El software (Navegador WEB u otro) para la administración del sistema es compatible con sistemas operativos Windows, Linux, Android y iOS	50 puntos si se cumple la característica.	50

Tabla 2. "Descripción de asignación de Puntos para Características técnicas adicionales"

Ítem	Descripción	Oferta
1	Interfaces adicionales Ethernet base-TX 10/100/1000 de tráfico de red para cada equipo (No debe incluir interfaces para alta disponibilidad, ni administración)	Ofertar en este campo el número de interfaces
2	Interfaces adicionales 10 Gbps SFP/SFP+ de tráfico de red para cada equipo (No debe incluir interfaces para alta disponibilidad, ni administración)	Ofertar en este campo el número de interfaces
3	Optical transceiver adicionales SFP+ 10-Gigabit multi-mode para cada equipo. (El número total de transceiver de este tipo no puede exceder el número total de interfaces ofertadas en ítem 2 de esta tabla.)	Ofertar en este campo el número de optical transceiver
4	Interfaces adicionales 40 Gbps QSFP+ de tráfico de red Para cada equipo (No debe incluir interfaces para alta disponibilidad, ni administración).	Ofertar en este campo el número de interfaces
5	Optical transceiver adicionales QSFP+ 40-Gigabit multi-mode para cada equipo. (El número total de transceiver de este tipo no puede exceder el número total de interfaces ofertadas en ítem 4 de esta tabla.)	Ofertar en este campo el número de optical transceiver
6	El software (Navegador WEB u otro) para la administración del sistema es compatible con sistemas operativos Windows, Linux, Android y iOS	Indicar en este campo si cumple o no la característica. En el caso afirmativo indicar el link a página WEB del fabricante donde se verifique este ítem.

Tabla 3. "Características técnicas adicionales"

NOTA: La tabla 3 debe ser diligenciada en concordancia a la tabla 2.

8.2. ESPECIFICACIONES TÉCNICAS COMPONENTE 2:

La evaluación de orden técnico se hará a partir de la siguiente tabla, por lo tanto el proponente debe diligenciar para cada uno de los "ítem" en la celda correspondiente a la columna con título: ***"Ubicación en la propuesta/Ficha Técnica fabricante (No. Página)"***, la ubicación, nombre y número de página del documento donde se puede validar el cumplimiento de las especificaciones técnicas de los equipos y elementos ofertados, toda la documentación de soporte técnico se debe entregar adjunta en medio físico y digital (CD-DVD).

ítem	ESPECIFICACION TECNICA ROUTER CON CARACTERISTICAS DE SEGURIDAD.	UBICACIÓN EN LA PROPUESTA/FICHA TÉCNICA FABRICANTE (NO. PÁGINA)
1	El equipo debe ser de máximo dos (2) unidad de Rack	
2	El equipo debe contar con mínimo dos (2) fuentes de poder.	
3	El equipo debe contar como mínimo cuatro (4) puertos de 1Gbps en cobre RJ45	
4	El equipo debe contar como mínimo dos (2) puertos para SFP de fibra óptica.	
5	El equipo debe tener un throughput de mínimo de 1Gbps en paquetes IMIX.	
6	El equipo debe contar como mínimo cuatro (4) GB de RAM	
7	El equipo debe contar como mínimo cuatro (8) GB de memoria FLASH	
8	Debe contar con un puerto de Consola del tipo RS-232 (puerto DB9 o puerto RJ-45)	
9	El equipo debe contar con mínimo una interface USB para el almacenamiento externo.	
10	El equipo debe soportar y tener habilitada la funcionalidad de túneles VPN IPSEC y GRE.	
11	El equipo debe soportar IPv6 e IPv4 a nivel de hardware y software	
12	Debe tener funcionalidades de protección de DoS	
13	Debe soportar Jumbo frames	
14	Debe soportar Rutas Estáticas, BGP, OSPF, OSPF v3, RIP v1/v2, IS-IS, IGMP v1/v2	
15	El equipo debe soportar trafico MPLS (LDP y RSVP), VPN MPLS, Capa 2 y Capa 3 MPLS.	
16	El equipo debe ser administrado a través de: CLI, WEB, SNMP, SSH.	
17	IEEE802.1D (STP)	
18	IEEE802.1p (CoS)	
19	IEEE802.1Q (VLANs)	
20	IEEE802.1S (MSTP)	
21	IEEE802.1X (Security)	
22	IEEE802.3ad (LACP)	
23	LLDP	
24	El equipo debe soportar y tener habilitado VRRP	

ítem	ESPECIFICACION TECNICA ROUTER CON CARACTERISTICAS DE SEGURIDAD.	UBICACIÓN EN LA PROPUESTA/FICHA TÉCNICA FABRICANTE (NO. PÁGINA)
25	Debe soportar la configuración de listas de control de acceso de nivel 3 y/o nivel 2	
26	Debe soportar NAT(Network Address Translation) estático, dinámico y sobrecarga	
27	Debe soportar DHCP (Dynamic Host Configuration Protocol) en modo cliente, servidor y relay.	
28	Debe tener la capacidad de almacenar mínimo diez (10) configuraciones en el mismo equipo las cuales pueden ser llamadas y cargadas en cualquier momento.	
29	El equipo debe estar en capacidad de poder realizar una restauración a la configuración anterior a la que se encuentra en operación atreves de la aplicación de un solo comando.	
30	El equipo debe tener Sistema operativo modular con separación de Plano de Control y Plano de Datos.	
31	Debe tener luces indicadoras de múltiples funciones como estado del equipo y estado de puertos	
32	El equipo debe soportar la configuración de rutas basadas en el origen.	
33	El equipo debe soportar la configuración de NAT 64	
34	El equipo debe soportar SD-WAN.	
35	El equipo debe permitir la creación de mínimo 32 Routers virtuales	

Tabla 4. “especificación técnica Router con características de seguridad.”

Nota: La caracterización técnica de los equipos y componentes solicitados se obtiene a partir de la revisión de los datasheet de los mismos. Se verifica que sea basada en estándares, y que cumpla con la tecnología de las marcas actualmente instaladas en la universidad y con las especificaciones técnicas solicitadas.

8.2.1. SOPORTE Y REEMPLAZO DE PARTES

El proveedor debe prestar el servicio de soporte técnico a los equipos adquiridos durante los tres (3) años contratados, con servicio en sitio, remoto, telefónico o a través correo electrónico.

El soporte de los equipos iniciará a partir de la entrega de los mismos en correcto funcionamiento, con las respectivas pruebas y recibo a satisfacción por parte del supervisor, y debe incluir actualización de software que debe ser realizado por el contratista y reemplazo de partes.

Cuando el diagnóstico sobre los equipos o partes determine falla total o parcial, el contratista deberá realizar el proceso de RMA. El equipo entregado o partes por RMA debe contar con iguales o superiores características y capacidades tanto en hardware como en software que el equipo o parte reemplazada. La atención de soporte y reemplazo de partes será en esquema 8x5xNBD: 5 días hábiles de la semana de 8:00 am a 5:00 pm, con remplazo de hardware al siguiente día hábil. Estos servicios hacen parte de la oferta incluyendo todos costos asociados para su cumplimiento (fletes, impuestos, transporte, importación, entre otros).

8.2.2. RECEPCION DE LOS EQUIPOS Y COMPONENTES

Los equipos y componentes deben entregarse en el Datacenter Olimpo ubicado en la Carrera 8 No. 40 - 62 Piso 4. Edificio Sabio Caldas, o donde la universidad indique, de acuerdo al cronograma propuesto y aprobado.

Durante la ejecución del contrato las pruebas de funcionamiento se realizarán según se define a continuación:

- ✓ **Equipos:** el contratista debe realizar las pruebas de funcionamiento de los equipos. Sobre este procedimiento se llevará registro en el documento con nombre "***Anexo 1. Protocolo de pruebas y recepción de equipos y/o componentes UDistrital"***. El procedimiento se debe realizar en presencia de personal técnico delegado por la supervisión, con la asesoría de la Red de Datos UDNET, quien realiza la recepción del equipo. Los equipos que no pasen la prueba de auto encendido Power On Self Test o que presenten deterioro y no pasen la revisión física, serán devueltos.

- ✓ **Componentes:** El contratista, junto con el personal técnico delegado por la supervisión, con la asesoría de la Red de Datos UDNET, realizará la revisión y pruebas de funcionamiento que apliquen. Sobre este procedimiento se llevará registro en el documento con nombre "***Anexo 1. Protocolo de pruebas y recepción de equipos y/o componentes UDistrital"***. Los componentes que no pasen la revisión, serán devueltos.

- ✓ En caso de que algún equipo o componente no sea aceptado será devuelto y los costos de desplazamientos (ida y vuelta, fletes, seguros, etc.), reemplazo de parte, estará a cargo y responsabilidad exclusivo del contratista y en ningún caso generará costo adicional a la Universidad Distrital.

La instalación de los equipos se realizara en las siguientes sedes de la Universidad:

SEDE	***DIRECCIÓN***
ASAB	Carrera 13 # 14 - 69
Calle 34	Calle 34 # 13 - 13
Macarena A	Carrera 3 # 26A - 40 / Carrera 1 Este # 33 - 54
Macarena B	Carrera 4A # 26D - 54
Tecnológica	Calle 68D Bis A Sur # 49F - 70
Vivero	Carrera 5 Este # 15-82 / Calle 14 # 7-46 Este

Tabla 5. "Sedes universidad Distrital."

Si el oferente ganador entrega equipos Router adicionales de valor agregado, se acordará con el contratista durante la ejecución del contrato la sede, o sedes, en las cuales se instalarán los equipos.

8.2.3. DOCUMENTACIÓN DE CARÁCTER TECNICO

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

- Hoja de datos de los equipos y componentes ofertados en formato Digital.
- Certificado expedido directamente por el fabricante en el que conste que es partner. Dicho certificado deberá estar vigente durante la validez de la propuesta y durante la ejecución del se solicitará nuevamente la certificación.

- Certificación del fabricante donde se garantiza que los equipos y componentes ofertados no se encuentran en periodo de fin de venta.
- Carta de compromiso de la empresa, donde se indique que los equipos y componentes a proveer son genuinos, nuevos y adquiridos a través de canal autorizado por el fabricante.
- Documento que discrimine los niveles de servicio (SLA) en esquema 8X5XNBD, para atender las solicitudes de soporte.
- El Oferente debe entregar documento con las políticas del fabricante sobre el ciclo de vida de los equipos.

9. DURACIÓN DEL CONTRATO

La duración del contrato en virtud del presente proceso está definida de la siguiente manera:

Componente 1

El plazo para la ejecución del contrato es de 3 años de los cuales la entrega del hardware y software, así como los servicios de licenciamiento, configuración, instalación, migración y puesta en correcto funcionamiento del Sistema de Seguridad Perimetral HA se realizará dentro de los primeros 120 días calendario.

El licenciamiento del software será durante tres (3) años, periodo durante el cual el proveedor prestará los servicios de soporte y actualizaciones (update y upgrade) de software.

Componente 2

El plazo para la ejecución del contrato es de 3 años de los cuales la entrega del hardware, así como los servicios de configuración, instalación y puesta en correcto funcionamiento de los equipos Router se realizará dentro de los primeros 120 días calendario.

El servicio de soporte será durante tres (3) años, periodo durante el cual el proveedor realizara actualizaciones (update y upgrade) de software y reemplazo de partes si se requiere.

10. VALOR Y FORMA DE PAGO

El valor del contrato o de los contratos que surjan de la presente convocatoria será hasta por la suma de la oferta u ofertas ganadoras del presente proceso de selección. La Universidad pagará al contratista la totalidad del valor del contrato por componente en un solo contado, previa entrega y cumplimiento de los siguientes requisitos:

- Entrega total de equipos, licencias y componentes según las especificaciones técnicas de cada componente.
- Diligenciamiento del “Anexo 1. Protocolo de pruebas y recepción de equipos y/o componentes UDistrital”, donde se relacione cada uno de los equipos y componentes con las pruebas de correcto funcionamiento. El documento debe contar con las respectivas firmas de aprobación.
- Configuración, migración, instalación y puesta en correcto funcionamiento los equipos adquiridos en el presente proceso según las especificaciones técnicas de cada componente.
- Informe de la instalación, configuración y puesta en correcto funcionamiento de los equipos.

- Documentos referidos en la circular No 001 y 002 de 2016 de la División de Recursos Financieros.
- 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 de la universidad.
- Presentación de la factura donde se debe discriminar cada uno de los ítems cobrados, así como el IVA respectivo.
- Acta de recibo a satisfacción por parte de la Supervisión.
- Certificación de cumplimiento del pago de seguridad social y parafiscales, suscrita por el representante legal o el revisor fiscal, según sea el caso
- Documento anexo a la factura en el cual se relacionen los siguientes campos:
  - ✓ Ítem
  - ✓ Referencia.
  - ✓ Descripción.
  - ✓ Serial.
  - ✓ Marca.
  - ✓ Costo unitario sin iva
  - ✓ Iva aplicado (%)
  - ✓ Costo total con iva
- Demás documentos exigidos por la Universidad.
- El pago se efectuara dentro de los sesenta (60) días siguientes a la presentación 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.
- Documento de manifiesto de importación de los equipos y elementos, en físico y digital, los cuales deben identificar explícitamente (subrayado o resaltado) los seriales de los equipos y componentes adquiridos por la Universidad.
- Manuales de operación y administración de los equipos en formato digital (idioma español y/o ingles).
- Cronograma de entrega y pruebas de los equipos y componentes, el cual será avalado y aprobado por el supervisor designado por la Universidad con el acompañamiento técnico de la Red de Datos UDNET.

Para el Componente 1:

- Certificación de soporte de fábrica del sistema de seguridad perimetral HA indicando:
  - Niveles de escalamiento.
  - Tiempo de cobertura.
  - Alcance y cobertura sobre el equipo y componentes.
  - Alcance y cobertura sobre actualización de software.

- 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 las funcionalidades que activa.
- Registro de transferencia de conocimiento.
- Acta donde el contratista se compromete a prestar los servicios de soporte y actualizaciones (update y upgrade) de software durante tres (3) años.

***Para el Componente 2*:**

- Documento expedido por el fabricante a nombre de la universidad con una descripción completa del tipo de contrato de soporte que ampara a los equipos, con sus respectivas referencias y seriales, fecha de inicio y fecha de finalización, el cual no debe contradecir lo establecido en la presente ficha técnica.
- Mecanismo que permita a la Universidad Distrital Francisco José de Caldas verificar de manera directa con el fabricante el soporte y garantía que ampara a los equipos, por un periodo mínimo de tres (3) años.
- Mecanismo o cuenta online para realizar descargas de software para los equipos adquiridos, por un periodo mínimo de tres (3) años.
- Documento con la descripción detallada del servicio de soporte (SLA) en formato Partner Support 8x5xNBD por tres (3) años para los equipos adquiridos y sus componentes (incluye actualizaciones de software).

11. EVALUACIÓN DE LAS PROPUESTAS

Los criterios a evaluar serán los siguientes:

FACTORES DE EVALUACIÓN/ CALIFICACIÓN	RESULTADO	FACTORES DE EVALUACIÓN/ CALIFICACIÓN
Evaluación Jurídica	Admisible / No Admisible	Evaluación Jurídica
Evaluación Financiera	Admisible / No Admisible	Evaluación Financiera
Evaluación Técnica	Admisible/ No Admisible	Evaluación Técnica

Tabla 6. “Calificaciones.”

10.1. COMPONENTE 1:

Las propuestas que CUMPLEN con la evaluación, serán calificadas de acuerdo a la siguiente tabla:

CALIFICACION	PUNTAJE
ECONOMICA	700
CARACTERÍSTICAS TÉCNICAS ADICIONALES	300
CALIFICACION TOTAL	1000

Tabla 7. Calificaciones componente 1

10.1.1. EVALUACIÓN DEL FACTOR ECONÓMICO-ASIGNACIÓN DE PUNTAJE COMPONENTE 1

Para la calificación de este factor, se requiere que el proponente haya cotizado la totalidad de los ítems requeridos, so pena de rechazo de la propuesta. Este aspecto asignará un máximo de 700 puntos posibles, mediante la utilización del método de menor valor ofertado, diligenciando el formato de presentación de propuestas

10.1.2. CARACTERÍSTICAS TÉCNICAS ADICIONALES

Para este factor se tendrá una calificación se asignará hasta trecientos (300) puntos, para el proponente que ofrezca características técnicas adicionales descritas en el ítem "CARACTERÍSTICAS TÉCNICAS ADICIONALES"

Este puntaje se asignará entre todos los oferentes que una vez habilitado jurídico, técnico y financieramente.

Ítem	Descripción	Asignación de Puntos	Puntaje Máximo
1	Interfaces adicionales Ethernet base-TX 10/100/1000 de tráfico de red para cada equipo (No debe incluir interfaces para alta disponibilidad, ni administración)	10 puntos por cada Interfaz	40
2	Interfaces adicionales 10 Gbps SFP/SFP+ de tráfico de red para cada equipo (No debe incluir interfaces para alta disponibilidad, ni administración)	25 puntos por cada Interfaz	50
3	Optical transceiver adicionales SFP+ 10-Gigabit multi-mode para cada equipo. (El número total de transceiver de este tipo no puede exceder el número total de interfaces ofertadas en ítem 2 de esta tabla.)	25 puntos por cada optical transceiver	50
4	Interfaces adicionales 40 Gbps QSFP+ de tráfico de red Para cada equipo (No debe incluir interfaces para alta disponibilidad, ni administración).	30 puntos por cada Interfaz	60

5	Optical transceiver adicionales QSFP+ 40-Gigabit multi-mode para cada equipo. (El número total de transceiver de este tipo no puede exceder el número total de interfaces ofertadas en ítem 4 de esta tabla.)	25 puntos por cada optical transceiver.	50
6	El software (Navegador WEB u otro) para la administración del sistema es compatible con sistemas operativos Windows, Linux, Android y iOS	50 puntos si se cumple la característica.	50

Tabla 8. Puntos adicionales componente 1

10.2. COMPONENTE 2:

Las propuestas que CUMPLEN con la evaluación, serán calificadas de acuerdo a la siguiente tabla:

CALIFICACION	PUNTAJE
ECONOMICA	800
MAYOR CANTIDAD DE ROUTERS ADICIONALES	150
ACTUALIZACION DE SOFTWARE EN SERVICIO	50
CALIFICACION TOTAL	1000

Tabla 9. Calificaciones componente 2

10.2.1. EVALUACIÓN DEL FACTOR ECONÓMICO-ASIGNACIÓN DE PUNTAJE COMPONENTE 2

Para la calificación de este factor, se requiere que el proponente haya cotizado la totalidad de los ítems requeridos, so pena de rechazo de la propuesta. Este aspecto asignará un máximo de 800 puntos posibles, mediante la utilización del método de menor valor ofertado, diligenciando el formato de propuesta ecomonica

10.2.2. MAYOR CANTIDAD DE ROUTERS ADICIONALES

Se le asignará ciento cincuenta (150) puntos al proponente que ofrezca mayor cantidad de Routers adicionales a los requeridos en la propuesta economica. Este puntaje se asignará entre todos los oferentes, una vez estén habilitados jurídico, técnico y financieramente. La calificación se hará de acuerdo a la siguiente tabla:

Este puntaje se asignará entre todos los oferentes que una vez habilitado jurídico, técnico y financieramente.

item	Router	Asignación de Puntos	total
1	Un máximo de 3 Router adicionales a los ofertados en la propuesta económica.	50 puntos por cada equipo Router adicional.	150

Tabla 10. Puntaje adicional mayor cantidad de routers adicionales

Nota: Los equipos adicionales deben cumplir con los requerimientos solicitados en los presentes términos técnicos, (Instalación, soporte, etc).

10.2.3. ACTUALIZACION DE SOFTWARE EN SERVICIO

Se le asignará cincuenta (50) puntos al proponente que ofrezca equipos con la capacidad de actualización de software en servicio (ISSU). Este puntaje se asignará entre todos los oferentes, una vez estén habilitados jurídico, técnico y financieramente. La calificación se hará de acuerdo a la siguiente tabla:

Este puntaje se asignará entre todos los oferentes que una vez habilitado jurídico, técnico y financieramente.

item	Router	Asignación de Puntos	total
1	Capacidad de actualización de software sin interrupción del servicio	50 puntos	50

Tabla 11. Puntaje adicional actualización de software en servicio

11. PROPUESTA ECONÓMICA

Componente 1

ÍTEM	DESCRIPCIÓN	MARCA	REFERENCIA	VALOR (SIN IVA)	% IVA	VALOR (CON IVA)
1	Sistema de seguridad perimetral HA, compuesto por todo el hardware y software necesarios para su funcionamiento en alta disponibilidad, incluyendo todos los cables, accesorios y demás elementos necesarios según especificaciones técnicas.					
2	Servicios de Instalación, configuración, migración y puesta en correcto funcionamiento según especificaciones técnicas.					
3	Licenciamiento y soporte durante 3 años incluyendo todas las funcionalidades adquiridas según especificaciones técnicas.					
					TOTAL:	

Tabla 12. Propuesta económica componente 1

Componente 2

Ítem	Descripción	Marca	Referencia o número de parte	Cantidad	Valor Unitario	IVA	Valor Total
1	Router			6			
2	Instalación, configuración y puesta en funcionamiento de los equipos			6			
3	Servicio de soporte en formato partner support 8x5xNBD por (3) tres años para los equipos adquiridos y sus componentes (incluye actualizaciones de software y reemplazo de partes)			6			
	Total						

Tabla 13. Propuesta económica componente 2

8.3. GLOSARIO

- **DIFFSERV**: Differentiated Service. Indica un modelo de servicio múltiple que cumple con muchas de las solicitudes de calidad de servicio en Internet.

- **IPSEC**: IP Security. Es un estándar para redes de paquetes que apunta a lograr conexiones seguras a través de redes IP.

- **LDAP/AD:** Lightweight Directory Access Protocol. Es un protocolo estándar para consultar y modificar servicios de directorio.

- **NBD**: Next business day, siguiente día hábil.

- **PHISHING**: Es un tipo de estafa en Internet a través de la cual un atacante intenta engañar a la víctima para que la convenza de proporcionar información personal, datos financieros o códigos de acceso, pretendiendo ser una entidad confiable en la comunicación digital.

- **RMA**: Return Merchandise Authorization. Es la reparación o reemplazo de un producto electrónico o sus partes durante el período de soporte.

- **VPN**: Virtual Private Network. Es una red de telecomunicaciones privada, establecida entre sujetos que utilizan, como tecnología de transporte, un protocolo de transmisión público y compartido, como Internet.

ANEXO 1: Protocolo de pruebas y recepción de equipos y/o componentes UDistrital

PROTOCOLO DE PRUEBAS Y RECEPCION DE EQUIPOS

RED DE DATOS UDNET

FECHA: _____

HORA: _____

RESPONSABLES: _____

ÍTEM	*MARCA*	*MÓDELO EQUIPO O COMPONENTE (REFERENCIA EXACTA)*	*NÚMERO SERIAL*	*ESTADO FÍSICO: PASA*		*ENCENDIO AUTOTEST PARA EQUIPOS : PASA*		*VERSIÓN FIRMWARE ACTUALIZADA: PASA*		*FECHA DE RECEPCION*	*OBSERVACIONES*
				SI	*NO*	*SI*	*NO*	*SI*	*NO*		
1											
2											

Para constancia firma representante de la universidad y representante del contratista

FIRMA:
NOMBRE:
CARGO:

FIRMA:
NOMBRE:
CARGO: