UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

CONTRATAR LA ADQUISICIÓN, INSTALACIÓN Y PUESTA EN CORRECTO FUNCIONAMIENTO DE UNA SOLUCIÓN DE SEGURIDAD PERIMETRAL COMPUESTA POR DOS EQUIPOS PARA GARANTIZAR LA ALTA DISPONIBILIDAD (HA) PARA LA UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS INCLUYENDO LICENCIAMIENTO, SOPORTE Y ACTUALIZACIONES (UPDATE Y UPGRADE).

TABLA DE CONTENIDO

1 OBJETO

Contratar la adquisición, instalación y puesta en correcto funcionamiento de una solución de seguridad perimetral compuesta por dos equipos para garantizar la alta disponibilidad (HA) para la Universidad Distrital Francisco José de Caldas incluyendo licenciamiento, soporte y actualizaciones (UPDATE Y UPGRADE).

2 ANTECEDENTES

La Universidad Distrital Francisco José de Caldas actualmente cuenta con un sistema de seguridad perimetral de tecnología NextGeneration Firewall de marca PaloAlto® y referencia PAN 3260, el cual fue adquirido en la convocatoria pública 013 de 2018 mediante el contrato N° 1635 de 2018.

Este sistema de seguridad perimetral, actualmente maneja las siguientes utilidades o controles de seguridad: Sistema de detección de intrusos, Antivirus, filtrado de contenido, protección por geolocalización, fácil visualización del tráfico de la red, protección de vulnerabilidades, permite establecer las VPN (conexiones privadas a través de la red) Ipsec y SSL, IPS (Intrusión Prevención System), prevención contra amenazas de spyware y malware y bloqueo con reglas de puertos y direcciones IP.

El servicio de licenciamiento, garantía y soporte se adquirió inicialmente por un periodo de 3 años, el cual caducó el día 22 de enero de 2022, sin embargo, se han realizado las siguientes renovaciones:

Proceso	Estado	Tiempo de licenciamiento	Fecha de finalización
Renovación	Finalizado	6 meses	21 de Julio de 2022
Renovación	Finalizado	1 año	23 de octubre del 2023
Renovación	Finalizado	1 año	23 de octubre del 2024
Renovación	Activo	1 año	04 de enero del 2026

Tabla 1. Listado de renovaciones

Durante este tiempo, el sistema de seguridad (firewall) ha protegido la red perimetral de la Universidad, previniendo ataques informáticos externos a la universidad.

3 ALCANCE

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

- Entregar una solución de seguridad perimetral compuesta por dos equipos para garantizar la alta disponibilidad (HA), esta debe incluir todo el hardware, software, cables, accesorios y demás elementos necesarios para su correcta instalación y puesta en funcionamiento.
- La solución de seguridad perimetral compuesta por dos equipos para garantizar la alta disponibilidad (HA) debe ser instalada, configurada, probada y puesta en correcto funcionamiento

según las especificaciones técnicas definidas por la Universidad Distrital en el presente documento.

- Entregar el licenciamiento de Filtrado de URL para Dispositivos en HA, prevención de amenazas para dispositivos en HA, motor de análisis sandboxing y DNS Security para dispositivos en alta disponibilidad HA que administra la Red de Datos UDNET.
- Prestar el servicio de soporte de Partner en esquema 7x24 por un (1) año para toda la solución de seguridad perimetral HA incluyendo actualizaciones (update y upgrade).

4 CONDICIONES GENERALES

A continuación, se presentan las condiciones generales:

4.1 El proponente, con la presentación de 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.

4.2 El proponente debe cumplir con las obligaciones, términos y condiciones establecidas en el presente proceso incluyendo sus anexos y atender las instrucciones que el supervisor realice durante su ejecución.

4.3 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 revisaran entre las partes para aprobación por parte de la Universidad.

4.4 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.

4.5 El plazo para la ejecución del contrato será de seis (06) meses, para la entrega, instalación y puesta en correcto funcionamiento de la solución de seguridad perimetral, el licenciamiento de la solución, el soporte de fábrica y la garantía deben tener vigencia de un año a partir de la puesta en correcto funcionamiento y recibo a satisfacción por parte de la supervisión. Se considerar que el licenciamiento actual vence el día 04 de enero de 2026, es decir, la activación del licenciamiento y soporte debe empezar el 05 de enero del 2026.

4.6 Las partes deberán suscribir un cronograma de trabajo para garantizar el cumplimiento de las obligaciones estipuladas, acorde a la necesidad de la Universidad y la fecha de finalización de las licencias actuales. El cronograma hará parte del acta de inicio.

4.7 El contratista deberá suministrar los equipos solicitados y realizar los procesos de instalación, configuración, migración, puesta en funcionamiento y activación del licenciamiento de la solución de seguridad perimetral compuesta por dos equipos para garantizar la alta disponibilidad (HA).

4.8 El contratista debe entregar en medio físico y/o electrónico la certificación del fabricante, en la que conste la adquisición de los equipos a instalar con su respectivo serial y el licenciamiento a nombre de la Universidad Distrital Francisco José de Caldas por el periodo de un (1) año.

4.9 El contratista, en conjunto con el equipo técnico de la Red de Datos UDNET, deberá realizar la revisión y depuración de las configuraciones de la solución de seguridad perimetral Palo Alto® 3260, antes de realizar la migración de la configuración a la nueva solución de seguridad perimetral y se debe adjuntar el respectivo informe. Adicionalmente se debe tener en cuenta que las configuraciones sean totalmente compatibles con la nueva solución antes de realizar el proceso de migración.

4.10 El contratista debe realizar el proceso de migración de la configuración del sistema de seguridad perimetral actual al sistema de seguridad perimetral adquirido. Adicionalmente, deberá realizar nuevas configuraciones que sean necesarias de acuerdo a la necesidad de la Universidad.

4.11 El contratista debe brindar soporte presencial, remoto y/o telefónico en esquema 7x24 (es decir, siete (7) días a la semana, veinticuatro (24) horas al día por la vigencia de las licencias y soporte a adquirir).

4.12 El contratista se compromete a prestar los servicios de soporte y acompañamiento para cualquier cambio de configuración que se requiera durante el término de vigencia de la renovación y actualización del licenciamiento. El tiempo de atención de la incidencia presentada, no puede superar las 8 horas.

4.13 El contratista debe brindar asesoría y soporte técnico a la Universidad en la implementación y configuración de políticas de seguridad y nuevas versiones del software y funcionalidades si hay lugar a ello.

4.14 El contratista debe garantizar el soporte técnico durante la vigencia de los licenciamientos, encaminado a garantizar una adecuada operación de los productos adquiridos, de conformidad con las especificaciones técnicas.

4.15 El contratista debe garantizar el correcto funcionamiento de cada uno de los componentes de la solución de seguridad perimetral compuesta por dos equipos para garantizar la alta disponibilidad (HA) después de realizar cualquier actividad de instalación, configuración, atención de incidentes, actualización y/o soporte.

4.16 El contratista debe brindar el acceso a informes sobre buenas prácticas y postura de seguridad informática asociada a la solución de seguridad perimetral compuesta por dos equipos para garantizar la alta disponibilidad (HA) adquirida.

4.17 El contratista deberá ejecutar una evaluación de buenas prácticas de forma periódica por lo menos dos veces durante la vigencia del licenciamiento, con el objetivo de proporcionar un servicio de mejora continua sobre las configuraciones la solución de seguridad perimetral compuesta por dos equipos para garantizar la alta disponibilidad (HA). Dichas configuraciones serán revisadas por los administradores de la solución y el contratista deberá entregar el informe respectivo.

4.18 El contratista 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 o charlas para fomentar a la comunidad universitaria una cultura de seguridad

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

4.19 El contratista debe realizar jornadas de transferencia de conocimiento de mínimo 8 horas sobre la administración de la solución de seguridad perimetral y nuevas características dirigidas al personal técnico de la Universidad Distrital Francisco José de Caldas que realizará la administración de la solución de seguridad perimetral compuesta por dos equipos para garantizar la alta disponibilidad (HA). Los temas y cronograma se coordinarán con el supervisor y personal técnico de UDNET al inicio de la ejecución del contrato.

4.20 A partir del momento que se da acceso a los centros de gestión, cuartos de telecomunicaciones y equipos de la Universidad Distrital, el contratista adquiere total responsabilidad por la integridad física y lógica de los equipos intervenidos y su entorno, comprometiéndose a realizar un manejo adecuado de los elementos intervenidos y sus componentes, evitando que se presenten situaciones de degradación en el funcionamiento o inutilizar de manera lógica o física los elementos.

4.21 El contratista debe coordinar la logística y realizar la instalación configuración y puesta en correcto funcionamiento del equipo o parte a reemplazar en caso de RMA, así mismo, la devolución del equipo o parte afectada ante el fabricante durante la vigencia de la garantía.

4.22 Todo licenciamiento, actualización, migración de la configuración y optimización del sistema debe ser realizada en alta disponibilidad (HA) durante 1 año incluyendo todas las funcionalidades descritas en este documento. Estas actividades deben ser coordinadas previamente con la supervisión del contrato.

4.23 Los elementos que se requieran reemplazar deben ser nuevos, originales y ensamblados de fábrica.

4.24 Todo traslado de equipos y elementos estará a cargo del contratista, tanto para el retiro como para la entrega en las instalaciones de la Universidad.

4.25 En caso de ser necesario el traslado del equipo o sus componentes, el desplazamiento (ida y vuelta), los costos asociados a este desplazamiento (fletes, seguros, etc.) y la responsabilidad por el equipo y/o componentes están a cargo exclusivo del contratista y en ningún caso generará costo adicional a la Universidad Distrital.

4.26 Dar estricto cumplimiento al protocolo de bioseguridad establecido en la Universidad y cumplir con el objeto del presente contrato dando un adecuado manejo de las medidas de mitigación de la transmisión en caso de pandemia o cualquier evento de salud pública.

4.27 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/)

4.28 Las demás actividades afines al objeto contractual.

5 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 no podrán ser reveladas a los concursantes ni otra persona que no participe oficialmente en dicho proceso hasta que la Universidad Distrital los publique.

6 ESPECIFICACIONES TÉCNICAS MÍNIMAS

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

La solución de seguridad perimetral compuesta por dos equipos para garantizar la alta disponibilidad (HA) a adquirir debe cumplir con las características y estándares en el mercado que hay sobre este tema. A continuación, se listan las características técnicas mínimas a cumplir:

Ítem	Característica técnica	Descripción
1	Generalidades	La solución de Seguridad Perimetral (HA) debe estar compuesto por todo el hardware, software, accesorios y licenciamiento necesarios para su funcionamiento incluyendo alta disponibilidad HA.
2	Generalidades	El sistema debe contar con una totalidad de 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 la solución de seguridad perimetral HA.
3	Generalidades	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	Generalidades	Los equipos ofrecidos deben ser adecuados para montaje en rack 19”. Cada equipo puede ocupar máximo 3 unidades de Rack.
5	Generalidades	El software del sistema deberá ser ofertado en la última versión estable y recomendada por el fabricante
6	Generalidades	El sistema debe tener la capacidad de identificar al usuario de red con integración a Microsoft Active Directory, Radius o LDAP sin la necesidad de instalación de agente en el Controlador de dominio, ni en las estaciones de los usuarios.
7	Generalidades	El fabricante de la solución ofrecida por el proponente, debe pertenecer al cuadrante de líderes de Gartner para “*Enterprise Network Firewall*” o “*Firewalls de Redes Empresariales*” o lideres en la escala The Forrester WAVE™ en los últimos 3 años.

Ítem	Característica técnica	Descripción
8	Generalidades	Los equipos deben estar certificados para IPv6 en Firewall por USGv6 o IPv6 Ready.
9	Generalidades	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.
10	Generalidades	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.
11	Generalidades	Los equipos ofertados no se encuentran en periodo de fin de venta (end-of-life), ni en fin de venta (end-of-sale) y su ciclo de vida útil no es inferior a cinco (5) años
12	Generalidades	Debe permitir el control de políticas por identificación de País.
13	Generalidades	El proveedor debe presentar certificación expedida por la casa matriz donde se indica que es canal Partner Platinum (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).
14	Generalidades	La solución ofrecida debe tener un módulo en el sistema de seguridad o en la nube que permita enriquecer la comprensión de la implementación sobre la solución de seguridad perimetral compuesta por dos equipos para garantizar la alta disponibilidad (HA) adquirida. Dentro de las características principales debe: • Evaluar la configuración del firewall e identificar áreas de mejora (políticas de seguridad). • Proporcionar un acceso fácil a los datos de telemetría históricos y en tiempo real del firewall. • Detectar problemas del sistema, estado de salud del firewall. • Contemplar la adopción de buenas prácticas en materia de configuración de los diferentes módulos de seguridad de la solución, como mínimo estos: Control de Aplicaciones, Antivirus/Antimalware, Antispyware/Antibot, IPS, Sandboxing, Filtro Web, Gestión de Logs.
15	Alta disponibilidad (HA)	Soporta configuración de alta disponibilidad (HA) en los modos Activo/Pasivo y Activo/Activo en modo transparente y en Layer 3.
16	Alta disponibilidad (HA)	El modo HA (modo de Alta-Disponibilidad) debe permitir monitoreo de fallo de link.
17	Alta disponibilidad (HA)	El modo de alta disponibilidad debe contar con detección de fallas, en donde se visualice las posibles caídas y como solucionarlas.

Ítem	Característica técnica	Descripción
18	Capacidades y cantidades	El equipo Next Generation Firewall (NGFW) debe estar en la capacidad de identificar y procesar el tráfico en su totalidad inspeccionado en capa 7 de aplicación.
19	Capacidades y cantidades	Throughput de Next Generation Firewall (NGFW) de 18 Gbps medido con tráfico productivo real.
20	Capacidades y cantidades	Throughput de Prevención de Amenazas o Threat Prevention Throughput de 10 Gbps medido con tráfico productivo real, con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, control de amenazas avanzadas de día cero (Sandboxing), DNS Security, Filtro de Archivos, y Logging activo.
21	Capacidades y cantidades	Cada equipo debe tener la Capacidad de procesar mínimo 2.2 millones de conexiones de red simultáneas (concurrentes)
22	Capacidades y cantidades	Cada equipo debe tener la Capacidad de procesar mínimo 200.000 nuevas conexiones en red por segundo.
23	Capacidades y cantidades	Cada equipo debe contar con dos fuentes en el rango de 110v-220v AC hot-swappable ofreciendo redundancia en el suministro eléctrico.
24	Capacidades y cantidades	Cada equipo debe incluir Disco de Estado Sólido (SSD) de mínimo 450 GB para almacenamiento del sistema y logs.
25	Capacidades y cantidades	**Puertos de cobre:** Mínimo 8 Interfaces (1G/10G) RJ45 o (1G/10G) SFP+ de tráfico de red para cada equipo. (No debe incluir interfaces para alta disponibilidad, ni administración). **Nota:** En tal caso de que se dé cumplimiento incluyendo un módulo (1G/10G) SFP+, debe incluir como mínimo 4 optical transceiver SFP+ 10G Base-T RJ45 compatibles con el módulo.
26	Capacidades y cantidades	**Puertos de fibra**: Mínimo 8 Interfaces 10Gbps SFP/SFP+ de tráfico de red para cada equipo (No debe incluir interfaces para alta disponibilidad, ni administración) incluyendo Mínimo 4 optical transceiver SFP+ 10-Gigabit multi-mode. **Nota:** Se debe tener en cuenta que dichas interfaces no deben ser las mismas requeridas para el punto 25.
27	Capacidades y cantidades	Mínimo 1 Interfaz adicional para alta disponibilidad mínimo a 1Gbps (No deben estar incluidas en las interfaces para tráfico de Red, ni administración)
28	Capacidades y cantidades	Interfaz dedicada para administración 10/100/1000 para cada equipo
29	Capacidades y cantidades	1 interfaz de tipo consola

Ítem	Característica técnica	Descripción
30	Capacidades y cantidades	Capacidad de mínimo 60 zonas de seguridad.
31	Servicios y protocolos de red	Etiquetas VLAN Tags 802.1Q por dispositivo / interfaz: 4094/4094
32	Servicios y protocolos de red	Soporte de Agregación de links (LACP) 802.3ad
33	Servicios y protocolos de red	Debe soportar enrutamiento estático y dinámico (RIP, BGP y OSPFv2/v3) Para IPv4
34	Servicios y protocolos de red	Debe soportar enrutamiento estático y dinámico (OSPFv3) Para IPv6
35	Servicios y protocolos de red	Capacidad de balancear varios enlaces de internet sin el uso de políticas específicas.
36	Servicios y protocolos de red	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.
37	Servicios y protocolos de red	Debe contar con modos NAT IPv4: IP estática, IP dinámica, IP y puerto dinámicos
38	Servicios y protocolos de red	Los NAT debe permitir reserva de IP dinámica, IP y puerto dinámicos con túnel y sobresuscripción.
39	Control por política de firewall (aplicaciones, puertos y protocolos)	Soportar controles por zona de seguridad.
40	Control por política de firewall (aplicaciones, puertos y protocolos)	Controles de políticas por puerto y protocolo.
41	Control por política de firewall (aplicaciones,	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.

Ítem	Característica técnica	Descripción
	puertos y protocolos)	
42	Control por política de firewall (aplicaciones, puertos y protocolos)	Identificación de la información de todas las aplicaciones que circulan por la red, en donde se evidencie puertos, protocolos, técnicas de evasión o cifrado.
43	Control por política de firewall (aplicaciones, puertos y protocolos)	Las políticas por aplicaciones deben contar con la capacidad de permitir, denegar, inspeccionar y tener control sobre el tráfico de las aplicaciones.
44	Control por política de firewall (aplicaciones, puertos y protocolos)	Etiquetado de aplicaciones por riesgo con el fin de identificar con mayor facilidad.
45	Control por política de firewall (aplicaciones, puertos y protocolos)	Soportar objetos y Reglas multicast.
46	Control por política de firewall (aplicaciones, puertos y protocolos)	Soportar los atributos de agendamiento de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.
47	Control por política de firewall (aplicaciones, puertos y protocolos)	Debe contener aprendizaje automático, con el fin de identificar y detener los intentos de ataques informáticos de día cero.

Ítem	Característica técnica	Descripción
48	Control por política de firewall (aplicaciones, puertos y protocolos)	Debe contar con la funcionalidad de dar recomendaciones en las políticas creadas basado en buenas prácticas.
49	Control por política de firewall (aplicaciones, puertos y protocolos)	Control de políticas por usuarios, grupos de usuarios, IPs, redes y zonas de seguridad.
50	Control por política de firewall (aplicaciones, puertos y protocolos)	El sistema deberá tener la capacidad de reconocer aplicaciones, independiente del puerto y protocolo.
51	Control por política de firewall (aplicaciones, puertos y protocolos)	Debe ser posible la liberación y bloqueo solamente de aplicaciones sin la necesidad de liberación de puertos y protocolos.
52	Control por política de firewall (aplicaciones, puertos y protocolos)	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.
53	Control por política de firewall (aplicaciones, puertos y protocolos)	Para mantener la seguridad de la red, debe soportar el control sobre aplicaciones desconocidas y no solamente sobre aplicaciones conocidas.
54	Control por política de firewall	Permitir la restricción de usuarios sospechosos o malintencionados basado en comportamientos.

Ítem	Característica técnica	Descripción
	(aplicaciones, puertos y protocolos)	
55	Prevención de amenazas	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.
56	Prevención de amenazas	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.
57	Prevención de amenazas	Debe incluir seguridad contra ataques de denegación de servicios.
58	Prevención de amenazas	Debe permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, FTP, DNS, SMB, SMTP e POP3.
59	Prevención de amenazas	Soportar bloqueo de archivos por tipo.
60	Prevención de amenazas	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.
61	Prevención de amenazas	Debe ofrecer funcionalidades para análisis de Malware no conocidos incluidas en la propia herramienta.
62	Prevención de amenazas	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.
63	Prevención de amenazas	Debe detener los ataques de inyección de día cero, exploits, botnets y Ataques Persistentes Avanzados (APT).
64	Prevención de amenazas	Las detenciones que realice el sistema deben estar basadas en comportamiento y IA.
65	Prevención de amenazas	Debe utilizar una red de Inteligencia Global que le permita beneficiarse de la información recogida por los esfuerzos de investigación del fabricante.
66	Prevención de amenazas	Debe tener la capacidad de detectar software malicioso y tomar acciones para proteger el entorno.
67	Prevención de amenazas	Debe detectar y proteger de los ataques originarios desde la web, como por ejemplo la descarga de archivos comprometedores y ejecución de los mismo.
68	Prevención de amenazas	Debe contar con un entorno de inspección de códigos, sitios web o archivos maliciosos.

Ítem	Característica técnica	Descripción
69	Prevención de amenazas	El sistema debe estar en la capacidad de bloquear llamadas a servidores remotos en caso de ataques de día cero y amenazas persistentes. Con el fin de proteger los equipos que se pudiesen comprometer y realicen llamadas a servidores remotos desde la red de la Universidad.
70	Prevención de amenazas	Debe contar con la protección a través de la resolución de direcciones DNS. Con el fin de identificar dominios maliciosos
71	Prevención de amenazas	Los eventos generados deben contener la posibilidad de conocer el país de origen y destino, IP de origen y destino, URL, usuario que lo ejecuto y demás información relevante para su identificación.
72	Filtrado URL	Debe ser posible crear políticas por usuario, grupo de usuario, IPs, redes y zonas de seguridad.
73	Filtrado URL	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.
74	Filtrado URL	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría URL.
75	Filtrado URL	Debe permitir al menos 60 categorías predefinidas de URLs, con la capacidad de crear categorías adicionales personalizadas, de acuerdo con las necesidades específicas de la entidad.
76	Filtrado URL	Debe soportar la creación de categorías URL custom.
77	Filtrado URL	Debe soportar la exclusión de URLs del bloqueo por categoría.
78	Filtrado URL	Las detenciones que realice la solución deben estar basadas en comportamiento y IA.
79	Filtrado URL	Debe contar con un sistema de inteligencia de amenazas para validar la reputación de las URLs e IPs solicitadas por los usuarios en la navegación.
80	Filtrado URL	Debe permitir la creación de listas blancas y negras con el fin de agrupar URL, según de la necesidad de la Universidad
81	Filtrado URL	Debe tener una base de datos de al menos 200 millones de URLs categorizadas o debe tener la capacidad de poder aplicar técnicas de aprendizaje de maquina (Machine Learning) localmente sobre los NGFW para poder identificar nuevas categorías, por ejemplo, sitios de phishing o malware, con la capacidad de poder bloquear los mismos.
82	Filtrado de datos	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 vía expresión regular.

Ítem	Característica técnica	Descripción
83	Filtrado de datos	Permitir la detección de portales de phishing estableciendo políticas que eviten el envío de credenciales válidas de usuarios a sitios no autorizados.
84	Filtrado de datos	Con el fin de proteger las credenciales de la comunidad Universitaria, debe evitar la filtración a sitios web de terceros y la reutilización de credenciales sustraídas mediante la habilitación de la autenticación de varios factores.
85	Identificación de usuarios	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.
86	Identificación de usuarios	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.
87	Identificación de usuarios	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.
88	Identificación de usuarios	Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en servidores accedidos remotamente, incluso que no sean servidores Windows.
89	Calidad de servicio	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.
90	Calidad de servicio	Las VPN deberán estar en la capacidad o tener disponible en futuras actualizaciones la capacidad de configurar PPK poscuánticas en IKEv2, basadas en el estándar RFC 8784 o en el presente a través de la actualización de certificados a una longitud de 4096 bits RSA, tal como lo sugiere el NIST.
91	Calidad de servicio	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
92	Calidad de servicio	El QoS debe permitir la definición de clases por: • Ancho de banda garantizado • Ancho de banda máxima • Cola de prioridad.

Ítem	Característica técnica	Descripción
93	Calidad de servicio	Soportar priorización RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.
94	Calidad de servicio	Soportar marcación de paquetes de servicios diferenciados (Diffserv)
95	VPN embebida	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)
96	VPN embebida	La VPN IPSEc debe soportar mínimo: • Cifrado 3DES • Cifrado AES (128 bits, 256 bits) • Autenticación: MD5, SHA-1, SHA-256, SHA-384, SHA-512 • Intercambio de calves: clave manual, IKEv1 e IKEv2 • Autenticación vía certificado IKE PKI.
97	VPN embebida	Debe poseer interoperabilidad VPN IPSec mínimo con los siguientes fabricantes: Cisco, Checkpoint, Juniper, Palo Alto Networks, Fortinet, Sonic Wall.
98	VPN embebida	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.
99	VPN embebida	Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.
100	VPN embebida	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
101	VPN embebida	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
102	VPN embebida	El cliente de VPN client-to-site debe ser compatible al menos con: Windows 8, Windows 10, Windows 11 y últimas versiones de Mac.
103	VPN embebida	Capacidad de soportar mínimo 1800 clientes de VPN SSL (Client) simultáneos sin generar costos adicionales a la solución de seguridad perimetral. La VPN SSL deberá permitir mínimo la creación del túnel seguro y la conexión entre la red corporativa y el endpoint del usuario sin implementar características de cumplimiento o postura.
104	VPN embebida	Capacidad de soportar mínimo 1000 túneles de VPN IPSEC (Site to Site) simultáneos sin generar costos adicionales a la solución de seguridad perimetral. La VPN IPSEC deberá permitir mínimo la creación del tunel seguro y la conexión entre las redes corporativas sin implementar características de cumplimiento o postura.

Ítem	Característica técnica	Descripción
105	VPN embebida	Throughput de VPN de mínimo 9 Gbps IPsec.
106	DNS Security	La solución compuesta por dos equipos para garantizar la alta disponibilidad (HA), debe ser alimentada por un servicio de inteligencia global capaz de identificar millones de dominios maliciosos con análisis en tiempo real sin depender de firmas estáticas.
107	DNS Security	El servicio de protección de DNS debe poder habilitarse sin modificar la configuración de DNS de la red local o desviar el tráfico DNS a servidores externos.
108	DNS Security	La solución compuesta por dos equipos para garantizar la alta disponibilidad (HA), debe ser un servicio que funcione integrado en la plataforma de NGFW, sin requerir adicionar hardware adicional y sin impactar el rendimiento del NGFW.
109	DNS Security	El servicio de protección de DNS debe alimentarse de múltiples fuentes de inteligencia de amenazas actualizadas en tiempo real, incluyendo telemetría de comportamiento de usuarios o dispositivos, y/o información proveniente de fuentes externas confiables y reconocidas internacionalmente
110	DNS Security	La solución compuesta por dos equipos para garantizar la alta disponibilidad (HA), debe ser capaz de predecir y detener dominios maliciosos de malware basados en algoritmos de generación de dominio (DGA).
111	DNS Security	Debe utilizar machine learning y/o inteligencia artificial para detectar nuevos dominios nunca vistos autogenerados por algoritmos DGA
112	DNS Security	Debe poseer políticas para bloquear dominios DGA o interrumpir las consultar de DNS a dichos dominios.
113	DNS Security	Debe detectar e interrumpir robo de datos ocultos o tunelizados en tráfico DNS.
114	DNS Security	Debe analizar las consultas de DNS, incluyendo las tasas de consultas y patrones, entropía y frecuencia de n-grams o DGA Bajo Machine Learning / Artificial Intelligence para detectar posibles intentos de tunelización.
115	DNS Security	Debe permitir como acción ante peticiones DNS maliciosas: alertar, bloquear las conexiones y además responder a la petición con IP sumidero (sinkhole) con el fin de identificar al usuario/equipo realizando consultas DNS maliciosas.
116	DNS Security	Debe clasificar los dominios maliciosos en categorías específicas asociadas al tipo de riesgo, como, por ejemplo: malware, DGA, DNS tunneling, Comando y Control, DNS dinámicos, phising o dominios recientemente registrados.
117	DNS Security	Debe perimir la acción a tomar dependiendo de la categoría a la que pertenezca el dominio, pudiendo tomar acciones diferentes para cada tipo de categoría.
118	DNS Security	La solución compuesta por dos equipos para garantizar la alta disponibilidad (HA), debe brindar el contexto de cada dominio incluyendo historial completo para informar el origen y reputación de cada dominio.

Ítem	Característica técnica	Descripción
119	Consola de administración y monitoreo	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
120	Consola de administración y monitoreo	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.
121	Consola de administración y monitoreo	La administración del sistema debe soportar acceso vía SSH, cliente WEB (HTTPS) y API abierta
122	Consola de administración y monitoreo	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.
123	Consola de administración y monitoreo	Debe permitir la validación de las políticas, avisando cuando haya reglas que ofusquen o tengan conflicto con otras (shadowing)
124	Consola de administración y monitoreo	Debe posibilitar la visualización y comparación de configuraciones actuales, la configuración anterior y configuraciones más antiguas (Control de versiones).
125	Consola de administración y monitoreo	Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizó, IP de acceso, el horario del cambio, entre otros.
126	Consola de administración y monitoreo	Debe permitir la generación de mapas geográficos en tiempo real para la visualización de orígenes y destinos del tráfico generado en la Universidad.
127	Consola de administración y monitoreo	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.
128	Consola de administración y monitoreo	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.

Ítem	Característica técnica	Descripción
129	Consola de administración y monitoreo	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 mostrar la versión actual del sistema y componentes. • 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.
130	Reportes	Informe de uso de aplicaciones por usuario o por grupo de usuario.
131	Reportes	Informes de actividad de usuario o grupo de usuarios, en donde se evidencie sitios visitados junto el tiempo de navegación.
132	Reportes	Informes por categorías, como, por ejemplo: Trafico, Amenazas, Filtrado red, amenazas y tendencias.
133	Reportes	El Dashboard deben contener reportería con marcaciones de tendencia, es decir, información relevante que ayude a identificar comportamientos en la red.

Tabla 2 - Características mínimas de carácter obligatorio

7 CRONOGRAMA

El contratista presentará el cronograma a seguir durante la ejecución del contrato, el cual debe ser verificado y aprobado por parte de la universidad, con la asesoría de la Red de Datos UDNET. Dicho documento se coordinará una vez se firme el acta de inicio y debe incluir la entrega del licenciamiento de los componentes, recursos a utilizar y actividades que se ejecutarán para dar cumplimiento al contrato.

8 LICENCIAMIENTO Y SOPORTE

El licenciamiento y servicio de soporte de toda la solución de seguridad perimetral compuesta por dos equipos para garantizar la alta disponibilidad (HA), será **por un (1) año a partir del siguiente día de la fecha de finalización del licenciamiento actual.** El contratista debe garantizar que para esta fecha ya se haya realizado la instalación, migración y pruebas de funcionamiento de los equipos adquiridos.

El servicio de soporte debe ser en esquema 7x24: siete (7) días a la semana, veinticuatro (24) horas al día. 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 nuevas funcionalidades, que se generen durante el periodo de licenciamiento.

El proveedor debe otorgar el soporte técnico de todos los componentes del sistema, incluyendo solución a problemas con la instalación de todos los componentes técnicos descritos en el presente documento, durante el tiempo del licenciamiento, asegurando que este servicio se preste en sitio, remoto, telefónico o correo electrónico, con personal certificado en el software.

El soporté técnico incluirá la actualización permanente de las herramientas y elementos que componen la solución, 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.

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). Una vez terminado el proceso de RMA, el contratista debe garantizar el correcto funcionamiento de la solución del sistema de seguridad perimetral compuesta por dos equipos para garantizar la alta disponibilidad (HA),.

9 DOCUMENTACIÓN DE CARÁCTER TÉCNICO

Documentación que debe entregarse con la propuesta:

a. El proponente debe adjuntar una certificación vigente, suscrita directamente por el fabricante donde conste que este certificado para brindar servicios y distribución autorizada, el cual debe estar vigente durante la validez de la propuesta, de igual manera durante el tiempo del licenciamiento.
b. Documento corporativo de fabrica en donde se encuentra la descripción detallada de las características de los equipos adquiridos y del licenciamiento aquí solicitado, en español o inglés.
c. El proponente debe adjuntar una certificación vigente, suscrita directamente por el fabricante, en la cual conste que otorgará garantía durante el término que se encuentren vigente el licenciamiento.
d. El proponente debe presentar certificación expedida por la casa matriz y dirigida a la Universidad donde se indica que es canal Partner Platinum (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).
e. El proponente deberá presentar certificación expedida por el fabricante de la marca ofertada, indicando que los equipos y componentes ofertados no se encuentran en periodo de fin de venta, y que mínimo tienen un ciclo de vida útil no inferior a cinco (5) años.

f. Anexos de los estudios previos

NOTA: No se aceptan auto certificaciones o auto facturas.

10 EVALUACIÓN TÉCNICA DE LAS PROPUESTAS

Se llevará a cabo por parte de la Unidad de 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 TÉCNICAMENTE" O "NO CUMPLE TÉCNICAMENTE".

Los criterios por evaluar serán los siguientes:

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
1	Generalidades	La solución de Seguridad Perimetral (HA) debe estar compuesto por todo el hardware, software, accesorios y licenciamiento necesarios para su funcionamiento incluyendo alta disponibilidad HA.		
2	Generalidades	El sistema debe contar con una totalidad de 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 la solución de seguridad perimetral HA.		
3	Generalidades	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		

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
4	Generalidades	Los equipos ofrecidos deben ser adecuados para montaje en rack 19". Cada equipo puede ocupar máximo 3 unidades de Rack.		
5	Generalidades	El software del sistema deberá ser ofertado en la última versión estable y recomendada por el fabricante		
6	Generalidades	El sistema debe tener la capacidad de identificar al usuario de red con integración a Microsoft Active Directory, Radius o LDAP sin la necesidad de instalación de agente en el Controlador de dominio, ni en las estaciones de los usuarios.		
7	Generalidades	El fabricante de la solución ofrecida por el proponente, debe pertenecer al cuadrante de líderes de Gartner para "*Enterprise Network Firewall*" o "*Firewalls de Redes Empresariales*" o lideres en la escala The Forrester WAVE™ en los últimos 3 años.		
8	Generalidades	Los equipos deben estar certificados para IPv6 en Firewall por USGv6 o IPv6 Ready.		
9	Generalidades	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.		
10	Generalidades	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.		
11	Generalidades	Los equipos ofertados no se encuentran en periodo de fin de venta (end-of-life), ni en fin de venta (end-of-sale) y su ciclo de vida útil no es inferior a cinco (5) años		

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
12	Generalidades	Debe permitir el control de políticas por identificación de País.		
13	Generalidades	El proveedor debe presentar certificación expedida por la casa matriz donde se indica que es canal Partner Platinum (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).		
14	Generalidades	La solución ofrecida debe tener un módulo en el sistema de seguridad o en la nube que permita enriquecer la comprensión de la implementación sobre la solución de seguridad perimetral compuesta por dos equipos para garantizar la alta disponibilidad (HA) adquirida. Dentro de las características principales debe: • Evaluar la configuración del firewall e identificar áreas de mejora (políticas de seguridad). • Proporcionar un acceso fácil a los datos de telemetría históricos y en tiempo real del firewall. • Detectar problemas del sistema, estado de salud del firewall. • Contemplar la adopción de buenas prácticas en materia de configuración de los diferentes módulos de seguridad de la solución, como mínimo estos: Control de Aplicaciones, Antivirus/Antimalware, Antispyware/Antibot, IPS, Sandboxing, Filtro Web, Gestión de Logs.		

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
15	Alta disponibilidad (HA)	Soporta configuración de alta disponibilidad (HA) en los modos Activo/Pasivo y Activo/Activo en modo transparente y en Layer 3.		
16	Alta disponibilidad (HA)	El modo HA (modo de Alta-Disponibilidad) debe permitir monitoreo de fallo de link.		
17	Alta disponibilidad (HA)	El modo de alta disponibilidad debe contar con detección de fallas, en donde se visualice las posibles caídas y como solucionarlas.		
18	Capacidades y cantidades	El equipo Next Generation Firewall (NGFW) debe estar en la capacidad de identificar y procesar el tráfico en su totalidad inspeccionado en capa 7 de aplicación.		
19	Capacidades y cantidades	Throughput de Next Generation Firewall (NGFW) de 18 Gbps medido con tráfico productivo real.		
20	Capacidades y cantidades	Throughput de Prevención de Amenazas o Threat Prevention Throughput de 10 Gbps medido con tráfico productivo real, con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, control de amenazas avanzadas de día cero (Sandboxing), DNS Security, Filtro de Archivos, y Logging activo.		
21	Capacidades y cantidades	Cada equipo debe tener la Capacidad de procesar mínimo 2.2 millones de conexiones de red simultáneas (concurrentes)		
22	Capacidades y cantidades	Cada equipo debe tener la Capacidad de procesar mínimo 200.000 nuevas conexiones en red por segundo.		

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
23	Capacidades y cantidades	Cada equipo debe contar con dos fuentes en el rango de 110v-220v AC hot-swappable ofreciendo redundancia en el suministro eléctrico		
24	Capacidades y cantidades	Cada equipo debe incluir Disco de Estado Sólido (SSD) de mínimo 450 GB para almacenamiento del sistema y logs.		
25	Capacidades y cantidades	**Puertos de cobre:** Mínimo 8 Interfaces (1G/10G) RJ45 o (1G/10G) SFP+ de tráfico de red para cada equipo. (No debe incluir interfaces para alta disponibilidad, ni administración). **Nota:** En tal caso de que se dé cumplimiento incluyendo un módulo (1G/10G) SFP+, debe incluir como mínimo 4 optical transceiver SFP+ 10G Base-T RJ45 compatibles con el módulo.		
26	Capacidades y cantidades	**Puertos de fibra**: Mínimo 8 Interfaces 10Gbps SFP/SFP+ de tráfico de red para cada equipo (No debe incluir interfaces para alta disponibilidad, ni administración) incluyendo Mínimo 4 optical transceiver SFP+ 10-Gigabit multi-mode. **Nota:** Se debe tener en cuenta que dichas interfaces no deben ser las mismas requeridas para el punto 25.		
27	Capacidades y cantidades	Mínimo 1 Interfaz adicional para alta disponibilidad mínimo a 1Gbps (No deben estar incluidas en las interfaces para tráfico de Red, ni administración)		
28	Capacidades y cantidades	Interfaz dedicada para administración 10/100/1000 para cada equipo		
29	Capacidades y cantidades	1 interfaz de tipo consola		

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
30	Capacidades y cantidades	Capacidad de mínimo 60 zonas de seguridad.		
31	Servicios y protocolos de red	Etiquetas VLAN Tags 802.1Q por dispositivo / interfaz: 4094/4094		
32	Servicios y protocolos de red	Soporte de Agregación de links (LACP) 802.3ad		
33	Servicios y protocolos de red	Debe soportar enrutamiento estático y dinámico (RIP, BGP y OSPFv2/v3) Para IPv4		
34	Servicios y protocolos de red	Debe soportar enrutamiento estático y dinámico (OSPFv3) Para IPv6		
35	Servicios y protocolos de red	Capacidad de balancear varios enlaces de internet sin el uso de políticas específicas.		
36	Servicios y protocolos de red	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.		
37	Servicios y protocolos de red	Debe contar con modos NAT IPv4: IP estática, IP dinámica, IP y puerto dinámicos		
38	Servicios y protocolos de red	Los NAT debe permitir reserva de IP dinámica, IP y puerto dinámicos con túnel y sobresuscripción.		
39	Control por política de firewall	Soportar controles por zona de seguridad.		

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
	(aplicaciones, puertos y protocolos)			
40	Control por política de firewall (aplicaciones, puertos y protocolos)	Controles de políticas por puerto y protocolo.		
41	Control por política de firewall (aplicaciones, puertos y protocolos)	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.		
42	Control por política de firewall (aplicaciones, puertos y protocolos)	Identificación de la información de todas las aplicaciones que circulan por la red, en donde se evidencie puertos, protocolos, técnicas de evasión o cifrado.		
43	Control por política de firewall (aplicaciones, puertos y protocolos)	Las políticas por aplicaciones deben contar con la capacidad de permitir, denegar, inspeccionar y tener control sobre el tráfico de las aplicaciones.		
44	Control por política de firewall (aplicaciones, puertos y protocolos)	Etiquetado de aplicaciones por riesgo con el fin de identificar con mayor facilidad.		
45	Control por política de firewall	Soportar objetos y Reglas multicast.		

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
	(aplicaciones, puertos y protocolos)			
46	Control por política de firewall (aplicaciones, puertos y protocolos)	Soportar los atributos de agendamiento de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.		
47	Control por política de firewall (aplicaciones, puertos y protocolos)	Debe contener aprendizaje automático, con el fin de identificar y detener los intentos de ataques informáticos de día cero.		
48	Control por política de firewall (aplicaciones, puertos y protocolos)	Debe contar con la funcionalidad de dar recomendaciones en las políticas creadas basado en buenas prácticas.		
49	Control por política de firewall (aplicaciones, puertos y protocolos)	Control de políticas por usuarios, grupos de usuarios, IPs, redes y zonas de seguridad.		
50	Control por política de firewall (aplicaciones, puertos y protocolos)	El sistema deberá tener la capacidad de reconocer aplicaciones, independiente del puerto y protocolo.		
51	Control por política de firewall	Debe ser posible la liberación y bloqueo solamente de aplicaciones sin la necesidad de liberación de puertos y protocolos.		

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
	(aplicaciones, puertos y protocolos)			
52	Control por política de firewall (aplicaciones, puertos y protocolos)	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.		
53	Control por política de firewall (aplicaciones, puertos y protocolos)	Para mantener la seguridad de la red, debe soportar el control sobre aplicaciones desconocidas y no solamente sobre aplicaciones conocidas.		
54	Control por política de firewall (aplicaciones, puertos y protocolos)	Permitir la restricción de usuarios sospechosos o malintencionados basado en comportamientos.		
55	Prevención de amenazas	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.		
56	Prevención de amenazas	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.		
57	Prevención de amenazas	Debe incluir seguridad contra ataques de denegación de servicios.		

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
58	Prevención de amenazas	Debe permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, FTP, DNS, SMB, SMTP e POP3.		
59	Prevención de amenazas	Soportar bloqueo de archivos por tipo.		
60	Prevención de amenazas	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.		
61	Prevención de amenazas	Debe ofrecer funcionalidades para análisis de Malware no conocidos incluidas en la propia herramienta.		
62	Prevención de amenazas	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.		
63	Prevención de amenazas	Debe detener los ataques de inyección de día cero, exploits, botnets y Ataques Persistentes Avanzados (APT).		
64	Prevención de amenazas	Las detenciones que realice el sistema deben estar basadas en comportamiento y IA.		
65	Prevención de amenazas	Debe utilizar una red de Inteligencia Global que le permita beneficiarse de la información recogida por los esfuerzos de investigación del fabricante.		
66	Prevención de amenazas	Debe tener la capacidad de detectar software malicioso y tomar acciones para proteger el entorno.		
67	Prevención de amenazas	Debe detectar y proteger de los ataques originarios desde la web, como por ejemplo		

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
		la descarga de archivos comprometedores y ejecución de los mismo.		
68	Prevención de amenazas	Debe contar con un entorno de inspección de códigos, sitios web o archivos maliciosos.		
69	Prevención de amenazas	El sistema debe estar en la capacidad de bloquear llamadas a servidores remotos en caso de ataques de día cero y amenazas persistentes. Con el fin de proteger los equipos que se pudiesen comprometer y realicen llamadas a servidores remotos desde la red de la Universidad.		
70	Prevención de amenazas	Debe contar con la protección a través de la resolución de direcciones DNS. Con el fin de identificar dominios maliciosos		
71	Prevención de amenazas	Los eventos generados deben contener la posibilidad de conocer el país de origen y destino, IP de origen y destino, URL, usuario que lo ejecuto y demás información relevante para su identificación.		
72	Filtrado URL	Debe ser posible crear políticas por usuario, grupo de usuario, IPs, redes y zonas de seguridad.		
73	Filtrado URL	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.		
74	Filtrado URL	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría URL.		
75	Filtrado URL	Debe permitir al menos 60 categorías predefinidas de URLs, con la capacidad de crear categorías adicionales personalizadas,		

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
		de acuerdo con las necesidades específicas de la entidad.		
76	Filtrado URL	Debe soportar la creación de categorías URL custom.		
77	Filtrado URL	Debe soportar la exclusión de URLs del bloqueo por categoría.		
78	Filtrado URL	Las detenciones que realice la solución deben estar basadas en comportamiento y IA.		
79	Filtrado URL	Debe contar con un sistema de inteligencia de amenazas para validar la reputación de las URLs e IPs solicitadas por los usuarios en la navegación.		
80	Filtrado URL	Debe permitir la creación de listas blancas y negras con el fin de agrupar URL, según de la necesidad de la Universidad		
81	Filtrado URL	Debe tener una base de datos de al menos 200 millones de URLs categorizadas o debe tener la capacidad de poder aplicar técnicas de aprendizaje de maquina (Machine Learning) localmente sobre los NGFW para poder identificar nuevas categorías, por ejemplo, sitios de phishing o malware, con la capacidad de poder bloquear los mismos.		
82	Filtrado de datos	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 vía expresión regular.		
83	Filtrado de datos	Permitir la detección de portales de phishing estableciendo políticas que eviten el envío de credenciales válidas de usuarios a sitios no autorizados.		

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
84	Filtrado de datos	Con el fin de proteger las credenciales de la comunidad Universitaria, debe evitar la filtración a sitios web de terceros y la reutilización de credenciales sustraídas mediante la habilitación de la autenticación de varios factores.		
85	Identificación de usuarios	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.		
86	Identificación de usuarios	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.		
87	Identificación de usuarios	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.		
88	Identificación de usuarios	Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en servidores accedidos remotamente, incluso que no sean servidores Windows.		
89	Calidad de servicio	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.		

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
90	Calidad de servicio	Las VPN deberán estar en la capacidad o tener disponible en futuras actualizaciones la capacidad de configurar PPK poscuánticas en IKEv2, basadas en el estándar RFC 8784 o en el presente a través de la actualización de certificados a una longitud de 4096 bits RSA, tal como lo sugiere el NIST.		
91	Calidad de servicio	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		
92	Calidad de servicio	El QoS debe permitir la definición de clases por: • Ancho de banda garantizado • Ancho de banda máxima • Cola de prioridad.		
93	Calidad de servicio	Soportar priorización RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.		
94	Calidad de servicio	Soportar marcación de paquetes de servicios diferenciados (Diffserv)		
95	VPN embebida	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)		
96	VPN embebida	La VPN IPSEc debe soportar mínimo: • Cifrado 3DES • Cifrado AES (128 bits, 256 bits) • Autenticación: MD5, SHA-1, SHA-256, SHA-384, SHA-512		

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
		• Intercambio de calves: clave manual, IKEv1 e IKEv2 • Autenticación vía certificado IKE PKI.		
97	VPN embebida	Debe poseer interoperabilidad VPN IPSec mínimo con los siguientes fabricantes: Cisco, Checkpoint, Juniper, Palo Alto Networks, Fortinet, Sonic Wall.		
98	VPN embebida	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.		
99	VPN embebida	Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.		
100	VPN embebida	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		
101	VPN embebida	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		
102	VPN embebida	El cliente de VPN client-to-site debe ser compatible al menos con: Windows 8, Windows 10, Windows 11 y últimas versiones de Mac.		
103	VPN embebida	Capacidad de soportar mínimo 1800 clientes de VPN SSL (Client) simultáneos sin generar costos adicionales a la solución de seguridad perimetral. La VPN SSL deberá		

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
		permitir mínimo la creación del túnel seguro y la conexión entre la red corporativa y el endpoint del usuario sin implementar características de cumplimiento o postura.		
104	VPN embebida	Capacidad de soportar mínimo 1000 túneles de VPN IPSEC (Site to Site) simultáneos sin generar costos adicionales a la solución de seguridad perimetral. La VPN IPSEC deberá permitir mínimo la creación del tunel seguro y la conexión entre las redes corporativas sin implementar características de cumplimiento o postura.		
105	VPN embebida	Throughput de VPN de mínimo 9 Gbps IPsec.		
106	DNS Security	La solución compuesta por dos equipos para garantizar la alta disponibilidad (HA), debe ser alimentada por un servicio de inteligencia global capaz de identificar millones de dominios maliciosos con análisis en tiempo real sin depender de firmas estáticas.		
107	DNS Security	El servicio de protección de DNS debe poder habilitarse sin modificar la configuración de DNS de la red local o desviar el tráfico DNS a servidores externos.		
108	DNS Security	La solución compuesta por dos equipos para garantizar la alta disponibilidad (HA), debe ser un servicio que funcione integrado en la plataforma de NGFW, sin requerir adicionar hardware adicional y sin impactar el rendimiento del NGFW.		
109	DNS Security	El servicio de protección de DNS debe alimentarse de múltiples fuentes de inteligencia de amenazas actualizadas en tiempo real, incluyendo telemetría de comportamiento de usuarios o dispositivos,		

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
		y/o información proveniente de fuentes externas confiables y reconocidas internacionalmente		
110	DNS Security	La solución compuesta por dos equipos para garantizar la alta disponibilidad (HA), debe ser capaz de predecir y detener dominios maliciosos de malware basados en algoritmos de generación de dominio (DGA).		
111	DNS Security	Debe utilizar machine learning y/o inteligencia artificial para detectar nuevos dominios nunca vistos autogenerados por algoritmos DGA		
112	DNS Security	Debe poseer políticas para bloquear dominios DGA o interrumpir las consultar de DNS a dichos dominios.		
113	DNS Security	Debe detectar e interrumpir robo de datos ocultos o tunelizados en tráfico DNS.		
114	DNS Security	Debe analizar las consultas de DNS, incluyendo las tasas de consultas y patrones, entropía y frecuencia de n-grams o DGA Bajo Machine Learning / Artificial Intelligence para detectar posibles intentos de tunelización.		
115	DNS Security	Debe permitir como acción ante peticiones DNS maliciosas: alertar, bloquear las conexiones y además responder a la petición con IP sumidero (sinkhole) con el fin de identificar al usuario/equipo realizando consultas DNS maliciosas.		
116	DNS Security	Debe clasificar los dominios maliciosos en categorías específicas asociadas al tipo de riesgo, como, por ejemplo: malware, DGA, DNS tunneling, Comando y Control, DNS dinámicos, phising o dominios recientemente registrados.		

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
117	DNS Security	Debe perimir la acción a tomar dependiendo de la categoría a la que pertenezca el dominio, pudiendo tomar acciones diferentes para cada tipo de categoría.		
118	DNS Security	La solución compuesta por dos equipos para garantizar la alta disponibilidad (HA), debe brindar el contexto de cada dominio incluyendo historial completo para informar el origen y reputación de cada dominio.		
119	Consola de administración y monitoreo	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		
120	Consola de administración y monitoreo	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.		
121	Consola de administración y monitoreo	La administración del sistema debe soportar acceso vía SSH, cliente WEB (HTTPS) y API abierta		
122	Consola de administración y monitoreo	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		

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
		• Debugging • Captura de paquetes.		
123	Consola de administración y monitoreo	Debe permitir la validación de las políticas, avisando cuando haya reglas que ofusquen o tengan conflicto con otras (shadowing)		
124	Consola de administración y monitoreo	Debe posibilitar la visualización y comparación de configuraciones actuales, la configuración anterior y configuraciones más antiguas (Control de versiones).		
125	Consola de administración y monitoreo	Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizó, IP de acceso, el horario del cambio, entre otros.		
126	Consola de administración y monitoreo	Debe permitir la generación de mapas geográficos en tiempo real para la visualización de orígenes y destinos del tráfico generado en la Universidad.		
127	Consola de administración y monitoreo	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.		
128	Consola de administración y monitoreo	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.		
129	Consola de administración y monitoreo	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.		

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
		• Debe mostrar la versión actual del sistema y componentes. • 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.		
130	Reportes	Informe de uso de aplicaciones por usuario o por grupo de usuario.		
131	Reportes	Informes de actividad de usuario o grupo de usuarios, en donde se evidencie sitios visitados junto el tiempo de navegación.		
132	Reportes	Informes por categorías, como, por ejemplo: Trafico, Amenazas, Filtrado red, amenazas y tendencias.		
133	Reportes	El Dashboard deben contener reportería con marcaciones de tendencia, es decir, información relevante que ayude a identificar comportamientos en la red.		
134	Documentación	Certificación vigente, suscrita directamente por el fabricante donde conste que la empresa oferente está certificada para brindar servicios y distribución autorizada por el tiempo de vigencia de la cotización y de ejecución del contrato		
135	Documentación	Documento corporativo de fabrica en donde se encuentra la descripción detallada		

Ítem	Característica técnica	Descripción	Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)	Cumple/No cumple
		de las características de los equipos adquiridos y del licenciamiento aquí solicitado, en español o inglés.		
136	Documentación	Certificación vigente, suscrita directamente por el fabricante, en la cual conste que otorgará garantía durante el término que se encuentren vigente el licenciamiento.		
137	Documentación	Certificación expedida por la casa matriz y dirigida a la Universidad donde se indica que la empresa oferente es canal Partner Platinum (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).		
138	Documentación	Certificación expedida por el fabricante de la marca ofertada, indicando que los equipos y componentes ofertados no se encuentran en periodo de fin de venta, y que mínimo tienen un ciclo de vida útil no inferior a cinco (5) años.		
139	Documentación	Carta de presentación de propuesta firmada por el representante legal (Anexo 1 de los estudios previos)		
140	Documentación	Certificaciones de experiencia (Anexo 2 de los estudios previos)		
141	Documentación	Propuesta Económica (Anexo 3 de los estudios previos)		

Tabla 3. Criterios de evaluación

Nota 1: Los oferentes sólo deberán diligenciar la columna llamada “Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página)” de la tabla 3. Criterios de evaluación, la columna llamada “Cumple/No Cumple” será diligenciada por la parte técnica de la Universidad.

Nota 2: Cada uno de los ítems descritos en la tabla 3. Criterios de evaluación deberán estar en la documentación presentada, **NO** se acepta un CUMPLE, se debe diligenciar el número de página exacta en donde se encuentra.

Nota 3: La tabla 3. Criterios de evaluación, hace parte de la calificación técnica, por lo tanto, debe ser diligenciado en su totalidad y será causal de rechazo de la propuesta que lo diligencie parcialmente o en forma inadecuada.

11 CALIFICACIÓN

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

Tabla de calificación		
Ítem	**Factor**	**Puntaje**
1	Económica	800
2	Tiempo de licencias y soporte adicionales	200
CALIFICACIÓN TOTAL		**1000**

Tabla 4. Calificación

11.1. Propuesta económica

El cálculo se determina de la siguiente manera:

P= (MVTO / VTPE) * 800

P= Puntaje obtenido por un oferente
MVTO= Menor valor ofertado entre todos los oferentes
VTPE= Valor total por el oferente evaluado.

NOTA: El puntaje definitivo se dará hasta con dos (2) números decimales, redondeando la cifra al número entero mayor, siempre y cuando la cifra decimal sea mayor a 0.5, en caso de que el primer decimal sea igual o inferior a 0.5 se redondeará por debajo.

Es necesario establecer que, si al final, solo una oferta quedara habilitada en los requerimientos jurídicos, financieros y técnicos, se le calculará el puntaje en la parte económica y se adjudicará el contrato a la empresa que presente dicha oferta, si cumple con los mínimos establecidos

11.2 Tiempo de Licenciamiento y soporte

El tiempo de licenciamiento y soporte adicional deberá cumplir con las características definidas en el numeral "LICENCIAMIENTO Y SOPORTE" de las especificaciones técnicas.

Se asignará 200 puntos al oferente que ofrezca el mayor tiempo adicional de licenciamiento y soporte, los demás serán calculados así:

Ítem	Tiempo de licenciamiento y soporte adicional	Puntos
1	6 meses	200
2	5 meses	180
3	4 meses	160
4	3 meses	140
5	2 meses	120
6	1 mes	100

Tabla 5. Licencias Adicionales

12 OFERTA ECONÓMICA

El oferente deberá diligenciar en su totalidad el anexo 3 de los estudios previos, indicando en la propuesta, el valor de los equipos, del licenciamiento y del soporte, en pesos colombianos incluido IVA.

La propuesta debe indicar de manera explícita que el licenciamiento y soporte tendrá vigencia de un (1) año, a partir de la puesta en correcto funcionamiento de la solución compuesta por dos equipos para garantizar la alta disponibilidad (HA).

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.

13 FORMA DE PAGO

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 de la Universidad.

La universidad pagará al contratista el valor del contrato en pagos parciales de la siguiente forma:

Pago 1 - Correspondiente al valor de los equipos: El primer pago corresponde al valor del sistema de seguridad perimetral en HA, compuesto por todo el hardware y software necesarios para su funcionamiento en alta disponibilidad (HA), incluyendo todos los cables, accesorios y demás elementos necesarios. Previa presentación y aprobación de los siguientes documentos:

a) Documento generado por el fabricante en donde se presente una descripción completa de los equipos y licenciamiento adquiridos:
   i. Nombre de usuario final, a nombre de la Universidad Distrital
   ii. Fecha de inicio, fecha de finalización de los licenciamientos
   iii. Referencia de producto.
   iv. Serial de los equipos.
   v. Cantidad de licencias adquiridas
   vi. Código de activación (en caso de que aplique)

b) Documento generado por el fabricante en donde se presente una descripción completa de la garantía asociada a los equipos adquiridos.

c) Acta de inicio firmada por el contratista y el supervisor del contrato por parte de la Universidad Distrital.

d) Cronograma de ejecución.

e) Documento de manifiesto de importación de los equipos y elementos en medio físico y digital, los cuales deben identificar explícitamente (subrayado o resaltado) los seriales de los equipos y componentes adquiridos por la Universidad.

f) "Protocolo de pruebas y recepción de equipos y/o componentes Universidad Distrital" de los términos y especificaciones técnicas de la solución de seguridad perimetral compuesta por dos equipos para garantizar la alta disponibilidad (HA), donde se relacione cada uno de los equipos y componentes con las pruebas de correcto funcionamiento. Se debe generar un archivo por cada equipo donde se observe el serial del mismo y la secuencia de arranque. El documento debe contar con las respectivas firmas de aprobación

g) Acta de recepción de equipos.

Pago 2 - Correspondiente al valor de los siguientes servicios: El segundo pago corresponde al valor del licenciamiento y los servicios de instalación, configuración, soporte y puesta en correcto funcionamiento del Firewall de seguridad perimetral en HA, realizado una vez termine el licenciamiento vigente. Previa presentación aprobación de los siguientes documentos:

a) 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.

b) 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.

c) Informe técnico de la instalación, configuración y puesta en correcto funcionamiento de la solución compuesta por dos equipos para garantizar la alta disponibilidad (HA) adquirida, así como las pruebas y los resultados de las mismas. El informe debe incluir diagramas y topologías de interconexión.

d) Documento expedido por el fabricante, a nombre de la Universidad Distrital Francisco José de Caldas, en donde se indica el contrato de soporte adquirido para los equipos, con sus respectivas referencias, seriales, alcance, fecha de inicio y fecha de finalización; así mismo debe indicar el mecanismo para verificación directa con el fabricante de la garantía y soporte que ampara a los equipos, por un periodo mínimo de cinco (5) años.

e) Documento de Pruebas de alta disponibilidad generado por la Universidad Distrital en conjunto con el contratista.
f) Actas de asistencia y contenido de la transferencia de conocimiento.

Para todos los pagos el contratista deberá entregar la siguiente documentación:

a) Factura incluido IVA discriminado, con un periodo de vencimiento no inferior a cuarenta y cinco (45) días.
b) Documento anexo a la factura en el cual se relacionen los siguientes campos:
   i. Ítem.
   ii. Referencia.
   iii. Descripción.
   iv. Serial.
   v. Marca.
   vi. Costo unitario sin IVA.
   vii. IVA aplicado (%).
   viii. Costo total con IVA.
c) Acta de recibo a satisfacción por parte de la Supervisión.
d) Documentos referidos en la circular No 004 de 2024 de la Oficina Financiera de la Universidad Distrital.
e) Certificación de cumplimiento del pago de seguridad social y parafiscales, suscrita por el representante legal y/o el revisor fiscal, según sea el caso.
f) 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.

14 GLOSARIO

- **Seguridad perimetral:** Integración de mecanismos y sistemas, tanto electrónicos como mecánicos, para la protección de periféricos físicos, detección y prevención de intrusiones.
- **Firewall:** Sistema de seguridad de red que restringe el tráfico de internet entrante, saliente o dentro de una red privada.
- **Diffserv:** Differentiated Service. Indica un modelo de servicio múltiple que cumple con muchas de las solicitudes de calidad de servicio en Internet.
- **Filtrado web:** Control sobre qué tipos de sitios web estarán disponibles dentro de la red y cuales no se mostrarán a los usuarios.
- **HA – High Availability (Alta disponibilidad):** Protocolo de diseño de sistemas que busca garantizar el correcto funcionamiento y un alto grado de continuidad de los servicios prestados.

- **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.
- **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
- **7x24**: siete (7) días a la semana, veinticuatro (24) horas al día.
- **NBD:** Next business day, siguiente día hábil.
- **RMA:** Return Merchandise Authorization. Es la reparación o reemplazo de un producto electrónico o sus partes durante el período de soporte.
- **Phising:** es una técnica de ingeniería social que usan los ciberdelincuentes para robar información personal o corporativa a través del correo.