## CONVOCATORIA PÚBLICA No.009 2025

El objeto de la presente Convocatoria Pública es **CONTRATAR LA ADQUISICIÓN, INSTALACIÓN Y PUESTA EN CORRECTO FUNCIONAMIENTO DE UNA SOLUCIÓN DE SEGURIDAD PERIMETRAL EN ALTA DISPONIBILIDAD (HA) PARA LA UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS INCLUYENDO SOPORTE Y ACTUALIZACIONES (UPDATE Y UPGRADE).**

## ADENDA No. 1

Dentro del marco de la Ley 30 de 1992, el Acuerdo No 003 de 2015 expedido por el Consejo Superior Universitario, la Resolución No. 262 de 2015 expedida por la Rectoría de la Universidad Distrital y demás normas que la complementan, adicionan o reglamentan, y teniendo en cuenta que algunas empresas interesadas en el proceso remitieron a la Universidad observaciones extemporaneas al Pliego de Condiciones definitivo y que, una vez estudiadas por el Comité Asesor de Contratación, éste determino realizar las modificaciones que considero pertinentes de acuerdo a lo solicitado por la parte técnica.

Mediante la presente Adenda, la Universidad Distrital Francisco José de Caldas aclara y/o modifica el Pliego de Condiciones que rige el proceso de la Convocatoria Pública No.009 2025, tal como a continuación se describe:

**1.** Modificar el numeral **1.33.14 ESPECIFICACIONES TÉCNICAS MÍNIMAS;** que en lo sucesivo queda así:

**1.33.14 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.<br>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 |

| Ítem | Característica técnica | Descripción |
|---|---|---|
| | | 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 |
| 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 en alguno de los niveles superiores de certificación según la marca, teniendo en cuenta que en orden ascendente los niveles de certificación son: Select, Advanced o Expert / Professional, Premier o Elite / Innovator, Platinum o Diamond / Premier, Gold o Platinum / o el 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:<br>• Evaluar la configuración del firewall e identificar áreas de mejora (políticas de seguridad).<br>• Proporcionar un acceso fácil a los datos de telemetría históricos y en tiempo real del firewall.<br>• Detectar problemas del sistema, estado de salud del firewall.<br>• 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. |
| 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 |

| Ítem | Característica técnica | Descripción |
|---|---|---|
| | | 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).<br>**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.<br>**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 |
| 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 |

| Ítem | Característica técnica | Descripción |
|---|---|---|
| 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, 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 (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. |
| 48 | Control por política de firewall | Debe contar con la funcionalidad de dar recomendaciones en las políticas creadas basado en buenas prácticas. |

| Ítem | Característica técnica | Descripción |
|---|---|---|
| | (aplicaciones, puertos y protocolos) | |
| 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 (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. |
| 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. |

| Ítem | Característica técnica | Descripción |
|---|---|---|
| 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. |
| 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. |

| Ítem | Característica técnica | Descripción |
|---|---|---|
| 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. |
| 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:<br>• Dirección de origen<br>• Dirección de destino<br>• Por usuario y grupo de LDAP/AD<br>• Por aplicaciones<br>• Por puerto |
| 92 | Calidad de servicio | El QoS debe permitir la definición de clases por:<br>• Ancho de banda garantizado<br>• Ancho de banda máxima<br>• 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) |

| Ítem | Característica técnica | Descripción |
|---|---|---|
| 96 | VPN embebida | La VPN IPSEc debe soportar mínimo:<br>• Cifrado 3DES<br>• Cifrado AES (128 bits, 256 bits)<br>• Autenticación: MD5, SHA-1, SHA-256, SHA-384, SHA-512<br>• Intercambio de calves: clave manual, IKEv1 e IKEv2<br>• 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:<br>• Antes o durante la autenticación del usuario en la estación<br>• Después de la autenticación del usuario en la estación<br>• 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 túnel 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, 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 |

| Ítem | Característica técnica | Descripción |
|---|---|---|
| | | 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. |
| 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:<br>• Creación y administración de políticas de firewall y control de aplicaciones<br>• Creación y administración de políticas de IPS y Anti-Spyware<br>• Creación y administración de políticas de filtro de URL<br>• Monitoreo de logs<br>• Herramientas de investigación de logs<br>• Debugging<br>• 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 | Debe posibilitar la visualización y comparación de configuraciones actuales, la configuración |

| Ítem | Característica técnica | Descripción |
|---|---|---|
| | administración y monitoreo | 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):<br>• Debe mostrar la situación del dispositivo y del clúster.<br>• Debe mostrar la versión actual del sistema y componentes.<br>• Debe poder mostrar las principales aplicaciones.<br>• Debe poder mostrar las principales aplicaciones por riesgo.<br>• Debe poder mostrar los administradores autenticados en la plataforma de seguridad.<br>• Debe poder mostrar el número de sesiones simultáneas<br>• Debe poder mostrar el estado de las interfaces.<br>• 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. |

**2.** Modificar el numeral **1.33.15 DOCUMENTACIÓN DE CARÁCTER TÉCNICO;** que en lo sucesivo queda así:

**1.33.15 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 proveedor debe presentar certificación expedida por la casa matriz donde se indica que es canal Partner en alguno de los niveles superiores de certificación según la marca, teniendo en cuenta que en orden ascendente los niveles de certificación son: Select, Advanced o Expert / Professional, Premier o Elite / Innovator, Platinum o Diamond / Premier, Gold o Platinum / o el 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.

**3.** Modificar el numeral **2.4 FACTORES DE EVALUACIÓN;** que en lo sucesivo queda así:

**2.4 FACTORES DE EVALUACIÓN**

La Universidad Distrital Francisco José de Caldas, en desarrollo del deber de selección objetiva, escogerá la propuesta más favorable a la entidad y a los fines que busca con el presente proceso de selección.

Todas las propuestas presentadas válidamente y que sean clasificadas como "HÁBILITADA", serán analizadas aplicando los mismos criterios para todas ellas. Se entiende por ofrecimiento más favorable, aquel que teniendo en cuenta los factores de escogencia y su ponderación precisa, detallada y concreta, resulte ser el más ventajoso para la Universidad.

Se adjudicará el proceso de selección a la propuesta que, cumpliendo con los requisitos jurídicos, financieros y técnicos señalados en los presentes Pliegos de Condiciones, obtenga el mayor puntaje, luego de superar la siguiente evaluación de requisitos habilitantes:

| ASPECTOS A EVALUAR | CALIFICACION / ASIGNACIÓN DE PUNTAJE |
|---|---|
| ESTUDIO JURIDICO | ADMISIBLE / NO ADMISIBLE |
| ESTUDIO FINANCIERO | ADMISIBLE / NO ADMISIBLE |
| ESTUDIO TECNICO | ADMISIBLE / NO ADMISIBLE |

Las propuestas admitidas, serán evaluadas de acuerdo con la siguiente tabla:

| ASIGNACIÓN DE PUNTAJE | | | |
|---|---|---|---|
| **ITEM** | **FACTORES** | | **PUNTOS MÁXIMOS QUE ASIGNA** |
| 1 | PROPUESTA ECONÓMICA | Se asignarán 800 puntos posibles a la oferta seleccionada, por menor valor total ofertada, los demás serán calculados como se describe en el ítem 10.1 Propuesta Económica. | 800 |
| 2 | TIEMPO DE LICENCIAMIENTO, SOPORTE Y MANTENIMIENTO | Se asignarán 200 puntos a la empresa que ofrezca mayor tiempo de soporte sobre la solución bajo las mismas especificaciones descritas en el numeral 6. ESPECIFICACIONES TÉCNICAS MÍNIMAS, los demás serán calculados como se describe en el ítem 10.2. Tiempo de licenciamiento, soporte y mantenimiento. | 200 |

**2.4.1 EVALUACIÓN TECNICA DE LAS PROPUESTAS**

Se llevará a cabo por parte de la Red de datos UDNET de la Universidad Distrital y se tendrá en cuenta el cumplimiento de los requerimientos solicitados en las correspondientes especificaciones técnicas y su resultado será cumple o no cumple. Para la evaluación de las propuestas solamente serán tenidas en cuenta, aquellas que cumplan en su totalidad con los requisitos de las presentes especificaciones técnicas.

La evaluación se hará de acuerdo a los siguientes criterios:

| 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.<br>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. | | |
| 8 | Generalidades | Los equipos deben estar certificados para IPv6 en Firewall por USGv6 o IPv6 Ready. | | |

| Ítem | Característica técnica | Descripción | Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página) | Cumple/No cumple |
|---|---|---|---|---|
| 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 en alguno de los niveles superiores de certificación según la marca, teniendo en cuenta que en orden ascendente los niveles de certificación son: Select, Advanced o Expert / Professional, Premier o Elite / Innovator, Platinum o Diamond / Premier, Gold o Platinum / o el 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:<br>• Evaluar la configuración del firewall e identificar áreas de mejora (políticas de seguridad).<br>• Proporcionar un acceso fácil a los datos de telemetría históricos y en tiempo real del firewall.<br>• Detectar problemas del sistema, estado de salud del firewall.<br>• 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, | | |

| Ítem | Característica técnica | Descripción | Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página) | Cumple/No cumple |
|---|---|---|---|---|
| | | 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. | | |
| 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 | | |

| Ítem | Característica técnica | Descripción | Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página) | Cumple/No cumple |
|---|---|---|---|---|
| | | interfaces para alta disponibilidad, ni administración).<br><br>**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.<br><br>**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 | | |
| 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 | Debe contar con modos NAT IPv4: IP | | |

| Ítem | Característica técnica | Descripción | Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página) | Cumple/No cumple |
|---|---|---|---|---|
| | protocolos de red | 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 | | 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 (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. | | |

| Ítem | Característica técnica | Descripción | Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página) | Cumple/No cumple |
|---|---|---|---|---|
| 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 (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 (aplicaciones, puertos y protocolos) | Permitir la restricción de usuarios sospechosos o malintencionados basado en comportamientos. | | |
| 55 | Prevención de | Para seguridad del ambiente contra | | |

| Ítem | Característica técnica | Descripción | Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página) | Cumple/No cumple |
|---|---|---|---|---|
| | amenazas | 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 | Debe detectar y proteger de los ataques | | |

| Ítem | Característica técnica | Descripción | Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página) | Cumple/No cumple |
|---|---|---|---|---|
| | amenazas | 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. | | |
| 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 | | |

| Ítem | Característica técnica | Descripción | Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página) | Cumple/No cumple |
|---|---|---|---|---|
| | | 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. | | |
| 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 | Debe poseer Soporte a identificación de | | |

| Ítem | Característica técnica | Descripción | Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página) | Cumple/No cumple |
|---|---|---|---|---|
| | usuarios | 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:<br>• Dirección de origen<br>• Dirección de destino<br>• Por usuario y grupo de LDAP/AD<br>• Por aplicaciones<br>• Por puerto | | |
| 92 | Calidad de servicio | El QoS debe permitir la definición de clases por:<br>• Ancho de banda garantizado<br>• Ancho de banda máxima<br>• 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:<br>• Cifrado 3DES<br>• Cifrado AES (128 bits, 256 bits)<br>• Autenticación: MD5, SHA-1, SHA-256, SHA-384, SHA-512<br>• Intercambio de calves: clave manual, IKEv1 e IKEv2<br>• Autenticación vía certificado IKE PKI. | | |

| Ítem | Característica técnica | Descripción | Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página) | Cumple/No cumple |
|---|---|---|---|---|
| 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:<br>• Antes o durante la autenticación del usuario en la estación<br>• Después de la autenticación del usuario en la estación<br>• 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 túnel 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. | | |

| Ítem | Característica técnica | Descripción | Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página) | Cumple/No cumple |
|---|---|---|---|---|
| 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 | | |

| Ítem | Característica técnica | Descripción | Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página) | Cumple/No cumple |
|---|---|---|---|---|
| | | 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. | | |
| 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:<br>• Creación y administración de políticas de firewall y control de aplicaciones<br>• Creación y administración de políticas de IPS y Anti-Spyware<br>• Creación y administración de políticas de filtro de URL<br>• Monitoreo de logs<br>• Herramientas de investigación de logs<br>• Debugging<br>• Captura de paquetes. | | |
| 123 | Consola de administración y | Debe permitir la validación de las políticas, avisando cuando haya reglas que ofusquen | | |

| Ítem | Característica técnica | Descripción | Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página) | Cumple/No cumple |
|---|---|---|---|---|
| | monitoreo | 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):<br>• Debe mostrar la situación del dispositivo y del clúster.<br>• Debe mostrar la versión actual del sistema y componentes.<br>• Debe poder mostrar las principales aplicaciones.<br>• Debe poder mostrar las principales aplicaciones por riesgo.<br>• Debe poder mostrar los administradores autenticados en la plataforma de seguridad.<br>• Debe poder mostrar el número de sesiones simultáneas<br>• Debe poder mostrar el estado de las interfaces.<br>• Debe poder mostrar el uso de CPU. | | |
| 130 | Reportes | Informe de uso de aplicaciones por usuario o por grupo de usuario. | | |

| Ítem | Característica técnica | Descripción | Ubicación en la propuesta / Link a página WEB del fabricante (No. de Página) | Cumple/No cumple |
|---|---|---|---|---|
| 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 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 | El proveedor debe presentar certificación expedida por la casa matriz donde se indica que es canal Partner en alguno de los niveles superiores de certificación según la marca, teniendo en cuenta que en orden ascendente los niveles de certificación son: Select, Advanced o Expert / Professional, Premier o Elite / Innovator, Platinum o Diamond / Premier, Gold o Platinum / o el 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) | | |

La tabla anterior 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.

**2.4.2 EVALUACIÓN DEL FACTOR ECONÓMICO-ASIGNACIÓN DE PUNTAJE**

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 Anexo No. 3

La presentación del Anexo No. 3 no es subsanable.

Se le asignará el mayor puntaje al proponente que oferte el menor valor (IVA incluido) de la solución requerida. Este menor valor se calculará entre todos los oferentes que, una vez habilitados jurídica, técnica y financieramente, hubieren presentado oferta para una solución en particular.

Será calculado así:

**P= (MVTO / VTPE) * 800**

En donde:

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 al proponente que presente dicha oferta, si cumple con los mínimos establecidos.
**La propuesta económica se presentará en el formato establecido en el Anexo No. 3, en formato pdf., y en formato Excel.**

Se debe ofertar el valor de todos los elementos más el IVA. Este valor debe incluir la totalidad de los costos directos e indirectos, que genere el bien y demás inherentes a la ejecución del contrato, por ningún motivo se considerarán costos adicionales.

Si el PROPONENTE no discrimina el impuesto al valor agregado (I.V.A.) y el bien causa dicho impuesto, la Universidad lo considerará INCLUIDO en el valor total de la PROPUESTA y así lo aceptará el PROPONENTE.

Por ningún motivo, se reconocerá reajuste del precio durante la vigencia del contrato.

**2.4.3 TIEMPO DE LICENCIAMIENTO, SOPORTE Y MANTENIMIENTO**

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 |

El contenido del presente ADENDA No. 1, forma parte integral del Pliego de Condiciones y modifica en lo pertinente los numerales que le sean contrarios. Las demás condiciones continúan como están establecidas en el Pliego de Condiciones.

Dado en Bogotá, D. C. a los catorce (14) días del mes de agosto de dos mil veinticinco (2025).

**COMITÉ ASESOR DE CONTRATACIÓN**
**UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS**