UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

CONSOLIDADO DE OBSERVACIONES AL PROYECTO DE PLIEGO CONVOCATORIA No 009 DE 2025
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).

OBSERVACIONES REALIZADAS POR LA EMPRESAS EQUIPO LICITACIONES REDNEET SAS. NIT. 900.434.462-7

OBSERVACIÓN No. 1

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).

El requerimiento 13, hace referencia a la certificación expedida por el fabricante e indica que el canal debe ser partner platinum (o equivalente a la marca) o superior de los productos adquiridos con licenciamiento, adicional menciona el orden ascendente silver, gold, platinum o equivalente.
Teniendo en cuenta el requerimiento, es de nuestro entendimiento que cuando menciona silver, gold, platinum o equivalente, se pueden presentar oferentes que cumplan con cualquiera de estas tres (3) categorías (silver y/o gold, y/o platinum o sus equivalentes). Solicitamos a la entidad confirmar si correcto nuestro entendimiento.

RESPUESTA DE LA UNIVERSIDAD: Se aclara que el Partner debe ser mínimo canal Platinum o equivalente en la clasificación de la marca ofertada. Los niveles Silver y Gold se mencionaron para indicar que se busca un partner en el nivel más alto de certificación.

OBSERVACIÓN No. 2

Consola de administración y monitoreo

	monitoreo	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.

Se solicita a la entidad realizar la validación del ítem "consola de administración", considerando que, según la jerarquización de equipos, los firewalls son considerados activos de red y, por tanto, equipos de front. Por este motivo, los equipos destinados a la administración y gestión de la información, siguiendo buenas prácticas, deben ser independientes. Esto permite que, en caso de una caída o ataque al equipo de front, sea posible rastrear la causa raíz y restablecer las funcionalidades a través de un equipo intermedio no expuesto al tráfico de transición. Por lo tanto, se solicita modificar este ítem para garantizar el correcto funcionamiento del servicio. Se recomienda eliminar la opción de que la consola de administración pueda estar integrada en el equipo de seguridad, estableciendo que el repositorio y monitoreo debe estar alojado en un equipo independiente. Esto tiene como propósito no sacrificar el procesamiento de un equipo de propósito específico y asegurar la posibilidad de validar, ante una eventual caída del firewall, la causa raíz y disponer de un punto de restablecimiento y corrección.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, el oferente puede ofrecer la administración y monitoreo de manera independientes siempre que se ajuste al presupuesto del proceso.

OBSERVACIÓN No. 3

24	Cada equipo debe incluir Disco de Estado Sólido (SSD) de mínimo 450 GB para almacenamiento del sistema y logs.

Teniendo en cuenta como ustedes lo solicitan que cada equipo, el disco duro es de 450 GB, se están penalizando con una retención de información baja, además de ser una mala práctica de seguridad:
Dicho lo anterior solicitamos a la entidad requerir que el componente para el almacenamiento de logs sea manera independiente del appliance de seguridad de red, dado que si se limita el tamaño del disco en la misma solución esto puede generar la perdida de los registros y en caso de requerirlos en una auditoría interna o externa no los van a tener disponibles lo cual inmediatamente se convierte en un hallazgo para el auditor afectando la política de seguridad de la información de la entidad.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, teniendo en cuenta que la retención de logs se realiza mediante servidores externos de syslogs que se encargan de realizar el análisis y generación de reportes de la información.

OBSERVACIÓN No. 4

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.

Solicitamos respetuosamente a la entidad considerar la modificación de este ítem y solictarlo de la siguiente manera:
Capacidad de soportar mínimo 1800 clientes de VPN SSL (Client). 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.
Teniendo en cuenta que la funcionalidad requerida por la entidad está relacionada con el uso de VPN, la cual puede ser habilitada en algunos equipos mediante licenciamiento adicional, sin afectar el cumplimiento técnico del requerimiento

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, dado que se redactó de la manera "*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*" con el fin de que los oferentes cumplan sin generar un costo adicional a la Universidad en caso de que se requiera un licenciamiento específico.

OBSERVACIÓN No. 5

	amenazas	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.

Solicitamos respetuosamente a la entidad aclarar si requiere un sandbox como funcionalidad dentro del appliance de seguridad de red o si hace referencia a un tipo de solución tipo Sandbox cloud.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, el ítem 68 que dice "*Debe contar con un entorno de inspección de códigos, sitios web o archivos maliciosos.*" hace referencia a que la solución de seguridad debe realizar la inspección de amenazas en ambientes controlados como lo es un sandbox.

OBSERVACIONES REALIZADAS POR LA EMPRESAS GAMMA INGENIEROS S.A.S

PAULA ANDREA LOAIZA +57 3154599250 Paula.loaiza@gammaingenieros.com

OBSERVACIÓN No. 1

Documento: ***3. Especificaciones Técnicas Firewall***
Requerimiento: *Pagina 9, Punto 25*

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.
19	Capacidades y cantidades	Throughput de Next Generation Firewall (NGFW) de 18 Gbps medido con tráfico productivo real.

Observación 1:

Se solicita amablemente a la entidad ***modificar el requerimiento contenido en el ítem 25****, de forma que las interfaces puedan operar a un* ***1 Gbps****, y no necesariamente de 1/10 Gbps, ya que el requerimiento actual impone una configuración que genera un* ***sobredimensionamiento innecesario en la cantidad de interfaces de alta velocidad (10G)****.*
En el ***ítem 26*** *de la misma ficha técnica ya se exige que el equipo cuente con* ***mínimo 8 interfaces de 10 Gbps SFP/SFP+*** *para tráfico de red, lo cual garantiza la capacidad de conectividad de alta velocidad exigida por la entidad.*
Adicional a estas, el ítem 25 requiere otras ***8 interfaces (RJ45 o SFP+) con soporte 10G****, lo cual eleva el número total de interfaces de 10 Gbps a* ***16****.*

Sin embargo, para un ***throughput de NGFW el cual solicita la entidad que sea de 18 Gbps****, no es funcional ya que en la práctica el equipo* ***no puede aprovechar de forma efectiva las 16 interfaces a 10 Gbps****, ya que el total de capacidad de procesamiento estaría superado por el flujo de datos potencial. Por ende, Esta condición genera una* ***incongruencia técnica y un sobredimensionamiento innecesario****, que no solo encarece la solución, sino que también restringe la participación de equipos con arquitectura optimizada que cumplen funcionalmente con los objetivos de rendimiento y conectividad.*
Referencia: *Página 9, Punto 19:*
Throughput de Next Generation Firewall (NGFW) de 18 Gbps medido con tráfico productivo real.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, respecto a la consulta sobre si se hará uso operativo y simultáneo de todas las interfaces a 10 Gbps SFP/SFP+, se confirma que la arquitectura de red prevista obedece a un cambio en la topología de análisis de tráfico de red contemplado por la Universidad y por lo tanto se establece la necesidad de contar con dicha capacidad de interfaces SFP/SFP+. Adicionalmente, el uso de interfaces de cobre está previsto para conectar equipos con tecnología de cobre a 10G evitando hacer uso de las interfaces SFP+ que únicamente pueden ser usadas por equipos con interfaces de fibra.

OBSERVACIÓN No. 2

Observación 2: *Se solicita amablemente a la entidad ampliar el requerimiento de throughput del Next Generation Firewall (NGFW) de 18 Gbps a mínimo 25 Gbps, medido con tráfico productivo real. Esta solicitud se realiza con la finalidad de garantizar un rendimiento óptimo y sostenible en el tiempo, evitando que la solución quede limitada en capacidad de procesamiento a corto o mediano plazo. Ampliar el throughput permite:*

- *Soportar adecuadamente el crecimiento progresivo del tráfico de red generado por nuevos servicios, usuarios, sedes remotas y aplicaciones críticas.*
- *Aprovechar de forma efectiva la infraestructura de red solicitada, que incluye múltiples interfaces de alta velocidad (1G o 2.5G o 5G o 10G), sin generar cuellos de botella ni degradación en la experiencia del usuario.*

Referencia: *Pagina 17, Punto 105:*
Throughput de VPN de mínimo 9 Gbps IPsec.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, el throughput de 18 Gbps para el NGFW obedece a las necesidades actuales de la Universidad teniendo en cuenta que las especificaciones técnicas previstas corresponden a un cambio en la topología de análisis de tráfico de red contemplado por la Universidad.

Las empresas que participaron en el estudio de mercado ofrecen equipos con las características solicitadas.

OBSERVACIÓN No. 3

Observación 3: *Se solicita amablemente a la entidad ampliar el requerimiento de throughput para túneles VPN IPsec de 9 Gbps a mínimo 45 Gbps.*
Esta solicitud tiene como objetivo garantizar un rendimiento sostenido, confiable y escalable en los canales seguros de comunicación, asegurando que la solución no se vea limitada en el corto o mediano plazo. Un throughput ampliado en VPN IPsec permite:

- *Soportar con mayor eficiencia el tráfico cifrado entre sedes, usuarios remotos y servicios en la nube, que tiende a incrementarse significativamente con la digitalización y el trabajo híbrido.*
- *Evitar cuellos de botella en escenarios de tráfico simultáneo, especialmente cuando múltiples usuarios o sedes acceden a recursos institucionales mediante VPN al mismo tiempo.*
- *Asegurar la calidad del servicio (QoS) y la experiencia de usuario, incluso con servicios de alto consumo de ancho de banda (videoconferencias, acceso remoto a bases de datos, escritorios virtuales).*

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, el requerimiento de throughput mínimo de 9 Gbps para túneles IPsec ha sido definido con base en la capacidad de demanda actual y el crecimiento proyectado de la infraestructura tecnológica de la Universidad Distrital. Cabe resaltar que el valor se ha establecido como requisito mínimo, por lo cual no existe restricción para que los proponentes oferten equipos con capacidades superiores.

OBSERVACIONES REALIZADAS POR LA EMPRESAS DATASEC S.A.S SERGIO DÍAZ +57 3213184645sergio.diaz@datasec.com.co DIRECCIÓN: Cra 14A # 101 – 1

OBSERVACIÓN No. 1

Implementación de equipos Firewall Perimetrales

Se solicita amablemente a la entidad aclarar si la implementación del equipo se realizará a distancia cero, es decir, si el nuevo equipo será instalado en el mismo rack o datacenter donde se encuentran actualmente los dispositivos a los cuales estará interconectado. Esta información es necesaria para determinar si se deben contemplar adecuaciones de infraestructura física, tales como:

- *Rediseño o extensión de cableado estructurado (cobre o fibra)*
- *Ajustes en la disposición física del rack*
- *Revisión o ampliación de capacidad eléctrica o de ventilación*
- *Instalación de elementos pasivos adicionales (organizadores, bandejas, patch panels, etc.)*

RESPUESTA DE LA UNIVERSIDAD: Se aclara que la instalación de los dispositivos se realizará en el datacenter donde actualmente se encuentra la seguridad perimetral a reemplazar. No se necesita adecuaciones de infraestructura física.

OBSERVACIÓN No. 2

Página 9, Punto 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.

***Solicitud**: Se solicita amablemente a la entidad evaluar y modificar el requerimiento relacionado con las velocidades de las interfaces de red mencionadas anteriormente, de manera que se permita el cumplimiento mediante ocho (8) interfaces con velocidades de 1G o 2.5G o 5G o 10G, indistintamente, ya sea mediante interfaces RJ45 nativas o SFP/SFP+ con transceivers compatibles. Ya que existe un requerimiento complementario en el punto 26 de la ficha técnica, donde se exigen 8 interfaces de 10G SFP/SFP+, lo cual asegura que el equipo cuenta con capacidad adecuada en fibra óptica y puertos de alta velocidad. Por tanto, mantener un segundo requerimiento con condiciones específicas sobre los puertos de cobre o fibra resulta restrictivo.*

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, el requerimiento ha sido definido con base en las necesidades actuales y previendo a futuro sobre la infraestructura tecnológica de la Universidad Distrital teniendo en cuenta que las especificaciones técnicas previstas obedecen a un cambio en la topología de análisis de tráfico de red contemplado por la Universidad. Adicionalmente, el uso de interfaces de cobre está previsto para conectar equipos con tecnología de cobre a 10G evitando hacer uso de las interfaces SFP+ que únicamente pueden ser usadas por equipos con interfaces de fibra.

OBSERVACIONES REALIZADAS POR LA EMPRESAS COINSA S.A.S JUAN CARLOS RIOS NEIRA REPRESENTANTE LEGAL

OBSERVACIÓN No. 1

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).

El requerimiento 13, hace referencia a la certificación expedida por el fabricante e indica que el canal debe ser partner platinum (o equivalente a la marca) o superior de los productos adquiridos con licenciamiento, adicional menciona el orden ascendente silver, gold, platinum o equivalente.

Teniendo en cuenta el anterior requerimiento, es de nuestro entendimiento que cuando menciona silver, gold, platinum o equivalente, se pueden presentar oferentes que cumplan con cualquiera de estas tres (3) categorías (silver, gold, platinum o equivalentes). Solicitamos a la entidad confirmar si correcto nuestro entendimiento.

RESPUESTA DE LA UNIVERSIDAD: Se aclara que el Partner debe ser mínimo canal Platinum o equivalente en la clasificación de la marca ofertada. Los niveles Silver y Gold se mencionaron para indicar que se busca un partner en el nivel más alto de certificación.

OBSERVACIÓN No. 2

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).

Respetuosamente solicitamos a la entidad que el requisito habilitante de certificación de canal no se limite a "Platinum o superior", y se acepte la participación de canales en cualquier nivel oficialmente reconocido por el fabricante que habilite comercialización, implementación y soporte de la solución ofertada. En el programa del fabricante de la solución que proponemos, los niveles Silver,gold y Platinum cuentan con las mismas capacidades técnicas y de soporte para ejecutar proyectos (acceso a licenciamiento oficial, herramientas de ingeniería, apertura de casos y escalamiento a la casa matriz, actualizaciones y asistencia técnica); ***las diferencias entre niveles se circunscriben principalmente a condiciones comerciales (metas, descuentos y marketing), no a la idoneidad técnica ni a la calidad del soporte entregado al cliente****. Mantener el requisito exclusivamente en "Platinum" restringe injustificadamente la pluralidad de oferentes sin elevar el estándar técnico; por lo anterior, solicitamos permitir niveles equivalentes que garanticen el mismo alcance de implementación y soporte, compromiso que acreditamos con certificación vigente del fabricante y con la designación de ingenieros certificados para la ejecución del proyecto y la atención de los SLA.*

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, el Partner debe ser mínimo canal Platinum o equivalente en la clasificación de la marca ofertada. Se solicita de esta manera dado que entre mayor sea el nivel de Partner de la empresa, garantiza una mejor resolución de problemas e incidentes que se llegarán a presentar junto implementaciones requeridas por Universidad Distrital, ya que cuentan con una mayor cantidad de certificaciones técnicas.

OBSERVACIÓN No. 3

Consola de administración y monitoreo

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.		

24	Capacidades y cantidades	Cada equipo debe incluir Disco de Estado Sólido (SSD) de mínimo 450 GB para almacenamiento del sistema y logs.

Solicitamos amablemente a la entidad permitir en el requerimiento 120: *que la consola de administración y monitoreo sea considerada como un componente separado del firewall, ya que alojarla en el mismo appliance, con solo 450 GB de almacenamiento, limita la retención de logs y representa un riesgo ante auditorías internas o externas. Esta práctica puede derivar en hallazgos por*

incumplimiento de controles como el 8.15 y 5.32 de la norma ISO/IEC 27001:2022, al no garantizar disponibilidad ni integridad de los registros en caso de incidente o falla del equipo. La separación del monitoreo sigue buenas prácticas (NIST SP 800-92) y asegura trazabilidad continua sin afectar el rendimiento del firewall.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, teniendo en cuenta que la retención de logs se realiza mediante servidores externos de syslogs que se encargan de realizar el análisis y generación de reportes de la información.

OBSERVACIÓN No. 4

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.

Solicitamos respetuosamente retirar del requerimiento 103 las siguientes palabras:
***Sin generar costos adicionales a la solución de seguridad perimetral**, dicho lo anterior el requerimiento quedaría así:*

Capacidad de soportar mínimo 1800 clientes de VPN SSL (Client). 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.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, dado que se redactó de la manera "*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*" con el fin de que los oferentes cumplan sin generar un costo adicional a la Universidad en caso de que se requiera un licenciamiento específico.

OBSERVACIÓN No. 5

68	Prevención de amenazas	Debe contar con un entorno de inspección de códigos, sitios web o archivos maliciosos.

Solicitamos respetuosamente a la entidad aclarar qué tipo de código hace referencia o si hace referencia a que el oferente debe presentar alguna solución o funcionalidad tipo sandbox para el appliance de seguridad de red.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, el ítem 68 que dice "*Debe contar con un entorno de inspección de códigos, sitios web o archivos maliciosos.*" hace referencia a que la solución de seguridad debe realizar la inspección de amenazas en ambientes controlados como lo es un sandbox.

OBSERVACIONES REALIZADAS POR LA EMPRESAS WEXLER
licitaciones@wexler.com.co

OBSERVACIÓN No. 1

1. *De acuerdo a lo establecido dentro del punto "1.33.14. LICENCIAMIENTO Y SOPORTE":*

> 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),.

No se evidencia los requisitos en base a la formación del personal requerido para el servicio de soporte técnico solicitado, es por ello que se solicita de manera cordial considerar anexar dos perfiles: uno para gerente de proyectos e ingeniero de soporte con la siguiente formación:

" Gerente de proyectos: Ingeniero de telecomunicaciones con al menos 10 años de experiencia desde la emisión de la tarjeta profesional, especialización GERENCIA DE PROYECTOS DE TECNOLOGIAS DE LA INFORMACION y certificados vigentes en: PMP, ITIL 4 (ITIL FOUNDATION CERTIFICATE IN IT SERVICE MANAGEMENT), CISM, y certificado en network security profesional en la tecnología a ofertar"

"Ingeniero de soporte: Ingeniero de telecomunicaciones con al menos 4 años de experiencia desde la emisión de la tarjeta profesional y certificados vigentes en: Profesional Security Operations de la marca del fabricante a ofertar, Professional Network Security de la marca del fabricante a ofertar, Specialist Security Operations en la marca del fabricante a ofertar y Solution Specialist Network Security de la marca del fabricante a ofertar"

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, la organización interna del proyecto es responsabilidad del contratista, el cual debe garantizar que las condiciones contractuales se cumplan.

OBSERVACIÓN No. 2

Partiendo de la relevancia del proyecto se recomienda que dentro de las especificaciones técnicas se solicite que las herramientas de seguridad perimetral incluyan un módulo de SD-WAN, así: "La Solución deberá soportar balanceado de enlaces WAN inteligente (SD-WAN Seguro) sin licencia adicional basado en: Aplicaciones cloud, SLA y Mejor calidad de enlace basado en (Jitter, latencia, ancho de banda, perdida de paquetes)". Lo anterior se justifica en la proyección de las tendencias actuales en cuanto a funcionalidades complementarias que otorgan valor adicional a inversiones en equipamiento de tal categoría.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, la infraestructura y topología de red de la Universidad Distrital no permiten actualmente la integración ni el aprovechamiento efectivo de tecnologías SD-WAN.

OBSERVACIÓN No. 3

De acuerdo con lo establecido en el punto "1.33.14 ESPECIFICACIONES TÉCNICAS MÍNIMAS":

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.

De manera atenta solicitamos a la entidad confirmar la cantidad de puertos requeridos para cada una de las plataformas incluidas en el presente proyecto, esto con el fin de dimensionar adecuadamente el equipamiento y ajustar al mínimo indispensable los puertos necesarios para la operación. Esta solicitud se fundamenta en la necesidad de optimizar los recursos asignados considerando que la densidad de puertos actualmente planteada implicaría la adquisición de equipos sobredimensionados lo cual podría afectar la viabilidad técnica y financiera del proyecto.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, como se menciona en los ítems 25 y 26 se necesitan como mínimo 8 interfaces de cobre y 8 interfaces de fibra, el requerimiento ha sido definido con base en las necesidades actuales y previendo a futuro sobre la infraestructura tecnológica de la Universidad Distrital teniendo en cuenta que las especificaciones técnicas previstas obedecen a un cambio en la topología de análisis de tráfico de red contemplado por la Universidad. Las especificaciones técnicas están considerando los mínimos requeridos, el oferente puede ofertar el equipo con cantidades iguales o superiores.

COMITÉ ASESOR DE CONTRATACIÓN