15.

Fusagasugá, 2025-09-01.

Señores
DATASEC

Asunto y/ó Ref: Respuesta Observaciones Invitación Privada 038 de 2025

Cordial saludo,

De manera atenta, me dirijo a usted con el fin de dar respuesta a las observaciones allegadas en referencia a la Invitación Privada 038 de 2025, que tiene como objeto: ***"CONTRATAR EL SERVICIO DE SEGURIDAD PERIMETRAL Y CONFIGURACION DE CONECTIVIDAD MEDIANTE TECNOLOGÍA SD-WAN PARA LA UNIVERSIDAD DE CUNDINAMARCA".***

OBSERVACIONES:
DATASEC

OBSERVACIÓN 1:

EXPERIENCIA HABILITANTE

2	**EXPERIENCIA HABILITANTE (FORMATO No. 6)**	El oferente deberá presentar máximo **TRES (03)** certificaciones o actas de terminación o acta de liquidación sobre el cumplimiento de contratos que reúnan las siguientes características: 1) Ejecutado y terminado o liquidado en Colombia con entidades públicas y/o privadas, durante los últimos cinco (05) años contados antes de la fecha de presentación de ofertas e incluido en el REGISTRO ÚNICO DE PROPONENTES. 2) La sumatoria de los contratos que se pretenda acreditar como experiencia habilitante deberá ser como mínimo el setenta y cinco por ciento (75%) del presupuesto del presente proceso es decir **MIL TRESCIENTOS CUARENTA Y TRES (1343) SMMLV**. La verificación se hará con base en la sumatoria de los valores totales ejecutados (incluido IVA) de los contratos expresados en SMMLV de acuerdo con la información contenida en el **REGISTRO ÚNICO DE PROPONENTES RUP**, sobre los contratos que cumplan con los requisitos establecidos en los términos de referencia. **NOTA:** Únicamente se podrá acreditar la experiencia requerida cuando el proponente haya desarrollado de manera directa las actividades que constituyen tal experiencia para el presente proceso de selección. 3) Los objetos de los contratos a acreditar deberán ser afines a la naturaleza del objeto a contratar en la presente invitación. 4) Cada uno de los contratos a acreditar deberá tener inscritos mínimo **DOS (02) CODIGOS UNSPSC** que la Universidad de Cundinamarca establece en el ítem 3 ***Registro Único de Proponentes (RUP)*** del numeral 3.1 del módulo ***REQUISITOS TÉCNICOS HABILITANTES.***

De acuerdo con la experiencia habilitante, la universidad estipula que los contratos a acreditar deberán ser afines a la naturaleza del objeto a contratar, siendo el siguiente: ***CONTRATAR EL SERVICIO DE SEGURIDAD PERIMETRAL Y CONFIGURACION DE CONECTIVIDAD MEDIANTE TECNOLOGÍA SD-WAN PARA LA UNIVERSIDAD DE CUNDINAMARCA.***

Es de nuestro entendimiento que el objeto contractual para acreditar en el presente proceso deberá tener como mínimo actividades de adquisición y/o instalación y/o configuración y/o puesta en marcha y/o prestación de servicios mediante soluciones de seguridad perimetral, por favor confirmar si nuestro entendimiento es correcto.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que el entendimiento planteado por el proponente es correcto: la experiencia habilitante debe acreditar actividades relacionadas con soluciones de seguridad perimetral y configuración SD-WAN, ya sea en instalación, configuración, puesta en marcha o prestación de servicios.

OBSERVACIÓN 2:

Referencia 2:

9	**DOCUMENTOS TÉCNICOS Y/O DATASHEET**	El oferente debe allegar junto con la propuesta económica los documentos técnicos y/o datasheet del fabricante de las soluciones ofertadas, donde se evidencie el cumplimiento de cada uno de los ítems solicitados en los requerimientos técnicos de las soluciones ofertadas.

Solicitamos amablemente a la universidad aclarar si se cargará algún formato en específico y editable para el diligenciamiento del cumplimiento técnico y/o datasheet de las soluciones ofertadas en su punto a punto, lo anterior teniendo en cuenta que el anexo de condiciones técnicas se encuentra en formato PDF y no es posible diligenciar los apartados técnicos.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que no se cargará un formato editable diferente al Anexo de Condiciones Técnicas publicado en PDF y cada oferente será responsable de aportar la ficha técnica oficial de los equipos y soluciones que oferte, la cual debe permitir a la Universidad verificar de manera puntual y objetiva el cumplimiento de los requerimientos técnicos establecidos en el pliego.

Dichas fichas deberán ser emitidas por el fabricante o distribuidor autorizado, y contener información verificable que corresponda exactamente a las referencias propuestas.

OBSERVACIÓN 3:

Respetuosamente se solicita a la entidad reconsiderar la solicitud a los diferentes oferentes con relación a la certificación ISO/IEC 27001:2022 o superior, ajustándolo de tal forma que se admita la certificación ***ISO/IEC 27001 en cualquiera de sus versiones*** *con una vigencia mínima de un (1) año para el proceso de SOC.*

RESPUESTA: La Universidad de Cundinamarca, en atención a la observación recibida, se permite aclarar que la exigencia de la certificación **ISO/IEC 27001:2022 o superior** se

mantiene como requisito habilitante dentro del presente proceso.

Esta decisión responde a que la Universidad de Cundinamarca se encuentra actualmente en proceso de certificación institucional bajo la versión ISO/IEC 27001:2022, lo que implica la adopción de los controles, lineamientos y mejores prácticas más actualizadas en gestión de seguridad de la información. En ese sentido, exigir a los oferentes la misma versión garantiza que exista alineación entre los controles implementados por la Universidad y los servicios ofrecidos por el contratista, asegurando coherencia en la gestión del riesgo, interoperabilidad de procesos y una mayor solidez frente a auditorías de terceros y entes de control.
Por lo anterior no es viable aceptar versiones anteriores de la norma, aunque vigentes, podría generar brechas de cumplimiento entre los controles internos de la Universidad y los procesos ejecutados por el contratista, afectando la capacidad de respuesta frente a incidentes de seguridad y la estrategia de mejora continua institucional.

OBSERVACIÓN 6:

Referencia 6:

6.2.5 CERTIFICACION PARTNER - (VEINTE 20 PUNTOS)

Se otorgarán **VEINTE (20) PUNTOS** oferente que presente una certificación oficial emitida por el fabricante de la marca ofertada, que acredite su calidad de partner, distribuidor autorizado o integrador certificado.

Nota: Para efectos contractuales, el ofrecimiento que realice el futuro proponente y en caso de adjudicación, se incorpora al contrato como una obligación del contratista.

Se solicita amablemente a la universidad incluir dentro de los requerimientos para la certificación expedida por el fabricante de la marca ofertada que se incluya el listado de elementos con los cuales se prestará el servicio dedicado a la universidad (evidenciando los números de parte de los equipos y/o suscripciones para el proceso), lo anterior, permite a la universidad identificar en la etapa de presentación de las propuesta y establecer cuáles son herramientas avaladas por el fabricante ofertado y que estas sean nuevas de fábrica.

Por otra parte, esto favorece la calificación de la universidad en los aspectos técnicos solicitados, los cuales deben encontrarse en línea con el punto a punto técnico a presentar por los proponentes.
De igual forma, solicitamos que este documento sea dirigido a la universidad, especificando el número y objeto del proceso actual.

RESPUESTA: La Universidad de Cundinamarca, en atención a la observación recibida, se permite se permite precisar que se mantiene la exigencia de certificación expedida por el fabricante de la marca ofertada, como requisito para garantizar que los equipos y licencias ofrecidos sean avalados oficialmente y cumplan con las condiciones de calidad y soporte requeridas.

No obstante, no se incorporará como obligatorio que el fabricante emita un documento adicional que incluya el listado detallado de elementos (números de parte de equipos o suscripciones) dirigido a la Universidad, ya que, por lo general, el oferente que resulte

adjudicado puede proceder con la adquisición de los equipos una vez notificado de la adjudicación del presente proceso contractual, por lo que la verificación del cumplimiento técnico se realizará con base en las fichas técnicas oficiales del fabricante, que deberán evidenciar las características solicitadas en el pliego. y la certificación de fabricante que respalde al oferente y garantice que los equipos y servicios provienen de canal autorizado por fabrica.

De esta manera, se asegura que los elementos ofertados se ajusten a los requerimientos de la Universidad, sin que sea necesario imponer documentos adicionales al fabricante que puedan restringir la pluralidad de oferentes.

OBSERVACIÓN 7 a:

Referencia 7:

PAGOS	CONDICIÓN
Pagos mensuales de acuerdo con el servicio efectivamente prestado, previa verificación por parte de la supervisión. El pago final estará condicionado al Acta de Recibo a Satisfacción debidamente verificada por el supervisor.	Para cada pago se deberá anexar el informe de supervisión donde conste el cumplimiento total del objeto contractual.

Solicitamos amablemente a la entidad evaluar y modificar un cambio en la forma de pago contemplada en el proyecto, lo anterior teniendo en cuenta que actualmente para la adquisición de los equipos y licencias nosotros como proveedor debemos realizar una compra masiva al fabricante y/o mayorista el cual nos otorga un tiempo de pago máximo a 60 días, durante este tiempo de pago no se alcanza a cubrir el valor total de las licencias y por la tanto debemos incurrir en costos de financiamiento para cubrir el costo total de los equipos y licencias.

Se propone a la universidad para no acarrear costos de financiamiento al proyecto evaluar e incluir un pago de al menos el 50% contra entra de los equipos y licencias, y el 50% restante quede de manera mensualizada.

Lo propuesto permite mejorar los márgenes de costo del proyecto provocando mejora en las condiciones económicas y de los ítems ponderables favorables al proyecto.

RESPUESTA: La Universidad de Cundinamarca, en atención a la observación recibida, se permite aclarar que la forma de pago definida en los términos de la presente invitación publica responde a las disposiciones contractuales y financieras establecidas en la normatividad vigente de la Universidad para la contratación pública, que obligan a la entidad a realizar los pagos con base en la verificación del cumplimiento de las obligaciones contractuales y la disponibilidad presupuestal correspondiente.

En este sentido, no es posible acceder a la modificación planteada por el oferente respecto

a establecer un pago anticipado del 50% contra entrega de equipos y licencias, ya que la Universidad no puede realizar desembolsos parciales anticipados sin que medie la debida ejecución contractual y la verificación del cumplimiento.

OBSERVACIÓN 7 b:

Referencia 7:

RECURSO	FORMACION	POSTGRADO	CERTIFICACIONES	EXPERIENCIA	DEDICACION	FUNCIONES
Un (01) Ingeniero Gerente de Proyecto	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicación o carreras afines. Tarjeta Profesional con expedición mínimo de cinco (5) años	Posgrado en Gerencia de Proyectos y/o Certificación PMP.	Certificación Itil Foundation v3 o superior	Experiencia general de cinco (5) años en gerencia de proyectos deTI, de los cuales mínimo tres (3) años de experiencia especifica gerenciando y/o coordinando proyectos de seguridad informática. La experiencia se cuenta a partir de la expedición de la tarjeta profesional	100 % al proyecto, de requerirse de manera presencial o virtual en las instalaciones de la entidad	Definir los objetivos y los alcances del proyecto. Desarrollar un plan de trabajo detallado, estableciendo metas, cronograma, recursos. Identificar riesgos y establecer un plan de mitigación

Se solicita amablemente a la entidad modificar este requerimiento, de manera que, en lugar de exigir un número de años, se considere la siguiente redacción:

"Experiencia mínima en cinco (5) proyectos gerenciando y/o coordinando proyectos de TI y/o Seguridad Informática".

Este cambio ***no reduce la calidad ni la idoneidad del perfil solicitado****, pues se mantiene la obligación de la cual el oferente acredite su experiencia relacionada con la gestión o coordinación de proyectos en TI y/o Seguridad Informática.*

RESPUESTA: La Universidad de Cundinamarca, ser permite indicar que el requisito de años mínimos de experiencia se mantiene, dado que este criterio permite verificar de manera objetiva y uniforme la trayectoria continua y comprobada del personal propuesto, garantizando así que el mismo cuenta con el conocimiento y la práctica acumulada necesarios para asumir la complejidad del proyecto.

La experiencia acreditada en términos de proyectos ejecutados puede variar en alcance, tiempo de dedicación y responsabilidades asumidas, lo que dificulta que sea un indicador suficiente de idoneidad. En contraste, la exigencia en años de experiencia profesional asegura que la persona haya participado en diferentes etapas del ciclo de vida de proyectos de TI y/o seguridad informática, fortaleciendo la capacidad técnica y de gestión que requiere la Universidad para este proceso.

OBSERVACIÓN 8:

Documento 038_ESPECIFICACIONES – Pagina 11

b. Especificaciones Técnicas Mínimas para equipos SD-WAN

Referencia 8:

Para los equipos del DATACENTER se deben tener en cuenta:

- Se espera obtener dos usuarios lectura capaces de soportar y generar investigaciones, búsquedas avanzadas, generación de reportes, monitoreo completo de los eventos de seguridad sin necesidad de contar con un tercero.
- Por otro lado, se espera obtener un usuario con permisos capaces de Administrar usuarios, configurar de políticas de seguridad, control de aplicaciones, administración de dispositivos, monitoreo y generación de informes con el fin de tener una administración compartida del firewall junto al oferente adjudicado del presente proyecto.
- El oferente que resulte adjudicado debe instalar, configurar e implementar los

De acuerdo con lo establecido en los requerimientos del proyecto, se menciona que se espera obtener un usuario con permisos para la administración compartida del firewall junto con el oferente adjudicado.

En este sentido, se solicita respetuosamente a la universidad precisar si la administración de las plataformas de seguridad contempladas en el proyecto SD-WAN deberá realizarse de manera compartida entre la universidad y el oferente. En caso afirmativo, agradeceríamos se indique el tiempo de dedicación esperado por parte del oferente para llevar a cabo dichas actividades, ya que este aspecto puede impactar directamente en incrementos presupuestales no contemplados en el proyecto.

Se propone a la universidad contemplar una bolsa de 150 horas para este tipo de actividades de administración, consultoría, afinamientos posteriores a la implementación.

RESPUESTA: La Universidad de Cundinamarca, ser permite aclarar que sí habrá administración compartida entre el proponente adjudicado y la Universidad, pero el alcance se encuentra limitado a las fases de implementación, capacitación y acompañamiento inicial. No se prevé la asignación de bolsas adicionales de horas, dado que estas actividades forman parte del servicio contratado y no implican costos adicionales, como se evidencia a

27. El CONTRATISTA deberá realizar una transferencia de conocimiento dirigida al personal designado por la Universidad, del área de servicios tecnológicos adscrita a la Dirección de Sistemas y Tecnología (hasta 10 participantes), que incluya la solución WAN propuesta, conceptos técnicos y mejores prácticas para la administración, configuración y operación de las herramientas de monitoreo, gestión y plataformas ofrecidas, incluyendo NGFW, SD-WAN, WAF y SIEM. Esta capacitación deberá permitir a los ingenieros conocer, gestionar y administrar la topología y los equipos involucrados, y podrá realizarse de forma virtual o presencial, según lo solicite la Universidad.

continuación en la obligación especifica del contratista No. 27.

OBSERVACIÓN 9:

7.8. FORMA DE PAGO

La Universidad de Cundinamarca pagará al contratista el valor del Contrato de la siguiente forma:

PAGOS	CONDICIÓN
Pagos mensuales de acuerdo con el servicio efectivamente prestado, previa verificación por parte de la supervisión. El pago final estará condicionado al Acta de Recibo a Satisfacción debidamente verificada por el supervisor.	Para cada pago se deberá anexar el informe de supervisión donde conste el cumplimiento total del objeto contractual.

Con el mayor respeto, solicitamos a la entidad reconsiderar la modalidad de pago estipulada en el pliego de condiciones. Proponemos una alternativa que permite el flujo financiero más equilibrado y garantiza la adecuada ejecución del contrato, alineados los pagos con los hitos más relevantes del proyecto de la siguiente manera:

- ***60%** al inicio del contrato y contra entrega de los equipos y suscripciones.*
- ***30%** durante la fase de avance medio del proyecto, coincidiendo con la implementación y puesta en marcha de las herramientas al servicio de la universidad.*
- ***10%** restante a la finalización y conformidad de este.*

Consideramos que esta modalidad de pago contribuye a la sostenibilidad financiera del proyecto y asegura la disponibilidad de los recursos necesarios para el cumplimiento oportuno y exitoso de los objetivos propuestos.

RESPUESTA: Universidad de Cundinamarca, en atención a la observación recibida, se permite aclarar que la forma de pago definida en los términos de la presente invitación publica responde a las disposiciones contractuales y financieras establecidas en la normatividad vigente de la Universidad para la contratación pública, que obligan a la entidad a realizar los pagos con base en la verificación del cumplimiento de las obligaciones contractuales y la disponibilidad presupuestal correspondiente.

En este sentido, no es posible acceder a la modificación planteada por el oferente respecto a establecer un pago anticipado del 50% contra entrega de equipos y licencias, ya que la

Universidad no puede realizar desembolsos parciales anticipados sin que medie la debida ejecución contractual y la verificación del cumplimiento.

Agradecemos el interés manifestado y la disposición del oferente para participar en esta convocatoria.

Cordialmente,

Firmado digitalmente por HURTADO MESA ANA LUCIA
Fecha: 2025.09.02 [illegible]

ANA LUCIA HURTADO MESA
Directora de Sistemas y Tecnología
Universidad de Cundinamarca

Proyectó: Ing. Jeniffer Castillo Fernández
Área de Servicios Tecnológicos

15-30.7

15.

Fusagasugá, 2025-09-02.

Señores
GAMMA INGENIEROS

Asunto y/ó Ref: Respuesta Observaciones Invitación Privada 038 de 2025

Cordial saludo,

De manera atenta, me dirijo a usted con el fin de dar respuesta a las observaciones allegadas en referencia a la Invitación Privada 038 de 2025, que tiene como objeto: ***"CONTRATAR EL SERVICIO DE SEGURIDAD PERIMETRAL Y CONFIGURACION DE CONECTIVIDAD MEDIANTE TECNOLOGÍA SD-WAN PARA LA UNIVERSIDAD DE CUNDINAMARCA".***

OBSERVACIONES:
GAMMA INGENIEROS

OBSERVACIÓN 1:

Observación 1: PAGINA 36 Documento 038_ESPECIFICACIONES

Certificaciones Exigidas al Proceso de SOC del Oferente
ISO27001: El oferente debe presentar junto con su propuesta el certificado ISO 27001 del 2022 o superior (SGSI) para su proceso de SOC y **este debe de tener al menos un (1) año de vigencia.**

Se solicita amablemente a la entidad modificar el requisito que actualmente establece que "El oferente debe presentar junto con su propuesta el certificado ISO 27001 del 2022 o superior (SGSI) para su proceso de SOC y este debe de tener al menos un (1) año de vigencia", de manera que quede redactado como:
"El proponente debe presentar junto con su propuesta el certificado ISO 27001:2013 o superior (SGSI) para su proceso de SOC y este debe de tener al menos un (1) año de vigencia".
La norma ISO/IEC 27001:2013 es plenamente válida a nivel internacional y continúa siendo reconocida por los organismos de acreditación y certificación. La versión 2022 es una actualización de la norma, pero no invalida la vigencia de los certificados 2013, los cuales conservan su reconocimiento dentro del período de transición definido por ISO.

RESPUESTA: La Universidad de Cundinamarca, en atención a la observación recibida, se permite aclarar que la exigencia de la certificación **ISO/IEC 27001:2022 o superior** se mantiene como requisito habilitante dentro del presente proceso.
Esta decisión responde a que la Universidad de Cundinamarca se encuentra actualmente en proceso de certificación institucional bajo la versión ISO/IEC 27001:2022, lo que implica la adopción de los controles, lineamientos y mejores prácticas más actualizadas en gestión de seguridad de la información. En ese sentido, exigir a los oferentes la misma versión garantiza que exista alineación entre los controles implementados por la Universidad y los servicios ofrecidos por el contratista, asegurando coherencia en la gestión del riesgo, interoperabilidad de procesos y una mayor solidez frente a auditorías de terceros y entes de control.
Por lo anterior no es viable aceptar versiones anteriores de la norma, aunque vigentes, podría generar brechas de cumplimiento entre los controles internos de la Universidad y los procesos ejecutados por el contratista, afectando la capacidad de respuesta frente a incidentes de seguridad y la estrategia de mejora continua institucional.

OBSERVACIÓN 2:

observación 2: PAGINA 40 Documento 038_ESPECIFICACIONES

10. PERFILES REQUERIDOS

RECURSO	FORMACION	POSTGRADO	CERTIFICACIONES	EXPERIENCIA	DEDICACION	FUNCIONES
Un (01) Ingeniero Gerente de Proyecto	Título Ingeniero Eléctrico, electrónico, sistemas, telecomunicación o carreras afines. Tarjeta Profesional con expedición mínimo de cinco (5) años	Posgrado en Gerencia de Proyectos y/o Certificación PMP.	Certificación Itil Foundation v3 o superior	Experiencia general de cinco (5) años en gerencia de proyectos de TI, de los cuales mínimo tres (3) años de experiencia especifica gerenciando y/o coordinando proyectos de seguridad informática. La experiencia se cuenta a partir de la expedición de la tarjeta profesional	100 % al proyecto, de requerirse de manera presencial o virtual en las instalaciones de la entidad	Definir los objetivos y los alcances del proyecto. Desarrollar un plan de trabajo detallado, estableciendo metas, cronograma, recursos. Identificar riesgos y establecer un plan de mitigación

Respetuosamente se solicita a la entidad ajustar este requisito, de manera que quede redactado como: "Experiencia general mínima de 5 proyectos como gerente de proyectos de TI, de los cuales al menos en 3 se hayan ejecutado en este último y se haya tenido participación en un 100% Exigir cinco (5) años de experiencia general limita de forma considerable la participación de oferentes y profesionales competentes, restringiendo la pluralidad de propuestas en el proceso.

RESPUESTA: La Universidad de Cundinamarca, ser permite indicar que el requisito de años mínimos de experiencia se mantiene, dado que este criterio permite verificar de manera objetiva y uniforme la trayectoria continua y comprobada del personal propuesto, garantizando así que el mismo cuenta con el conocimiento y la práctica acumulada

necesarios para asumir la complejidad del proyecto.

La experiencia acreditada en términos de proyectos ejecutados puede variar en alcance, tiempo de dedicación y responsabilidades asumidas, lo que dificulta que sea un indicador suficiente de idoneidad. En contraste, la exigencia en años de experiencia profesional asegura que la persona haya participado en diferentes etapas del ciclo de vida de proyectos de TI y/o seguridad informática, fortaleciendo la capacidad técnica y de gestión que requiere la Universidad para este proceso.

OBSERVACIÓN 3:

Observación 3: Pagina 39 Documento 038_ESPECIFICACIONES

9. LICENCIAMIENTO, ACTUALIZACIONES Y TRANSFERENCIA DE CONOCIMIENTO

- El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, VPNs equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.
- La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering debe proveerse por al menos un (1) años.
- La plataforma es requerida por un periodo de un (1) años en un esquema 7x24 ante el fabricante.
- Transferencia de conocimiento de la solución WAN propuesta, conceptos técnicos y mejores prácticas para la administración, configuración y funcionalidades de las herramientas de monitoreo,

gestión y plataforma de administración ofrecidos, configuración y funcionalidades del NGFW, SDWAN, WAF, SIEM dirigido al área de servicios tecnológicos adscrito a la Dirección de Sistemas y Tecnología.

Se solicita amablemente a la entidad confirmar si, además de la transferencia de conocimiento relacionada con el uso de las tecnologías adquiridas en el marco del proyecto, se requiere contemplar una bolsa de horas para la administración y/o gestión de las plataformas de seguridad. Esta precisión es fundamental con el fin de realizar un dimensionamiento adecuado del proyecto, ya que, de requerirse dicho esquema de soporte adicional, podría tener implicaciones en los costos de la propuesta.

RESPUESTA: La Universidad de Cundinamarca, ser permite aclarar que sí habrá administración compartida entre el proponente adjudicado y la Universidad, pero el alcance se encuentra limitado a las fases de implementación, capacitación y acompañamiento inicial. No se prevé la asignación de bolsas adicionales de horas, dado que estas actividades forman parte del servicio contratado y no implican costos adicionales, como se evidencia a

continuación en la obligación especifica del contratista No. 27.

27. El CONTRATISTA deberá realizar una transferencia de conocimiento dirigida al personal designado por la Universidad, del área de servicios tecnológicos adscrita a la Dirección de Sistemas y Tecnología (hasta 10 participantes), que incluya la solución WAN propuesta, conceptos técnicos y mejores prácticas para la administración, configuración y operación de las herramientas de monitoreo, gestión y plataformas ofrecidas, incluyendo NGFW, SD-WAN, WAF y SIEM. Esta capacitación deberá permitir a los ingenieros conocer, gestionar y administrar la topología y los equipos involucrados, y podrá realizarse de forma virtual o presencial, según lo solicite la Universidad.

OBSERVACIÓN 4:

Observación 4:

7.8. FORMA DE PAGO

La Universidad de Cundinamarca pagará al contratista el valor del Contrato de la siguiente forma:

PAGOS	CONDICIÓN
Pagos mensuales de acuerdo con el servicio efectivamente prestado, previa verificación por parte de la supervisión. El pago final estará condicionado al Acta de Recibo a Satisfacción debidamente verificada por el supervisor.	Para cada pago se deberá anexar el informe de supervisión donde conste el cumplimiento total del objeto contractual.

Se solicita respetuosamente a la entidad una modificación en la modalidad de pago originalmente estipulada como mensualizada. Recomendamos a la entidad una propuesta que contempla una distribución en pagos parciales, correspondientes al 50% al inicio del contrato y contra entrega de los equipos y suscripciones, 30% durante el avance medio del proyecto y la implementación y puesta en marcha de las herramientas al servicio de la universidad y el 20% restante a la finalización y conformidad del mismo.
Esta forma de pago debe ser evaluada en función de su impacto en la ejecución presupuestaria, la suficiencia financiera del proveedor y las garantías de cumplimiento del servicio, a fin de asegurar que no se vea comprometida la correcta prestación del objeto contractual.

RESPUESTA: La Universidad de Cundinamarca, en atención a la observación recibida, se permite aclarar que la forma de pago definida en los términos de la presente invitación publica responde a las disposiciones contractuales y financieras establecidas en la normatividad vigente de la Universidad para la contratación pública, que obligan a la entidad a realizar los pagos con base en la verificación del cumplimiento de las obligaciones contractuales y la disponibilidad presupuestal correspondiente.

En este sentido, no es posible acceder a la modificación planteada por el oferente respecto a establecer un pago anticipado del 50% contra entrega de equipos y licencias, ya que la

Universidad no puede realizar desembolsos parciales anticipados sin que medie la debida ejecución contractual y la verificación del cumplimiento.

Agradecemos el interés manifestado y la disposición del oferente para participar en esta convocatoria.

Cordialmente,

Firmado digitalmente por HURTADO MESA ANA LUCIA
Fecha: 2024.09.02 19:01:46 -05'00'

ANA LUCIA HURTADO MESA
Directora de Sistemas y Tecnología
Universidad de Cundinamarca

Proyectó: Ing. Jeniffer Castillo Fernández
Área de Servicios Tecnológicos

15-30.7

15.

Fusagasugá, 2025-09-04.

Señores
RAMTEK S.A.S

Asunto y/ó Ref: Respuesta Observaciones Invitación Privada 038 de 2025

Cordial saludo,

De manera atenta, me dirijo a usted con el fin de dar respuesta a las observaciones allegadas en referencia a la Invitación Privada 038 de 2025, que tiene como objeto: ***"CONTRATAR EL SERVICIO DE SEGURIDAD PERIMETRAL Y CONFIGURACION DE CONECTIVIDAD MEDIANTE TECNOLOGÍA SD-WAN PARA LA UNIVERSIDAD DE CUNDINAMARCA".***

OBSERVACIONES:
RAMTEK S.A.S

OBSERVACIÓN 1:

Nota Aclaratoria N°2: Todos los firewalls deben tener licenciamiento que incluya IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, soporte de fábrica. y orquestación central.

Se solicita amablemente a la entidad revisar y modificar el uso del término "Video Filtering", ya que corresponde específicamente a una funcionalidad propia del fabricante Fortinet, esto con el fin de garantizar la pluralidad de oferentes y evitar un posible direccionamiento hacia un proveedor en particular.

RESPUESTA: Atendiendo a la observación recibida, la Universidad de Cundinamarca acoge la observación realizada, toda vez que el término "Video Filtering" corresponde a una denominación propia del fabricante Fortinet, lo que podría interpretarse como una restricción de la pluralidad de oferentes.
El objetivo de la Universidad no es direccionar la contratación hacia un proveedor en particular, sino asegurar que la solución ofertada cumpla con la capacidad de gestionar, filtrar y controlar contenidos de video en el tráfico de red, con el fin de garantizar un uso eficiente del ancho de banda y la adecuada operación de aplicaciones críticas institucionales.
Por lo anterior se verá ajustado en la respectiva adenda del Anexo de Especificaciones

Técnicas Definitivas.

OBSERVACIÓN 2:

Observación 2:

ix. Identificación y control de aplicaciones: 5000+ firmas de aplicaciones, identificación del primer paquete, inspección profunda de paquetes, firmas de aplicaciones personalizadas, descifrado SSL, TLS1.3 con cifrados obligatorios e inspección profunda.
x. SD-WAN (control de tráfico con reconocimiento de aplicaciones): Políticas de aplicaciones granulares, selección de rutas basada en SLA de aplicaciones, medición dinámica del ancho de banda de rutas SD-WAN, reenvío activo/activo y activo/en espera, soporte de superposición para transporte cifrado, dirección basada en sesión de aplicaciones, mediciones de SLA basadas en sondas
xi. SD-WAN avanzada (corrección de WAN): Corrección de errores de reenvío (FEC) para la compensación de pérdida de paquetes, duplicación de paquetes para el mejor rendimiento de las aplicaciones en tiempo real, integración de Active Directory para políticas de dirección SD-WAN basadas en el usuario, agregación de enlaces por paquete con distribución de paquetes entre miembros agregados
xii. Implementación de SD-WAN: Implementación flexible hub-to-spoke (malla parcial), spoke-to-spoke (malla completa), multi-WAN.
xiii. Modelado del tráfico QoS basado en límites de ancho de banda por aplicación y enlace WAN, límites de velocidad por aplicación y enlace WAN, priorización del tráfico de aplicaciones por enlace WAN, marca/remarca bits DSCP para influir en la QoS del tráfico en dispositivos de salida, dirección de aplicaciones basada en el marcado ToS.
xiv. Enrutamiento avanzado (IPv4/IPv6): Enrutamiento estático, puerta de enlace interna (iBGP, OSPF v2/v3, RIP v2), puerta de enlace externa (eBGP), VRF, redistribución de rutas, fuga de rutas, confederación BGP, reflectores de enrutador, resumen y agregación de rutas, asimetría de rutas.
xv. VPN/Overlay: Site-to-site ADVPN - túneles VPN dinámicos, VPN basado en políticas, IKEv1, IKEv2, DPD, PFS, ESP y soporte ESPHMAC, Compatibilidad con cifrado simétrico (IKE/ES P): AES- 128 y AES-256 modos: CBC, CNTR, XCBC, GCM, Pre-shared and PKI authentication con certificados RSA, intercambio de claves.
xvi. Diffie-Hellman (Group 1, 2, 5, 14 through 21 and 27 through 32), MD5, y SHA-based HMAC.
xvii. Multicast: Multicast forwarding, PIM spare (rfc 4601), dense mode (rfc 3973), PIM rendezvous point.
xviii. Networking Avanzado: DHCP v4/v6, DNS, NAT - source, destino, NAT estático, destination NAT, PAT, NAPT, Soporte Full IPv4/v6.
xix. Seguridad On-premise: - Inspección SSL, control de aplicaciones, prevención de intrusiones, antivirus, filtrado web, DLP y protección avanzada contra amenazas. Segmentación: micro, macro, VDOM de una sola tarea, VDOM múltiple.

Solicitamos a la entidad revisar y ajustar los requerimientos técnicos establecidos, ya que las funcionalidades, términos y condiciones descritos corresponden a características específicas de la

marca Fortinet. Esto podría restringir la pluralidad de oferentes y afectar los principios de transparencia y selección objetiva en el proceso de contratación.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que los términos incluidos en el anexo técnico no buscan direccionar el proceso hacia un fabricante en particular, ya que las funcionalidades descritas corresponden a requerimientos de nivel de servicio y de capacidades técnicas mínimas que debe garantizar cualquier solución de seguridad perimetral y conectividad SD-WAN de última generación, independientemente de la marca.

Muchas de las características mencionadas, como inspección profunda de paquetes (DPI), identificación de aplicaciones, cifrado TLS 1.3, modelado de tráfico QoS, enrutamiento avanzado IPv4/IPv6, compatibilidad con estándares de seguridad AES, integración de VPNs dinámicas y segmentación lógica (micro, macro, VDOM), son funcionalidades estándar en los principales fabricantes de soluciones de seguridad perimetral y SD-WAN (Fortinet, Palo Alto, Cisco, Check Point, Sophos, entre otros).

Se reitera que las especificaciones fueron formuladas con base en estándares internacionales y mejores prácticas de ciberseguridad, con el objetivo de asegurar la continuidad del servicio, la resiliencia de la infraestructura tecnológica de la Universidad y el cumplimiento de niveles de disponibilidad exigidos (99.98%). En ese sentido, se mantiene la pluralidad de oferentes, en la medida en que varios fabricantes cumplen con los lineamientos solicitados.

OBSERVACIÓN 3:

Observación 3:

xv. VPN/Overlay: Site-to-site ADVPN - túneles VPN dinámicos, VPN basado en políticas, IKEv1, IKEv2, DPD, PFS, ESP y soporte ESPHMAC, Compatibilidad con cifrado simétrico (IKE/ES P): AES- 128 y AES-256 modos: CBC, CNTR, XCBC, GCM, Pre-shared and PKI authentication con certificados RSA, intercambio de claves.

Solicitamos amablemente a la entidad modificar o sustituir el término "Site-to-site ADVPN", ya que corresponde a una terminología propietaria y exclusiva del fabricante Fortinet. Esta especificación podría limitar la pluralidad de oferentes y restringir la participación de otros fabricantes que ofrecen funcionalidades equivalentes bajo denominaciones distintas, tales como túneles VPN dinámicos, VPN automatizada o Dynamic Mesh VPN. En este sentido, sugerimos reemplazar dicho término por una descripción más general que permita una mayor apertura en la participación.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que fue incluido con el

propósito de describir la funcionalidad requerida de VPN dinámicas que permitan establecer túneles automáticos, flexibles y de rápida recuperación ante fallas, lo cual constituye un requisito fundamental para garantizar la continuidad y estabilidad de la conectividad en los diferentes sitios de la Universidad de Cundinamarca.

Sin embargo, reconocemos que la denominación utilizada corresponde a un término propietario del fabricante Fortinet, lo cual podría dar lugar a interpretaciones restrictivas en relación con la pluralidad de oferentes.

Por lo anterior, se acoge la observación y se procederá a ajustar el texto eliminando la referencia exclusiva y reemplazándola por una descripción más amplia y neutral, el cual se verá ajustado en la respectiva adenda del Anexo de Especificaciones Técnicas Definitivas.

OBSERVACIÓN 4:

xix. Seguridad On-premise: - Inspección SSL, control de aplicaciones, prevención de intrusiones, antivirus, filtrado web, DLP y protección avanzada contra amenazas. Segmentación: micro, macro, VDOM de una sola tarea, VDOM múltiple.

Se solicita amablemente a la entidad revisar o ajustar este requerimiento, ya que la funcionalidad VDOM (Virtual Domains) es una característica propietaria y nativa de la marca Fortinet, lo cual podría limitar la pluralidad de oferentes. Se recomienda sustituir este requerimiento por una descripción funcional más general, como: "El dispositivo debe permitir la virtualización lógica de funciones o la segmentación independiente de políticas y administración de red".

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la intención de este requerimiento no es direccionar la contratación hacia un fabricante en particular, sino garantizar que la solución ofertada cuente con la capacidad de segmentar y virtualizar de forma lógica las funciones de seguridad, permitiendo la administración independiente de políticas, configuraciones y recursos de red dentro de un mismo dispositivo físico.

Por lo anterior, se acoge la observación y se procederá a ajustar el texto eliminando la referencia exclusiva y reemplazándola por una descripción más amplia y neutral, el cual se verá ajustado en la respectiva adenda del Anexo de Especificaciones Técnicas Definitivas.

OBSERVACIÓN 5:

Observación 5:

xi. SD-WAN avanzada (corrección de WAN): Corrección de errores de reenvío (FEC) para la compensación de pérdida de paquetes, duplicación de paquetes para el mejor rendimiento de las aplicaciones en tiempo real, integración de Active Directory para políticas de dirección SD-WAN basadas en el usuario, agregación de enlaces por paquete con distribución de paquetes entre miembros agregados

---

Se solicita amablemente a la entidad revisen este requisito técnico, dado que su redacción está directamente alineada con funcionalidades específicas del fabricante Fortinet, lo que podría limitar la pluralidad de oferentes y generar un direccionamiento técnico hacia una única marca.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que el requerimiento no busca direccionar la solución hacia un fabricante en específico, sino garantizar que la infraestructura de conectividad contratada cuente con capacidades técnicas avanzadas que permitan la corrección de errores, priorización de tráfico y manejo de enlaces de alta disponibilidad, aspectos que resultan críticos para la continuidad académica y administrativa de la Universidad.

La terminología utilizada responde a prácticas técnicas ampliamente conocidas en el sector, tales como Forward Error Correction (FEC), duplicación de paquetes, integración con sistemas de directorio y agregación de enlaces, funcionalidades que no son exclusivas de una sola marca y pueden encontrarse implementadas en diferentes soluciones del mercado.

Lo que se pretende con esta especificación es asegurar que los servicios de conectividad contratados puedan mantener la calidad de experiencia en aplicaciones críticas como videoconferencias, plataformas académicas, servicios en la nube, etc., incluso en escenarios de pérdida de paquetes o degradación de la red, lo que se traduce en continuidad del servicio educativo y estabilidad operativa. En ese sentido, se mantendrá la exigencia planteada, con la claridad de que corresponde a funcionalidades de nivel avanzado presentes en diversas soluciones de conectividad SD-WAN y no está limitado a un fabricante en particular.

OBSERVACIÓN 6:

xxii. La solución de SD-WAN debe figurar como líder en el cuadrante mágico de Garner para SD-WAN de 2024.

Respetuosamente se solicita a la entidad considerar la modificación del requisito que establece que "la solución de SD-WAN debe figurar como líder en el cuadrante mágico de Gartner para SD-WAN de 2024", dado que este criterio limita de manera significativa la pluralidad de oferentes, Gartner basa su cuadrante mágico en aspectos comerciales y de mercado, los cuales no necesariamente reflejan de

forma objetiva las capacidades técnicas reales de una solución.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que el criterio establecido en el pliego no busca direccionar la contratación hacia un fabricante en específico, sino garantizar que la solución ofertada haya sido reconocida por un ente evaluador independiente como una alternativa robusta, confiable y validada en el mercado internacional.

Por lo anterior se mantiene la exigencia de Gartner como mecanismo de aseguramiento de calidad, toda vez que la inclusión en el cuadrante mágico responde a criterios de innovación, visión de mercado, capacidad de ejecución, escalabilidad y respaldo comercial, elementos que son determinantes en una solución de la magnitud requerida por la Universidad.

Cabe aclarar que el cuadrante de Gartner para SD-WAN no incluye un único fabricante, sino múltiples oferentes reconocidos a nivel global (Cisco, Palo Alto, Fortinet, VMware, HPE Aruba, entre otros). Por lo tanto, la condición no restringe la pluralidad de participantes, sino que asegura que las soluciones ofertadas estén alineadas con las mejores prácticas internacionales. En este sentido, se mantendrá la exigencia de que la solución se encuentre catalogada como líder en el cuadrante mágico de Gartner 2024, en aras de proteger la inversión institucional y garantizar la calidad del servicio contratado.

OBSERVACIÓN 7:

Observación 7:

Rendimiento
El equipo deberá cumplir con las siguientes características mínimas de desempeño ya activas y funcionales:
• Rendimiento de Firewall 100 Gbps
• Rendimiento de IPS 12 Gbps
• Rendimiento de NGFW (FW + IPS + Control de Aplicaciones) 11 Gbps
• Rendimiento Proteccion de amenazas (FW + IPS + Control de Aplicaciones + AntiMalware) 10 Gbps
• Rendimiento IPSec VPN 50 Gbps
• Soporte de 7 Millones sesiones concurrentes
• Rendimiento de Inspección SSL 3 Gbps
• Soporte de 5000 usuarios VPN SSL concurrentes
• Rendimiento de VPN SSL 3 Gbps
Conectividad
El equipo deberá contar con las siguientes interfaces de conexión:
• 16 interfaces de 1 GE RJ45
• 8 interfaces de 1 GE SFP
• 4 interfaces de 10 GE SFP+. Cada equipo debe incluir dos (2) Transceivers 10GE SFP+ LC

Solicitamos amablemente a la entidad revisar y ajustar el requerimiento técnico, ya que estos términos, funcionalidades y condiciones corresponden a características propias de un fabricante específico, lo cual podría generar un direccionamiento técnico que limita la pluralidad de oferentes, transparencia y selección objetiva.

RESPUESTA: La Universidad de Cundinamarca se permite informar que después de revisar las características descritas, se concluye que los valores de rendimiento y características técnicas establecidas (Firewall, IPS, NGFW, protección de amenazas, VPN, inspección SSL, sesiones concurrentes e interfaces de conectividad) no corresponden a especificaciones exclusivas de un fabricante en particular. Estos parámetros fueron definidos con base en las necesidades actuales y proyectadas de la infraestructura de la Universidad, así como en referencias internacionales de buenas prácticas para dimensionamiento de equipos de seguridad perimetral.

El objetivo es garantizar un mínimo de desempeño y capacidad que asegure la continuidad de los servicios críticos institucionales, sin direccionar la solución hacia una marca específica. Por lo anterior la Universidad reitera que la redacción del Anexo de Especificaciones Técnicas permite la participación de múltiples fabricantes, siempre que los equipos ofertados cumplan con los parámetros mínimos de rendimiento definidos. No se exige la implementación de funcionalidades propietarias ni denominaciones exclusivas de una marca en particular.

En conclusión, los valores y funcionalidades solicitadas en este punto se mantienen sin modificaciones, al tratarse de requerimientos mínimos indispensables para la operación estable y segura de la red universitaria.

OBSERVACIÓN 8:

Observación 8:

Rendimiento
El equipo deberá cumplir con las siguientes características mínimas de desempeño ya activas y funcionales:
• Rendimiento de Firewall 35 Gbps
• Rendimiento de IPS 8 Gbps
• Rendimiento de NGFW (FW + IPS + Control de Aplicaciones) 7 Gbps
• Rendimiento Proteccion de amenazas (FW + IPS + Control de Aplicaciones + AntiMalware) 6 Gbps
• Rendimiento IPSec VPN 10 Gbps
• Soporte de 3 Millones sesiones concurrentes
• Rendimiento de Inspección SSL 3 Gbps
• Soporte de 500 usuarios VPN SSL concurrentes
• Rendimiento de VPN SSL 2 Gbps
Conectividad
El equipo deberá contar con las siguientes interfaces de conexión:
• 8 interfaces de 1 GE RJ45
• 2 interfaces de 10 GE SFP+. Cada equipo debe incluir un (1) Transceiver 10GE SFP+ LC

Solicitamos amablemente a la entidad revisar y ajustar el requerimiento técnico, ya que estos términos, funcionalidades y condiciones corresponden a características propias de un fabricante específico, lo cual podría generar un direccionamiento técnico que limita la pluralidad de oferentes, transparencia y selección objetiva.

RESPUESTA: La Universidad de Cundinamarca agradece la observación presentada frente a los requerimientos técnicos definidos en el numeral correspondiente.

Es importante aclarar que las especificaciones incluidas en el apartado de Rendimiento y Conectividad fueron establecidas con el objetivo de garantizar niveles mínimos de desempeño y disponibilidad que aseguren la continuidad de los servicios críticos de la Universidad, en coherencia con las necesidades actuales y la proyección de crecimiento institucional.

Sin embargo, entendemos la inquietud planteada respecto a que algunos de los términos descritos puedan asociarse a características de fabricantes específicos, lo cual podría generar una percepción de direccionamiento. En ese sentido, la Universidad precisa que:

- Criterio de desempeño mínimo: Los valores de rendimiento (Firewall, IPS, NGFW, VPN, SSL, sesiones concurrentes, entre otros) son parámetros de referencia de desempeño mínimo que deben cumplir los equipos a ofertar, independientemente de la marca o fabricante. Estos no corresponden a una única tecnología propietaria, sino a estándares de mercado que cualquier fabricante de soluciones de seguridad perimetral y conectividad de nivel empresarial puede cumplir.
- Pluralidad de oferentes: Para garantizar la pluralidad y libre concurrencia, se evaluarán soluciones de diferentes fabricantes siempre que estas cumplan con los umbrales mínimos definidos. Los oferentes podrán acreditar con fichas técnicas oficiales del fabricante que sus equipos cumplen o superan dichos requerimientos.
- Transparencia y selección objetiva: Con este enfoque, se reitera que no se limita la participación a un fabricante específico, sino que se busca asegurar que la solución implementada tenga la capacidad técnica suficiente para soportar la infraestructura crítica de la Universidad.

En conclusión, se mantiene el requerimiento técnico como un criterio de desempeño mínimo y no como una condición exclusiva de un proveedor en particular.

OBSERVACIÓN 9:

Se solicita amablemente a la entidad revisar y modificar los términos, ya que corresponden específicamente al fabricante Fortinet con el fin de garantizar la pluralidad de oferentes y evitar el direccionamiento hacia un proveedor específico.

Observación 9:

Rendimiento
El equipo deberá cumplir con las siguientes características mínimas de desempeño ya activas y funcionales:
• Rendimiento de Firewall 25 Gbps
• Rendimiento de IPS 5 Gbps
• Rendimiento de NGFW (FW + IPS + Control de Aplicaciones) 3 Gbps
• Rendimiento Proteccion de amenazas (FW + IPS + Control de Aplicaciones + AntiMalware) 2.5 Gbps
• Rendimiento IPSec VPN 10 Gbps
• Soporte de 2 Millones sesiones concurrentes
• Rendimiento de Inspección SSL 1 Gbps
• Soporte de 200 usuarios VPN SSL concurrentes
• Rendimiento de VPN SSL 1 Gbps
Conectividad
El equipo deberá contar con las siguientes interfaces de conexión:
• 16 interfaces de 1 GE RJ45
• 2 interfaces de 10 GE SFP+. Cada equipo debe incluir un (1) Transceiver 10GE SFP+ LC

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la intención de los valores y características mínimas publicadas en el anexo técnico no es direccionar el proceso hacia un fabricante en particular, sino establecer parámetros de referencia que garanticen que la solución a implementar cuente con la robustez, confiabilidad y desempeño requerido para soportar el servicio de seguridad perimetral y la conectividad bajo tecnología SD-WAN.

En consecuencia, los oferentes podrán proponer soluciones equivalentes que cumplan como mínimo los niveles de rendimiento solicitados (firewall, IPS, VPN, inspección SSL, usuarios concurrentes, interfaces de conectividad, entre otros), siempre y cuando garanticen la prestación adecuada del servicio y los objetivos técnicos definidos en el pliego de condiciones.

OBSERVACIÓN 10:

El dispositivo debe contar con tecnología ASIC para permitir acelerar los procesos (no solo por CPU) y de esta manera permita mejorar el rendimiento del procesamiento de trafico
La solución deberá pertenecer al cuadrante de líder de Gartner para su última edición de Network Firewall
La solución deberá estar calificada como recomendada en el SVM de firewall de NSS LABS

Se solicita amablemente a la entidad revisar y modificar los términos, ya que corresponden específicamente al fabricante Fortinet con el fin de garantizar la pluralidad de oferentes y evitar el

direccionamiento hacia un proveedor específico.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la intención de este requerimiento no es direccionar la contratación hacia un fabricante en particular, sino garantizar que la solución ofertada cuente con mecanismos de aceleración a nivel de hardware (por ejemplo, ASIC, NPU, FPGA u otros procesadores dedicados) que permitan:

- Optimizar el rendimiento en el procesamiento de tráfico de red.
- Asegurar que las funciones de firewall, inspección de contenido y servicios de seguridad no dependan únicamente del CPU general.
- Mantener baja latencia y alto desempeño incluso con servicios de inspección profunda de paquetes (DPI), cifrado/descifrado SSL/TLS y prevención de intrusiones (IPS) habilitados.

Por lo anterior, se acoge la observación y se procederá a ajustar el texto eliminando la referencia exclusiva y reemplazándola por una descripción más amplia y neutral, el cual se verá ajustado en la respectiva adenda del Anexo de Especificaciones Técnicas Definitivas.

OBSERVACIÓN 11:

Debe tener la capacidad de generar una advertencia al administrador cuando este configure una política duplicada

Se solicita amablemente a la entidad revisar y modificar los términos, ya que corresponden específicamente al fabricante Fortinet con el fin de garantizar la pluralidad de oferentes y evitar el direccionamiento hacia un proveedor específico.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la intención de este requerimiento es establecer un mecanismo que permita prevenir errores de configuración, evitando la duplicidad de reglas o políticas que puedan afectar la administración y el desempeño de la solución. No obstante, entendiendo que la redacción actual puede asociarse a una funcionalidad propia de un fabricante en específico, con el fin de garantizar la pluralidad de oferentes y la selección objetiva, se ajustará el requerimiento bajo un enfoque más general.

Por lo anterior, se acoge la observación y se procederá a ajustar el texto eliminando la referencia exclusiva y reemplazándola por una descripción más amplia y neutral, el cual se verá ajustado en la respectiva adenda del Anexo de Especificaciones Técnicas Definitivas.

OBSERVACIÓN 12:

La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP

Se solicita amablemente a la entidad considerar reformular este requerimiento para aceptar mecanismos de captura de paquetes que, aunque no estén ligados explícitamente a una política de seguridad, permitan la identificación del tráfico asociado a las mismas. Esto con el fin de evitar favorecer a un único fabricante y así promover la libre concurrencia y pluralidad de oferentes.

RESPUESTA: La Universidad de Cundinamarca se permite informar que la intención del requerimiento no es direccionar hacia un fabricante específico, sino garantizar que la Universidad de Cundinamarca pueda contar con una herramienta que permita realizar análisis forense de red cuando se presenten incidentes de seguridad. Para ello, es indispensable que la solución ofrezca la posibilidad de capturar y exportar tráfico en un formato estándar e interoperable como lo es PCAP, ampliamente reconocido en la industria.

No obstante, acogemos la observación en cuanto a la redacción, por lo que se ajustará para evitar restricciones a la pluralidad de oferentes. En lugar de exigir estrictamente que la captura esté ligada a una política de seguridad puntual,

Por lo anterior, se acoge la observación y se procederá a ajustar el texto eliminando la referencia exclusiva y reemplazándola por una descripción más amplia y neutral, el cual se verá ajustado en la respectiva adenda del Anexo de Especificaciones Técnicas Definitivas.

OBSERVACIÓN 13:

Observación 13:

Soporte a ruteo dinámico RIP V1, V2, OSPF y BGP

Respetuosamente solicitamos a la entidad revisar este requisito, ya que la exigencia simultánea de los protocolos RIP v1, RIP v2, OSPF y BGP podría limitar la participación de fabricantes lo que puede afectar la pluralidad de los oferentes.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que este requerimiento se ha establecido con el fin de garantizar la interoperabilidad y flexibilidad de la solución de seguridad perimetral y conectividad en diferentes escenarios de integración de red, especialmente en entornos donde conviven múltiples tecnologías y versiones de protocolos.

No obstante, entendemos que la exigencia explícita y simultánea de RIP v1 y RIP v2 puede percibirse como una condición restrictiva para algunos fabricantes. En este sentido, precisando el alcance, se aclara que lo que se requiere es que la solución ofertada cuente con compatibilidad con protocolos de enrutamiento dinámico estándar de la industria (OSPF y BGP como principales, y RIP v2 cuando aplique), de forma que se garantice la conectividad y enrutamiento entre las diferentes sedes y con las soluciones actualmente desplegadas.

Por lo anterior, se acoge la observación y se procederá a ajustar el texto eliminando la

referencia exclusiva y reemplazándola por una descripción más amplia y neutral, el cual se verá ajustado en la respectiva adenda del Anexo de Especificaciones Técnicas Definitivas.

OBSERVACIÓN 14:

El módulo de antimalware debe haber sido desarrollado por el mismo fabricante de la solución de firewall, así como las firmas deberán ser de su propiedad y no por medio de licenciamiento o concesiones de un tercero, esto con el fin de garantizar la idoneidad de la protección, así como los tiempos de respuesta del soporte de la misma.

Se solicita amablemente a la entidad modificar o eliminar el requisito que exige que el módulo de antimalware y sus firmas sean desarrollados exclusivamente por el mismo fabricante del firewall, ya que este criterio es propio del fabricante Fortinet, limitando la pluralidad de oferentes.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que no es exclusivo de un único fabricante el desarrollo del módulo de antimalware y la generación de sus propias firmas. Existen diferentes proveedores de soluciones de firewall de nueva generación que cuentan con laboratorios propios y motores de protección desarrollados directamente por ellos (ej. Cisco Talos, SophosLabs, Check Point ThreatCloud, Palo Alto WildFire, entre otros).

En este sentido, el requisito establecido no limita la pluralidad de oferentes, ya que varios fabricantes reconocidos cumplen con la condición de disponer de tecnología y firmas de seguridad propias, sin depender de terceros.

OBSERVACIÓN 15:

El Antivirus deberá integrarse de forma nativa con una solución sandbox del mismo fabricante, de tal manera que envíen muestras de archivos a dicho dispositivo para su análisis.

Se solicita amablemente a la entidad revisar el requerimiento que establece que "el antivirus debe integrarse de forma nativa con una solución sandbox del mismo fabricante", ya que esto es nativo de Fortinet lo que podría limitar la participación de otras marcas restringiendo la pluralidad de oferentes. Se sugiere plantear el requerimiento como funcional, permitiendo integración efectiva con soluciones de sandboxing sin exigir que ambas provengan del mismo fabricante.

RESPUESTA: Atendiendo a la observación recibida, la Universidad de Cundinamarca acoge la observación realizada, toda vez que el término integrarse de forma nativa con una solución sandbox se interpreta como una restricción de pluralidad de oferentes.

El objetivo de la Universidad no es direccionar la contratación hacia un proveedor en particular, sino asegurar que la solución ofertada cumpla con la capacidad de gestionar, filtrar y controlar contenidos. Por lo anterior se verá ajustado en la respectiva adenda del Anexo de Especificaciones Técnicas Definitivas.

OBSERVACIÓN 16:

Debe contar con la capacidad de bloquear contenido de youtube usando el Channel ID

Se solicita amablemente a la entidad revisar y modificar los términos, ya que corresponden específicamente al fabricante Fortinet con el fin de garantizar la pluralidad de oferentes y evitar el direccionamiento hacia un proveedor específico.

RESPUESTA: Atendiendo a la observación recibida, la Universidad de Cundinamarca se acoge la observación realizada, toda vez que el término bloque de contenidos usando Channel ID se interpreta como una restricción de pluralidad de oferentes.

El objetivo de la Universidad no es direccionar la contratación hacia un proveedor en particular, sino asegurar que la solución ofertada cumpla con la capacidad de gestionar, filtrar y controlar contenidos. Por lo anterior se verá ajustado en la respectiva adenda del Anexo de Especificaciones Técnicas Definitivas.

OBSERVACIÓN 17:

El sistema de detección y prevención de intrusos deberá estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, La interfaz de administración del sistema de detección y prevención de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola
para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso.

Se solicita amablemente a la entidad revisar el requerimiento que establece que el sistema de detección y prevención de intrusos (IPS) debe estar completamente integrado al "appliance", sin requerir componentes externos, ya que esta condición corresponde a la arquitectura de un único fabricante (Fortinet). Esta especificación limita la pluralidad de oferentes, por lo que se recomienda formular el requerimiento como funcional, permitiendo distintas formas de integración de IPS dentro del firewall.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que no es exclusivo de un único fabricante que el sistema de detección y prevención de intrusos (IPS) debe estar completamente integrado al appliance. Existen diferentes proveedores de soluciones de firewall de nueva generación que cuentan con laboratorios propios y motores de protección desarrollados directamente por ellos (ej. SophosLabs, Check Point ThreatCloud, WildFire, entre otros).

En este sentido, el requisito establecido no limita la pluralidad de oferentes, ya que varios fabricantes reconocidos cumplen con la condición de disponer de tecnología sin depender de terceros.

OBSERVACIÓN 18:

Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque, así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP.

Se solicita amablemente a la entidad revisar y modificar los términos, ya que corresponden específicamente al fabricante Fortinet con el fin de garantizar la pluralidad de oferentes y evitar el direccionamiento hacia un proveedor específico.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la especificación relacionada con la posibilidad de almacenar información del paquete que detonó la detección del ataque y al menos los 5 paquetes sucesivos, así como su visualización en formato PCAP, no hace referencia a un fabricante específico. El formato PCAP constituye un estándar abierto y ampliamente soportado en la industria de seguridad y redes, compatible con diversas herramientas y soluciones, por lo que no limita la pluralidad de oferentes. es importante resaltar que la Funcionalidad de captura de paquetes (packet capture en IPS/IDS) la mayoría de las fabricantes de firewalls/IDS/IPS (Fortinet, Cisco, Palo Alto, Sophos, Check Point) permiten generar capturas de paquetes en formato PCAP para análisis forense.

OBSERVACIÓN 19:

Debe ser posible inspeccionar aplicaciones tipo Cloud como dropbox, icloud entre otras entregando información como login de usuarios y transferencia de archivos.

Se solicita amablemente a la entidad revisar este requerimiento, ya que describe una funcionalidad propia de Fortinet, lo cual limita la pluralidad de oferentes. Se sugiere expresar el requisito en términos funcionales.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la especificación relacionada con la posibilidad de inspeccionar aplicaciones tipo Cloud como dropbox, icloud entre otras entregando información como login de usuarios y transferencia de archivos, no hace referencia a un fabricante específico.
Pues esta característica la ofrecen fabricantes como Palo AltoNetworks, Fortinet, Cisco (con Firepower/Umbrella), Check Point y Sophos, esto confirma que no es un estándar de la industria, sino una funcionalidad avanzada que solo algunos fabricantes líderes implementan de forma nativa.

OBSERVACIÓN 20:

De las aplicaciones Cloud como Dropbox que permiten compartir archivos, debe ser posible ver que archivos fueron subidos y descargados por los usuarios.

Se solicita amablemente a la entidad revisar el requerimiento dado que este nivel de visibilidad

específica es una funcionalidad propia de la solución Fortinet, lo cual podría limitar la pluralidad de oferentes. Se sugiere reformular el requerimiento de forma más amplia o permitir el cumplimiento por medios equivalentes.

RESPUESTA: La Universidad de Cundinamarca acoge la observación, se realizará el ajuste por lo cual la solución deberá permitir la inspección de tráfico de aplicaciones en la nube (por ejemplo, servicios de almacenamiento o sincronización de archivos), de forma que sea posible identificar usuario y/o actividad de transferencia de archivos (upload/download), garantizando administración, auditoría y detección sin depender de una implementación específica de un proveedor.

Por lo tanto, los ajustes se verán reflejados en el Anexo Técnico de Especificaciones Definitivas.

OBSERVACIÓN 21:

El licenciamiento debe incluir servicios de IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, y soporte de fábrica durante la vigencia del contrato.

Se solicita amablemente a la entidad revisar y modificar el uso del término "Video Filtering", ya que corresponde específicamente al fabricante Fortinet con el fin de garantizar la pluralidad de oferentes y evitar el direccionamiento hacia un proveedor.

RESPUESTA: Atendiendo a la observación recibida, la Universidad de Cundinamarca acoge la observación realizada, toda vez que el término "Video Filtering" corresponde a una denominación propia del fabricante Fortinet, lo que podría interpretarse como una restricción de la pluralidad de oferentes.

El objetivo de la Universidad no es direccionar la contratación hacia un proveedor en particular, sino asegurar que la solución ofertada cumpla con la capacidad de gestionar, filtrar y controlar contenidos de video en el tráfico de red, con el fin de garantizar un uso eficiente del ancho de banda y la adecuada operación de aplicaciones críticas institucionales.

Por lo anterior se verá ajustado en la respectiva adenda del Anexo de Especificaciones Técnicas Definitivas.

OBSERVACIÓN 22:

La solución debe poder restaurar los portales web de forma automática en caso de presentarse una modificación no autorizada.
La plataforma propuesta debe identificar vulnerabilidades a un número ilimitado de aplicativa web de la , sin requerir licenciamiento adicional.

Se solicita amablemente a la entidad revisar y modificar los términos, ya que corresponden

específicamente al fabricante Fortinet con el fin de garantizar la pluralidad de oferentes y evitar el direccionamiento hacia un proveedor específico.

RESPUESTA: La Universidad de Cundinamarca acoge la observación y se realizarán los ajustes pertinentes:

1. Sobre la restauración automática de portales web ante modificaciones no autorizadas:
   El requerimiento se reformulará en términos funcionales, indicando que la solución debe contar con mecanismos de protección y recuperación ante alteraciones no autorizadas en aplicaciones o portales web, sin limitar la forma en que cada fabricante implementa esta funcionalidad.
2. Sobre la identificación de vulnerabilidades en aplicativos webs:
   Se modificará el requisito para que la solución proporcione herramientas de análisis de vulnerabilidades en aplicaciones web, sin imponer la condición de número ilimitado ni excluir la posibilidad de licenciamiento adicional. Se priorizará la funcionalidad de detectar y reportar vulnerabilidades relevantes para la seguridad de los aplicativos de la entidad.
   Por lo tanto, los ajustes se verán reflejados en el Anexo Técnico de Especificaciones Definitivas.

OBSERVACIÓN 23:

La solución debe contar con características de Machine Learning.

Se solicita amablemente a la entidad revisar esta característica ya que corresponden específicamente al fabricante Fortinet, con el fin de garantizar la pluralidad de oferentes y evitar el direccionamiento hacia un proveedor específico.

RESPUESTA: La Universidad de Cundinamarca acoge la observación y procederá a revisar y modificar el requerimiento señalado. El mismo será reformulado en términos funcionales, de manera que se garantice el cumplimiento de la necesidad técnica de la entidad, pero sin restringir la participación a un fabricante específico.
Por lo tanto, los ajustes se verán reflejados en el Anexo Técnico de Especificaciones Definitivas.

OBSERVACIÓN 24:

La solución debe contar con características de Machine Learning.

Se solicita respetuosamente modificar o eliminar esta característica, ya que el uso de Machine Learning para la detección de amenazas y análisis del tráfico es propio y nativo Fortinet, incluir este requerimiento de manera específica puede restringir la participación de otros fabricantes, lo cual podría limitar la pluralidad de oferentes.

RESPUESTA: La Universidad de Cundinamarca acoge la observación y procederá a modificar el requerimiento. En lugar de exigir de manera explícita el uso de Machine Learning como mecanismo de detección de amenazas y análisis de tráfico, se reformulará el criterio en términos funcionales, señalando que la solución debe incorporar mecanismos avanzados de detección y análisis de amenazas que garanticen la protección, sin restringir la tecnología a una implementación propia de un fabricante específico.

Por lo tanto, los ajustes se verán reflejados en el Anexo Técnico de Especificaciones Definitivas.

OBSERVACIÓN 25:

Debe incorporar funcionalidad de Sandbox Cloud

Se solicita amablemente a la entidad modificar o eliminar esta característica, ya que la funcionalidad de Sandbox Cloud es propio y nativo Fortinet, incluir este requerimiento de manera específica puede restringir la participación de otros fabricantes, lo cual podría limitar la pluralidad de oferentes.

RESPUESTA: La Universidad de Cundinamarca acoge la observación y procederá a modificar el requerimiento. En lugar de exigir de manera específica la funcionalidad de Sandbox Cloud propia de un fabricante, se reformulará el criterio en términos funcionales, estableciendo que la solución debe permitir mecanismos de análisis avanzado de archivos y amenazas en entornos aislados (sandboxing), ya sea de forma local o en la nube, garantizando así la detección y prevención frente a amenazas de día cero.

Por lo tanto, los ajustes se verán reflejados en el Anexo Técnico de Especificaciones Definitivas.

OBSERVACIÓN 26:

La solución de Web Application Firewall debe tener la capacidad de enviarle las IP detectadas como maliciosas sean informadas y sea adicionada automáticamente a un grupo de direcciones IPs para que puedan ser utilizadas en las políticas de la plataforma de NGFW.

Se solicita amablemente a la entidad revisar y modificar los términos, ya que corresponden específicamente al fabricante Fortinet con el fin de garantizar la pluralidad de oferentes y evitar el direccionamiento hacia un proveedor específico.

RESPUESTA: La Universidad de Cundinamarca no acoge la observación, toda vez que cualquier marca está en la capacidad de ofrecer el módulo antimalware, en la reportaría cada fabricante es libre de realizar las advertencias de acuerdo con su ficha técnica de manera se garantiza la protección e idoneidad de la solución ofrecida.
Por lo tanto, los ajustes se verán reflejados en el Anexo Técnico de Especificaciones

Definitivas.

OBSERVACIÓN 27:

La solución debe integrar firmas de amenazas y ataques conocidos y deberá proteger de ataques nuevos o de día cero actualizándose durante el tiempo de la garantía.
Cross-Site Scripting (XSS)
SQL Injection
Remote File Inclusión
Local File Inclusión
OS Commands
Troyanos y virus
Exploits
Información Sensible del servidor
Fujas de Información
Firmas personalizadas
Con esto la herramienta debe ser capaz de proteger de las siguientes amenazas:
- Adobe Flash Binary (AMF) protocol Attack.
- Botnet
- Browser Exploit Against SSL /TLS
- Clickjacking
- Cookie Tampering
- Credit Card Theft
- Cross Site request forgery
- Cross site Scripting
- DoS
- HTTP Header Overflow
- Local File Inclusion
- Malicious Robots
- Man in the Middle
- Remote File Inclusion
- Server information leakage
- SQL Injection
- Malformed XML

solicitamos a la entidad revisar y ajustar los requerimientos técnicos establecidos, ya que las funcionalidades, términos y condiciones descritos corresponden a características específicas de la marca Fortinet. Esto podría restringir la pluralidad de oferentes y afectar los principios de transparencia y selección objetiva en el proceso de contratación.

RESPUESTA: La Universidad de Cundinamarca agradece su observación y su compromiso con los principios de transparencia y pluralidad en la contratación pública.

Hemos revisado los requerimientos técnicos y coincidimos en que la redacción actual, al emplear términos y funcionalidades que son reconocidos por estar asociados a un

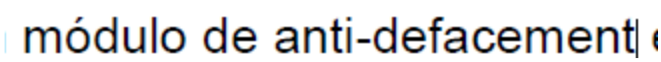
fabricante específico, estamos seguros que queremos de la participación de otras soluciones equivalentes y de alta calidad en el mercado.

En aras de garantizar una competencia justa, se ha decidido aclrar y ajustar la terminología de los pliegos de condiciones. El objetivo es describir las funcionalidades de seguridad que la entidad necesita, utilizando un lenguaje más genérico y estandarizado en la industria. Esto permitirá a todos los oferentes presentar soluciones que cumplan con los objetivos de protección de amenazas sin ser excluidos por la nomenclatura específica de un producto.
El nuevo enfoque se centrará en los siguientes puntos:

- Protección contra Amenazas Web: En lugar de enumerar ataques con términos específicos, se solicitará que la solución sea capaz de mitigar las vulnerabilidades de seguridad web más comunes, como la inyección de código (Cross-site Scripting, SQL Injection) y la inclusión de archivos (Local/Remote File Inclusion).
- Mitigación de Vulnerabilidades Específicas: Se requerirá la capacidad de protección contra ataques de día cero y exploits conocidos, así como la prevención de fugas de información y la defensa contra bots maliciosos, ataques DoS/DDoS, y vulnerabilidades del protocolo web como HTTP Header Overflow.
- Defensa contra Amenazas de la Capa de Aplicación: Se exigirá la funcionalidad para proteger contra ataques como Cookie Tampering y falsificación de solicitudes entre sitios (CSRF), enfocándonos en la capacidad de la herramienta para asegurar la capa de aplicación.

Estas modificaciones buscan asegurar que la solución adjudicada cumpla con todos los requerimientos de seguridad necesarios, al mismo tiempo que se fomenta la libre concurrencia de oferentes, garantizando así la selección de la mejor propuesta disponible en el mercado.
Por lo tanto, los ajustes se verán reflejados en el Anexo Técnico de Especificaciones Definitivas.

OBSERVACIÓN 28:



Se solicita amablemente a la entidad modificar el término "módulo de antidefacement" está ligado principalmente a Fortinet, por lo que incluirlo textualmente en un pliego puede limitar la participación de otros fabricantes.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la inclusión de un módulo de Protección contra Web Defacement en la solución de seguridad propuesta ofrece un valor agregado significativo para la Universidad, ya que permite reforzar la estrategia de defensa en profundidad en el ámbito de las aplicaciones web. Este tipo de controles no solo se centra en detener ataques en tránsito (funcionalidad propia de un WAF), sino que amplía la cobertura hacia la integridad del contenido y la continuidad del servicio, aspectos fundamentales en el contexto de una institución académica que gestiona información pública

de interés para estudiantes, docentes, investigadores y comunidad en general.
Al asegurar la detección inmediata de modificaciones no autorizadas y habilitar la capacidad de restauración automática, se logra reducir drásticamente el tiempo de exposición frente a incidentes que pueden afectar la reputación institucional, la confianza de los usuarios y la veracidad de la información publicada.

El requerimiento de que el módulo opere sin agentes adicionales también aporta ventajas prácticas en términos de eficiencia operativa, reducción de la carga en servidores, facilidad de despliegue y compatibilidad con entornos heterogéneos, al basarse en protocolos estándar como FTP, SSH o SMB.

OBSERVACIÓN 29:

MACHINE LEARNING
La solución deberá contar con la funcionalidad de auto aprendizaje de aplicaciones, la cual permita crear una línea base del comportamiento de la aplicación para creación de diferentes políticas de protección de un número ilimitado de aplicaciones web.

Se solicita respetuosamente modificar o eliminar esta característica, ya que el uso de Machine Learning para la detección de amenazas y análisis del tráfico es propio y nativo Fortinet, incluir este requerimiento de manera específica puede restringir la participación de otros fabricantes, lo cual podría limitar la pluralidad de oferentes.

RESPUESTA: La Universidad de Cundinamarca acoge la observación y procederá a modificar el requerimiento. En lugar de exigir de manera explícita el uso de Machine Learning como mecanismo de detección de amenazas y análisis de tráfico, se reformulará el criterio en términos funcionales, señalando que la solución debe incorporar mecanismos avanzados de detección y análisis de amenazas que garanticen la protección, sin restringir la tecnología a una implementación propia de un fabricante específico.

Por lo tanto, los ajustes se verán reflejados en el Anexo Técnico de Especificaciones Definitivas.

OBSERVACIÓN 30:

ANTIMALWARE
La solución deberá contar con un módulo de escaneo AntiMalware para hacer una revisión de los archivos que sean posteados o subidos a las aplicaciones web, permitiendo ejecutar Detección y bloqueo de malware conocido a nivel de los archivos que se suben a las aplicaciones web.

Respetuosamente se solicita a la entidad revisar esta especificación, ya que corresponde a una funcionalidad propietaria de Fortinet, lo cual podría limitar la participación de soluciones equivalentes de otros fabricantes. Se sugiere considerar una redacción más abierta que permita el cumplimiento mediante mecanismos con funcionalidades similares, garantizando así los principios de libre concurrencia y pluralidad de oferentes.

RESPUESTA: La Universidad de Cundinamarca no acoge la observación ya que cualquier marca está en la capacidad de ofrecer el módulo antimalware de manera se garantiza la protección e idoneidad de la solución ofrecida.

OBSERVACIÓN 31:

PROTECCION DE FUGA DE INFORMACION
La solución debe contar con un módulo para la prevención de fuga de información, la cual permite crear reglas personalizadas basadas en patrones, este módulo deberá ser completamente funcional sin requerir licencias adicionales o integraciones con plataformas de terceros.

Se solicita amablemente a la entidad modificar la forma en que se está redactando el requisito ya que esta condición puede limitar la participación de fabricantes con soluciones DLP. Se sugiere modificar el requerimiento para permitir la presentación de soluciones equivalentes que cumplan con la funcionalidad solicitada, sin restringir la libre concurrencia.

RESPUESTA: La Universidad de Cundinamarca acoge la observación y procederá a modificar el requerimiento. En lugar de exigir de manera explícita donde el módulo para la prevención de fuga de la información deberá habilitarse mediante licenciamiento de seguridad, siempre que se garantice su operación completa sin necesidad de adquirir o integrar plataformas de terceros ajenos al fabricante de la solución; se reformulará el criterio en términos funcionales, sin restringir la tecnología a una implementación propia de un fabricante específico.

Por lo tanto, los ajustes se verán reflejados en el Anexo Técnico de Especificaciones Definitivas.

OBSERVACIÓN 32:

La solución debe permitir la creación de reglas de autenticación, dichas reglas de autenticación deberán permitir:
Autenticación por medio de LDAP o Radius.
Autenticación de doble factor por medio de Token.
(SSO) Single Sign-On para portales tales como OWA, SharePoint, etc.

Se solicita a la entidad revisar y ajustar los requerimientos técnicos, ya que estos términos, funcionalidades y condiciones corresponden a características propias de Fortinet, lo cual podría limitar la pluralidad de oferentes.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que las funcionalidades descritas en la especificación no son exclusivas de un único fabricante. La autenticación mediante protocolos estándar como LDAP o RADIUS, la implementación de doble factor de autenticación a través de tokens, así como la integración con servicios de Single Sign-On (SSO) para aplicaciones como OWA o SharePoint, son características ampliamente soportadas por los principales fabricantes de soluciones de seguridad perimetral (Fortinet, Palo Alto Networks, Check Point, Sophos, Cisco, entre otros).
En este sentido, el requisito puede ser cumplido por múltiples marcas del mercado, garantizando la pluralidad de oferentes.

OBSERVACIÓN 33:

La solución debe tener la capacidad de validar el protocolo HTTP, haciendo una revisión como mínimo de los siguientes parámetros:	
-	Hostname.
-	Versión Http.
-	Método del Request.
-	Tamaño del Request.
-	Tamaño del Contenido.
-	Tamaño del Body.
-	Tamaño del Header.
-	Numero de Cookies en el request.
-	Numero de Parámetros en la URL.

Solicitamos amablemente a la entidad revisar y ajustar los requerimientos técnicos, ya que estos términos, funcionalidades y condiciones corresponden a características propias de Fortinet, lo cual podría limitar la pluralidad de oferentes, transparencia y selección objetiva.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que las especificaciones solicitadas no son exclusivas de un único fabricante. La validación del *protocolo HTTP a nivel de parámetros como hostname, versión, método de request, tamaño del request, tamaño del contenido, body, header, número de cookies y número de parámetros en la URL corresponde a funcionalidades estándar de los motores de inspección profunda de paquetes (IPS/IDS) y/o de los módulos de seguridad web (WAF)* incluidos en los firewalls de nueva generación.

Fabricantes como Palo Alto Networks, Check Point, Cisco, Sophos, WatchGuard, entre otros, también ofrecen estas capacidades en sus soluciones, por lo que el requisito puede ser cumplido por múltiples marcas del mercado y no se limita exclusivamente a Fortinet.

OBSERVACIÓN 34:

ADMINISTRACION Y GESTION DE PLATAFORMA
Gestión vía HTTPS y CLI.
Deberá contar con API por medio del método RESTful sobre HTTPS.
La solución debe contar con dashboards, que muestren como mínimo información en tiempo real del tráfico, Historia de Ataques, sesiones por política e información del sistema.
Menú tipo dropdown para navegar por la información
Mostrar los orígenes del tráfico o usuarios que generan tráfico.
Mostrar las aplicaciones y su categorización según riesgo.
Visibilidad de destinos del tráfico.
Visibilidad de los sitios web más consultados por los usuarios.
Visibilidad de las amenazas que han ocurrido en la red.

Solicitamos amablemente a la entidad revisar y ajustar los requerimientos técnicos, ya que estos

términos, funcionalidades y condiciones corresponden a características propias de Fortinet, lo cual podría limitar la pluralidad de oferentes, transparencia y selección objetiva.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que as especificaciones solicitadas no son exclusivas de un solo fabricante. Funcionalidades como la gestión vía HTTPS y CLI, la disponibilidad de API RESTful sobre HTTPS, la visualización mediante dashboards en tiempo real con información de tráfico, ataques, sesiones e información del sistema, así como la visibilidad de usuarios, aplicaciones categorizadas por nivel de riesgo, destinos de tráfico, sitios web más consultados y amenazas detectadas en la red, corresponden a características estándar presentes en los firewalls de nueva generación de los principales fabricantes del mercado (Fortinet, Palo Alto Networks, Check Point, Cisco, Sophos, WatchGuard, SonicWall, entre otros).
En consecuencia, dichos requerimientos pueden ser cumplidos por múltiples soluciones de seguridad perimetral, garantizando pluralidad de oferentes.

OBSERVACIÓN 35:

b. La solución deberá poderse integrar de forma nativa con los NGFW solicitados para las sedes y el equipo actualmente ubicado en la sede

Respetuosamente se solicita a la entidad revisar esta especificación, ya que corresponde a una funcionalidad nativa de Fortinet, lo cual podría limitar la participación de otros oferentes.

RESPUESTA: Atendiendo a la observación recibida, la Universidad de Cundinamarca se acoge la observación realizada, toda vez que el término integrar de forma nativa se interpreta como una restricción de pluralidad de oferentes.

El objetivo de la Universidad no es direccionar la contratación hacia un proveedor en particular, sino asegurar que la solución ofertada cumpla con la capacidad de gestionar, filtrar y controlar contenidos. Por lo anterior se verá ajustado en la respectiva adenda del Anexo de Especificaciones Técnicas Definitivas.

OBSERVACIÓN 36:

Generalidades
Se requiere un (1) equipo tipo Appliance físico de propósito específico que permita registrar cada transacción de la plataforma de seguridad perimetral de la , para poder identificar y reaccionar a cualquier informe emitido por un log o registro de los dispositivos de seguridad perimetral ofertados tales como el Firewall de Nueva Generación y el Firewall de Aplicaciones web requerido.
El equipo deberá recolectar y emitir el reporte de eventos, actividades y tendencias ocurridas en las plataformas de seguridad perimetral ofertadas tales como el Firewall de Nueva Generación y el Firewall de Aplicaciones web requerido.
La solución de analítica, logs y reportes debe tener la capacidad en enviar eventos a la plataforma de NGFW y que estos actúen como triggers de acciones automáticas
Desempeño
La solución de análisis de logs debe dar soporte a las siguientes características:
- Capacidad de recibir hasta 200 GB de logs diarios.
- Capacidad de Almacenamiento de 8 Terabytes
- Tasa analítica sostenida (logs/seg): 4000
- Tasa sostenida del colector (registros/seg): 6000
Funciones y configuraciones requeridas para el analizador de red
Visor de tráfico en tiempo real.
Visor de tráfico histórico.
Visor personalizado de log de tráfico
Herramienta de búsqueda sobre los logs de tráfico.
Debe ser compatible con el equipo FG-600E que tiene la
Análisis de logs y reportes requeridos
Vista de búsqueda y manejo de logs.
Reportes basados en perfiles.
Inventario de plantillas predefinidas para reportes regulares.
Debe soportar de forma predefinida los reportes:
Eventos del sistema
Análisis de riesgo y aplicaciones
Reporte de Aplicaciones y Ancho de Banda
Reputación de Clientes
Análisis de seguridad
Reporte de Amenazas
Reportes de VPN

Respetuosamente se solicita a la entidad revisar esta especificación, ya que corresponde a una funcionalidad nativa de Fortinet, lo cual podría limitar la participación de otros oferentes.

RESPUESTA: Atendiendo a la observación recibida, la Universidad de Cundinamarca se acoge la observación realizada, toda vez que por error se estableció en la especificación *Debe ser compatible con el equipo FG-600E que tiene la Universidad y como es resaltado en la* ***Nota Aclaratoria N°1:*** *Actualmente, la sede FUSAGASUGÁ cuenta con el NGFW de marca FORTINET de referencia FG-600E, el cual debe ser configurado como Switch Core en la SEDE FUSAGASUGÁ, adicionalmente el contratista debe proporcionándole el licenciamiento y soporte con fabricante para su correcto funcionamiento. Este equipo ya no se tendrá que usar en la solución ofertada sino debe ser configurado como Switch Core en la SEDE FUSAGASUGÁ,* por lo anterior se interpreta como una restricción de pluralidad de oferentes.

El objetivo de la Universidad no es direccionar la contratación hacia un proveedor en particular. Por lo anterior se verá ajustado en la respectiva adenda del Anexo de Especificaciones Técnicas Definitivas.

OBSERVACIÓN 37:

a. SERVICIO DE SEGURIDAD PERIMETRAL Y SD-WAN

i. Appliance de seguridad perimetral deben tener la funcionalidad nativa de SD-WAN. Éstos irán ubicados en las Unidades Regionales de la Universidad de Cundinamarca: SEDE FUSAGASUGÁ (DOS (2) Appliance en HA), EXTENSIÓN

Solicitamos amablemente a la entidad revisar la funcionalidad nativa de SDWAN ya que es nativo de Fortinet, lo cual podría limitar la pluralidad de oferentes.

RESPUESTA: Atendiendo a la observación recibida, la Universidad de Cundinamarca se acoge la observación realizada, toda vez que el término funcionalidad nativa se interpreta como una restricción de pluralidad de oferentes.

El objetivo de la Universidad no es direccionar la contratación hacia un proveedor en particular, sino asegurar que la solución ofertada cumpla con la capacidad de gestionar, filtrar y controlar contenidos. Por lo anterior se verá ajustado en la respectiva adenda del Anexo de Especificaciones Técnicas Definitivas.

OBSERVACIÓN 38:

Capacidad de poder asignar parámetros de traffic shapping atreves de reglas de manera independiente

Solicitamos amablemente a la entidad revisar la característica, ya que es nativo de Fortinet, lo cual podría limitar la pluralidad de oferentes.

RESPUESTA: la Universidad de Cundinamarca que no se acoge la observación realizada, dentro de la revisión de los requisitos técnicos detallados en el pliego de condiciones de la

licitación en curso, particularmente los que se refieren a la funcionalidad de TRAFFIC SHAPPING. El *Traffic Shaping*, también conocido como *Quality of Service (QoS)*, es una función fundamental en los firewalls de próxima generación (NGFW) que permite controlar el ancho de banda y la prioridad del tráfico de red.

OBSERVACIÓN 39:

Filtrado WEB
Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 78 categorías y por lo menos 47 millones de sitios web en la base de datos.

Se solicita amablemente revisar el requisito y permitir equivalencia funcional para garantizar mayor pluralidad de oferentes, es una característica nativa de Fortinet.

RESPUESTA: la Universidad de Cundinamarca que no se acoge la observación realizada, dentro de la revisión de los requisitos técnicos detallados en el pliego de condiciones de la licitación en curso, particularmente los que se refieren a la funcionalidad de Filtrado WEB. Son funciones fundamentales en los firewalls de próxima generación (NGFW) que permite controlar el ancho de banda y la prioridad del tráfico de red.

OBSERVACIÓN 40:

Visibilidad
La solución debe estar en la capacidad de visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real, esto deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional.

Se solicita amablemente revisar esta característica y permitir equivalencias funcionales, ya que este requisito es una funcionalidad nativa de Fortinet, esto podría limitar la participación de otros oferentes.

RESPUESTA: la Universidad de Cundinamarca que no se acoge la observación realizada, dentro de la revisión de los requisitos técnicos detallados en el pliego de condiciones de la licitación en curso, particularmente los que se refieren a la funcionalidad de Visualizar tráfico de usuario. Son funciones fundamentales en los firewalls de próxima generación (NGFW) que permite controlar el ancho de banda y la prioridad del tráfico de red.

OBSERVACIÓN 41:

FIRST: El oferente debe presentar junto con su propuesta el certificado de membresía de FIRST para su proceso de SOC, con una vigencia mínima de un (1) año de expedición del certificado, la cual será tenida en cuenta como requisito adicional para asignación de puntaje dentro del presente proceso contractual.

Se solicita a la entidad eliminar este requisito ya que FIRST es más alertamiento de incidencias a nivel mundial sin un requerimiento técnico, ni unas especificaciones validas en seguridad informática.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la inclusión de este requisito obedece a la necesidad de garantizar que el oferente cuente con un SOC reconocido internacionalmente, con la capacidad de integrarse en tiempo real a redes globales de alerta temprana, intercambio de información y coordinación de respuesta frente a incidentes de seguridad cibernética.

La membresía FIRST aporta valor agregado en términos de:

- Prevención: acceso temprano a alertas globales de ciberseguridad.
- Respuesta: coordinación con equipos internacionales ante incidentes de gran escala.
- Confianza: validación de que el oferente cumple con parámetros de madurez y confianza exigidos por esta comunidad internacional.

Por lo anterior, la Universidad considera que este requerimiento no debe retirarse, ya que su inclusión no limita injustificadamente la participación, sino que busca asegurar un nivel de calidad, reconocimiento y capacidad de respuesta internacional, complementando las certificaciones formales exigidas dentro del Anexo de Especificaciones Técnicas.

OBSERVACIÓN 42:

Nota Técnica 5: El oferente debe allegar junto con la propuesta económica todos los soportes correspondientes a los perfiles solicitados como requisito habilitante del presente proceso remitirse al **numeral 10. PERFILES REQUERIDOS** del presente anexo. La NO presentación de estos soportes ocasionará que la propuesta técnica presentada sea inhabilitada para su evaluación. La Universidad no aceptará que una persona ocupe más de uno de los roles solicitados.

Se solicita respetuosamente a la entidad considerar que la exigencia de los perfiles del personal requerido sea aplicada únicamente una vez adjudicado el contrato, y no en la etapa de presentación de la oferta. Lo anterior, con el fin de garantizar una mayor pluralidad de oferentes y permitir la participación de proponentes.
Exigir la presentación de hojas de vida y certificaciones del personal en la fase de oferta puede restringir injustificadamente la participación de proponentes. Por tanto, se solicita a la entidad que la verificación de los perfiles profesionales se realice en la fase de legalización del contrato, garantizando así tanto la idoneidad del recurso humano como la transparencia y libre competencia del proceso.

RESPUESTA: Atendiendo a la observación recibida, la Universidad de Cundinamarca no se acoge la observación realizada ya que dentro del pliego de los términos ya se encuentra establecida como requisito carta de compromiso.

		requerimientos técnicos de las soluciones ofertadas.
10	CARTA DE COMPROMISO	El proponente deberá aportar junto con su propuesta carta de compromiso suscrita por el representante legal, en la que manifieste bajo la gravedad de

Proyectó: Monica Sotelo Asesor Jurídico Of. Compras	Aprobó: Dirección jurídica Aprobó: Dirección de Bienes y Servicios
Revisó: Asesor Dirección Jurídica	Aprobó: Jefatura Oficina de Compras

	EXPERIENCIA Y FORMACIÓN DEL PERSONAL REQUERIDO	juramento que cuenta con el personal requerido de acuerdo a los perfiles solicitados en el numeral **10. PERFILES REQUERIDOS** del anexo **ESPECIFICACIONES TÉCNICAS AL PROYECTO** para la ejecución del objeto de la presente invitación. **Nota 1:** El proponente adjudicatario deberá allegar dentro de los CINCO (05) días siguientes a la firma del contrato todos los soportes de educación y/o acreditación del personal destinado a la ejecución del presente objeto contractual, como lo son: título profesional, matrícula o tarjeta profesional. **Nota 2:** El personal ofrecido por el contratista en caso de cambio en la ejecución del contrato, salvo expresa solicitud que hará el supervisor del mismo, el cual se reserva el derecho a solicitarlo en caso de no existir entera satisfacción acerca de la idoneidad del mismo, previa notificación por escrito al oferente adjudicatario, debiendo éste asignar uno nuevo un iguales o mejores características, dentro de los tres (5) días siguientes a la solicitud.

OBSERVACIÓN 43:

Debe estar en capacidad de administrar switches y Access point para generar una red SD-LAN administrada y gestionada desde el mismo Firewall.

Se solicita amablemente revisar esta característica corresponde a una funcionalidad nativa de Fortinet, esta especificación podría restringir la participación de otros fabricantes que requieren controladores o plataformas externas para ofrecer la misma gestión, limitando la pluralidad de oferentes.

RESPUESTA: la Universidad de Cundinamarca se permite indicar que no se acoge a la observación, dentro de la revisión de los requisitos técnicos detallados en el pliego de condiciones de la licitación en curso, particularmente los que se refieren a la funcionalidad de SD-LAN. Son funciones fundamentales en los firewalls de próxima generación (NGFW) que permite controlar el ancho de banda y la prioridad del tráfico de red.

OBSERVACIÓN 44:

Licencias de aplicaciones: Ilimitadas El número de Aplicaciones a proteger no deberá estar limitado por licenciamiento.

Se solicita amablemente revisar esta característica corresponde a una funcionalidad nativa de Fortinet, esta especificación podría restringir la participación de otros fabricantes que requieren

controladores o plataformas externas para ofrecer la misma gestión, limitando la pluralidad de oferentes.

RESPUESTA: la Universidad de Cundinamarca se permite indicar que no acoge a la observación, dentro de la revisión de los requisitos técnicos detallados en el pliego de condiciones es necesario tener un licenciamiento ilimitado de las aplicaciones con el fin de ver a futuro un crecimiento en la infraestructura de la universidad y esto no puede ser impedimento para el crecimiento.

OBSERVACIÓN 45:

ANALISIS DE VULNERABILIDADES
La solución debe realizar análisis de vulnerabilidades sobre las aplicaciones web protegidas, de tal forma que se identifiquen vulnerabilidades existentes en los aplicativos webs de la Universidad de forma ilimitada, sin requerir licenciamiento adicional.

Se solicita amablemente revisar y modificar este requisito para permitir equivalencia funcional, esta característica corresponde principalmente a una funcionalidad nativa de Fortinet, ya que su WAF integra un motor de análisis de vulnerabilidades sin costo adicional. Esta condición podría limitar la participación de otros fabricantes que ofrecen la misma capacidad mediante licencias o módulos externos, afectando la pluralidad de oferentes.

RESPUESTA: la Universidad de Cundinamarca se permite indicar que no acoge a la observación, dentro de la revisión de los requisitos técnicos detallados en el pliego de condiciones es necesario tener una solución que garantice el análisis de vulnerabilidades sobre las aplicaciones web protegidas y no se esta haciendo referencia a un solo fabricante, ya que cualquiera puede cumplir con este requerimiento.

OBSERVACIÓN 46:

Licenciamiento y actualizaciones
El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, conexiones, VPNs equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.

Se solicita amablemente revisar y modificar este requisito para permitir equivalencia funcional, esta característica corresponde principalmente a una funcionalidad nativa de Fortinet, ya que su WAF integra un motor de análisis de vulnerabilidades sin costo adicional. Esta condición podría limitar la participación de otros fabricantes que ofrecen la misma capacidad mediante licencias o módulos externos, afectando la pluralidad de oferentes.

RESPUESTA: la Universidad de Cundinamarca se permite indicar que no acoge a la observación, dentro de la revisión de los requisitos técnicos detallados en el pliego de condiciones es necesario tener una solución que garantice el análisis de vulnerabilidades sobre las aplicaciones web protegidas y no se está haciendo referencia a un solo fabricante, ya que cualquiera puede cumplir con este requerimiento.

OBSERVACIÓN 47:

Respetuosamente solicitamos a la entidad revisar la totalidad de las especificaciones técnicas establecidas en el documento, ya que, en su conjunto parecen estar alineadas con características exclusivas de un único fabricante, lo cual podría restringir la participación de otros oferentes con soluciones funcionalmente equivalentes o superiores, esta situación podría afectar la pluralidad de oferentes.
Sugerimos, respetuosamente, que las especificaciones técnicas sean ajustadas o flexibilizadas evitando mencionar marcas propietarias o características que puedan relacionarse exclusivamente con un solo fabricante. Esto permitirá la participación de una mayor cantidad de oferentes que cumplan el objetivo del proceso, garantizando calidad y competitividad.

RESPUESTA: la Universidad de Cundinamarca se permite indicar que de acuerdo a las observaciones recibidas se realizaran los ajustes necesarios subsanando los términos que hacen referencia a un fabricante en específico.
Por lo anterior se verá ajustado en la respectiva adenda del Anexo de Especificaciones Técnicas Definitivas.

Agradecemos el interés manifestado y la disposición del oferente para participar en esta convocatoria.

Cordialmente,

Firmado digitalmente por HURTADO MESA ANA LUCIA
Fecha: 2025.04.04 14:57:16 -05'00'

ANA LUCIA HURTADO MESA
Directora de Sistemas y Tecnología
Universidad de Cundinamarca

Proyectó: Ing. Jeniffer Castillo Fernández
Ing. Ingrid Sanchez Reyes
Área de Servicios Tecnológicos

15-30.7

15.

Fusagasugá, 2025-09-02.

Señores
WEXLER

Asunto y/ó Ref: Respuesta Observaciones Invitación Privada 038 de 2025

Cordial saludo,

De manera atenta, me dirijo a usted con el fin de dar respuesta a las observaciones allegadas en referencia a la Invitación Privada 038 de 2025, que tiene como objeto: ***"CONTRATAR EL SERVICIO DE SEGURIDAD PERIMETRAL Y CONFIGURACION DE CONECTIVIDAD MEDIANTE TECNOLOGÍA SD-WAN PARA LA UNIVERSIDAD DE CUNDINAMARCA".***

OBSERVACIONES:
WEXLER

OBSERVACIÓN 1:

¿La Universidad confirma que el equipo Fortinet FG-600E actual en Fusagasugá quedará como Switch Core y sólo requiere licenciamiento y soporte?

RESPUESTA: La Universidad de Cundinamarca se permite confirmar que en efecto el equipo Fortinet FG-600E de Fusagasugá permanecerá como Switch Core, requiriendo el licenciamiento y soporte necesarios para su correcta operación como parte de la infraestructura core de red, cumpliendo funciones de switch central y de apoyo a la conectividad de la sede.

OBSERVACIÓN 2:

¿El licenciamiento solicitado (IPS, Malware, Application Control, URL/DNS Filtering, Antispam, etc.) debe incluirse para todos los equipos, o únicamente para los nuevos?

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que el licenciamiento de seguridad solicitado (IPS, Protección contra Malware, Application Control, URL/DNS Filtering, Antispam, entre otros) deberá aplicarse a todos los equipos contemplados dentro de la solución solicitada en el Anexo de Especificaciones Técnicas.

Esto incluye tanto los equipos principales como aquellos destinados a las sedes regionales, de manera que toda la infraestructura de seguridad perimetral quede cubierta de forma homogénea y con las mismas capacidades técnicas.

OBSERVACIÓN 3:

¿Se requiere integración con alguna nube específica (AWS, Azure, Google) además de las mencionadas?

RESPUESTA: La Universidad de Cundinamarca, en atención a la observación recibida, se permite aclarar que el alcance del presente proceso contractual contempla que la solución de seguridad perimetral y conectividad mediante tecnología SD-WAN pueda integrarse con servicios de nube pública líderes como AWS, Microsoft Azure y Google Cloud Platform (GCP), tal como está descrito en el Anexo de Especificaciones Técnicas.
Por lo anterior no se requiere integración adicional con otras nubes distintas a las mencionadas.

OBSERVACIÓN 4:

¿Cuál es la expectativa de crecimiento en usuarios concurrentes durante los 2 años del contrato? (esto impacta dimensionamiento de sesiones y throughput).

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que en atención a la observación presentada, la Universidad de Cundinamarca se permite aclarar que el contrato no tiene una vigencia de dos (2) años, sino de un (1) año, contado a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución establecidos en los pliegos.
En consecuencia, la expectativa de dimensionamiento de la solución (sesiones concurrentes y throughput) deberá proyectarse en función de un horizonte de un año de operación.
Para este periodo, se espera mantener una operación estable de usuarios concurrentes, considerando el comportamiento actual de la institución, con un crecimiento controlado y marginal, propio del uso académico y administrativo que la Universidad demanda en sus diferentes sedes y unidades regionales.

OBSERVACIÓN 5:

¿Se debe garantizar compatibilidad con equipos de terceros (switches, APs) o sólo con Fortinet?

RESPUESTA: La Universidad de Cundinamarca se permite se permite precisar que el presente proceso contractual tiene como eje principal la implementación de la solución de seguridad perimetral y conectividad SD-WAN con equipos que cumplan con lo descrito en el Anexo de Especificaciones Técnicas sin importar la marca de estos.

No obstante, si debe garantizar que la solución ofrecida pueda interoperar y coexistir de manera adecuada con equipos de terceros, en particular con los switches de acceso y puntos de acceso (APs) ya desplegados en la infraestructura institucional, los cuales forman parte del ecosistema tecnológico de la Universidad.

La compatibilidad requerida se refiere a la capacidad de la solución para integrarse sin generar conflictos de conectividad, gestión de tráfico o seguridad, y no necesariamente a la homologación completa de características avanzadas entre fabricantes.

OBSERVACIÓN 6:

¿Confirma el cliente que todas las sedes tendrán conectividad SD-WAN mediante fibra óptica o radio enlace, según la tabla técnica del documento?

RESPUESTA: La Universidad de Cundinamarca, en atención a la observación recibida, se permite aclarar que tal como se indica en la tabla técnica del Anexo de Especificaciones, todas las sedes contempladas dentro del alcance del proyecto deberán contar con conectividad SD-WAN, suministrada mediante fibra óptica o radio enlace, según la disponibilidad y factibilidad técnica en cada ubicación.

La infraestructura contratada deberá garantizar que cada sede esté integrada de forma plena a la red institucional mediante la capa SD-WAN, asegurando consistencia en la gestión del tráfico, priorización de aplicaciones y alta disponibilidad.

Por lo anterior el oferente deberá considerar en su propuesta las condiciones particulares de cobertura, disponibilidad de proveedores y medios de acceso (fibra o radio enlace), de forma que el servicio cumpla los niveles de calidad y continuidad exigidos en el Anexo de Especificaciones Técnicas.

OBSERVACIÓN 7:

¿Hay algún requerimiento especial para balanceo de tráfico (aplicaciones críticas, por ejemplo streaming de clases, videoconferencias)?

RESPUESTA: La Universidad de Cundinamarca, ser permite aclarar que sil se debe garantizar un balanceo de tráfico que dé prioridad a las aplicaciones críticas de la Universidad (como streaming y videoconferencias), asegurando calidad y continuidad, sin perjuicio de que las funciones más avanzadas de priorización a nivel de aplicación se gestionen en el marco del proyecto de SD-WAN y seguridad perimetral.

OBSERVACIÓN 8:

¿Se validará alta disponibilidad (HA) sólo en Fusagasugá y Datacenter, o también en otras sedes críticas?

RESPUESTA: La Universidad de Cundinamarca, ser permite aclarar que sí habrá administración compartida entre el proponente adjudicado y la Universidad, pero el alcance se encuentra limitado a las fases de implementación, capacitación y acompañamiento inicial. No se prevé la asignación de bolsas adicionales de horas, dado que estas actividades forman parte del servicio contratado y no implican costos adicionales, como se evidencia a continuación en la obligación especifica del contratista No. 27.

OBSERVACIÓN 9:

¿Se requiere integración con Active Directory para políticas de SD-WAN basadas en usuarios, como lo contempla el documento?

RESPUESTA: Universidad de Cundinamarca, en atención a la observación recibida, se permite aclarar que la forma de pago definida en los términos de la presente invitación publica responde a las disposiciones contractuales y financieras establecidas en la normatividad vigente de la Universidad para la contratación pública, que obligan a la entidad a realizar los pagos con base en la verificación del cumplimiento de las obligaciones contractuales y la disponibilidad presupuestal correspondiente.

En este sentido, no es posible acceder a la modificación planteada por el oferente respecto a establecer un pago anticipado del 50% contra entrega de equipos y licencias, ya que la

Universidad no puede realizar desembolsos parciales anticipados sin que medie la debida ejecución contractual y la verificación del cumplimiento.

OBSERVACIÓN 10:

¿La Universidad espera que se implemente un esquema Hub-and-Spoke o Full Mesh, o se deja abierto a propuesta técnica?

RESPUESTA: Universidad de Cundinamarca, en atención a la observación recibida, se permite aclarar que se debe garantizar un balanceo de tráfico que dé prioridad a las aplicaciones críticas de la Universidad (como streaming y videoconferencias), asegurando calidad y continuidad, sin perjuicio de que las funciones más avanzadas de priorización a nivel de aplicación se gestionen en el marco del proyecto de SD-WAN y seguridad perimetral.

OBSERVACIÓN 11:

¿Existe flexibilidad para ajustar los tiempos de atención y resolución definidos por criticidad de los incidentes (Crítico, Alto, Medio, Bajo), o estos deben cumplirse estrictamente como están establecidos en el pliego técnico?".

RESPUESTA: Universidad de Cundinamarca, en atención a la observación recibida, se permite aclarar que los tiempos de atención y resolución definidos por criticidad en el pliego técnico deben cumplirse estrictamente, pues son requeridos por la Universidad para asegurar la disponibilidad de los servicios. No se contempla flexibilidad general, salvo casos excepcionales debidamente justificados.

OBSERVACIÓN 12:

"¿La Universidad estaría dispuesta a que la generación de tickets (uno por cada incidente detectado o reportado) se integre directamente con su herramienta ITSM actual mediante API o Syslog, en lugar de implementar una nueva plataforma web de tickets?"

RESPUESTA: Universidad de Cundinamarca, en atención a la observación recibida, se permite aclarar que no es posible sustituir este requerimiento mediante integración con la herramienta ITSM actualmente utilizada por la Universidad, incluso si la integración se realiza a través de API o Syslog, toda vez que esta exigencia de contar con una plataforma propia de tickets provista por el contratista busca garantizar independencia y trazabilidad en la atención de incidentes y requerimientos asociados al servicio contratado, así como claridad en la responsabilidad del oferente respecto al registro, seguimiento, control y cierre de tickets, evitando dependencias tecnológicas o limitaciones derivadas de plataformas institucionales cuyo alcance no está contemplado en el objeto contractual.

Adicionalmente, contar con una plataforma independiente permite que la Universidad realice un monitoreo y auditoría objetiva de los niveles de servicio (SLAs) pactados, sin que la información se mezcle con otras áreas o procesos que no hacen parte del contrato.

Agradecemos el interés manifestado y la disposición del oferente para participar en esta convocatoria.

Cordialmente,

Firmado digitalmente por HURTADO MESA ANA LUCIA
Fecha: 2025.09.02 19:51:44 -05'00'

ANA LUCIA HURTADO MESA
Directora de Sistemas y Tecnología
Universidad de Cundinamarca

Proyectó: Ing. Jeniffer Castillo Fernández
Área de Servicios Tecnológicos

15-30.7

15.

Fusagasugá, 2025-09-04.

Señores
UNE EPM TELECOMUNICACIONES S.A.

Asunto y/ó Ref: Respuesta Observaciones Invitación Privada 038 de 2025

Cordial saludo,

De manera atenta, me dirijo a usted con el fin de dar respuesta a las observaciones allegadas en referencia a la Invitación Privada 038 de 2025, que tiene como objeto: ***"CONTRATAR EL SERVICIO DE SEGURIDAD PERIMETRAL Y CONFIGURACION DE CONECTIVIDAD MEDIANTE TECNOLOGÍA SD-WAN PARA LA UNIVERSIDAD DE CUNDINAMARCA".***

OBSERVACIONES:

UNE EPM TELECOMUNICACIONES S.A.

OBSERVACIÓN 12:

Agradecemos a la entidad indicar en que tiempo establece requiere se encuentre implementado el servicio.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que en los términos de la presente invitación numeral 7.2. TERMINO DE EJECUCIÓN, LUGAR DE EJECUCIÓN Y VIGENCIA se establece lo siguiente:

El termino de ejecución del contrato *A partir del cumplimiento de los requisitos de perfeccionamiento (Expedición del Certificado de Disponibilidad Presupuestal y Suscripción del Contrato) y ejecución (Expedición del Registro Presupuestal, Aprobación de Garantías y Acta de Inicio), hasta el treinta y uno (31) de octubre de 2026.*
La prestación del servicio se iniciará el primero (1°) de noviembre de 2025 y culminará el treinta y uno (31) de octubre de 2026, previa instalación, configuración y/o puesta en marcha de la solución ofertada.

OBSERVACIÓN 13:

Se solicita a la entidad indicar si es posible unificar en un solo equipo seguridad perimetral y SDWAN.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que actualmente por medio del equipo de seguridad perimetral se tiene configurado la conexión SD-WAN, permitiendo administrar de forma centralizada la conectividad y al mismo tiempo implementar políticas de ciberseguridad avanzadas.

OBSERVACIÓN 14:

¿Se solicita a la entidad indicar si las sedes descritas en la tabla 9 al 11 no requieren Backup? y si estas requieren agregarse a la solución con un solo UK.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que para la Unidad Agroambiental El Vergel – Facatativá, Unidad Agroambiental La Esperanza – Fómeque, Unidad Agroambiental El Tíbar – Ubaté, Oficina de Proyectos Especiales y Relaciones Interinstitucionales de Bogotá y la Extensión Zipaquirá – Sede Antigua, no se requiere la implementación de servicios de respaldo (backup).
Lo anterior obedece a que, dada la reducida cantidad de usuarios que hacen uso del servicio en estas sedes, no resulta necesario disponer de dos canales de internet ni de equipos de seguridad perimetral en alta disponibilidad (HA).

OBSERVACIÓN 15:

Se solicita a la entidad indicar si es posible presentar oferta bajo equipo virtualizado en DC del Operador el equipo NGFW así se garantiza la misma disponibilidad en HA desde el DC y se optimizan 4 equipos físicos y licencias dos en fusa y dos en DC.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que el servicio a contratar especifica que el despliegue de la solución debe incluir Appliance de seguridad perimetral, no se acepta solución virtualizada.

OBSERVACIÓN 16:

Agradecemos indicar el serial para el equipo existente FG-600E para la compra de la licencia o en caso dado si se brinda una solución de esta misma tecnología desean utilizar este equipo para la solución?

RESPUESTA: La Universidad de Cundinamarca se permite informar que el equipo de marca FORTINET de referencia FG-600E con serial FG6H0E5819902908, solo debe ser configurado como Switch Core en la SEDE FUSAGASUGÁ.

OBSERVACIÓN 17:

Agradecemos indicar la Cantidad de dominios a proteger

RESPUESTA: La Universidad de Cundinamarca se permite informar que actualmente solo contamos con el dominio UCUNDINAMARCA.EDU.CO

OBSERVACIÓN 18:

Agradecemos indicar si el WAF puede estar en WAFCLOUD del fabricante y si la entidad suministraría el recurso de cómputo.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que dentro de la solución solicitada de un servicio de Protección y Seguridad para las aplicaciones WEB (WAF) de la Universidad, en alta disponibilidad (HA), que permita bloquear amenazas en tiempo real, sin bloquear a los usuarios (estudiantes, funcionarios y docentes) minimizando los falsos positivos que puedan llegar a generar demasiada gestión administrativa por parte del área de Servicios Tecnológicos, puede estar en la NUBE pero deben tener en cuenta los requerimientos técnicos establecidos en el anexo de la presente invitación; por consiguiente y aclarando la universidad no suministra el recurso de cómputo.

OBSERVACIÓN 19:

Con el fin de presentar una solución costo eficiente es posible entregar la gestión centralizada en un sistema MSSP alojada en la nube del oferente

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la solución no puede ser alojada ni administrada en una plataforma distinta al equipo de seguridad perimetral remitirse al anexo de especificaciones técnicas del presente proceso.

OBSERVACIÓN 20:

Agradecemos mayor alcance y claridad a lo requerido en este texto "Infraestructura de la nube incluyendo AWS"

RESPUESTA: La Universidad de Cundinamarca, ser permite indicar que el requisito hace referencia tener compatibilidad a futuro con la plataforma en nube de AWS, ya que se cuenta con esta nube pública.

OBSERVACIÓN 21:

Con el fin de garantiza pluralidad de oferentes agradecemos de ser posible presentar solución SIEM con otro fabricante ya que la ficha técnica está orientada a una sola fabrica

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que en el anexo técnico se han establecido los requerimientos mínimos necesarios para la correcta prestación del

servicio. En este sentido, no se limita la participación a un único fabricante, siempre que las soluciones propuestas cumplan con las especificaciones y sean compatibles e interoperables con la infraestructura existente, garantizando así el adecuado funcionamiento del servicio.

OBSERVACIÓN 22:

Se solicita a la entidad ampliar el rango del tiempo de respuesta ya que se está interpretando como si las sedes se encontrasen localizadas en una misma localidad por lo cual los tiempos de desplazamiento no serían los mismos para cada sede o región

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que los tiempos de respuesta definidos en el anexo técnico corresponden a los requerimientos mínimos establecidos por la entidad, y por tanto no es posible ampliarlos. Estos parámetros se encuentran alineados con la criticidad de los servicios y la continuidad operativa que debe garantizarse en todas las sedes, independientemente de su ubicación geográfica.

OBSERVACIÓN 23:

Se solicita a la entidad indicar el lugar físico de trabajo y de ser posible homologar certificaciones por experiencia del personal

RESPUESTA: La Universidad de Cundinamarca se permite informar que el lugar de trabajo destinado para la prestación del servicio será el **Centro de Operaciones de Seguridad (SOC) del oferente adjudicado**. Así mismo, se aclara que no se aceptará la homologación de certificaciones mediante experiencia del personal, dado que las certificaciones solicitadas son de carácter obligatorio y constituyen un requisito mínimo para garantizar la idoneidad técnica del servicio.

Agradecemos el interés manifestado y la disposición del oferente para participar en esta convocatoria.

Cordialmente,

ANA LUCIA HURTADO MESA
Directora de Sistemas y Tecnología
Universidad de Cundinamarca

Proyectó: Ing. Ingrid Sanchez Reyes
Área de Servicios Tecnológicos

15-30.7

15.

Fusagasugá, 2025-09-02.

Señores
MEDIA COMMERCE PARTNERS S.A.S.

Asunto y/ó Ref: Respuesta Observaciones Invitación Privada 038 de 2025

Cordial saludo,

De manera atenta, me dirijo a usted con el fin de dar respuesta a las observaciones allegadas en referencia a la Invitación Privada 038 de 2025, que tiene como objeto: ***"CONTRATAR EL SERVICIO DE SEGURIDAD PERIMETRAL Y CONFIGURACION DE CONECTIVIDAD MEDIANTE TECNOLOGÍA SD-WAN PARA LA UNIVERSIDAD DE CUNDINAMARCA".***

OBSERVACIONES TÉCNICAS:

MEDIA COMMERCE PARTNERS S.A.S.

OBSERVACIÓN 1:

2. CONFIGURACIÓN DE LA RED DE INTERNET MEDIANTE TECNOLOGÍA SD- WAN
se solicita a la Universidad indicar serial del equipo FG-600E propiedad de la universidad para cotizar licenciamiento y soporte de fábrica.

RESPUESTA: La Universidad de Cundinamarca se permite informar que el equipo de marca FORTINET de referencia FG-600E cuenta con el serial FG6H0E5819902908.

OBSERVACIÓN 2:

a. SERVICIO DE SEGURIDAD PERIMETRAL Y SD-WAN
se solicita a la Universidad indicar Data Center actual donde se encuentran los servicios actualmente implementados

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que, conforme a la distribución establecida en el anexo técnico del presente proceso, en cada sede o unidad regional deberá implementarse el servicio de seguridad perimetral de acuerdo con los lineamientos definidos.

De manera complementaria, en el Data Center se encuentran centralizados los servicios de seguridad perimetral en alta disponibilidad (HA), así como las soluciones de Web Application Firewall (WAF) y de Security Information and Event Management (SIEM), los cuales garantizan la continuidad operativa, la protección de aplicaciones críticas y la gestión centralizada de eventos de seguridad.
La ubicación y dirección física del Data Center será informada exclusivamente al proveedor adjudicado en la fase de implementación, dado que este servicio también hace parte de un proceso de licitación en curso y la información corresponde a activos críticos de seguridad de la Universidad.

OBSERVACIÓN 3:

a. SERVICIO DE SEGURIDAD PERIMETRAL Y SD-WAN
se solicita a la Universidad de confirmar si la Universidad es la encargada de entregar los puertos de los Switch para que se puedan conectar los firewalls y configurar él HA.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que cuenta con la infraestructura necesaria, incluyendo switches de distribución y puertos disponibles, para garantizar la conexión y la configuración de los equipos de seguridad perimetral. La asignación y habilitación de dichos puertos se realizará en coordinación con el proveedor adjudicado durante la fase de implementación, a fin de asegurar la correcta integración y funcionamiento del servicio.

OBSERVACIÓN 4:

Certificaciones Exigidas al Proceso de SOC del Oferente
se solicita respetuosamente a la Universidad retirar alcance y puntaje adicional de membresía de FIRST para el SOC entendiendo que es una afiliación a un grupo selectivo "FIRST es el Foro de Equipos de Respuesta a Incidentes y Seguridad" y no es una certificación o estándar como ISO 27001 que "permite la gestión y control de los riesgos de la seguridad de la información en las organizaciones para las cuales la información y la tecnología son activos importantes de su negocio. Mediante las mejores prácticas de seguridad de la información ". por lo anterior al no ser un estándar internacional se solicita retirar esta condición.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la inclusión de este requisito obedece a la necesidad de garantizar que el oferente cuente con un SOC reconocido internacionalmente, con la capacidad de integrarse en tiempo real a redes globales de alerta temprana, intercambio de información y coordinación de respuesta frente a incidentes de seguridad cibernética.

La membresía FIRST aporta valor agregado en términos de:
- Prevención: acceso temprano a alertas globales de ciberseguridad.
- Respuesta: coordinación con equipos internacionales ante incidentes de gran escala.
- Confianza: validación de que el oferente cumple con parámetros de madurez y confianza exigidos por esta comunidad internacional.

Por lo anterior, la Universidad considera que este requerimiento no debe retirarse, ya que su inclusión no limita injustificadamente la participación, sino que busca asegurar un nivel de calidad, reconocimiento y capacidad de respuesta internacional, complementando las certificaciones formales exigidas dentro del Anexo de Especificaciones Técnicas.

Agradecemos el interés manifestado y la disposición del oferente para participar en esta convocatoria.

Cordialmente,

Firmado digitalmente por HURTADO MESA ANA LUCIA
Fecha: 2025.09.02 [illegible]

ANA LUCIA HURTADO MESA
Directora de Sistemas y Tecnología
Universidad de Cundinamarca

Proyectó: Ing. Jeniffer Castillo Fernández
Ing. Ingrid Sanchez Reyes
Área de Servicios Tecnológicos

15-30.7

15.

Fusagasugá, 2025-09-03.

Señor
CESAR PAEZ GOMEZ
CEO & Founder

Asunto y/ó Ref: Respuesta Observaciones Invitación Privada 038 de 2025

Cordial saludo,

De manera atenta, me dirijo a usted con el fin de dar respuesta a las observaciones allegadas en referencia a la Invitación Privada 038 de 2025, que tiene como objeto: ***"CONTRATAR EL SERVICIO DE SEGURIDAD PERIMETRAL Y CONFIGURACION DE CONECTIVIDAD MEDIANTE TECNOLOGÍA SD-WAN PARA LA UNIVERSIDAD DE CUNDINAMARCA".***

OBSERVACIONES TÉCNICAS:

CEO & Founder

OBSERVACIÓN 1:

Observación 1 – Restricción tecnológica a un único fabricante (pág. 7)
El pliego exige que los equipos de seguridad correspondan a la marca Fortinet, configurando un amarre tecnológico que restringe la participación de otros fabricantes. Esto vulnera los principios de pluralidad de oferentes y selección objetiva (art. 24 Ley 80/93) y contraría el criterio de equivalencia funcional (Ley 1150/07). Solicitud: Reformular el requerimiento en términos de capacidades técnicas y resultados esperados, sin referencia a marcas específicas, para ampliar la competencia y garantizar la neutralidad tecnológica.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que en la página 7 del documento se hace referencia a la marca Fortinet en la Nota Aclaratoria N° 1, en la cual se indica que actualmente la sede Fusagasugá cuenta con un NGFW de marca Fortinet, referencia FG-600E, el cual debe ser configurado como Switch Core en dicha sede.

Asimismo, se establece que el contratista deberá suministrar el licenciamiento y soporte del fabricante para garantizar su correcto funcionamiento. Sin embargo, es importante precisar que esta mención corresponde exclusivamente al equipo ya existente en la Universidad y no implica que los equipos requeridos para la implementación de la solución deban ser necesariamente de la marca Fortinet.

OBSERVACIÓN 2:

Observación 2 – Exigencia de módulos propietarios (pág. 7 y 15)
Requerimientos como "Video Filtering nativo" o sandbox del mismo fabricante limitan la posibilidad de ofertar soluciones equivalentes de distintos proveedores. Estas restricciones son contrarias al principio de selección objetiva y a la obligación de definir condiciones proporcionales al objeto contractual. Solicitud: Permitir que los oferentes acrediten funcionalidades mediante arquitecturas distintas, siempre que cumplan con los objetivos de seguridad planteados.

RESPUESTA: Atendiendo a la observación recibida, la Universidad de Cundinamarca acoge la observación realizada, toda vez que el término "Video Filtering" corresponde a una denominación propia del fabricante Fortinet, lo que podría interpretarse como una restricción de la pluralidad de oferentes. Con respecto al termino de sandbox este no es una término de una denominación propia del fabricante Fortinet, cuando se hace referencia que *el Antivirus deberá integrarse de forma nativa con una solución sandbox del mismo fabricante,* si se pudiese interpretar como una restricción de pluralidad de oferentes.

El objetivo de la Universidad no es direccionar la contratación hacia un proveedor en particular, sino asegurar que la solución ofertada cumpla con la capacidad de gestionar, filtrar y controlar contenidos de video en el tráfico de red, con el fin de garantizar un uso eficiente del ancho de banda y la adecuada operación de aplicaciones críticas institucionales.
Por lo anterior se verá ajustado en la respectiva adenda del Anexo de Especificaciones Técnicas Definitivas.

OBSERVACIÓN 3:

Observación 3 – Terminología y fichas técnicas copiadas de un fabricante (pág. 9, 10 y 11)
Se identifican términos como "VDOM" y descripciones idénticas a fichas comerciales de Fortinet. Esto constituye una restricción encubierta a la competencia y vulnera el principio de igualdad. Solicitud: Sustituir la terminología propietaria por conceptos genéricos como "segmentación por instancias virtuales" o "capacidad de virtualización".

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la intención de este requerimiento no es direccionar la contratación hacia un fabricante en particular, sino garantizar que la solución ofertada cuente con la capacidad de segmentar y virtualizar de forma lógica las funciones de seguridad, permitiendo la administración independiente de políticas, configuraciones y recursos de red dentro de un mismo dispositivo físico.

Por lo anterior, se acoge la observación y se procederá a ajustar el texto eliminando la referencia exclusiva y reemplazándola por una descripción más amplia y neutral, el cual se verá ajustado en la respectiva adenda del Anexo de Especificaciones Técnicas Definitivas.

OBSERVACIÓN 4:

Observación 4 – Exigencia de tecnología ASIC (pág. 13)
La obligación de contar con procesadores ASIC excluye otras arquitecturas de alto rendimiento (CPU, FPGA), lo cual constituye una barrera injustificada de acceso (art. 5 Ley 1150/07). Solicitud: Admitir cualquier arquitectura que demuestre cumplimiento con las métricas de rendimiento exigidas.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la intención de este requerimiento no es direccionar la contratación hacia un fabricante en particular, sino garantizar que la solución ofertada cuente con mecanismos de aceleración a nivel de hardware (por ejemplo, ASIC, NPU, FPGA u otros procesadores dedicados) que permitan:

- Optimizar el rendimiento en el procesamiento de tráfico de red.
- Asegurar que las funciones de firewall, inspección de contenido y servicios de seguridad no dependan únicamente del CPU general.
- Mantener baja latencia y alto desempeño incluso con servicios de inspección profunda de paquetes (DPI), cifrado/descifrado SSL/TLS y prevención de intrusiones (IPS) habilitados.

Por lo anterior, se acoge la observación y se procederá a ajustar el texto eliminando la referencia exclusiva y reemplazándola por una descripción más amplia y neutral, el cual se verá ajustado en la respectiva adenda del Anexo de Especificaciones Técnicas Definitivas.

OBSERVACIÓN 5:

Observación 5 – Ranking de Gartner como criterio de habilitación (pág. 13)
La exigencia de que la solución se encuentre en el "cuadrante mágico de Gartner" carece de sustento técnico y constituye un criterio subjetivo de carácter comercial. La jurisprudencia ha reiterado que solo son válidos requisitos objetivos y verificables.
Solicitud: Sustituir esta exigencia por normas técnicas internacionales reconocidas (ej. ISO/IEC 27001, Common Criteria, NIST).

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que el criterio establecido en el pliego no busca direccionar la contratación hacia un fabricante en específico, sino garantizar que la solución ofertada haya sido reconocida por un ente evaluador independiente como una alternativa robusta, confiable y validada en el mercado internacional.

Por lo anterior se mantiene la exigencia de Gartner como mecanismo de aseguramiento de calidad, toda vez que la inclusión en el cuadrante mágico responde a criterios de innovación, visión de mercado, capacidad de ejecución, escalabilidad y respaldo comercial, elementos que son determinantes en una solución de la magnitud requerida por la Universidad.

Cabe aclarar que el cuadrante de Gartner para SD-WAN o plataformas de proteccion no incluye un único fabricante, sino múltiples oferentes reconocidos a nivel global (Cisco, Palo Alto, Fortinet, VMware, HPE Aruba, entre otros). Por lo tanto, la condición no restringe la

pluralidad de participantes, sino que asegura que las soluciones ofertadas estén alineadas con las mejores prácticas internacionales. En este sentido, se la exigencia de que la solución esté o halla estado catalogada como líder en el cuadrante mágico de Gartner se mantiene, en aras de proteger la inversión institucional y garantizar la calidad del servicio contratado.

OBSERVACIÓN 6:

Observación 6 – Sobredimensionamiento del throughput (pág. 11)
El pliego exige capacidades de hasta 100 Gbps, mientras que la necesidad real de la Universidad no supera los 600 Mbps. Este requerimiento es desproporcionado frente al objeto contractual, violando el principio de planeación (art. 25 Ley 80/93). Solicitud: Ajustar las especificaciones a la realidad del tráfico institucional y permitir escalabilidad modular hacia el futuro.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que se esta haciendo referencia a las especificaciones mínimas de desempeño del Throughput WAF HTTP como mínimo de 100 Mbps, donde no estamos sobredimensionando el requerimiento, al contrario, es un valor bajo que cualquier fabricante serio puede cumplir, y de esta manera se garantiza que el oferente presente equipos con rendimiento real y comprobable.

OBSERVACIÓN 7:

Observación 7 – Configuración rígida de interfaces (pág. 11)
La definición exacta de puertos coincide con modelos específicos, limitando alternativas del mercado. Solicitud: Formular el requisito en términos de capacidad total, número mínimo de interfaces y posibilidad de expansión.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que estas especificaciones técnicas son las mínimas requeridas, y de acuerdo a la comparación realizada con los equipos actuales en el mercado hay diferentes fabricantes que sí pueden cumplir y superar el requerimiento actual.

OBSERVACIÓN 8:

Observación 8 – Exclusividad en firmas antimalware (pág. 9 y 15)
La obligación de utilizar únicamente firmas propietarias impide integrar motores líderes de seguridad reconocidos mundialmente. Solicitud: Permitir que los oferentes acrediten la integración de motores equivalentes, garantizando diversidad de soluciones.

RESPUESTA: Atendiendo a la observación recibida, la Universidad de Cundinamarca acoge la observación realizada, de acuerdo a verificación realizada y puesto que el objetivo de la Universidad no es direccionar la contratación hacia un proveedor en particular, sino asegurar que la solución ofertada cumpla con la capacidad de gestionar, filtrar y controlar contenidos de video en el tráfico de red, con el fin de garantizar un uso eficiente del ancho de banda y la adecuada operación de aplicaciones críticas institucionales.
Por lo anterior se verá ajustado en la respectiva adenda del Anexo de Especificaciones

Técnicas Definitivas.

OBSERVACIÓN 9:

Observación 9 – Exigencia de integración nativa de todos los módulos (pág. 20)
El requerimiento favorece soluciones monolíticas de un solo fabricante, restringiendo arquitecturas modulares interoperables.
Solicitud: Aceptar integraciones a través de estándares abiertos (STIX, TAXII, Syslog, API), garantizando neutralidad tecnológica.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que el requerimiento de integración nativa de todos los módulos tiene como finalidad garantizar:

- **Gestión centralizada y unificada**: al contar con una única consola de administración, se asegura una operación más eficiente, disminuyendo la complejidad en la gestión y el riesgo de errores en la configuración o correlación de eventos.
- **Compatibilidad total**: al provenir todos los módulos de un mismo fabricante, se evita la dependencia de integraciones de terceros o de estándares que pueden tener limitaciones, demoras en soporte o problemas de interoperabilidad en la práctica.
- **Soporte unificado**: contar con un solo fabricante permite que el soporte técnico, actualizaciones y parches de seguridad se atiendan de forma integral y sin riesgos de transferencia de responsabilidades entre distintos proveedores.
- **Tiempo de respuesta ante incidentes**: la integración nativa permite una correlación inmediata de eventos entre los diferentes módulos (firewall, IPS, WAF, antimalware, etc.), lo que agiliza la detección y respuesta a amenazas.

Por estas razones, la Universidad considera indispensable que todos los componentes de seguridad provengan de un mismo fabricante y se integren de manera nativa, lo que garantiza continuidad operativa, robustez en la protección y simplificación en la administración de la plataforma de seguridad perimetral.

OBSERVACIÓN 10:

Observación 10 – Exclusión de agentes en servidores (pág. 19)
La prohibición de agentes desconoce que existen enfoques modernos de seguridad basados en agentes livianos que no afectan el rendimiento.
Solicitud: Permitir su uso siempre que cumpla con los estándares de desempeño.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la inclusión de un módulo de Protección contra Web Defacement en la solución de seguridad propuesta ofrece un valor agregado significativo para la Universidad, ya que permite reforzar la estrategia de defensa en profundidad en el ámbito de las aplicaciones web. Este tipo de controles no solo se centra en detener ataques en tránsito (funcionalidad propia de un WAF), sino que amplía la cobertura hacia la integridad del contenido y la continuidad del servicio, aspectos fundamentales en el contexto de una institución académica que gestiona información pública de interés para estudiantes, docentes, investigadores y comunidad en general.

Al asegurar la detección inmediata de modificaciones no autorizadas y habilitar la capacidad de restauración automática, se logra reducir drásticamente el tiempo de exposición frente a incidentes que pueden afectar la reputación institucional, la confianza de los usuarios y la veracidad de la información publicada.

El requerimiento de que el módulo opere sin agentes adicionales también aporta ventajas prácticas en términos de eficiencia operativa, reducción de la carga en servidores, facilidad de despliegue y compatibilidad con entornos heterogéneos, al basarse en protocolos estándar como FTP, SSH o SMB.

OBSERVACIÓN 11:

Observación 11 – Requerimientos subjetivos (pág. 17)
Términos como "fácil" o "rápidamente" impiden la evaluación objetiva.
Solicitud: Redactar los requisitos en parámetros verificables (ej. número de clics, tiempo máximo de despliegue).

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que al hacer referencia a los términos "fácil" y "rápidamente", prevalece de la necesidad institucional de que la solución WAF ofrezca usabilidad, simplicidad de administración y reducción en la complejidad operativa.

OBSERVACIÓN 12:

Observación 12 – Integración WAF–NGFW obligatoria (pág. 18)
La exigencia de integración automática solo es posible con fabricantes específicos. Solicitud: Admitir la interoperabilidad mediante protocolos estándar de comunicación.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que el requerimiento de integración de todos los módulos tiene como finalidad garantizar:

- **Gestión centralizada y unificada**: al contar con una única consola de administración, se asegura una operación más eficiente, disminuyendo la complejidad en la gestión y el riesgo de errores en la configuración o correlación de eventos.
- **Compatibilidad total**: al provenir todos los módulos de un mismo fabricante, se evita la dependencia de integraciones de terceros o de estándares que pueden tener limitaciones, demoras en soporte o problemas de interoperabilidad en la práctica.
- **Soporte unificado**: contar con un solo fabricante permite que el soporte técnico, actualizaciones y parches de seguridad se atiendan de forma integral y sin riesgos de transferencia de responsabilidades entre distintos proveedores.
- **Tiempo de respuesta ante incidentes**: la integración nativa permite una correlación inmediata de eventos entre los diferentes módulos (firewall, IPS, WAF, antimalware, etc.), lo que agiliza la detección y respuesta a amenazas.

Por estas razones, la Universidad considera indispensable que todos los componentes de seguridad provengan de un mismo fabricante y se integren de manera nativa, lo que

garantiza continuidad operativa, robustez en la protección y simplificación en la administración de la plataforma de seguridad perimetral.

OBSERVACIÓN 13:

Observación 13 – SD-WAN nativa obligatoria (pág. 9 y 11)
Restringir la funcionalidad a implementaciones nativas desconoce alternativas modulares.
Solicitud: Permitir cualquier implementación certificada que cumpla con la función.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que el requerimiento de que la funcionalidad de SD-WAN sea nativa obedece a criterios de simplicidad operativa, seguridad integral, desempeño optimizado y soporte unificado. Contar con esta capacidad integrada en la plataforma de seguridad perimetral garantiza mayor eficiencia en la gestión, evita riesgos de incompatibilidad y asegura continuidad operativa en los servicios institucionales.

OBSERVACIÓN 14:

Observación 14 – Licenciamiento definido como "ilimitado" (pág. 9)
El concepto "ilimitado" puede restringir modelos escalables de otros fabricantes.
Solicitud: Ajustar el requisito a un modelo basado en usuarios concurrentes o capacidad modular.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que en la relación a su observación en la página 9 no se hace referencia ningún termino de licenciamiento ilimitado, donde se hace referencia es a la cantidad ilimitada para el uso de VPN que se ve reflejado en el punto 9 de la página 39.

OBSERVACIÓN 15:

Observación 15 – Topologías de interconexión predefinidas (pág. 11)
El pliego menciona esquemas específicos (hub-to-spoke, full mesh), limitando otras topologías equivalentes.
Solicitud: Permitir cualquier topología que garantice conectividad segura entre sedes.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que el requerimiento de que la implementación del servicio de red en SD-WAN sea flexible hub-to-spoke (malla parcial), spoke-to-spoke (malla completa) y multi-WAN, al contar con esta capacidad integrada en la plataforma de seguridad perimetral garantiza mayor eficiencia en la gestión, evita riesgos de incompatibilidad y asegura continuidad operativa en los servicios institucionales. Y no es factible para la universidad por costos o presupuesto aplicaciones dinámicas en nube.

OBSERVACIÓN 16:

Observación 16 – Consola de gestión propietaria (pág. 22)

La exigencia de administración exclusiva en consola limita la integración con herramientas de terceros.
Solicitud: Permitir integración vía SNMP, CLI, API o estándares abiertos.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que el requerimiento hace referencia a una consola o aplicativo web que debe hacer entrega el oferente adjudicado dando cumplimiento a las necesidades establecidas. Es importante aclarar que dicha consola no es propiedad de la universidad.

OBSERVACIÓN 17:

Observación 17 – Filtros DNS atados a un fabricante (pág. 17)
Solicitamos que el requisito se formule de manera genérica, permitiendo equivalentes funcionales.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la intención de este requerimiento no es direccionar la contratación hacia un fabricante en particular, sino garantizar que la solución cuente con servicios de seguridad confiables.

Por lo anterior, se acoge la observación y se procederá a ajustar el texto eliminando la referencia exclusiva y reemplazándola por una descripción más amplia y neutral, el cual se verá ajustado en la respectiva adenda del Anexo de Especificaciones Técnicas Definitivas.

OBSERVACIÓN 18:

Observación 18 – Exigencia de licenciamiento comercial predeterminado (pág. 7)
Al transcribir paquetes comerciales se excluye a oferentes que presentan soluciones equivalentes con licenciamiento diferente.
Solicitud: Formular las condiciones en términos de funcionalidades y no de marcas comerciales.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la intención de este requerimiento no es direccionar la contratación hacia un fabricante en particular, sino garantizar que la solución cuente con servicios de seguridad confiables.

Por lo anterior, se acoge la observación y se procederá a ajustar el texto eliminando la referencia exclusiva y reemplazándola por una descripción más amplia y neutral, el cual se verá ajustado en la respectiva adenda del Anexo de Especificaciones Técnicas Definitivas.

OBSERVACIÓN 19:

Observación 19 – Métricas SOC indefinidas (pág. 25)
Se solicita capacidad SOC sin especificar indicadores de desempeño, lo cual vulnera el principio de planeación. Solicitud: Establecer métricas mínimas como MTTR, número de eventos procesados por segundo o disponibilidad del servicio.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que en el anexo de

especificaciones técnicas, entre las páginas 29 a la 47, se encuentra definido el servicio de SOC, en el cual se detallan las características técnicas y los requisitos que deberán cumplirse.

OBSERVACIÓN 20:

Observación 20 – Integración con Active Directory ambigua (pág. 14)
No se definen roles de acceso ni privilegios.
Solicitud: Incluir al menos perfiles diferenciados de administrador, operador y auditor.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que, en relación con la integración con Active Directory, la referencia corresponde al directorio activo institucional, basado en la tecnología de Microsoft Windows. En consecuencia, no es posible contemplar ni ampliar este requerimiento a otros tipos de servicios de directorios corporativos.

OBSERVACIÓN 21:

Observación 21 – Reportes sin periodicidad (pág. 55)
La falta de definición sobre la frecuencia de reportes genera inseguridad jurídica.
Solicitud: Establecer periodicidad mínima mensual.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que el anexo técnico cuenta con un total de 41 páginas. En cuanto a la periodicidad de los reportes, esta será definida de manera conjunta con el oferente que resulte adjudicado al presente proceso.

OBSERVACIÓN 22:

Observación 22 – Políticas de actualización ambiguas (pág. 49)
No se diferencia entre actualizaciones críticas de seguridad y actualizaciones generales.
Solicitud: Aclarar los alcances y tiempos de aplicación.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que el anexo técnico cuenta con un total de 41 páginas. Respecto a las políticas de configuración, niveles de criticidad y periodicidad de las actualizaciones, estos aspectos serán informados oportunamente al oferente que resulte adjudicado al presente proceso.

OBSERVACIÓN 23:

Observación 23 – Terminología de marketing tecnológico (pág. 11)
Términos como "Zero Touch" corresponden a marcas registradas. Solicitud: Reemplazarlos por expresiones neutrales como "configuración automatizada".

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la expresión "Zero Touch Provisioning" no se está haciendo referencia a una marca registrada de un fabricante específico, sino se establece a un término de uso genérico en la industria de redes y telecomunicaciones, reconocido incluso en estándares internacionales como el IETF RFC 8572.

OBSERVACIÓN 24:

Observación 24 – SLA sin parámetros cuantificables (pág. 53)
Se habla de disponibilidad sin definir valores objetivos.
Solicitud: Establecer un mínimo de 99,9% de disponibilidad con mecanismos de verificación.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que en el anexo técnico se establecen las métricas de SLA que deberán considerarse (fluctuación, pérdida de paquetes y latencia, monitoreo en tiempo real, filtro basado en intervalo de tiempo, informes de SLA de enlace WAN, uso de sesión por aplicación, entre otras). Sin embargo, no se fijan valores de referencia específicos, dado que estos parámetros podrán variar según la solución tecnológica ofrecida y las condiciones propias de la infraestructura a implementar.

En este sentido, los valores de referencia se definirán de manera conjunta con el oferente que resulte adjudicado, garantizando que se ajusten a las necesidades operativas de la Universidad y a las capacidades técnicas de la solución seleccionada.

OBSERVACIÓN 25:

Observación 25 – Licenciamiento VPN ambiguo (pág. 35)
No se especifica si el licenciamiento es nominativo o concurrente.
Solicitud: Aclarar esta condición para permitir ofertas comparables.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que en el anexo de especificaciones técnicas pagina 10 se establece que:

xv. VPN/Overlay: Site-to-site ADVPN - túneles VPN dinámicos, VPN basado en políticas, IKEv1, IKEv2, DPD, PFS, ESP y soporte ESPHMAC, Compatibilidad con cifrado simétrico (IKE/ES P): AES- 128 y AES-256 modos: CBC, CNTR, XCBC, GCM, Pre-shared and PKI authentication con certificados RSA, intercambio de claves.

Por lo anterior no especificamos si el licenciamiento debía ser nominativo o concurrente, puesto que hay otros parámetros en los cuales se establece políticas para que satisfagan la necesidad.

OBSERVACIÓN 26:

Observación 26 – Integración con correo institucional (pág. 22)
No se especifica compatibilidad con la plataforma actual de la Universidad (O365 o Google). Solicitud: Definir explícitamente la plataforma de referencia.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la integración con el servicio de correo institucional deberá realizarse sobre la plataforma actualmente en uso por la Universidad, correspondiente a Microsoft Office 365, garantizando plena compatibilidad con sus funcionalidades.

OBSERVACIÓN 27:

Observación 27 – Roles de administración no definidos (pág. 30)
No se diferencian perfiles de acceso.
Solicitud: Establecer mínimo tres perfiles diferenciados (administrador, operador, auditor).

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la administración del aplicativo de seguridad perimetral será compartida junto con el oferente, donde los ingenieros contaran con un usuario con permisos capaces de Administrar usuarios, configurar políticas de seguridad, control de aplicaciones, administración de dispositivos, monitoreo y generación de informes, esto se encuentra en la página 65 de los términos de la invitación obligación 22.

OBSERVACIÓN 28:

Observación 28 – Algoritmos de cifrado obsoletos (pág. 13)
Se mencionan algoritmos en desuso (DES, 3DES).
Solicitud: Actualizar a estándares modernos (AES-GCM, SHA-512, ChaCha20-Poly1305).

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la mención a algoritmos como DES y 3DES en el anexo técnico corresponde únicamente a efectos de compatibilidad heredada. No obstante, para el cumplimiento del presente proceso se dará prioridad al uso de algoritmos recomendados por estándares internacionales, tales como AES (en sus modos CBC y GCM). Adicionalmente se establece que son requerimientos mínimos a tener en cuenta el oferente para la solución a ofertar.

OBSERVACIÓN 29:

Observación 29 – Cobertura SOC ambigua (pág. 5)
No se define con precisión qué componentes serán monitoreados.
Solicitud: Aclarar si cubre firewalls, endpoints, aplicaciones críticas y nube.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que el presente proceso engloba todo el tema de servicio de seguridad perimetral para lo cual y de acuerdo a las **Capacidades de descubrimiento, monitoreo y correlación:** La solución debe realizar monitoreo en tiempo real y continuo de los eventos de seguridad, desempeño y disponibilidad de los dispositivos, entre otras funciones que se establecen el pliego de especificaciones técnicas del proceso.

OBSERVACIÓN 29:

Observación 29 – Cobertura SOC ambigua (pág. 5)
No se define con precisión qué componentes serán monitoreados.
Solicitud: Aclarar si cubre firewalls, endpoints, aplicaciones críticas y nube.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que el presente proceso engloba todo el tema de servicio de seguridad perimetral para lo cual y de acuerdo con las

Capacidades de descubrimiento, monitoreo y correlación: La solución debe realizar monitoreo en tiempo real y continuo de los eventos de seguridad, desempeño y disponibilidad de los dispositivos, entre otras funciones que se establecen el pliego de especificaciones técnicas del proceso.

OBSERVACIÓN 30:

Observación 30 – Transferencia de conocimiento indefinida (pág. 39)
No se establecen parámetros mínimos de capacitación.
Solicitud: Definir horas, modalidad (presencial/virtual) y entregables.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la transferencia de conocimiento dentro de los términos de la presente invitación en la obligación 27 dice lo siguiente: El CONTRATISTA deberá realizar una transferencia de conocimiento dirigida al personal designado por la Universidad, del área de servicios tecnológicos adscrita a la Dirección de Sistemas y Tecnología (hasta 10 participantes), que incluya la solución WAN propuesta, conceptos técnicos y mejores prácticas para la administración, configuración y operación de las herramientas de monitoreo, gestión y plataformas ofrecidas, incluyendo NGFW, SD-WAN, WAF y SIEM. Esta capacitación deberá permitir a los ingenieros conocer, gestionar y administrar la topología y los equipos involucrados, y podrá realizarse de forma virtual o presencial, según lo solicite la Universidad.

OBSERVACIÓN 31:

Observación 31 – Cronograma insuficiente (pág. 41)
El plazo otorgado resulta limitado frente a la complejidad del proyecto, lo que reduce la pluralidad de oferentes.
Solicitud: Ampliar mínimo una semana para permitir propuestas sólidas y competitivas.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que, en esta etapa del proceso, no es posible realizar modificaciones ni al cronograma, ni a los requisitos habilitantes establecidos en los pliegos de condiciones.

Lo anterior obedece a que el servicio actual se encuentra en su fase final y los plazos definidos en el cronograma ya no permiten la introducción de cambios que impliquen ajustes a las reglas de participación. En consecuencia, deben mantenerse los términos publicados, con el fin de garantizar la transparencia, la igualdad entre oferentes y el cumplimiento de los tiempos contractuales.

OBSERVACIÓN 32:

Observación 32 – Terminación unilateral sin compensación (cláusula general)
Se señala que la Universidad puede rechazar o terminar sin motivación. Esto contradice los principios de transparencia y responsabilidad. Solicitud: Establecer que cualquier decisión esté motivada y se reconozca el pago de lo ejecutado en caso de terminación anticipada.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que, en esta etapa del proceso, no es posible realizar modificaciones ni al cronograma, ni a los requisitos habilitantes establecidos en los pliegos de condiciones.

Lo anterior obedece a que el servicio actual se encuentra en su fase final y los plazos definidos en el cronograma ya no permiten la introducción de cambios que impliquen ajustes a las reglas de participación. En consecuencia, deben mantenerse los términos publicados, con el fin de garantizar la transparencia, la igualdad entre oferentes y el cumplimiento de los tiempos contractuales.

Agradecemos el interés manifestado y la disposición del oferente para participar en esta convocatoria.

Cordialmente,

Firmado digitalmente por HURTADO MESA ANA LUCIA
Fecha: 2025.09.04 07:57:28 -05'00'

ANA LUCIA HURTADO MESA
Directora de Sistemas y Tecnología
Universidad de Cundinamarca

Proyectó: Ing. Ingrid Sanchez Reyes
Área de Servicios Tecnológicos

15-30.7

15.

Fusagasugá, 2025-09-02.

Señor
LUIS DOMINGO HERNANDEZ CACERES
MERCANET S.A.S.

Asunto y/ó Ref: Respuesta Observaciones Invitación Privada 038 de 2025

Cordial saludo,

De manera atenta, me dirijo a usted con el fin de dar respuesta a las observaciones allegadas en referencia a la Invitación Privada 038 de 2025, que tiene como objeto: ***"CONTRATAR EL SERVICIO DE SEGURIDAD PERIMETRAL Y CONFIGURACION DE CONECTIVIDAD MEDIANTE TECNOLOGÍA SD-WAN PARA LA UNIVERSIDAD DE CUNDINAMARCA".***

OBSERVACIONES TÉCNICAS:

MERCANET S.A.S.

OBSERVACIÓN 1:

> La prestación del servicio se iniciará el primero (1°) de noviembre de 2025 y culminará el treinta y uno (31) de octubre de 2026, previa instalación, configuración y/o puesta en marcha de la solución ofertada.

El proyecto involucra la alineación de al menos tres proveedores distintos (colocation, seguridad perimetral y conectividad). En ese contexto, es importante precisar si el pliego contempla la posibilidad de ajustar el cronograma en caso de retrasos imputables a alguno de los otros proveedores, de manera que no se generen incumplimientos injustificados para el contratista de conectividad.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que el cronograma establecido en el proceso contempla tiempos de ejecución de carácter referencial y deberá ser ajustado en la etapa de implementación y configuración, de acuerdo con la coordinación de actividades entre los diferentes proveedores involucrados (colocation, seguridad perimetral y conectividad).

En caso de presentarse retrasos imputables a terceros que afecten la implementación del servicio de conectividad, dichos escenarios serán analizados por la supervisión del contrato y podrán dar lugar a ajustes razonables en los plazos de ejecución, siempre que se encuentre

debidamente justificado y documentado, con el fin de evitar incumplimientos no atribuibles al contratista.

OBSERVACIÓN 2:

Solicitamos a la entidad modificar el requisito de experiencia habilitante, de manera que se permita a los oferentes presentar hasta seis (6) certificaciones o actas de liquidación para demostrar la experiencia en contratos ejecutados.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que, en esta etapa del proceso, no es posible realizar modificaciones a los requisitos habilitantes establecidos en los pliegos de condiciones, dentro de los cuales se encuentra el criterio de experiencia.

Lo anterior obedece a que el servicio actual se encuentra en su fase final y los plazos definidos en el cronograma ya no permiten la introducción de cambios que impliquen ajustes a las reglas de participación. En consecuencia, deben mantenerse los términos publicados, con el fin de garantizar la transparencia, la igualdad entre oferentes y el cumplimiento de los tiempos contractuales.

OBSERVACIÓN 4:

Solicitamos a la entidad eliminar el requisito de la membresía First, ya que más que una certificación es un esquema de información sobre alertamiento y amenazas de seguridad.

6.2.3 MEMBRESIA FIRST - (CINCUENTA 50 PUNTOS)

Se otorgarán **CINCUENTA (50) PUNTOS** al oferente que, adicionalmente presente en su propuesta el certificado de membresía de FIRST para su proceso de SOC, con una vigencia mínima de un (1) año contado a partir de su expedición, la cual debe estar vigente durante la ejecución del contrato.

RESPUESTA: La Universidad de Cundinamarca se permite aclarar que la inclusión de este requisito obedece a la necesidad de garantizar que el oferente cuente con un SOC reconocido internacionalmente, con la capacidad de integrarse en tiempo real a redes globales de alerta temprana, intercambio de información y coordinación de respuesta frente a incidentes de seguridad cibernética.

La membresía FIRST aporta valor agregado en términos de:

- Prevención: acceso temprano a alertas globales de ciberseguridad.
- Respuesta: coordinación con equipos internacionales ante incidentes de gran escala.
- Confianza: validación de que el oferente cumple con parámetros de madurez y confianza exigidos por esta comunidad internacional.

Por lo anterior, la Universidad considera que este requerimiento no debe retirarse, ya que su

inclusión no limita injustificadamente la participación, sino que busca asegurar un nivel de calidad, reconocimiento y capacidad de respuesta internacional, complementando las certificaciones formales exigidas dentro del Anexo de Especificaciones Técnicas.

Agradecemos el interés manifestado y la disposición del oferente para participar en esta convocatoria.

Cordialmente,

Firmado digitalmente por HURTADO MESA ANA LUCIA
Fecha: 2024.09.02 18:05:02 -05'00'

ANA LUCIA HURTADO MESA
Directora de Sistemas y Tecnología
Universidad de Cundinamarca

Proyectó: Ing. Jeniffer Castillo Fernández
Ing. Ingrid Sanchez Reyes
Área de Servicios Tecnológicos

15-30.7