UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

CONSOLIDADO DE OBSERVACIONES AL PLIEGO DE CONDICIONES CONVOCATORIA No 007 DE 2026 "ADQUIRIR UNA SOLUCIÓN DE DETECCIÓN, PREVENCIÓN Y RESPUESTA ANTE CIBERAMENAZAS A NIVEL DE RED, QUE GARANTICE LA ADMINISTRACIÓN Y ANALÍTICA DE TRÁFICO CENTRALIZADA, INTEGRACIÓN CON LA INFRAESTRUCTURA DE SEGURIDAD ACTUAL DE LA UNIVERSIDAD, CAPACIDADES DE VISIBILIDAD, MONITOREO Y CORRELACIÓN DE EVENTOS PARA ENDPOINTS ESTRATÉGICOS, INCLUYENDO LOS COMPONENTES DE HARDWARE Y SOFTWARE NECESARIOS PARA SU IMPLEMENTACIÓN, CONFIGURACIÓN Y OPERACIÓN ON PREMISE, SOPORTE TÉCNICO ESPECIALIZADO 7X24 Y GARANTÍA".

OBSERVACIONES REALIZADAS POR LA EMPRESA INFO COMUNICACIONES S.A.S NIT: 830.044.415-3 BIBIANA DEVIA CAMELO REPRESENTANTE LEGAL DIRECCIÓN: AUTOPISTA MEDELLÍN KM 3.5, TERMINAL TERRESTRE DE CARGA DE BOGOTÁ, OF. C4 Y C5 CORREOS ELECTRÓNICOS: bibiana@infocomunicaciones.net - lquiroga@infocomunicaciones.net 3176431579

OBSERVACIÓN No. 1

OBSERVACIÓN : 2.2 INDICADORES FINANCIEROS.

INFO COMUNICACIONES S.A.S. solicita respetuosamente a la Universidad la flexibilización de los indicadores financieros, con el ánimo de ampliar la pluralidad de oferentes. La compañía cuenta con más de 28 años de experiencia atendiendo soluciones y requerimientos de empresas del sector público y privado a nivel nacional. Durante este tiempo ha mantenido la solidez de su flujo de caja y la disponibilidad de recursos de corto y mediano plazo necesarios para desarrollar las operaciones requeridas por sus clientes.

Respetuosamente solicitamos a la Universidad modificar el requisito de razón de cobertura de intereses, actualmente establecido en un valor mayor o igual a 2,00, y fijarlo en un valor mayor o igual a 1,45, con el propósito de ampliar la pluralidad de oferentes sin afectar la capacidad financiera requerida para la ejecución del contrato. La compañía mantiene una adecuada capacidad de pago, respaldada por:

- *Flujo de caja operativo positivo.*
- *Cumplimiento oportuno de sus obligaciones financieras.*
- *Estructura patrimonial sólida.*
- *Estabilidad de sus ingresos recurrentes.*
- *Índice de liquidez sólido.*

Asimismo, el contrato estará respaldado por la póliza de cumplimiento exigida, que garantiza a la entidad el cumplimiento de las obligaciones derivadas del contrato.

Por lo anterior, solicitamos a la entidad acoger la modificación propuesta y establecer la razón de cobertura de intereses en un valor mayor o igual a 1,45. Este ajuste mantiene un nivel adecuado de exigencia financiera, favorece la pluralidad de oferentes y reconoce la capacidad de la compañía para atender oportunamente sus obligaciones contractuales.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. La Universidad requiere que la empresa a la que se adjudique el contrato tenga musculo financiero máxime que al ser un Contrato de compraventa la forma de pago requiere que la empresa tenga una liquidez operativa y capacidad para cubrir obligaciones a corto plazo.

OBSERVACIÓN No. 2

OBSERVACIÓN 2: 2.2 INDICADORES FINANCIEROS.

Con el ánimo de ampliar y fomentar la pluralidad de oferentes, solicitamos respetuosamente a la Universidad modificar el requisito de Capital de Trabajo, actualmente establecido en un valor mayor o igual al 100 % de la oferta económica, y fijarlo en un valor mayor o igual al 96,5 % de la oferta económica.

El capital de trabajo de la compañía se encuentra muy próximo al 100 % requerido y evidencia una capacidad financiera suficiente para asumir las obligaciones derivadas del contrato. Adicionalmente, la totalidad de nuestros proveedores otorga plazos de crédito superiores a 60 días, como resultado de relaciones comerciales consolidadas durante varios años y del cumplimiento oportuno de las obligaciones adquiridas. Estas condiciones comerciales fortalecen la disponibilidad de recursos durante la ejecución, sin necesidad de incrementar el endeudamiento financiero, y respaldan la capacidad de la compañía para asumir nuevos compromisos y ejecutar integralmente el contrato, en caso de resultar adjudicataria.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. La Universidad requiere que la empresa a la que se adjudique el contrato tenga musculo financiero máxime que al ser un Contrato de compraventa la forma de pago requiere que la empresa tenga una liquidez operativa y capacidad para cubrir obligaciones a corto plazo.

OBSERVACIONES REALIZADAS POR LA EMPRESA HEIMCORE SAS NIT: 900.425.697-2 DIRECCIÓN: CALLE 98 NO. 70 - 91 OF 202 EDIFICIO VARDI CORREO ELECTRÓNICO: info@heimcore.com.co NÚMERO DE TELÉFONO: 300 3764569 / 300 8025736 / 601 5804352 / 3186267462

OBSERVACIÓN No. 1

A continuación, y de la manera más respetuosa, presentamos las siguientes observaciones técnicas depuradas al proceso en mención, orientadas a precisar el alcance funcional, preservar la pluralidad de oferentes y mantener el cumplimiento de los objetivos técnicos definidos por la Universidad.

Observación No. 1 - Arquitectura física, virtual o software del fabricante sobre hardware dedicado

Ubicación del requerimiento:

Numeral 1.2 - Alcance técnico, literal a, y Anexo 10 - Requerimientos técnicos, ítems 1, 2, 3 y 4. Allí se solicita un nodo central en Calle 40, un sensor o colector en Bosa Porvenir y componentes físicos para la operación on-premise.

Observación: Teniendo en cuenta la respuesta a la observación de los pre pliegos, se solicita confirmar si nuestro entendimiento es correcto, en cuanto a que el equipo en el que se instale, debe garantizar la infraestructura dedicada requerida para el correcto funcionamiento de la solución.

RESPUESTA DE LA UNIVERSIDAD: La observación es correcta. El equipo físico ofertado sobre el cual se implemente la solución deberá garantizar la infraestructura dedicada requerida para su correcto funcionamiento, conforme a los requerimientos técnicos establecidos en el proceso.

OBSERVACIÓN No. 2

Observación No. 2 - Consola centralizada de la solución e integración con el SIEM institucional

Ubicación del requerimiento:

Anexo 10 - Requerimientos técnicos, ítems 21, 24, 39, 40 y 48, donde se solicita interfaz web, administración centralizada, integración con SIEM y gestión/visualización de información desde una consola centralizada.

Observación: Con base en la respuesta a la observación presentada en pre pliegos, se solicita a la entidad confirmar nuestro entendimiento, en cuanto a que la consola centralizada puede ser la consola del NDR.

RESPUESTA DE LA UNIVERSIDAD: La observación es correcta. La consola centralizada corresponde a la consola de administración de la solución NDR ofertada.

OBSERVACIÓN No. 3

Observación No. 3 - Módulos SFP+ Cisco originales o compatibles certificados

Ubicación del requerimiento:

Anexo 10 - Requerimientos técnicos, ítem 11, donde se solicita SFP+ fabricante Cisco, argumentando que el switch core es de esta marca y que un fabricante diferente podría traer complicaciones en la garantía del switch core.

Observación:

Con base en la respuesta a la observación de pre pliegos, se solicita a la entidad confirmar si es posible ofertar SFP+ de otros fabricantes que no sea exclusivamente Cisco, siempre que cumplan con lo requerido en la ficha técnica y sean compatibles con los equipos Cisco

actuales. En caso afirmativo, por favor eliminar el requerimiento de fabricante específico, dado que, por un lado, existen fabricantes que se integran nativamente y cuentan con garantía de integración con Cisco y por otro lado el proceso es de Ciberseguridad, y exigir un fabricante para un SFP+ limita la pluralidad de oferentes.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. La Universidad requiere que los módulos SFP+ sean del fabricante Cisco, con el fin de garantizar la compatibilidad, el correcto funcionamiento y mantener las condiciones de soporte y garantía de la infraestructura de red existente.

OBSERVACIÓN No. 4

Observación No. 4 – Ofrecimientos técnicos adicionales

ÍTEM	DESCRIPCIÓN	ASIGNACIÓN DE PUNTOS	TOTAL
1	Ampliación de las capacidades de visibilidad, monitoreo y correlación de eventos sobre endpoints adicionales a los cuatrocientos (400) requeridos en el presente proceso, mediante agentes, sensores, telemetría de red u otros mecanismos soportados por el fabricante, durante la vigencia del contrato.	Se otorgarán hasta 100 puntos al proponente que cubra la mayor cantidad de Endpoints.	100
2	Ampliación del tiempo de licenciamiento y soporte técnico para la plataforma de detección, prevención y respuesta ante ciberamenazas a nivel de red.	Se otorgarán hasta 200 puntos al proponente que ofrezca más tiempo de licenciamiento	200

Con respecto al ítem 2, se solicita a la entidad aclaración sobre el tiempo de licenciamiento.

• ¿La ampliación es únicamente para la solución de protección de EndPoints (Ítem 3 de la propuesta económica)?

3	Suministro de mecanismos para las capacidades de visibilidad, monitoreo y correlación de eventos para cuatrocientos (400) endpoints, por un periodo mínimo de un (1) año, como complemento a las capacidades de detección y respuesta de red de la solución ofertada		400

• ¿La ampliación es únicamente para la línea base de 400 licencias?

RESPUESTA DE LA UNIVERSIDAD: La observación es incorrecta. La ampliación de tiempo de licenciamiento y soporte técnico solicitada en el item 1 de la tabla "Ofrecimientos técnicos adicionales" es para todos los componentes de software la solución (solución de detección, prevención y respuesta de red, capacidades de visibilidad, monitoreo y correlación de eventos 400 endpoints y endpoints ofertados como "ofrecimientos adicionales").

OBSERVACIÓN No. 5

Observación No. 5 - 4. ESPECIFICACIONES TÉCNICAS CIBERSEGURIDAD

3	Arquitectura y componentes físicos de la solución	La solución deberá incluir los componentes físicos necesarios para la implementación de un nodo central de administración, análisis y correlación de eventos, el cual deberá ser instalado en la sede Calle 40 y un sensor o colector de tráfico en la sede Bosa Porvenir

Se solicita muy amablemente a la entidad, confirmar el throughput y/o velocidad de red en las dos sedes nombradas (Calle 40 y Bosa) Esto para diseñar y costear de manera correcta la solución de NDR a ofertar a la entidad

RESPUESTA DE LA UNIVERSIDAD: El throughput en la sede Calle 40 ha presentado un punto máximo de 4 Gbps manteniéndose en un promedio de 3.2 Gbps, mientras que en la sede Bosa Porvenir presenta picos máximos de 1 Gbps manteniéndose en un promedio de 0.7 Gbps.

OBSERVACIÓN No. 6

Observación No. 6 - 4. ESPECIFICACIONES TÉCNICAS CIBERSEGURIDAD

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

Se solicita muy amablemente a la entidad permitir que se oferten soluciones tipo SaaS y no únicamente las que operen de manera local, siempre que sea posible gestionar los datos bajo estrictos estándares de seguridad y gobernanza completa de los datos, así como el cumplimiento de retención y gestión de datos de la entidad. Esta solicitud se realiza dado que los principales fabricantes de soluciones de detección y respuesta como lo solicitado en el pliego, ofrecen sus soluciones en modalidad SaaS, sin resignar seguridad, gobernanza ni latencia.

Acorde a la audiencia celebrada el día 29/Julio, la entidad explicó que requiere seguridad en la información y gobernanza de datos, y es evidente que los fabricantes de Ciberseguridad que cuentan con soluciones en nube ya incluyen tanto la seguridad como la gobernanza de datos dentro de sus soluciones.

Así como lo exige la misma entidad en el Anexo Técnico, los principales analistas del mercado sitúan en las primeras posiciones, soluciones tipo SaaS porque el propio concepto de estas plataformas está diseñado para operar como sistemas centralizados de correlación, analítica y respuesta que requieren ingesta masiva de telemetría distribuida, inteligencia global y actualización continua, lo cual se optimiza en arquitecturas cloud multi tenant; de hecho, Gartner define XDR explícitamente como una solución "SaaS-based" que integra múltiples controles en una plataforma unificada. Es decir, entre mayor telemetría de las fuentes globales de Threat Intelligence, más robusta es la plataforma.

Por otro lado, el modelo SaaS habilita ventajas críticas identificadas en informes de mercado: elasticidad para procesar grandes volúmenes de datos, acceso a inteligencia de amenazas global compartida entre clientes, reducción del time-to-value al evitar despliegues complejos on-prem, y operación continúa orientada a SOC modernos e incluso MSSP (multi-tenant).

Sin embargo, para permitir la pluralidad de oferentes, se solicita a la entidad permitir ofertar soluciones tipo on-premises y/ tipo SaaS.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. La Universidad definió que la solución deberá implementarse bajo una arquitectura On-Premise, conforme a las necesidades institucionales relacionadas con la administración de la infraestructura, la gobernanza de la información y la operación de la solución.

OBSERVACIÓN No. 7

b. Los componentes de la solución no deberán encontrarse en estado de End of Sale (EOS) ni End of Life (EOL) al momento de la presentación de la oferta. El fabricante deberá garantizar un ciclo de vida y soporte no inferior a cinco (5) años, incluyendo actualizaciones de seguridad y soporte técnico.

Se solicita muy amablemente a la entidad confirmar si el estado EOS y/o EOL es posible garantizarlo mediante links y/o catálogos oficiales del fabricante.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. El cumplimiento del requisito debe acreditarse mediante certificación del fabricante que permitan verificar que los componentes ofertados no se encuentran en estado End of Sale (EOS) ni End of Life (EOL), y que cuentan con el ciclo de vida y soporte requerido.

OBSERVACIÓN No. 8

Observación 8 - 4. ESPECIFICACIONES TÉCNICAS CIBERSEGURIDAD

a. **Suministro de hardware:** Componentes físicos necesarios para la correcta implementación y operación de la solución ofertada (servidores, appliances, sensores, interfaces de captura, módulos, cableados y demás elementos requeridos según la solución del oferente).

La arquitectura prevista para la implementación de la solución debe contemplar un nodo (físico) central de administración y análisis ubicado en la sede Calle 40 de la Universidad Distrital y un sensor o colector de tráfico (físico) en la sede Bosa Porvenir. Además, con el fin de fortalecer las capacidades de monitoreo y análisis de tráfico de red sobre los segmentos priorizados por la Universidad, debe permitir la incorporación de nuevos sensores, los cuales podrán ser desplegados de manera virtual o física sobre la infraestructura tecnológica de la Universidad, sin que ello genere costos adicionales a la Universidad.

El hardware propuesto deberá permitir el almacenamiento, consulta de eventos, alertas y telemetría histórica generada por la solución, garantizando una retención mínima de noventa (90) días disponibles para análisis por parte de la Universidad.

Se solicita muy amablemente a la entidad aclarar si la universidad será la responsable de proveer el canal de comunicaciones entre la sede Calle 40 y el sensor ubicado en la sede Bosa Porvenir.

RESPUESTA DE LA UNIVERSIDAD: La observación es correcta. La Universidad será la responsable de suministrar el canal de comunicaciones entre la sede Calle 40 y la sede Bosa Porvenir, requerido para la operación de la solución.

OBSERVACIÓN No. 9

Observación 9 – Certificación de Vigencia y soporte del hardware

3.2.2 CERTIFICACIÓN DE VIGENCIA Y SOPORTE DEL HARDWARE:

Certificación expedida por fabrica donde se acredite que los equipos ofertados corresponden a productos nuevos, originales, vigentes dentro del portafolio oficial del fabricante, no se encuentran en estado de fin de vida (EOL) ni fin de soporte (EOS), y cuentan con garantía y soporte oficial del fabricante por un período no inferior al requerido por la Universidad. Dicha certificación deberá tener una fecha de expedición no mayor a treinta (30) días calendario anteriores a la fecha de cierre del presente proceso.

Se solicita muy amablemente a la entidad confirmar si el estado EOS y/o EOL es posible garantizarlo mediante links y/o catálogos oficiales del fabricante.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. El cumplimiento del requisito debe acreditarse mediante certificación del fabricante que permitan verificar que los componentes ofertados no se encuentran en estado End of Sale (EOS) ni End of Life (EOL), y que cuentan con el ciclo de vida y soporte requerido.

OBSERVACIONES REALIZADAS POR LA EMPRESA COMPAÑÍA DE INGENIEROS DE SISTEMAS ASOCIADOS – COINSA S.A.S. JUAN CARLOS RIOS NEIRA C.C. 79.569.840 DE BOGOTÁ D.C REPRESENTANTE LEGAL

OBSERVACIÓN No. 1

La COMPAÑÍA DE INGENIEROS DE SISTEMAS ASOCIADOS – COINSA S.A.S., identificada con NIT 800.143.512-5, representada legalmente por Juan Carlos Ríos Neira identificado con C. C. No.: 79.569.840 de Bogotá, manifiesta su interés en participar en el proceso de selección de la referencia.

En aras de garantizar los principios de libre concurrencia, transparencia, objetividad y selección equitativa, nos permitimos presentar las siguientes observaciones y solicitudes de aclaración de orden técnico al Pliego de Condiciones / Anexo Técnico, para su respetuosa evaluación y respuesta:

Observación 1. Visita técnica y/o entrega de información de infraestructura

Referencia: Especificaciones Técnicas, numerales 2, 3 y 6; proceso de implementación, literal e).

Situación identificada: La solución debe instalarse en Calle 40 y Bosa Porvenir e integrarse con puntos Core, DMZ y Data Center. Sin embargo, los documentos no incluyen diagrama de red, inventario de switches, disponibilidad de puertos, rack, energía, direccionamiento, mecanismos de SPAN, rutas, latencias ni condiciones de acceso a las sedes.

Solicitud de aclaración o ajuste: Programar una visita técnica a las sedes involucradas o, en su defecto, publicar un documento de alistamiento con topología lógica y física, equipos y versiones, puertos disponibles, capacidad de puertos en los switches, ubicación de Core/DMZ/Data Center, condiciones de rack, energía, red de gestión, direccionamiento, acceso remoto y restricciones de intervención.

RESPUESTA DE LA UNIVERSIDAD: Se acepta la observación. Dando claridad:

1. Por razones de seguridad de la infraestructura tecnológica de la Universidad, no se debe publicar información detallada sobre la topología de red, direccionamiento, accesos, configuraciones o demás aspectos de la infraestructura interna solicitados por el oferente.

2. Los interesados podrán realizar visita técnica para levantamiento de información y preparación de la oferta de la siguiente manera:
- Sede Calle 40 (Carrera 8 # 40 - 62) el día 10 de agosto de 8 am a 10 am - **Única fecha**
- Sede Bosa Porvenir (Calle 52 Sur # 93D - 97) el día 10 de agosto de a 11 am a 1 pm - **Única fecha**

Las personas que asistan deben llevar la identificación de la empresa y certificado de pago de parafiscales.

OBSERVACIÓN No. 2

Observación 2. Cantidad y ubicación de los puntos de captura

Referencia: Especificaciones Técnicas, proceso de implementación, literal e), numeral i.

Situación identificada: Las pruebas deben validar tráfico proveniente de Core, DMZ y Data Center institucionales, pero no se establece cuántos puntos SPAN o port mirroring se entregarán, en qué sedes se encuentran, si el tráfico llegará agregado al nodo o al sensor, ni la capacidad de cada enlace.

Solicitud de aclaración o ajuste: Publicar la cantidad, ubicación y capacidad de los puertos de captura; indicar el origen de cada SPAN, la sobresuscripción esperada, las VLAN o segmentos incluidos y la responsabilidad de configurar los equipos de red institucionales.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. Por razones de seguridad de la infraestructura tecnológica de la Universidad, no se debe publicar información detallada sobre la topología de red, direccionamiento, accesos, configuraciones o demás aspectos de la infraestructura interna solicitados por el oferente. Esta información será entregada a la empresa que resulte adjudicataria del contrato.

OBSERVACIÓN No. 3

Observación 3. Captura de tráfico en bruto y periodo de conservación de PCAP

Referencia: Especificaciones Técnicas, ítems 83 y 100 a 105; respuesta al prepliego sobre retención.

Situación identificada: Las respuestas al prepliego aclararon que los noventa días no aplican necesariamente a la totalidad del tráfico en bruto; no obstante, esta precisión no quedó incorporada de manera expresa en el texto definitivo. Tampoco se define si la captura será continua, selectiva, asociada a eventos o bajo demanda.

Solicitud de aclaración o ajuste: Incorporar en adenda que la retención de noventa días aplica a eventos, alertas, registros y telemetría, y definir el alcance de captura de paquetes, periodo mínimo de conservación de PCAP, tráfico o segmentos a capturar y criterios de activación.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. Se aclara que el periodo mínimo de noventa (90) días de retención corresponde a los eventos, alertas, registros y telemetría generados por la solución, conforme a la arquitectura ofertada. En cuanto a la captura y conservación de tráfico de red en bruto (PCAP) u otros mecanismos equivalentes soportados por el fabricante, su alcance, forma de captura y periodo de conservación dependerán de la arquitectura y capacidades de la solución ofertada, siempre que se garantice el cumplimiento de las funcionalidades de investigación forense, respuesta a incidentes y exportación de evidencia técnica establecidas en los numerales 83, 100 a 105 de la tabla de especificaciones técnicas.

OBSERVACIÓN No. 4

Observación 4. Recursos para sensores virtuales adicionales

Referencia: Especificaciones Técnicas, ítems 4, 5 y 22; respuesta al prepliego.

Situación identificada: Se permite incorporar sensores físicos o virtuales sin costo adicional dentro de la capacidad contratada, pero no se indican los recursos de virtualización que aportará la Universidad, versiones de hipervisor, CPU, RAM, almacenamiento, interfaces ni licencias necesarias.

Solicitud de aclaración o ajuste: Aclarar que los recursos de infraestructura virtual serán suministrados por la Universidad y publicar las plataformas disponibles. Precisar si el adjudicatario solo deberá desplegar y configurar el software o también suministrar licencias y recursos adicionales.

Endpoints e integraciones institucionales

RESPUESTA DE LA UNIVERSIDAD: La observación es correcta. La incorporación de nuevos sensores diferentes a lo solicitados en el presente proceso, sean físicos o virtuales serán suministrados por la Universidad, sin embargo, estos no deben generar costos adicionales de licenciamiento, siempre que no se supere la capacidad (throughput) o capacidades adquiridas por la Universidad.

OBSERVACIÓN No. 5

Observación 5. Alcance exacto de los cuatrocientos endpoints

Referencia: Pliego, numeral 1.2 literal b); Especificaciones Técnicas, ítems 48 a 50 y 94.

Situación identificada: Se requieren capacidades sobre 400 endpoints, pero no se informa la distribución por sistema operativo, tipo de equipo, sede, perfil de uso, conectividad remota, versiones instaladas ni si los 400 equipos son parte de los aproximadamente 4.000 actualmente protegidos.

Solicitud de aclaración o ajuste: Publicar la distribución de los 400 endpoints por sistema operativo y versión, tipo de dispositivo, sede y modalidad de conexión. Confirmar si serán seleccionados dentro del parque existente y si la Universidad entregará el listado y las ventanas de despliegue.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. Los cuatrocientos (400) endpoints corresponden a los activos estratégicos que la Universidad ha definido para complementar las capacidades de visibilidad, monitoreo y correlación de la solución. La información específica relacionada con el sistema operativo y versión, tipo de dispositivo, sede y modalidad de conexión serán suministrada al contratista seleccionado durante la etapa de implementación, por lo que no se considera necesario publicar dicha información en el presente proceso.

OBSERVACIÓN No. 6

Observación 6. Responsabilidad sobre conectores, scripts y cambios de API

Referencia: Especificaciones Técnicas, ítems 35 a 40; garantía y soporte.

Situación identificada: Cuando la integración se implemente mediante API, scripts o conectores, no se establece quién será propietario del desarrollo, quién mantendrá el código ni el alcance de ajustes ante cambios de versión de plataformas de terceros durante la garantía.

Solicitud de aclaración o ajuste: Definir si los scripts o conectores deberán entregarse documentados a la Universidad y precisar que los ajustes durante la vigencia se limitarán a las versiones y APIs declaradas al inicio, salvo que se acuerden cambios de alcance.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. Los ítems 35 a 40 citados establecen las capacidades de integración que debe ofrecer la solución mediante APIs o mecanismos soportados por el fabricante. La implementación, configuración y documentación de los mecanismos de integración necesarios para el correcto funcionamiento de la solución serán responsabilidad del contratista, conforme a las condiciones establecidas en el proceso

OBSERVACIÓN No. 7

Observación 7. Alcance del sandboxing y licencias de sistemas operativos

Referencia: Especificaciones Técnicas, ítems 16, 52 y 65 a 77.

Situación identificada: Se exigen capacidades de sandboxing para múltiples sistemas operativos, análisis de documentos y archivos protegidos. No se define si el componente debe ser físico o virtual, cuántas instancias o imágenes se requieren ni quién suministra las licencias de los sistemas operativos utilizados en el entorno de análisis.

Solicitud de aclaración o ajuste: Indicar los sistemas operativos e imágenes mínimas requeridas, cantidad de entornos concurrentes y responsabilidad sobre sus licencias. Confirmar que el sandbox podrá ser nativo, componente del mismo fabricante o integración soportada, conforme a las respuestas al prepliego.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. Los items 16, 52, 65 a 77 definen las capacidades que debe ofrecer la solución para el análisis avanzado de amenazas, sin imponer una arquitectura o configuración específica para su implementación. En este sentido, el sandbox podrá ser nativo o implementarse mediante integraciones soportadas por el fabricante, siempre que se cumplan las capacidades establecidas en el presente proceso, todo recurso necesario para el funcionamiento del sandbox debe ser cubierto por el contratista.

OBSERVACIÓN No. 8

Observación 8. Contradicción sobre el ciclo de soporte del software

Referencia: Especificaciones Técnicas, numeral 5 literal b); Pliego, numeral 3.2.3; respuestas al prepliego.

Situación identificada: Las Especificaciones Técnicas, ajustadas con ocasión de las respuestas al prepliego, exigen soporte no inferior a dos años para el software NDR. En contraste, el numeral 3.2.3 del Pliego definitivo exige una proyección de soporte no inferior a cinco años para el licenciamiento. Ambos requisitos son incompatibles.

Solicitud de aclaración o ajuste: Unificar los documentos y confirmar que para los componentes de software de ciberseguridad se exigirá el periodo de dos (2) años aceptado en las respuestas al prepliego, mientras que los cinco (5) años aplicarán a los componentes de hardware. Redacción sugerida: Para los componentes de software de ciberseguridad, el fabricante deberá garantizar ciclo de vida y soporte no inferior a dos (2) años. Para el hardware, el ciclo de vida y soporte será no inferior a cinco (5) años.

RESPUESTA DE LA UNIVERSIDAD: Se acepta la observación. Se aclara que, para el licenciamiento ofertado, la proyección de soporte oficial por parte del fabricante deberá ser no inferior a dos (2) años, conforme a lo establecido en las respuestas al prepliego. El requisito correspondiente a un periodo de cinco (5) años aplica a los componentes de hardware suministrados como parte de la solución, de acuerdo con lo establecido en el proceso.

Quedando el punto 3.2.3. CERTIFICACIÓN DE VIGENCIA Y SOPORTE DEL LICENCIAMIENTO del pliego y el numeral 5. Certificaciones técnicas del documento de especificaciones de la siguiente manera:

a. Certificación del fabricante o canal autorizado: Certificación expedida por el fabricante en la cual conste que el oferente es un distribuidor autorizado, que está en capacidad de instalar, configurar, soportar, realizar mantenimiento y cumplir con las garantías que acompañan los productos en el territorio colombiano de la marca ofertada, en niveles superiores de certificación, según la clasificación del fabricante. Dicha certificación deberá tener una fecha de expedición no mayor a treinta (30) días calendario anteriores a la fecha de cierre del presente proceso. Se aclara que, en caso de que el oferente presente una solución compuesta por hardware y software de fabricantes diferentes, deberá presentar la certificación correspondiente para cada uno de los componentes, expedida por el respectivo fabricante o por su canal autorizado.

b. Certificación de vigencia y soporte del hardware: Certificación expedida por fabrica donde se acredite que los equipos ofertados corresponden a productos nuevos, originales, vigentes dentro del portafolio oficial del fabricante, no se encuentran en estado de fin de vida (EOL) ni fin de soporte (EOS) al momento de la presentación de la oferta, que cuentan con una proyección de soporte oficial por parte del fabricante no inferior a cinco (5) años, y con garantía y soporte oficial del fabricante por un período no inferior al requerido por la Universidad (1 año). Dicha certificación deberá tener una fecha de expedición no mayor a treinta (30) días calendario anteriores a la fecha de cierre del presente proceso.

c. Certificación de vigencia y soporte del licenciamiento: Certificación expedida por el fabricante, en la que se indique que la solución y el licenciamiento ofertado corresponden a productos vigentes dentro del portafolio oficial del fabricante, que no se encuentran en estado de fin de vida (EOL) ni fin de soporte (EOS) al momento de la presentación de la oferta, y que cuentan con una proyección de soporte oficial por parte del fabricante no inferior a dos (2) años, incluyendo actualizaciones, parches de seguridad y mantenimiento, garantizando así la continuidad tecnológica de la solución durante su ciclo de vida. Dicha certificación deberá tener una fecha de expedición no mayor a treinta (30) días calendario anteriores a la fecha de cierre del presente proceso.

OBSERVACIÓN No. 9

Observación 9. Certificaciones separadas para fabricante de software y fabricante de hardware

Referencia: Pliego, numerales 3.2.1 a 3.2.3; Especificaciones Técnicas, numeral 5 literal c).

Situación identificada: La solución puede estar compuesta por software especializado y servidores o appliances de otro fabricante. No resulta claro si un único fabricante debe respaldar licenciamiento, hardware y todos los servicios, o si se aceptan certificaciones independientes de cada fabricante.

Solicitud de aclaración o ajuste: Confirmar que se aceptarán cartas separadas: una del fabricante de la solución de ciberseguridad para licenciamiento y soporte, y otra del fabricante del hardware para vigencia, garantía, ciclo de vida y soporte. La carta del fabricante de software no debería exigir respaldo sobre componentes que no fabrica.

RESPUESTA DE LA UNIVERSIDAD La observación es correcta. Cuando la solución esté compuesta por componentes de diferentes fabricantes, se aceptarán las certificaciones emitidas por cada fabricante respecto de los componentes de su competencia, siempre que en conjunto acrediten el cumplimiento de los requisitos establecidos en el presente proceso.

OBSERVACIÓN No. 10

Observación 10. Definición del "nivel superior" de partner

Referencia: Pliego, numeral 3.2.1; Especificaciones Técnicas, numeral 5 literal c).
Situación identificada: Se exige un nivel superior dentro del esquema de certificación del fabricante, pero no se define el nombre, jerarquía o condición mínima aceptable. Los programas de canal no utilizan nomenclaturas uniformes.

Solicitud de aclaración o ajuste: Solicitar que la Entidad indique la denominación exacta del nivel requerido para cada fabricante o acepte el nivel que, mediante carta vigente, autorice al oferente a comercializar, implementar y soportar la solución en Colombia, siempre que no corresponda al nivel básico cuando exista una jerarquía formal.

RESPUESTA DE LA UNIVERSIDAD No se acepta la observación. Cuando el fabricante cuente con un esquema formal de categorización de canales o partners, se entenderá por nivel superior aquel que acredite al oferente para comercializar, implementar y brindar soporte sobre la solución ofertada en Colombia, conforme al programa oficial de jerarquización del fabricante. La acreditación deberá demostrarse mediante certificación vigente expedida por el fabricante.

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

OBSERVACIONES REALIZADAS POR LA EMPRESA SONDA SANDRA MIREYA CAUCALI ROJAS GERENTE DE CUENTA SENIOR TEL: +57 6016466565 CEL: 573014969333 AUTOP. NORTE No. 118 - 68 BOGOTÁ COLOMBIA www.sonda.com

OBSERVACIÓN No. 1

Solicitud	*Texto Original*	*Recomendación*	*Justificación Técnica*	*RESPUESTA UNIVERSIDAD*
Aclaración	*Actualmente, la Universidad dispone de soluciones de seguridad en endpoints y servidores, incluyendo aproximadamente 4.000 equipos protegidos con herramientas de detección y respuesta ante amenazas, así como plataformas de seguridad perimetral y monitoreo de eventos, tales como firewall de próxima generación y sistemas de gestión de eventos de seguridad (SIEM). No obstante, estas soluciones operan de manera parcialmente integrada, lo que limita la correlación avanzada de eventos, la visibilidad completa del tráfico de red (tanto norte-sur como este-oeste) y la capacidad de respuesta coordinada frente a ciberamenazas sofisticadas.*	*Solicitamos de manera amable ajustar la solicitud de cantidad de licenciamiento a 4000 dado que:* *- "La universidad cuenta actualmente con 4000 equipos protegidos" (texto original).* *- "La arquitectura prevista para la implementación de la solución debe contemplar un nodo (físico) central de administración y análisis ubicado en la sede Calle 40 de la Universidad Distrital y un sensor o colector de tráfico (físico) en la sede Bosa Porvenir".* *- "Y el objeto del contrato es ADQUIRIR UNA SOLUCIÓN DE DETECCIÓN, PREVENCIÓN Y RESPUESTA ANTE CIBERAMENAZAS A NIVEL DE RED" no de segmentos de red*		No se acepta la observación. La referencia a los aproximadamente 4.000 equipos protegidos corresponde al estado actual de la infraestructura de ciberseguridad de la Universidad y hace referencia a la solución de protección de endpoints actualmente implementada, la cual es independiente del presente proceso. En este contexto, el requerimiento de 400 activos corresponde a los equipos estratégicos que enviarán telemetría al nodo central de administración y análisis, conforme a la arquitectura definida por la Universidad. Estos equipos se encuentran distribuidos en la infraestructura tecnológica de la Universidad y no se limitan a las sedes donde se ubicarán el nodo central y el sensor de la solución. Por lo anterior, no procede ampliar el licenciamiento a 4.000 activos, ya que ello modificaría el alcance técnico y el objeto del presente proceso.

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

Solicitud	Texto Original	Recomendación	Justificación Técnica	RESPUESTA UNIVERSIDAD
Ajustar	*La solución deberá contemplar los componentes físicos necesarios para su correcta implementación, operación, monitoreo y administración bajo arquitectura On-Premise.*	*Se recomienda amablemente a la Universidad Distrital ampliar la cobertura del ítem hacia una arquitectura híbrida eficiente, donde los sensores/colectores se ubican On-Premise para la captura pasiva, mientras que el análisis de inteligencia de amenazas, machine learning y correlación masiva se realizan localmente o en la nube de forma ágil y escalable. Se solicita:* *"La solución deberá contemplar los componentes físicos necesarios para su correcta implementación, operación, monitoreo y administración bajo arquitectura On-Premise y/o Hbirida.*	*Operar bajo un esquema 100% On-Premise tradicional incrementa los costos de infraestructura, almacenamiento y mantenimiento operativo.*	No se acepta la observación. La Universidad ha definido como requerimiento técnico que la solución opere bajo una arquitectura 100 % On-Premise, de acuerdo con las necesidades de seguridad, administración, control de la información y lineamientos de la infraestructura tecnológica institucional.
Ajustar	*La solución deberá contar con capacidades de detección y respuesta a nivel de red (NDR), así como permitir la integración y correlación con soluciones de seguridad de endpoints (EDR) y mecanismos de análisis avanzado de amenazas mediante sandboxing, ya sea de forma nativa o mediante integraciones soportadas por el fabricante, con el fin de fortalecer las capacidades de visibilidad, detección y respuesta ante incidentes de seguridad.*	*Recomendamos respetuosamente a la Universidad Distrital no limitar las capacidades de análisis avanzado mediante sandboxing. El monitoreo de red exige detectar de forma rápida y eficiente los IOC (Indicadores de Compromiso) asociados a amenazas. Contar con esta información en tiempo real permite bloquear de inmediato los intentos de comunicación en los endpoints y defensas del cliente, evitando las demoras de una emulación que otorgue tiempo de ejecución al ciberdelincuente.* *Textualmente:* *"La solución deberá contar con capacidades de detección y respuesta a nivel de red (NDR), así como permitir la integración y correlación con soluciones de seguridad de endpoints (EDR) y mecanismos de análisis avanzado de amenazas mediante sandboxing o IOCs, ya sea de forma nativa o mediante integraciones soportadas por el fabricante, con el fin de fortalecer las capacidades de visibilidad, detección y respuesta ante incidentes de seguridad."*	*Cuando la telemetría detecta hashes u objetos maliciosos, es más importante enriquecee el contexto del incidente vinculando el indicador de amenaza, tácticas MITRE ATT&CK® y hashes identificados, interactuando con los mecanismos del ecosistema corporativo para contener el ataque,*	No se acepta la observación, en el ítem 16 la Universidad no está limitando las capacidades de detección al uso de mecanismos de sandboxing. El requerimiento establece que la solución cuente con capacidades NDR, integración con soluciones EDR y mecanismos de análisis avanzado de amenazas mediante sandboxing, ya sea de forma nativa o mediante integraciones soportadas por el fabricante. Por lo anterior, no se considera necesario modificar la redacción propuesta, teniendo en cuenta que los indicadores de compromiso (IOC) corresponden a una capacidad adicional de las soluciones NDR y no reemplazan el análisis avanzado de amenazas solicitado.

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

Solicitud	Texto Original	Recomendación	Justificación Técnica	RESPUESTA UNIVERSIDAD
Ajustar	*La solución deberá contar con un modelo de control de acceso basado en roles (RBAC), que permita:* *• La creación de roles personalizados.* *• La asignación granular de permisos por módulo, funcionalidad y alcance (por dominio o unidad organizacional).* *• La aplicación del principio de mínimo privilegio.* *• La delegación administrativa segmentada por unidades organizacionales.* *• La integración con servicios de directorio (LDAP/Active Directory).* *• El registro y auditoría de todas las acciones realizadas por los usuarios administradores.* *• La gestión centralizada de perfiles y políticas de acceso.*	*Recomendamos a la Universidad Distrital ajustar la asignación de permisos mediante roles estandarizados de la plataforma y segmentación por etiquetas (labels), en lugar de una configuración manual y granular.* *Exigir matrices de permisos manuales por módulo en una herramienta de detección automatizada eleva la complejidad operativa sin mejorar la postura de seguridad. En su lugar, integrar perfiles basados en roles y etiquetas lógicas garantiza de forma eficiente el principio de mínimo privilegio y la delegación administrativa.*	*Al tratarse de una arquitectura moderna basada en la nube orientada a la respuesta ágil de incidentes, los permisos de administración se estructuran a través de perfiles de roles predefinidos por función de trabajo en lugar de matrices de permisos manuales granulares por módulo, lo que simplifica la operación y evita brechas de configuración.*	No se acepta la observación. El ítem 26 define las capacidades que debe ofrecer la solución en materia de control de acceso y administración de permisos, sin imponer un mecanismo específico de implementación. Por tal razón, la solución podrá hacer uso de los métodos definidos por el fabricante, siempre que garantice la creación y administración de roles, la asignación de permisos y el cumplimiento del principio de mínimo privilegio, conforme a lo establecido en el presente numeral.
Ajustar	*La solución deberá proporcionar APIs o mecanismos de integración que permitan, como mínimo:* *• Iniciar acciones de remediación y respuesta en endpoints.* *• Obtención de datos de telemetría de endpoints para sistemas de terceros.* *• Acceso a información de alertas de aplicaciones para sistemas de terceros.* *• Enviar archivos para escanear y recuperar resultados de escaneo para sistemas de terceros.*	*Recomendamos respetuosamente a la Universidad Distrital no limitar las capacidades de análisis avanzado mediante sandboxing. "Enviar archivos para escanear y recuperar resultados de escaneo para sistemas de terceros".* *Está funcionalidad ya está siendo realizada por la platarforma actual de endpoint detection and response (EDR) por lo que se estaria duplicando funcionalidades.*	*En lugar de solicitar que la solución objeto del contrato NDR (detección y respuesta de red) gestione el intercambio físico de muestras/archivos entre aplicaciones, se sugiere enfocar el requerimiento en la capacidad de la plataforma para ingestar y sincronizar hashes maliciosos e indicadores de amenaza (IoCs) vía API con el ecosistema de seguridad existente, permitiendo una orquestación y respuesta integrada sin sobrecargar la red y sin duplicar funcionalides ya existentes.*	No se acepta la observación. El ítem 36 busca que la solución disponga de mecanismos de integración mediante APIs para interoperar con soluciones de terceros dentro del ecosistema de ciberseguridad de la Universidad. Lo anterior no significa que la solución deba reemplazar o asumir las funciones de la plataforma EDR actualmente implementada.
Ajustar	*La solución debe permitir la creación, ajuste e importación de reglas de detección basadas en el análisis de tráfico de red, comportamiento y anomalías, utilizando formatos estructurados y estandarizados de uso común en la industria, facilitando la interoperabilidad, reutilización y adaptación de reglas de detección existentes.*	*Se recomienda amablemente a la Universidad Distrital no cerrar el requerimiento a "importación de formatos de reglas estáticas de red", debido a que los motores modernos de NDR/Assessment automatizan este proceso para evitar la obsolescencia de firmas, los mecanismos actuales de caceria de amenazas utilizan IA para la deteccion del analisis de red.* *Textualmente:* *La solución debe permitir la creación y ajuste de reglas de detección basadas en el análisis de tráfico de red, comportamiento y anomalías, utilizando formatos estructurados y estandarizados de uso común en la industria, facilitando la interoperabilidad, reutilización y adaptación de reglas de detección existentes.*	*En lugar de requerir el mantenimiento manual y complejo de reglas escritas por el cliente, es más eficiente automatizar la detección correlacionando la telemetría en tiempo real contra diferentes fuentes de inteligencia global e Inteligencia Artificial, reduciendo los falsos positivos sin esfuerzo de ingeniería.*	No se acepta la observación. El ítem 51 define las capacidades mínimas que debe ofrecer la solución para la gestión de reglas de detección, sin limitar el uso de mecanismos automatizados, inteligencia artificial u otras funcionalidades incorporadas por el fabricante.

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

Solicitud	Texto Original	Recomendación	Justificación Técnica	RESPUESTA UNIVERSIDAD
Ajustar	*La solución deberá permitir el análisis de archivos u objetos identificados dentro del tráfico de red mediante sandboxing, análisis dinámico u otros mecanismos equivalentes soportados por el fabricante permitiendo su inspección en entornos controlados para la detección de comportamientos maliciosos. Esta función debe permitir:* *• Identificación de archivos u objetos sospechosos a partir del análisis del tráfico de red.* *• Envío automatizado de dichos objetos al entorno de sandbox para su análisis.* *• Integración con mecanismos o motores de análisis avanzado para la detección de amenazas desconocidas.* *• Generación de alertas y enriquecimiento de eventos a partir de los resultados del análisis avanzado realizado*	*Se recomienda amablemente a la Universidad Distrital aceptar el requerimiento mediante integracion con la arquitectura ACTUAL:* *"La solución deberá permitir el análisis de archivos u objetos identificados dentro del tráfico de red mediante sandboxing o con el EDR del ecosistema del cliente u otros mecanismos equivalentes soportados por el fabricante permitiendo su inspección en entornos controlados para la detección de comportamientos maliciosos" en lugar de exigir que la plataforma de monitoreo de red contenga un detonador nativo de archivos.*	*Esto permite un proceso más eficiente, cuando la plataforma procesa hashes de archivos (SHA256/MD5), los correlaciona con Inteligencia de Amenazas y se integra vía API con las soluciones de Sandboxing o EDR del cliente para recibir los indicadores maliciosos y activar respuestas automáticas en la red.*	No se acepta la observación. El ítem 52 no exige que la solución cuente con un mecanismo de sandboxing nativo. El requisito establece que el análisis podrá realizarse mediante sandboxing, análisis dinámico u otros mecanismos equivalentes soportados por el fabricante.
Ajustar	*La solución deberá permitir la gestión e incorporación de indicadores personalizados de compromiso (IOC) e indicadores de ataque (IOA), aplicables a los motores de análisis de red, sandbox y a las integraciones con otras herramientas de seguridad.*	*Se recomienda amablemente a la Universidad Distrital aceptar el requerimiento mediante integracion con la arquitectura ACTUAL:* *Textualmente:* *La solución deberá permitir la gestión e incorporación de indicadores personalizados de compromiso (IOC) e indicadores de ataque (IOA), aplicables a los motores de análisis de red, sandbox o a las integraciones con otras herramientas de seguridad.*	*La operatividad es algo que desgasta la operacion actual de ciberseguridad, automatizar la correlación de estos indicadores sin la complejidad operativa de mantener motores de inspección profunda pesados On-Premise y dando pluralidad a todos los oferentes.*	No se acepta la observación. El ítem 62 ya define la aplicación de indicadores de compromiso (IOC) e indicadores de ataque (IOA) sobre los diferentes mecanismos de análisis e integración soportados por la solución.
Ajustar	*La solución deberá permitir capacidades de análisis dinámico o sandboxing sobre artefactos sospechosos identificados en el tráfico de red, utilizando entornos controlados compatibles con uno o varios sistemas operativos, ya sea de forma nativa o mediante integraciones soportadas por el fabricante.*	*Recomendamos respetuosamente a la Universidad Distrital no limitar las capacidades de análisis avanzado mediante sandboxing. El monitoreo de red exige detectar de forma rápida y eficiente los IOC (Indicadores de Compromiso) asociados a amenazas. Contar con esta información en tiempo real permite bloquear de inmediato los intentos de comunicación en los endpoints y defensas del cliente (EDR ya implementado), evitando las demoras de una emulación que otorgue tiempo de ejecución al ciberdelincuente.* *Textualmente:* *"La solución deberá permitir capacidades de análisis dinámico o sandboxing sobre artefactos sospechosos identificados en el tráfico de red, utilizando entornos controlados compatibles con uno o varios sistemas operativos o con el EDR del ecosistema del cliente, ya sea de forma nativa o mediante integraciones soportadas por el fabricante."*	*La técnica en el análisis agnóstico de metadatos de comunicación, reduce el impacto en el rendimiento de la red y evita el desencriptado invasivo de paquetes de datos masivos. Se presenta mayor aprovechamiento del análisis cuando la interacción con Sandboxing se realiza mediante integraciones con el ecosistema de seguridad existente.*	No se acepta la solución. El ítem 65 no exige que la solución cuente con un mecanismo de sandboxing nativo. Se solicita que estas capacidades se implementen de forma nativa o mediante integraciones soportadas por el fabricante, siempre que se garantice el análisis de los artefactos sospechosos identificados en el tráfico de red

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

Solicitud	Texto Original	Recomendación	Justificación Técnica	RESPUESTA UNIVERSIDAD
Ajustar	*La solución deberá permitir la integración con agentes de endpoint, EDR u otros mecanismos equivalentes para el envío y análisis de archivos u objetos sospechosos mediante capacidades de análisis avanzado o sandboxing, ya sea de forma nativa o mediante integraciones soportadas por el fabricante.*	*Recomendamos respetuosamente a la Universidad Distrital no limitar las capacidades de análisis avanzado mediante sandboxing ya que estas cualidades estan incorporadas en la plataforma EDR (Endpoint Detection and Response).* *Textualmente:* *"La solución deberá permitir la integración con agentes de endpoint, EDR u otros mecanismos equivalentes para el envío y análisis de archivos u objetos sospechosos mediante capacidades de análisis avanzado o sandboxing o con el EDR del ecosistema del cliente, ya sea de forma nativa o mediante integraciones soportadas por el fabricante."*	*Las herramientas se integran con agentes de EDR y la infraestructura de seguridad para compartir la inteligencia de hashes maliciosos y correlacionar la presencia del archivo con comunicaciones maliciosas confirmadas en la red.*	No se acepta la observación. El ítem 67 define la integración con agentes de endpoint, EDR u otros mecanismos equivalentes, así como la implementación de estas capacidades de forma nativa o mediante integraciones soportadas por el fabricante.
Ajustar	*La solución debe ser capaz de procesar y analizar archivos, incluidos archivos protegidos por contraseña y documentos de oficina, independientemente de su origen*	*Se recomienda amablemente a la Universidad Distrital que la solución deba contar con la capacidad de ingestar, procesar y correlacionar hashes de archivos e Indicadores de Compromiso (IoCs) asociados a amenazas (incluyendo aquellos identificados en documentos u objetos maliciosos), ya sea de forma nativa o mediante integraciones vía API con el ecosistema de seguridad existente (EDR/Antivirus/Email Gateway) de la Universidad.*	*Exigir que una solución de Detección y Respuesta a Nivel de Red (NDR) / Evaluación de Compromisos descompile, desencripte o inspeccione directamente el contenido interno de archivos protegidos o documentos de oficina introduce serios riesgos de privacidad de datos personales/institucionales, genera cuellos de botella en el rendimiento de los enlaces de red de alta capacidad e invalida el principio de ligereza operativa. La inspección física del archivo corresponde a motores de EDR, mientras que la plataforma de monitoreo de red debe centrarse en correlacionar los hashes e indicadores resultantes para detener de forma inmediata cualquier comunicación con la infraestructura del adversario.*	No se acepta la observación. El ítem 72 define la capacidad de la solución para realizar análisis de archivos, independientemente de su origen, sin imponer un mecanismo específico para su implementación. Por tal razón, la solución podrá hacer uso de capacidades nativas o de integraciones soportadas por el fabricante, siempre que permita el procesamiento y análisis de los archivos conforme a lo establecido en el presente ítem.
Ajustar	*La solución debe permitir la creación e importación de reglas de detección de red utilizando formatos abiertos y estandarizados de uso común en la industria.*	*Se recomienda amablemente a la Universidad Distrital no cerrar el requerimiento a "importación de reglas de deteccion de red", debido a que los motores modernos de NDR/Assessment automatizan este proceso para evitar la obsolescencia de firmas, los mecanismos actuales de caceria de amenazas utilizan IA para la deteccion del analisis de red.* *La solución debe permitir la creación e importación de mecanismos automatizados de ingesta de inteligencia de amenazas de red utilizando formatos abiertos y estandarizados de uso común en la industria.*	*No utilizar lenguajes de reglas de red estáticas/abiertas escritas manualmente. Entrega mejores resultados automatizar a la detección a través de algoritmos propietarios de Machine Learning, Inteligencia Artificial y la correlación continua contra diferentes fuentes de ciberinteligencia global.*	No se acepta la observación. El ítem 81 define la capacidad de la solución para la creación e importación de reglas de detección de red utilizando formatos abiertos y estandarizados de uso común en la industria, sin impedir el uso de mecanismos automatizados de inteligencia de amenazas, aprendizaje automático o inteligencia artificial definidos por el fabricante. Por tal razón, no se considera necesario modificar la redacción del ítem.

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

Solicitud	***Texto Original***	***Recomendación***	***Justificación Técnica***	***RESPUESTA UNIVERSIDAD***
Ajustar	*La solución proporcionará un inventario lógico de activos monitoreados, incluyendo:* *• Información de la cuenta de usuario registrada en los sistemas operativos del dispositivo.* *• Información relacionada con actividad o ejecución de archivos, cuando dicha visibilidad se encuentre disponible mediante las capacidades ofertadas.* *• Espacios de direcciones de dispositivos (por ejemplo, direcciones IP, direcciones MAC).*	*Por favor confirmar de parte de la Universidad Distrital que es apropiado enmarcar el ítem en el inventario lógico centrado en la visibilidad de red e identidad del dispositivo alcanzado a través de los metadatos y agentes ligeros.*	*Realizar un seguimiento nativo del sistema de archivos local para registrar la ejecución de todos los archivos en el host, es una función reservada para las herramientas EDR.*	No se acepta la observación. El ítem 92 hace referencia al inventario lógico de los activos monitoreados y a la información que pueda obtenerse mediante las capacidades de la solución. La información relacionada con la actividad o ejecución de archivos aplica únicamente cuando dicha visibilidad se encuentre disponible, por lo que no se exige que la solución realice funciones propias de una plataforma EDR.
Ajustar	*La solución permitirá un sondeo activo y configurable de dispositivos para enriquecer la información del dispositivo y construir un mapa topológico de red completo.*	*Recomendamos amablemente a la Universidad Distrital adoptar técnicas pasivas no invasivas para recolectar metadatos. Esto optimiza el enriquecimiento del contexto de los activos y facilita la visualización gráfica de la distribución de compromisos, sin generar cargas innecesarias en la infraestructura.*	*La elaboración de topologías físicas de red corresponde a soluciones de gestión de infraestructura (NMS) y no a plataformas NDR/Assessment, cuya fortaleza radica en la visibilidad pasiva e ininterrumpida del riesgo de seguridad sin alterar el tráfico normal de la institución.*	No se acepta la observación. El ítem 98 define la capacidad para enriquecer la información de los dispositivos y construir un mapa topológico de la red, sin limitar los mecanismos de descubrimiento que pueda ofrecer la solución. Por tal razón, la solución podrá hacer uso de técnicas activas, pasivas o de una combinación de ambas, siempre que cumpla con las capacidades funcionales definidas en el presente ítem.
Aclaración	*La solución permitirá la búsqueda y recuperación de sesiones de red basándose en capturas de paquetes en el almacenamiento de tráfico.*	*De manera respuestuosa y en base a nuestro entendimiento por favor confirmar que son permitidos otros mecanimos equivalantes soportados por el fabricante y no solo captura de paqutes como lo expresado en los numerales 83, 101.*		No se acepta la observación. La solución podrá hacer uso de mecanismos equivalentes soportados por el fabricante, siempre que se cumpla con la funcionalidad requerida en el presente ítem.

Ajustar	*4. Requerimientos técnicos mínimos obligatorios, 6, Arquitectura y componentes físicos de la solución. La solución deberá permitir el almacenamiento y consulta de eventos, alertas, registros y telemetría histórica por un periodo mínimo de noventa (90) días, conforme a la arquitectura ofertada.*	*Se sugiere ajustar el requerimiento a:* *"La solución deberá permitir el envío, integración y consulta de eventos, alertas, registros y telemetría hacia la plataforma SIEM institucional o hacia la plataforma de almacenamiento definida por la Entidad, garantizando una retención mínima requerida por la entidad para fines de auditoría, cumplimiento normativo e investigación forense. La consulta de dicha información deberá realizarse de forma ágil e integrada entre ambas plataformas."*	*Optimiza la arquitectura existente. La Universidad ya cuenta con una plataforma SIEM diseñada para el almacenamiento, correlación y conservación de eventos de seguridad. Centralizar la retención histórica en esta plataforma evita duplicar funcionalidades y aprovecha la inversión tecnológica ya realizada.* *El NDR debe enfocarse en la detección y respuesta. La función principal de una solución NDR es proporcionar visibilidad, análisis del tráfico de red, detección de amenazas y respuesta temprana. La retención de largo plazo corresponde naturalmente al SIEM, donde se consolida la información de múltiples fuentes para auditoría e investigación.* *Fortalece la investigación forense. Mantener la telemetría del NDR integrada con el SIEM permite realizar búsquedas retrospectivas, correlacionar eventos de diferentes tecnologías y reconstruir incidentes que pudieron permanecer ocultos durante varios meses, sin depender exclusivamente de la capacidad de almacenamiento del NDR.* *Favorece el cumplimiento normativo. Una retención de al menos 18 meses facilita atender requerimientos de auditorías internas, organismos de control y lineamientos del MSPI, preservando evidencia técnica durante todo el ciclo de revisión.* *Reduce costos y evita duplicidad de almacenamiento. Al utilizar el SIEM institucional como repositorio central de eventos, la Entidad evita adquirir capacidad adicional de almacenamiento en el NDR, disminuyendo el costo total de propiedad (TCO), simplificando la administración y manteniendo una arquitectura más eficiente y escalable.* *La retención histórica de eventos corresponde al SIEM l, plataforma diseñada para centralizar, correlacionar y conservar registros de seguridad provenientes de*	No se acepta la observación. El ítem 6 solicita que la solución ofertada debe permitir el almacenamiento y la consulta de eventos, alertas, registros y telemetría histórica por un periodo mínimo de noventa (90) días, conforme a la arquitectura propuesta por el oferente.

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

Solicitud	*Texto Original*	*Recomendación*	*Justificación Técnica*	*RESPUESTA UNIVERSIDAD*
			múltiples fuentes. Permitir que el NDR integre su telemetría con el SIEM para garantizar una retención mínima de 18 meses optimiza la inversión existente, evita duplicidad de almacenamiento, reduce el costo total de propiedad y fortalece las capacidades de auditoría, cumplimiento e investigación forense mediante una arquitectura alineada con las mejores prácticas de ciberseguridad.	
Ajustar	*4. Requerimientos técnicos mínimos obligatorios, 13,Requisitos Generales, La solución deberá contar con capacidades de detección y respuesta a nivel de red (NDR), así como permitir la integración y correlación con soluciones de seguridad de endpoints (EDR) y mecanismos de análisis avanzado de amenazas mediante sandboxing, ya sea de forma nativa o mediante integraciones soportadas por el fabricante, con el fin de fortalecer las capacidades de visibilidad, detección y respuesta ante incidentes de seguridad.*	*Se sugiere respetuosamente a la Entidad ajustar el requerimiento con el fin de alinearlo con las capacidades propias de una solución NDR y las mejores prácticas de arquitecturas de ciberseguridad, permitiendo que las capacidades de sandboxing sean proporcionadas por la solución EDR existente o mediante integraciones soportadas por el fabricante, mientras la plataforma NDR concentra sus funcionalidades en la detección, investigación y respuesta a amenazas a nivel de red.* *Se propone ajustar a:* *"La solución deberá contar con capacidades de Detección y Respuesta a nivel de Red (NDR), permitiendo la integración y correlación con las soluciones de seguridad existentes, incluyendo la plataforma EDR de la Entidad, para complementar capacidades de análisis avanzado de amenazas, tales como sandboxing, análisis de comportamiento, inteligencia de amenazas, inteligencia artificial, analítica de tráfico y metadatos de red, detección retrospectiva de compromisos u otros mecanismos equivalentes soportados por el fabricante, ya sea de forma nativa o mediante integraciones certificadas, con el fin de fortalecer las capacidades de visibilidad, detección y respuesta ante incidentes de seguridad."*	*Fortalece una arquitectura de seguridad por capas. El sandboxing es una capacidad especializada para el análisis dinámico de archivos, mientras que una solución NDR está diseñada para detectar, investigar y responder a amenazas mediante el análisis continuo del tráfico y del comportamiento de la red. Integrar ambas capacidades permite que cada tecnología opere sobre el dominio para el cual fue diseñada, obteniendo una mayor efectividad. Aprovecha las capacidades del ecosistema de seguridad existente. La Universidad ya dispone de una solución EDR, plataforma donde el sandboxing aporta mayor valor al analizar archivos, procesos y actividades del endpoint. La integración entre el NDR y el EDR permite correlacionar ambos contextos sin duplicar funcionalidades ni exigir capacidades que no forman parte del objetivo principal de una solución NDR. Promueve una evaluación basada en capacidades y resultados. Permitir que el análisis avanzado de amenazas sea proporcionado de forma nativa o mediante integraciones certificadas favorece la interoperabilidad y la participación de arquitecturas modernas, manteniendo el mismo nivel de protección y permitiendo a la Entidad seleccionar la solución con mayor capacidad de detección y respuesta frente a amenazas reales en la red.*	No se acepta la observación. El ítem 16 no exige que las capacidades de análisis avanzado de amenazas mediante sandboxing sean nativas de la solución ofertada. Se establece que estas podrán implementarse de forma nativa o mediante integraciones soportadas por el fabricante, permitiendo su interoperabilidad con las soluciones de seguridad existentes, siempre que se cumplan las capacidades funcionales definidas en el presente ítem.

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

Solicitud	***Texto Original***	***Recomendación***	***Justificación Técnica***	***RESPUESTA UNIVERSIDAD***
Ajustar	*4. Requerimientos técnicos mínimos obligatorios, 26 Administración de la Plataforma, La solución deberá contar con un modelo de control de acceso basado en roles (RBAC), que permita:* *• La creación de roles personalizados.* *• La asignación granular de permisos por módulo, funcionalidad y alcance (por dominio o unidad organizacional).* *• La aplicación del principio de mínimo privilegio.* *• La delegación administrativa segmentada por unidades organizacionales. • La integración con servicios de directorio (LDAP/Active Directory). • El registro y auditoría de todas las acciones realizadas por los usuarios administradores.*	*Se sugiere respetuosamente a la Entidad ajustar el numeral de la siguiente manera:* *"La solución deberá contar con un modelo de control de acceso basado en roles (RBAC) que permita la asignación de privilegios bajo el principio de mínimo privilegio, la segregación de funciones, la integración con el proveedor de identidad institucional mediante estándares abiertos de autenticación y federación (SAML 2.0, OpenID Connect u otros equivalentes soportados por el fabricante), con soporte para autenticación multifactor (MFA), así como el registro y auditoría de las acciones realizadas por los usuarios de la plataforma."*	*La propuesta mantiene los controles de seguridad requeridos por la Entidad, incluyendo RBAC, mínimo privilegio, segregación de funciones, autenticación centralizada y trazabilidad, en línea con ISO/IEC 27002 y el MSPI.* *El objetivo debe centrarse en garantizar una autenticación segura e interoperable, permitiendo la integración con Active Directory, Microsoft Entra ID y otros proveedores de identidad mediante estándares abiertos, sin restringir la solución a un protocolo específico.* *Esta modificación fortalece la interoperabilidad y promueve una mayor pluralidad de oferentes, permitiendo evaluar soluciones NDR modernas que cumplen el mismo objetivo de seguridad mediante arquitecturas abiertas y ampliamente adoptadas por la industria.*	No se acepta la observación. El ítem 26 define las capacidades que debe ofrecer la solución en materia de control de acceso y administración de usuarios, sin restringir el uso de los mecanismos de autenticación e integración soportados por el fabricante, siempre que se cumplan los requisitos establecidos en el presente ítem.
Aclaración	*4. Requerimientos técnicos mínimos obligatorios, 29 Administración de la Plataforma, La solución deberá soportar mecanismos de copia de seguridad y restauración de la configuración, políticas, eventos, registros y demás componentes críticos para la operación de la plataforma*	*Se solicita respetuosamente aclarar este requisito, dado que las funciones descritas son ejecutadas automáticamente por la plataforma, sin requerir intervención del usuario. Agradecemos confirmar si esta interpretación es correcta y se considera válida para el cumplimiento del numeral.*		No se acepta la observación. El ítem 29 busca garantizar que la solución cuente con mecanismos de copia de seguridad y restauración de la información requerida para la operación de la plataforma, independientemente de si estos se ejecutan de forma manual o automática. Por lo anterior, la implementación automática de estas funciones se considera válida, siempre que se cumpla con el requisito establecido en el presente ítem.

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

Solicitud	***Texto Original***	***Recomendación***	***Justificación Técnica***	***RESPUESTA UNIVERSIDAD***
Ajustar	*4. Requerimientos técnicos mínimos obligatorios, 35 Integración, La solución deberá proporcionar APIs o mecanismos de integración que permitan, como mínimo:* *• Iniciar acciones de remediación y respuesta en endpoints.* *• Obtención de datos de telemetría de endpoints para sistemas de terceros.* *• Acceso a información de alertas de aplicaciones para sistemas de terceros.* *• Enviar archivos para escanear y recuperar resultados de escaneo para sistemas de terceros.*	*Se sugiere respetuosamente a la Entidad ajustar el numeral de la siguiente manera:* *"La solución deberá contar con APIs o mecanismos de integración bidireccional que permitan interoperar con las soluciones de seguridad existentes o futuras de la Entidad (EDR/EPP, SIEM, SOAR y sistemas de gestión de incidentes), posibilitando el intercambio de eventos, indicadores de compromiso (IoC), alertas y la orquestación de acciones de respuesta sobre los controles de seguridad correspondientes, mediante APIs documentadas y estándares abiertos soportados por el fabricante."*	*La propuesta mantiene el objetivo de la Entidad de fortalecer la detección y respuesta, promoviendo una arquitectura interoperable donde cada tecnología desempeñe su función específica mediante integraciones nativas y estándares abiertos.* *Las acciones de remediación sobre endpoints y el análisis de archivos son capacidades propias de soluciones EDR/EPP, mientras que una plataforma NDR aporta visibilidad, correlación y detección de amenazas a nivel de red, orquestando la respuesta a través de las herramientas especializadas.* *Esta modificación promueve la pluralidad de oferentes y la integración con el ecosistema de seguridad existente, permitiendo evaluar soluciones NDR modernas con amplias capacidades de integración sin limitar el proceso a fabricantes con suites propietarias integradas*	No se acepta la observación. El ítem 35 define las capacidades de integración que debe ofrecer la solución, incluyendo la interoperabilidad con herramientas de terceros mediante APIs o mecanismos soportados por el fabricante.
Aclaración	*4. Requerimientos técnicos mínimos obligatorios, 40 Integración, La solución deberá contar con la capacidad de integrarse con las herramientas de seguridad existentes en la Universidad Distrital, incluyendo el firewall de Palo Alto Networks (NGFW 3420), el EDR de Kaspersky y la plataforma de monitoreo y gestión de eventos SolarWinds Security Event Manager (SEM).*	*Respecto al numeral 4 (Requerimientos Técnicos Mínimos Obligatorios – 40. Integración), se solicita respetuosamente a la Entidad aclarar que el requisito de integración con la plataforma de gestión y monitoreo de eventos de seguridad SolarWinds Security Event Manager (SEM), o con las demás herramientas de seguridad existentes en la Universidad, se entenderá cumplido cuando dicha integración se realice mediante conectores nativos del fabricante o a través de mecanismos estándar de la industria oficialmente soportados, tales como APIs documentadas, Syslog (CEF, LEEF o JSON), Webhooks, listas dinámicas de bloqueo (EDL) u otros mecanismos equivalentes que garanticen el intercambio seguro y eficiente de información.*		No se acepta la observación. El ítem 40 establece la capacidad de integración con las herramientas de seguridad existentes en la Universidad. Dicha integración podrá realizarse mediante conectores nativos, APIs, Syslog u otros mecanismos equivalentes soportados por el fabricante, siempre que se garantice el cumplimiento de la funcionalidad requerida.

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

Solicitud	***Texto Original***	***Recomendación***	***Justificación Técnica***	***RESPUESTA UNIVERSIDAD***
Ajustar	*4. Requerimientos técnicos mínimos obligatorios, 83 Capacidades Avanzadas de Detección, Análisis de Amenazas y Comportamiento, La solución deberá permitir la exportación en formato PCAP del tráfico de red asociado a eventos detectados, con fines de análisis forense.*	*La solución deberá permitir la exportación de la evidencia técnica asociada a los eventos e incidentes detectados con fines de análisis forense, incluyendo como mínimo activos involucrados, indicadores de compromiso (IoC), infraestructura adversaria, marcas de tiempo y contexto del incidente, mediante formatos estándar (CSV, JSON, STIX u otros equivalentes) y/o APIs documentadas soportadas por el fabricante, incluyendo la evidencia derivada del análisis de metadatos cuando aplique*	*La propuesta mantiene el objetivo de la Entidad de disponer de evidencia técnica para la investigación forense, privilegiando formatos abiertos e interoperables ampliamente adoptados por la industria. Asimismo, permite evaluar soluciones NDR modernas que generan evidencia mediante metadatos enriquecidos o mecanismos equivalentes, preservando las capacidades de investigación e integración sin restringir el cumplimiento a una única arquitectura tecnológica.*	No se acepta la observación. El ítem 83 fue ajustado tras las observaciones realizadas en los prepliegos, quedando de la siguiente manera: "La solución deberá permitir recuperar la evidencia asociada a los eventos detectados para actividades de análisis forense e investigación de incidentes, mediante PCAP u otros mecanismos equivalentes soportados por el fabricante" Por tal razón se amplió para que se presente en formato PCAP u otros mecanismos equivalentes soportados por el fabricante.
Ajustar	*4. Requerimientos técnicos mínimos obligatorios, 100 Capacidades NDR La solución debe proporcionar capacidades de respuesta de red, A efectos de la investigación forense, respuesta a incidentes o cumplimiento normativo de incidentes cibernéticos, la solución debe proporcionar la capacidad de capturar y registrar el tráfico de red en bruto.*	*Se solicita respetuosamente a la Entidad ajustar el numeral de la siguiente manera:* *"Con fines de investigación forense, respuesta a incidentes y cumplimiento normativo, la solución deberá registrar, conservar y permitir la exportación de la evidencia técnica asociada a los incidentes detectados, incluyendo la telemetría y contexto de las comunicaciones involucradas, en formatos estándar o mediante APIs documentadas. Cuando la arquitectura ofertada contemple captura de paquetes (PCAP), esta podrá utilizarse como mecanismo complementario de evidencia.*	*La propuesta mantiene el objetivo funcional del requerimiento, garantizando la disponibilidad de evidencia técnica para la investigación y respuesta a incidentes, sin limitar su cumplimiento a un único mecanismo de captura. Las soluciones NDR modernas pueden proporcionar esta capacidad mediante telemetría y metadatos enriquecidos o mediante PCAP, según su arquitectura, preservando el mismo resultado operativo y promoviendo una mayor interoperabilidad y pluralidad de oferentes.*	No se acepta la observación. El ítem 100 establece como requisito la capacidad de capturar y registrar el tráfico de red en bruto con fines de investigación forense, respuesta a incidentes y cumplimiento normativo. La solución podrá ofrecer mecanismos adicionales para la conservación y exportación de evidencia mediante telemetría, metadatos, formatos estándar o APIs soportadas por el fabricante; sin embargo, estos no reemplazan la capacidad requerida de captura y registro del tráfico de red en bruto.

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

Solicitud	***Texto Original***	***Recomendación***	***Justificación Técnica***	***RESPUESTA UNIVERSIDAD***
Ajustar	*4. Requerimientos técnicos mínimos obligatorios, 101 Capacidades NDR La solución debe proporcionar capacidades de respuesta de red, El tráfico grabado puede capturarse en un formato que puede analizarse y reproducirse fácilmente, como PCAP (Captura de Paquetes).*	*Se solicita respetuosamente a la Entidad ajustar el numeral de la siguiente manera:* *"La solución deberá proporcionar evidencia técnica de las comunicaciones asociadas a los eventos e incidentes detectados, que permita su análisis e investigación forense, mediante captura de paquetes (PCAP), metadatos de red enriquecidos u otros mecanismos equivalentes soportados por el fabricante, exportables en formatos estándar (CSV, JSON, STIX o equivalentes) y/o mediante APIs documentadas."*	*La propuesta mantiene el objetivo funcional del requerimiento, garantizando la disponibilidad de evidencia técnica para la investigación de incidentes, sin restringir su cumplimiento a un único mecanismo de captura. Actualmente, las soluciones NDR modernas emplean diferentes arquitecturas para la obtención de evidencia, ya sea mediante PCAP o mediante metadatos enriquecidos de las comunicaciones, ambos enfoques ampliamente utilizados para soportar procesos de detección, análisis forense e integración con plataformas SIEM, SOAR y Threat Intelligence. Esta modificación promueve la interoperabilidad, la evolución tecnológica y una mayor pluralidad de oferentes, preservando el nivel de protección requerido por la Entidad.*	No se acepta la observación. El ítem 101 fue ajustado tras las observaciones realizadas en los prepliegos, quedando de la siguiente manera: "El tráfico grabado puede capturarse en un formato que puede analizarse y reproducirse fácilmente, como PCAP (Captura de Paquetes) u otros mecanismos equivalentes soportados por el fabricante." Por tal razón se amplió para que se presente en formato PCAP u otros mecanismos equivalentes soportados por el fabricante.

RESPUESTA DE LA UNIVERSIDAD: La Universidad dio respuesta en el cuadro de observaciones en la columna denominada RESPUESTA UNIVERSIDAD

COMITÉ ASESOR DE CONTRATACIÓN