UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

CONSOLIDADO DE OBSERVACIONES AL PREPLIEGO 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 INFO COMUNICACIONES S.A.S NIT: 830.044.415-3 DIRECCIÓN: AUTOPISTA MEDELLÍN KM 3.5, TERMINAL TERRESTRE DE CARGA DE BOGOTÁ, OF. C4 Y C5 CORREOS ELECTRÓNICOS: bibiana@infocomunicaciones.net - lquiroga@infocomunicaciones.net NÚMEROS CELULARES: 3176431579 – 3187826323 NÚMERO

OBSERVACIÓN No. 1

OBSERVACIÓN : 2.2 INDICADORES FINANCIEROS.

INFO COMUNICACIONES SAS, solicita muy respetuosamente a la Universidad el cambio de los indicadores financieros declarando que es una compañía con más de 28 años atendiendo soluciones y requerimientos a empresas del sector público y privado a nivel nacional, durante estos años ha mantenido la fortaleza de caja y recursos de corto y largo plazo para el desarrollo de la operación que requiere la entidad.

Se solicita a la Universidad que el indicador actual Capital de Trabajo ≥ al 100% de la oferta económica, sea modificado, para ser Capital de Trabajo ≥ al 70% de la oferta económica o del presupuesto oficial.

De igual manera, se solicita modificar el índice razón cobertura de interés mayor igual a 2.0 agradecemos sea modificado a Mayor e igual a 1.4. Este indicador 1.4 indica que nos encontramos en la capacidad cubrir las deudas actuales con un excedente de saldo y de adquirir nuevos compromisos sin necesidad de algún endeudamiento adicional. La totalidad de nuestros proveedores nos dan un crédito a más de 60 días, lo cual significa que cumplimos con las obligaciones adquiridas, la relación establecida durante varios años con los proveedores, refleja que se tiene una situación financiera sana, y la capacidad de adquirir nuevos compromisos y cumplirlos con confianza, seguridad y respaldo.

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

2.3.1 EXPERIENCIA DEL PROPONENTE:

INFO COMUNICACIONES SAS, solicita muy respetuosamente a la Universidad la aclaración o actualización de:

- *Item d, **valor de los contratos**: "La sumatoria del valor de los contratos acreditados deberá ser igual o superior a una (1) vez el valor estimado de la contratación.", solicitamos agregar la opción de ser expresado también en salarios mensuales legales vigentes, toda vez que hay contratos de 5 años, que son afectados en pesos por inflación y otros como devaluación y demás, pero que en salarios mínimos permanece constante. Agradecemos actualizarlo a: "La sumatoria del valor de los contratos acreditados deberá ser igual o superior a una (1) vez el valor estimado del presupuesto oficial expresado en Salarios Mínimos Legales Vigentes."*

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, En el apartado "*vii*" del ítem "*g*" del "*Análisis de la experiencia*", se especifica el calculo de los salarios mínimos por año.

"La actualización a "pesos de hoy" del valor de los contratos ejecutados se calculará en relación con el valor del salario mínimo del año de la fecha de terminación, es decir, el valor de los ítems se expresará en salarios mínimos correspondientes al año de terminación"

OBSERVACIÓN No. 3

OBSERVACION 3.2.4.1 ESPECIFICACIONES TÉCNICAS:

INFO COMUNICACIONES SAS, solicita muy respetuosamente a la Universidad la aclaración del throughput Item 19: "Cada Centro de Análisis deberá soportar el procesamiento del volumen de tráfico de la red institucional, incluyendo enlaces troncales de alta capacidad (mínimo 6 Gbps de tráfico o superior), sin degradación del análisis ni pérdida de visibilidad.", porque de acuerdo con la cotización presentada por la empresa Info Comunicaciones durante el proceso de estudio de mercado, los equipos ofertados soportan un throughput de hasta 4 Gbps. En este sentido, se solicita a la Universidad aclarar cuál es el valor real de throughput que debe ser considerado para la presentación de la propuesta económica.

El ítem 19 se encuentra relacionado en el documento ***PROYECTO DE PLIEGO DE CONDICIONES*** *(pagina 54) y en documento* ***ESPECIFICACIONES TÉCNICAS*** *(página 8).*

RESPUESTA DE LA UNIVERSIDAD: Se acepta la observación. Se modifica el ítem 19 de la tabla de requisitos mínimos quedando de la siguiente manera *"Cada Centro de Análisis deberá soportar el procesamiento del volumen de tráfico de la red institucional, incluyendo enlaces troncales de alta capacidad (mínimo 4 Gbps de tráfico o superior), sin degradación del análisis ni pérdida de visibilidad"*

OBSERVACIÓN No. 3

• Observación No.1 – Documento 27397 – Especificaciones Técnicas – 4. Requerimientos técnicos mínimos obligatorios

Ítem 4. - Arquitectura y componentes físicos de la solución.

La solución deberá permitir la creación e incorporación de nuevos sensores, los cuales podrán ser desplegados de manera física o virtual sobre la infraestructura tecnológica de la Universidad, sin que ello genere costos adicionales la Universidad.

Es necesario aclarar que si bien el licenciamiento propuesto permite a la Universidad implementar sensores físico o virtuales de acuerdo a sus necesidades, es necesario tener claro que esto se podrá hacer siempre y cuando no se supere la cantidad de tráfico, medida en Gbps, adquirido por la Universidad. En caso de ser superior a lo adquirido, esto si puede generar costos adicionales a la Entidad.

RESPUESTA DE LA UNIVERSIDAD: Se acepta observación. Se ajusta el ítem 4 los requerimientos técnicos mínimos, quedando de la siguiente manera: "*La solución deberá permitir la creación e incorporación de nuevos sensores, los cuales podrán ser desplegados de manera física o virtual sobre la infraestructura tecnológica de la Universidad siempre y cuando no sobrepase las capacidades contratadas y sin que ello genere costos adicionales la Universidad.*"

OBSERVACIÓN No. 4

Observación No.2 – Documento 27397 – Especificaciones Técnicas – 4. Requerimientos técnicos mínimos obligatorios

Ítem 19. - Arquitectura y Diseño de la Plataforma

Cada Centro de Análisis deberá soportar el procesamiento del volumen de tráfico de la red institucional, incluyendo enlaces troncales de alta capacidad (mínimo 6 Gbps de tráfico o superior), sin degradación del análisis ni pérdida de visibilidad..

Durante procesos anteriores, la Universidad ha solicitado información comercial de soluciones de NDR para 4Gbps y 6 Gbps. Solicitamos a la universidad, solo para tenerlo claro, si lo requerido por la Universidad es una solución de NDR para 4Gbps o 6 Gbps?

RESPUESTA DE LA UNIVERSIDAD: Se acepta la observación, se modifica el ítem 19 de la tabla de requisitos mínimos quedando de la siguiente manera "*Cada Centro de Análisis deberá soportar el procesamiento del volumen de tráfico de la red institucional, incluyendo enlaces troncales de alta capacidad (mínimo 4 Gbps de tráfico o superior), sin degradación del análisis ni pérdida de visibilidad*"

OBSERVACIÓN No. 5

Observación No.3 – Documento 27397 – Especificaciones Técnicas – 5. Certificaciones técnicas solicitadas

Numeral b.

Los componentes de la solución no deberán encontrarse en estado de End of Support (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. Solicitamos a la Universidad modificar este punto para los componentes de software de ciberseguridad, como lo es la solución de NDR y Endpoint. Esto debido a que los fabricantes de ciberseguridad definen sus EoL y EoS de sus soluciones de software de acuerdo con las versiones que se van liberando con mejores características técnicas y funcionales y no basado únicamente en el nombre de la solución. De esta forma solicitamos modificar este numeral para que las soluciones de software de ciberseguridad tengan una vigencia para la versión adquirida de al menos dos (2) años, quedando de la siguiente forma:

Los componentes de la solución no deberán encontrarse en estado de End of Support (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. Para los componentes de software de ciberseguridad, como lo es la solución de NDR y Endpoint Detection and Response (EDR) el fabricante deberá garantizar un ciclo de vida y soporte no inferior a dos (2) años.

RESPUESTA DE LA UNIVERSIDAD: Se acepta la observación y se modifica el literal "b" del apartado "*Certificaciones técnicas solicitadas*" de las especificaciones técnicas, de la siguiente manera:

"Los componentes de la solución no deberán encontrarse en estado de End of Support (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 para los componentes de hardware, incluyendo actualizaciones de seguridad y soporte técnico. Para los componentes de software de ciberseguridad, como lo es la solución de NDR el fabricante deberá garantizar un ciclo de vida y soporte no inferior a dos (2) años."

OBSERVACIONES REALIZADAS POR LA EMPRESA DATASEC JOHANNA LISBETH MOLINA <johanna.molina@datasec.com.co>

OBSERVACIÓN No. 1

Observaciones al Documento
3. EspecificacionesTecnicas_Ciberseguridad.pdf

Observacion 1

10	Arquitectura y componentes físicos de la solución	Especificaciones técnicas - Patch cord dúplex de fibra óptica LC/LC: • Debe contar con las siguientes características: 1. OM4 u OM5. 2. Longitud de Onda mínimo de 850/1300 nm. 3. Longitud 2.0 metros con conector LC-LC 4. Tipo: Uniboot ó Zip-cord 5. Cincuenta y Ciento Veinticinco micrones (50/125) µm. 6. Soportar 10G hasta 550 metros y 1Gbps hasta 1100 metros, certificados según el estándar IEEE 802.3ae. • Los conectores deben cumplir con los estándares de cableado como lo estipula la norma ANSI/TIA-568- 3-D • Deben ser probados para soportar velocidades de transmisión hasta de 10 Gb/s para enlaces de hasta 550m con una fuente de 850nm según los estándares IEEE 802.3ae 10 GbE. • Deben estar garantizado mínimo por 25 años. • El cable debe tener un retardante de fuego de alta calidad, libre de halógenos, no producir gases tóxicos, la chaqueta de la fibra debe ser del tipo (LSZH ó LSZH-3). • Estos deben ser elaborados por el mismo fabricante. • Deben ser originales de fábrica y precertificados por el fabricante como estipula la ANSI/TIA 568.3-D, deben venir en su bolsa original de empaque tal como salen de la fábrica. • Los elementos estarán identificados individualmente con el correspondiente logo de la prueba de laboratorio, de forma permanente. Serán certificados por UL ó CSA ó ETL, para garantizar que los elementos ofrecidos han sido avalados por estos laboratorios. Adicionalmente puede estár marcado con el número de la prueba de flamabilidad. • Debe tener ficha técnica del fabricante del producto, con número de parte donde se pueda verificar las especificaciones y parámetros de desempeño, a través de la página web del fabricante.

Requerimiento 1:

Se solicita amablemente a la entidad modificar el ítem para que la verificación de las características del patch cord de fibra óptica se evalúe sobre la ficha técnica del cableado suministrado y no como criterio de cumplimiento de la herramienta NDR, manteniéndose la compatibilidad de la solución con dicha infraestructura (10 Gb Ethernet sobre fibra multimodo OM4/OM5 con interfaces SFP+). Esta precisión tiene como finalidad no limitar la participación de los oferentes en el presente proceso.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. Las especificaciones técnicas del patch cord de fibra óptica corresponden a los elementos de conectividad requeridos para la integración de la solución con la infraestructura de red de la Universidad. El cumplimiento de estas características podrá ser verificado mediante la ficha técnica y/o documentación del fabricante del patch cord ofertado. Por tal razón, se mantienen el ítem 10 de la tabla de especificaciones técnicas mínimas, ya que, que son necesarias para garantizar la compatibilidad con la infraestructura de telecomunicaciones existente y las condiciones de soporte y garantía de los equipos de red de la Universidad.

OBSERVACIÓN No. 2

Observacion 2:

49	Visibilidad Extendida e Integración de la Solución NDR	Los mecanismos de visibilidad utilizados sobre los equipos de cómputo deberán incluir como mínimo las siguientes capacidades: • Recolección de telemetría y contexto de seguridad. • Bajo impacto sobre el rendimiento de los dispositivos monitoreados. • Posibilidad de despliegue o habilitación selectiva sobre hasta cuatrocientos (400) equipos definidos por la Universidad. • Integración con la plataforma central de análisis para el envío de información y correlación de eventos.

Requerimiento 2:

Se solicita amablemente a la entidad modificar el requisito para que los mecanismos de visibilidad puedan basarse en el análisis del tráfico de red e integración con la plataforma EDR institucional, sin exigir agentes instalados en los equipos de cómputo, manteniéndose la

recolección de telemetría y correlación sobre hasta cuatrocientos (400) activos. Esta precisión tiene como finalidad no limitar la participación de los oferentes en el presente proceso.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. El ítem 48 de la tabla de requisitos mínimos no exige el uso exclusivo de agentes instalados en los equipos de cómputo. Por el contrario, permite que las capacidades de visibilidad y correlación se implementen mediante agentes, sensores ligeros, telemetría de red u otros mecanismos soportados por el fabricante, de acuerdo con la tecnología ofrecida.

Por tal razón, el ítem ya contempla diferentes mecanismos para la recolección de información de seguridad, sin limitar la participación de los oferentes.

"La solución deberá permitir ampliar las capacidades de visibilidad y correlación sobre endpoints estratégicos, mediante agentes, sensores ligeros, telemetría de red u otros mecanismos soportados por el fabricante, con el fin de complementar la recolección de información de seguridad en escenarios donde el monitoreo basado únicamente en tráfico no sea suficiente (por ejemplo, usuarios remotos, tráfico cifrado o segmentos no instrumentados)."

OBSERVACIÓN No. 3

Observacion 3:

81	Capacidades NDR	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.

Requerimiento 3: *Se solicita amablemente a la entidad modificar el requisito para que la creación e incorporación de reglas de detección de red pueda realizarse mediante los mecanismos propios del fabricante (firmas, IOC, inteligencia de amenazas y análisis de comportamiento), sin exigir la importación de formatos abiertos de terceros, manteniéndose la capacidad de adaptar la detección al entorno.*

Esta precisión tiene como finalidad no limitar la participación de los oferentes en el presente proceso.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. El ítem 81 busca garantizar que la solución cuente con capacidades de interoperabilidad y flexibilidad para la creación e importación de reglas de detección mediante formatos abiertos y estandarizados de uso común en la industria.

Lo anterior no impide que los fabricantes utilicen mecanismos propios para la creación de reglas, firmas, indicadores de compromiso (IOC), inteligencia de amenazas o análisis de comportamiento; estas capacidades se consideran complementarias al requisito establecido.

OBSERVACIÓN No. 4

Observacion 4:

87	Capacidades NDR	La solución deberá permitir la integración con mecanismos de respuesta o contención sobre endpoints, firewalls u otras herramientas de seguridad, posibilitando acciones automatizadas o asistidas ante amenazas detectadas.

Requerimiento 4:

Se solicita amablemente a la entidad modificar el requisito para que las acciones de respuesta y contención puedan ejecutarse mediante integración y orquestación con las herramientas de seguridad existentes (EDR, firewalls, SIEM/SOAR), sin exigir el aislamiento o bloqueo

automático de forma nativa, manteniéndose la capacidad de respuesta asistida o automatizada ante amenazas. Esta precisión tiene como finalidad no limitar la participación de los oferentes en el presente proceso.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. El ítem 87 no exige que las acciones de respuesta o contención se realicen de forma nativa por la solución. Lo que se requiere es que esta permita la integración con mecanismos de respuesta o contención sobre endpoints, firewalls u otras herramientas de seguridad, posibilitando acciones automatizadas o asistidas ante amenazas detectadas.

OBSERVACIÓN No. 5

Observacion 5:

89	Capacidades NDR	La solución debe tener la capacidad de importar y/o personalizar reglas que permitan complementar las predeterminadas y extiendan su uso en el escaneo de objetos del tráfico de red, archivos, objetos e inspección profunda del tráfico, detección de infraestructuras c2c conocidas y reputación de dominios.

Requerimiento 5:
Se solicita amablemente a la entidad modificar el requisito para que la personalización de reglas e indicadores de detección pueda realizarse mediante políticas, IOC, reputación e inteligencia de amenazas propias del fabricante, sin exigir la importación de formatos abiertos de terceros, manteniéndose la capacidad de detección de tráfico malicioso e infraestructura C2. Esta precisión tiene como finalidad no limitar la participación de los oferentes en el presente proceso.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. El ítem 89 busca garantizar que la solución permita complementar y ampliar las capacidades de detección mediante la importación y/o personalización de reglas. Esto no limita el uso de mecanismos propios del fabricante, como políticas, indicadores de compromiso (IOC), reputación, inteligencia de amenazas u otros mecanismos de detección, los cuales pueden ser utilizados para dar cumplimiento al requisito.

Sin embargo, se aprovecha para modificar el ítem, teniendo en cuenta que en la redacción se cometio un error, quedando de la siguiente manera "La solución debe tener la capacidad de importar y/o personalizar reglas que permitan complementar las predeterminadas y extiendan su uso en el escaneo de objetos del tráfico de red, archivos, objetos e inspección profunda del tráfico, detección de infraestructuras "Command and Control (C2)" conocidas y reputación de dominios."

Este ajuste no modifica el alcance técnico ni funcional del requisito.

Observacion 6:

92	Capacidades NDR	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).

Requerimiento 6:

Se solicita amablemente a la entidad modificar el requisito para que la información de usuario del sistema operativo y ejecución de archivos sea exigible solo cuando esté disponible mediante integraciones, manteniéndose el inventario lógico de activos (IP/MAC, comunicaciones y relaciones) obtenido por la solución. Esta precisión tiene como finalidad no limitar la participación de los oferentes en el presente proceso.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. El ítem 92 no establece un mecanismo específico para la obtención de la información solicitada. Adicionalmente, la información relacionada con la actividad o ejecución de archivos ya se encuentra en el requisito mediante el enunciado: "Información relacionada con actividad o ejecución de archivos, cuando dicha visibilidad se encuentre disponible mediante las capacidades ofertadas". Por tal razón, el ítem permite que la información de la cuenta de usuario, la actividad de archivos y los demás atributos del inventario lógico de activos sean obtenidos mediante las capacidades propias de la solución o a través de las integraciones que este soporte, por lo que no se considera necesaria su modificación.

OBSERVACIÓN No. 7

Observacion 7:

98	Capacidades NDR	La solución permitirá un sondeo activo y configurable de dispositivos para enriquecer la información del dispositivo y construir un mapa topológico de red completo.

Requerimiento 7:

Se solicita amablemente a la entidad modificar el requisito para que el descubrimiento y enriquecimiento de información de dispositivos pueda realizarse mediante monitoreo pasivo del tráfico e integraciones, sin exigir sondeo activo (active polling), manteniéndose la construcción de la representación lógica de activos y relaciones de red. Esta precisión tiene como finalidad no limitar la participación de los oferentes en el presente proceso.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. El ítem 98 no limita que la solución emplee mecanismos de monitoreo pasivo del tráfico o integraciones con otras herramientas para el descubrimiento de activos. Sin embargo, la capacidad de realizar sondeo activo se mantiene como parte de los requerimientos técnicos de la solución, ya que permite descubrir activos silenciosos, obtener información adicional de los dispositivos y construir un inventario de activos más completo.

OBSERVACIÓN No. 8

Observacion 8:

102	Capacidades NDR	La solución debe proporcionar una interfaz de descarga para el tráfico grabado que soporte capacidades de filtrado usando la sintaxis BPF y expresiones regulares. Esta interfaz permitirá a los usuarios recuperar y analizar de forma eficiente subconjuntos específicos del tráfico registrado, facilitando una mejor respuesta a incidentes, la búsqueda de amenazas y la monitorización de la seguridad.

Requerimiento 8:
Se solicita amablemente a la entidad modificar el requisito para que el filtrado de la interfaz de descarga de tráfico se exprese de forma neutral (filtros de búsqueda y selección), sin exigir una sintaxis específica como BPF, manteniéndose la capacidad de recuperar y analizar subconjuntos del tráfico capturado para investigación forense y respuesta a incidentes. Esta precisión tiene como finalidad no limitar la participación de los oferentes en el presente proceso.

RESPUESTA DE LA UNIVERSIDAD: Se acepta la observación. Se modifica el ítem 102 para establecer que la solución deberá permitir el filtrado y selección del tráfico mediante los mecanismos soportados por el fabricante, conservando la capacidad de recuperar y analizar subconjuntos del tráfico para actividades de investigación forense, búsqueda de amenazas y respuesta a incidentes. El requisito quedará de la siguiente manera:

"La solución debe proporcionar una interfaz de descarga para el tráfico grabado que permita aplicar filtros de búsqueda y selección. Esta interfaz permitirá a los usuarios recuperar y analizar de forma eficiente subconjuntos específicos del tráfico registrado, facilitando la respuesta a incidentes, la búsqueda de amenazas y la monitorización de la seguridad."

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

TIPO DE CONSULTA	REFERENCIA	CONSULTA	RESPUESTA DE LA UNIVERSIDAD
TÉCNICO	*Suministro de hardware:[1.1] 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).*	*Se agradece a la entidad agregar o adicionar el poder Instalar los appliances de modo virtual dentro de la infraestructura de la entidad.*	No se acepta la observación. La Universidad requiere que los componentes necesarios para la implementación y operación de la solución sean suministrados en formato físico, teniendo en cuenta que no dispone de la infraestructura tecnológica necesaria para alojar la solución de manera virtual.
TÉCNICO	*Suministro de licenciamiento: Licenciamiento de una solución de detección, prevención y respuesta ante ciberamenazas a nivel de red, bajo arquitectura On-Premise[2.1], por un periodo mínimo de un (1) año, incluyendo el derecho a actualizaciones (updates y upgrades) durante la vigencia del licenciamiento.*	*Se agradece a la entidad eliminar este punto, dado que el procesamiento de detección, prevención y respuesta ante ciberamenazas a nivel de red es más eficiente a nivel energético en Cloud. O, en su defecto, permitir modelos híbridos o Cloud.*	No se acepta la observación. La Universidad requiere que la solución sea implementada bajo una arquitectura On-Premise, de acuerdo con las necesidades del proyecto y el alcance definido para el monitoreo, análisis y respuesta sobre el tráfico de la red institucional.
TÉCNICO	*4. Requerimientos técnicos mínimos obligatorios, 2, Arquitectura y componentes físicos de la solución, La solución deberá contemplar los componentes físicos necesarios para su correcta implementación, operación, monitoreo y administración bajo arquitectura On-Premise.*	*Se solicita a la entidad modificar de la siguiente forma: La solución deberá contemplar los componentes físicos/virtuales necesarios para su correcta implementación, operación, monitoreo y administración bajo arquitectura On-Premise/Cloud o híbrida. O, en su defecto, eliminar.*	No se acepta la observación. La Universidad requiere que la solución contemple los componentes físicos necesarios para su correcta implementación, operación, monitoreo y administración bajo una arquitectura On-Premise, de acuerdo con las necesidades y el alcance definido para el presente proceso.
TÉCNICO	*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 a la entidad modificar de la siguiente forma: La solución deberá permitir el almacenamiento y consulta de eventos, alertas, registros y telemetría histórica por un periodo mínimo de 18 meses y que dicha telemetría se mantenga en línea con fines de auditoría, cumplimiento y forense.*	No se acepta la observación. El periodo de almacenamiento y consulta histórica corresponde a un mínimo de noventa (90) días. Sin embargo, si la solución ofertada permite almacenar la información durante dieciocho (18) meses, estará cumpliendo con el requisito solicitado, al superar el mínimo exigido.

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

TIPO DE CONSULTA	REFERENCIA	CONSULTA	RESPUESTA DE LA UNIVERSIDAD
TÉCNICO	*4. Requerimientos técnicos mínimos obligatorios, 12 ,Requisitos Generales: La solución deberá permitir configuraciones orientadas a garantizar que la información analizada y los eventos de seguridad permanezcan bajo control y administración de la Universidad, conforme a las políticas institucionales de seguridad de la información.*	*Se sugiere modificar de la siguiente forma:" La solución deberá permitir configuraciones orientadas a garantizar que la información analizada y los eventos de seguridad puedan ser accedidos y gestionados 7x24x365 por la Universidad desde la plataforma entregada por la solución, conforme a las políticas institucionales de seguridad de la información."*	No se acepta la observación. El ítem 12 busca garantizar que la información analizada y los eventos de seguridad permanezcan bajo el control y administración de la Universidad, conforme a las políticas institucionales de seguridad de la información.
TÉCNICO	*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 solicita eliminar este numeral, dado que la funcionalidad de las soluciones de detección, prevención y respuesta ante ciberamenazas a nivel de red no realiza funcionalidades de sandboxing; esta funcionalidad es propia de una solución dedicada o de una solución de EDR, lo cual estaría sesgando la solución objeto de la solicitud.*	No se acepta la observación. El ítem 13 no exige que la solución NDR incorpore capacidades de sandboxing de forma nativa. El requisito establece que dichas capacidades podrán proporcionarse 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.
TÉCNICO	*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 solicita a la entidad eliminar este punto o modificar de la siguiente forma: La solución debe contar con un modelo de control de acceso basado en roles que permita tener trazas de auditoría de las acciones realizadas dentro de la plataforma, enfocadas en labores de configuración y acciones administrativas sobre la plataforma.*	No se acepta la observación. El ítem 26 establece los requerimientos mínimos para la administración segura de la plataforma, incluyendo el control de acceso basado en roles (RBAC), la asignación granular de permisos, la aplicación del principio de mínimo privilegio, la integración con servicios de directorio activo y el registro de las acciones administrativas. Las trazas de auditoría constituyen únicamente una de las capacidades requeridas y no sustituyen las demás funcionalidades solicitadas, por lo que se mantiene el ítem sin modificaciones.
TÉCNICO	*4. Requerimientos técnicos mínimos obligatorios, 28 Administración de la Plataforma, La solución debe soportar sincronización de tiempo con servidores NTP.*	*Se solicita eliminar este Numeral.*	No se acepta la observación. El ítem 28 se mantiene, teniendo en cuenta que la sincronización de tiempo con servidores NTP es un requisito necesario para

TIPO DE CONSULTA	REFERENCIA	CONSULTA	RESPUESTA DE LA UNIVERSIDAD
			garantizar la correcta correlación y trazabilidad de los eventos de seguridad.
TÉCNICO	*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 aclarar, dado que estas labores son automáticas de la plataforma y el cliente no debe ejecutar ninguna acción relacionada con las mismas; por lo tanto, es correcta nuestra apreciación de que este es un mecanismo válido.*	No se acepta la observación. Se aclara que el requisito busca que la solución cuente con mecanismos de copia de seguridad y restauración de la configuración, políticas, eventos, registros y demás componentes críticos para su operación. Estos mecanismos podrán ejecutarse de forma automática por la plataforma o mediante procesos manuales ejecutados por el administrador según la necesidad, siempre que garanticen la disponibilidad de la información y su recuperación cuando sea necesaria.
TÉCNICO	*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 solicita a la entidad eliminar este numeral, dado que esta es una solución de EDR y no está alineado al objeto de la solicitud.*	No se acepta la observación. El ítem 35 no exige que la solución NDR incorpore de forma nativa funcionalidades propias de una solución EDR. El ítem establece que la solución deberá proporcionar APIs o mecanismos de integración que permitan el intercambio de información y la ejecución de acciones con herramientas de terceros, fortaleciendo las capacidades de detección, análisis y respuesta ante incidentes de seguridad, incluyendo la integración con la solución EDR de la Universidad.
TÉCNICO	*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).*	*Se agradece a la entidad que, en el caso de SolarWinds, se busque una integración como Universal SIEM; es correcta nuestra apreciación.*	Se aclara que la integración con la plataforma SolarWinds podrá realizarse mediante los mecanismos de integración soportados por la solución y la plataforma, siempre que se garantice el intercambio de información y la interoperabilidad requerida con la infraestructura de seguridad de la Universidad.
TÉCNICO	*4. Requerimientos técnicos mínimos obligatorios, 42 Integración, La solución debe ser capaz de informar en tiempo real sobre el ancho de banda monitorizado, el estado de la interfaz de red y el estado de procesamiento de los tipos de tráfico de red.*	*Se sugiere modificar este punto de la siguiente forma: "La solución debe ser capaz de informar en tiempo real el estado de la interfaz de red y el estado de procesamiento de los tipos de tráfico de red, estado de colectores (activos o no), consumo de cpu, memoria, disco de los mismos."*	No se acepta la observación. El ítem 42 busca garantizar que la solución permita visualizar en tiempo real el ancho de banda monitorizado, el estado de las interfaces de red y el estado del procesamiento del tráfico, información necesaria para la operación y el monitoreo de la solución. Las métricas adicionales propuestas, como el estado de los colectores y el consumo de

TIPO DE CONSULTA	REFERENCIA	CONSULTA	RESPUESTA DE LA UNIVERSIDAD
			CPU, memoria y disco, pueden ser capacidades complementarias de la solución, pero no sustituyen el alcance del requisito establecido.
TÉCNICO	*4. Requerimientos técnicos mínimos obligatorios, 43 Integración, La solución deberá permitir la generación de reportes personalizables basados en eventos, alertas, incidentes y demás información recopilada por la plataforma.*	*Se solicita a la entidad eliminar la palabra " personalizables".*	No se acepta la observación. El ítem 43 busca que se puedan generar reportes ajustados a las necesidades de operación, monitoreo y análisis.
TÉCNICO	*4. Requerimientos técnicos mínimos obligatorios, 47 Integración, La solución deberá proporcionar paneles y tableros personalizables para la visualización y análisis de información operativa y de seguridad, incluyendo como mínimo eventos registrados, estado del sistema, actividad de red, indicadores de compromiso, activos involucrados, alertas generadas y resultados analíticos obtenidos por la plataforma.*	*Se solicita a la entidad eliminar la palabra " personalizables".*	No se acepta la observación. El ítem 47 busca que se puedan personalizar los paneles y tableros de acuerdo con las necesidades de monitoreo, operación y análisis de la información de seguridad.
TÉCNICO	*4. Requerimientos técnicos mínimos obligatorios, 49 Visibilidad Extendida e Integración de la Solución NDR, Los mecanismos de visibilidad utilizados sobre los equipos de cómputo deberán incluir como mínimo las siguientes capacidades:* *• Recolección de telemetría y contexto de seguridad.* *• Bajo impacto sobre el rendimiento de los dispositivos monitoreados.* *• Posibilidad de despliegue o habilitación selectiva sobre hasta cuatrocientos (400) equipos definidos por la Universidad.* *• Integración con la plataforma central de análisis para el envío de información y correlación de eventos.*	*Se solicita a la entidad eliminar el ítem "Posibilidad de despliegue o habilitación selectiva sobre hasta cuatrocientos (400) equipos definidos por la Universidad" o, en su defecto, modificarlo por "Independientemente de los activos licenciados, la solución debe entregar visibilidad de todos los elementos que se conecten a la red y detectar actividad de compromiso sobre ellos". A su vez confirmar la totalidad de activos que se conectaran a la red.*	No se acepta la observación. El ítem 49 busca garantizar que la solución permita ampliar las capacidades de visibilidad y correlación sobre hasta cuatrocientos (400) equipos definidos por la Universidad, mediante agentes, sensores ligeros, telemetría de red u otros mecanismos soportados por el fabricante. Lo anterior tiene como finalidad complementar la información recolectada por la solución en escenarios donde el monitoreo basado únicamente en el tráfico de red no sea suficiente.
TÉCNICO	*4. Requerimientos técnicos mínimos obligatorios, 52. Visibilidad Extendida e Integración de la Solución NDR, 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*	*Se solicita a la entidad eliminar este numeral, dado que esta es una solución de sandboxing o EDR y no está alineado al objeto de este proceso.*	No se acepta la observación. El ítem 52 no exige que la solución NDR incorpore de forma nativa una solución de sandboxing o EDR. El requisito establece que 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, ya sea de forma nativa o mediante integraciones.

TIPO DE CONSULTA	REFERENCIA	CONSULTA	RESPUESTA DE LA UNIVERSIDAD
	detección de comportamientos maliciosos. Esta función debe permitir:		
TÉCNICO	*4. Requerimientos técnicos mínimos obligatorios, 65 Capacidades Avanzadas de Detección, Análisis de Amenazas y Comportamiento, La solución deberá permitir capacidades de análisis dinámico o sandboxing sobre artefactos sospechosos identificados en el tráfico de red, utilizando entornos controlados*	*Se solicita a la entidad eliminar la palabra "sandboxing", dado que el requerimiento no está alineado al objeto de la solicitud.*	No se acepta la observación. El ítem 65 busca garantizar que la solución cuente con capacidades de análisis avanzado sobre artefactos sospechosos identificados en el tráfico de red, mediante análisis dinámico, sandboxing u otros mecanismos equivalentes soportados por el fabricante. Este requisito no exige una solución de sandboxing independiente, sino la capacidad de realizar dicho análisis de forma nativa o mediante integraciones soportadas por el fabricante.
TÉCNICO	*4. Requerimientos técnicos mínimos obligatorios, 67 Capacidades Avanzadas de Detección, Análisis de Amenazas y Comportamiento, 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*	*Se solicita a la entidad eliminar este numeral, dado que esta es una solución de sandboxing o EDR y no está alineado al objeto de este proceso.*	No se acepta la observación. El ítem 67 no exige que la solución NDR incorpore de forma nativa funcionalidades propias de una solución EDR o de sandboxing. El requisito establece que la solución deberá permitir la integración con agentes de endpoint, soluciones 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.
TÉCNICO	*4. Requerimientos técnicos mínimos obligatorios, 72 Capacidades Avanzadas de Detección, Análisis de Amenazas y Comportamiento, La solución debe ser capaz de procesar y analizar archivos, incluidos archivos protegidos por contraseña y documentos de oficina, independientemente de su origen*	*Se solicita a la entidad eliminar este numeral, dado que esta es una solución de sandboxing o EDR y no está alineado al objeto de este proceso.*	No se acepta la observación. El ítem 72 busca garantizar que la solución permita el procesamiento y análisis de archivos identificados durante las actividades de detección de amenazas, incluyendo archivos protegidos por contraseña y documentos de oficina, mediante las capacidades de análisis avanzado soportadas por el fabricante, ya sea de forma nativa o mediante integraciones.
TÉCNICO	*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.*	*Se solicita eliminar este requerimiento, dado que este numeral no permitiría la pluralidad de oferentes.*	Se acepta la observación, el ítem 83 se modifica 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"

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

TIPO DE CONSULTA	REFERENCIA	CONSULTA	RESPUESTA DE LA UNIVERSIDAD
TÉCNICO	*4. Requerimientos técnicos mínimos obligatorios, 83 Capacidades Avanzadas de Detección, Análisis de Amenazas y Comportamiento, La solución debe tener la capacidad de importar y/o personalizar reglas que permitan complementar las predeterminadas y extiendan su uso en el escaneo de objetos del tráfico de red, archivos, objetos e inspección profunda del tráfico, detección de infraestructuras c2c conocidas y reputación de dominios.*	*Se sugiere a la entidad modificar este punto por: "La solución debe tener la capacidad de automáticamente crear y/o ajustar reglas que permitan potenciar las predeterminadas y extiendan su uso en el escaneo de objetos del tráfico de red, archivos, objetos e inspección profunda del tráfico, detección de infraestructuras c2c conocidas y reputación de dominios."*	No se acepta la observación. El ítem 83 busca que la solución permita importar y/o personalizar reglas para complementar las capacidades de detección, de acuerdo con las necesidades de la Universidad. La creación o ajuste automático de reglas puede constituir una funcionalidad adicional de la solución, pero no sustituye la capacidad de importar o personalizar reglas requerida. Sin embargo, se aprovecha la observación para realizar un ajuste en la redacción del ítem, teniendo en cuenta que se presentó un error de digitación, quedando de la siguiente manera: "*La solución debe tener la capacidad de importar y/o personalizar reglas que permitan complementar las predeterminadas y extender las capacidades de detección en el análisis del tráfico de red, archivos y otros objetos inspeccionados, incluyendo la detección de infraestructuras Command and Control (C2) conocidas y la validación de reputación de dominios.*"
TÉCNICO	*4. Requerimientos técnicos mínimos obligatorios, 92 Capacidades NDR,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).*	*Se solicita modificar de la siguiente manera: La solución deberá operar sin agentes (agentless) para garantizar visibilidad total sobre todo dispositivo conectado (incluyendo IoT, cámaras e impresoras). Se requiere una solución con capacidad de análisis transversal de metadatos que elimine los puntos ciegos en la red. Al no depender de agentes, se garantiza la detección y respuesta ante incidentes en activos no administrados (como CCTV o IoT), los cuales suelen quedar fuera del alcance de las herramientas de inventario tradicionales, cerrando la brecha de*	No se acepta la observación. El ítem 92 no establece un mecanismo específico para la obtención de la información solicitada. Adicionalmente, la información relacionada con la actividad o ejecución de archivos ya se encuentra condicionada en el requisito mediante el enunciado: "Información relacionada con actividad o ejecución de archivos, cuando dicha visibilidad se encuentre disponible mediante las capacidades ofertadas". Por tal razón, el requisito permite que el inventario lógico de activos y la información asociada sean obtenidos mediante las capacidades propias de la solución, ya sea a través de mecanismos agentless, agentes, telemetría de red, integraciones u otros mecanismos soportados por el fabricante

TIPO DE CONSULTA	REFERENCIA	CONSULTA	RESPUESTA DE LA UNIVERSIDAD
		seguridad en los activos no administrados.	
TÉCNICO	*4. Requerimientos técnicos mínimos obligatorios, 96 Capacidades NDR La solución debe proporcionar capacidades de respuesta de red, incluida la integración con dispositivos de comunicación de red, para permitir acciones de aislamiento, contención o respuesta asistida o automatizada del host. La solución también facilitará la recopilación de información adicional sobre los activos de la red para apoyar la respuesta a incidentes y la mitigación de amenazas.*	*Se solicita a la entidad eliminar la palabra "aislamiento".*	No se acepta la observación. El ítem 96 establece capacidades de respuesta de red que incluyen distintas acciones como aislamiento, contención o respuesta asistida o automatizada del host, con el fin de fortalecer la capacidad de la solución para la mitigación de amenazas e incidentes de seguridad.
TÉCNICO	*4. Requerimientos técnicos mínimos obligatorios, 98 Capacidades NDR La solución debe proporcionar capacidades de respuesta de red, La solución permitirá un sondeo activo y configurable de dispositivos para enriquecer la información del dispositivo y construir un mapa topológico de red completo.*	*Se solicita a la entidad modificar por "La solución debe tener la capacidad de recopilar, procesar y analizar metadatos de red directamente de los activos, con soporte nativo para ecosistemas en dispositivos Windows, Linux, macOS y Chrome OS"*	No se acepta la observación. El ítem 98 mantiene el requerimiento de sondeo activo y configurable de dispositivos como parte del mecanismo de descubrimiento de activos. Esta capacidad permite la identificación de activos no visibles por otros mecanismos y contribuye a la construcción de un inventario y mapa topológico de red más completo
TÉCNICO	*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 a la entidad modificar para mayor pluralidad de oferentes por : "A efectos de la investigación forense, respuesta a incidentes o cumplimiento normativo de incidentes cibernéticos, la solución debe proporcionar la capacidad de capturar, registrar, reportar y tener acceso a la telemetría asociada con los incidentes reportados por la solución"*	No se acepta la observación. El ítem 100 busca garantizar que la solución cuente con la capacidad de capturar y registrar el tráfico de red en bruto, como elemento fundamental para actividades de investigación forense, respuesta a incidentes y cumplimiento normativo. La telemetría y los reportes constituyen capacidades complementarias de la solución, pero no reemplazan la necesidad de contar con la captura del tráfico en bruto para su análisis detallado.
TÉCNICO	*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 a la entidad eliminar este numeral o modificar por: El proceso de recolección de datos para medir el compromiso debe basarse en metadatos, es decir, no debe depender exclusivamente de los paquetes de datos completos (logs, pcaps, taps).*	Se acepta la observación. Con el fin de permitir la pluralidad de oferentes y reconocer diferentes aproximaciones tecnológicas, se ajusta el ítem para permitir que la captura del tráfico pueda realizarse en formato PCAP u otros mecanismos equivalentes soportados por el fabricante, siempre que permitan su análisis y reproducción para fines de investigación forense, quedando de la siguiente manera: "*El tráfico grabado puede capturarse en un formato que puede analizarse y reproducirse fácilmente, como PCAP*

TIPO DE CONSULTA	REFERENCIA	CONSULTA	RESPUESTA DE LA UNIVERSIDAD
			(Captura de Paquetes) u otros mecanismos equivalentes soportados por el fabricante."
TÉCNICO	*4. Requerimientos técnicos mínimos obligatorios, 104 Capacidades NDR, La solución permitirá la búsqueda y recuperación de sesiones de red basándose en capturas de paquetes en el almacenamiento de tráfico.*	*Se solicita a la entidad modificar de la siguiente forma:" La solución debe realizar búsqueda retrospectiva de hasta 24 meses sobre la data almacenada, permitiendo identificar comunicaciones históricas relacionadas con nuevos Indicadores de Compromiso (IOCs) incorporados en la plataforma"*	No se acepta la observación. El ítem 104 busca garantizar la capacidad de la solución para realizar búsqueda y recuperación de sesiones de red basadas en la información capturada del tráfico, permitiendo su análisis forense a nivel de comunicación y sesión. El análisis basado en indicadores de compromiso (IOC) constituye una capacidad complementaria de threat hunting, sin embargo no reemplaza la necesidad de contar con la posibilidad de recuperación de sesiones de red a partir de la información almacenada para fines de investigación forense.
Juridica	*4. PREPLIEGO CONV 007 DE 2026 NOTA 1: La carga tributaria que se genere con ocasión de la firma, ejecución y liquidación del contrato, está a cargo y es de responsabilidad exclusiva del oferente - contratista.*	*La redacción actual establece que todos los impuestos, tasas y contribuciones estarán a cargo del proponente, lo cual resulta demasiado amplio y puede generar interpretaciones que asignen cargas tributarias que no corresponden. Es importante precisar que cada parte debe responder únicamente por los impuestos, tasas y contribuciones que le sean aplicables de conformidad con la normativa vigente. De esta manera se garantiza un equilibrio contractual y se evita que el contratista asuma obligaciones fiscales que legalmente corresponden a la entidad o a terceros. Por lo anterior, se sugiere modificar la redacción para que quede claramente establecido que cada parte asumirá los tributos que le correspondan según la ley.*	No se acepta la observación, ya que en los numerales 1.33.8, 1.33.9 y 1.33.10 del pliego de condiciones, indica los impuestos, tasas y contribuciones que están a cargo del contratista

UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

TIPO DE CONSULTA	*REFERENCIA*	*CONSULTA*	**RESPUESTA DE LA UNIVERSIDAD**
Juridica	*Pliego de Condiciones 1.33.7 MULTAS*	*Agradecemos considerar que los descuentos por concepto de multa se aplicarán exclusivamente sobre el valor de la factura correspondiente al mes en que se configure el incumplimiento, y no sobre el valor total del contrato. Esta precisión resulta fundamental para garantizar proporcionalidad y equidad en la aplicación de sanciones*	No se acepta la observación. El objeto del presente proceso corresponde a un contrato de compraventa, cuyo alcance comprende el suministro, entrega, instalación, configuración, puesta en funcionamiento y demás actividades requeridas para la implementación de una solución de ciberseguridad. En este sentido, la estructura contractual no contempla la prestación de un servicio con pagos periódicos o mensuales, ni la facturación mensual de las obligaciones contractuales. Por tanto, no resulta procedente establecer que las multas se apliquen sobre el valor de una factura mensual, dado que dicho esquema de pago no hace parte de las condiciones del proceso.
Juridica	*Pliego de Condiciones 1.33.7 CLÁUSULA PENAL PECUNIARIA*	*Se solicita que la cláusula penal pecuniaria se limite exclusivamente a casos de incumplimiento total, declarados mediante acto administrativo motivado, y que los incumplimientos parciales, defectuosos o tardíos sean tratados mediante multas . Estos no configuran necesariamente un incumplimiento grave que justifique una penalidad del 20% sobre el valor total del contrato, lo cual podría resultar desproporcionado frente al impacto real del hecho y vulnerar el principio de razonabilidad previsto en la normativa vigente.*	No se acepta la observación. La Entidad precisa que las multas y la cláusula penal pecuniaria son mecanismos diferentes, con finalidades distintas, las multas constituyen un mecanismo dirigido a conminar al contratista al cumplimiento oportuno de sus obligaciones cuando se presenta mora o retraso en la ejecución contractual. Por su parte, la cláusula penal pecuniaria tiene como finalidad constituir una estimación anticipada de los perjuicios derivados del incumplimiento de las obligaciones contractuales, total o parcial, cuando dicho incumplimiento afecta la correcta ejecución del objeto contratado. No resulta procedente limitar la aplicación de la cláusula penal exclusivamente a los eventos de incumplimiento total, toda vez que pueden presentarse incumplimientos parciales que comprometan el cumplimiento del objeto contractual, afecten la finalidad perseguida con la contratación o generen un perjuicio significativo para la Universidad. En todo caso, la imposición de multas o de la cláusula penal pecuniaria no opera de manera automática. Su aplicación estará precedida del procedimiento establecido en

TIPO DE CONSULTA	REFERENCIA	CONSULTA	RESPUESTA DE LA UNIVERSIDAD
			el artículo 29 del Manual de Supervisión e Interventoría de la Universidad, garantizando el debido proceso.
Juridica	*Pliego de Condiciones* *Minuta del Contrato*	*Solicitamos amablemente y de ser posible compartir la Minuta del Contrato que eventualmente se suscribiría, con el fin de conocer las disposiciones relativas a las estipulaciones contractuales que se estarán aceptando con la presentación de la oferta.*	No se acepta la observación. La Entidad elabora la minuta contractual una vez se surte el proceso de selección y se realiza la adjudicación, la cual se estructura con fundamento en la oferta adjudicada, las condiciones establecidas en el pliego de condiciones y la normatividad vigente aplicable. No obstante, una vez adjudicado el proceso y durante la etapa de perfeccionamiento del contrato, la Universidad podrá revisar conjuntamente con el contratista el contenido de la minuta, con el fin de incorporar los ajustes que resulten procedentes, siempre que no impliquen modificaciones a las condiciones esenciales del proceso de selección, ni desconozcan los principios que rigen la contratación estatal.
Juridica	*Pliego de Condiciones* *En el REGISTRO ÚNICO DE PROPONENTES "RUP" se verificará que el oferente se encuentre inscrito,* *con anterioridad a la fecha de cierre del presente proceso, en al menos (1) de las actividades clasificadas en la tabla UNSPSC referenciada a continuación*	*Según el texto citado, agradecemos confirmar que la clasificación UNSPSC debe estar registrada de manera general en el RUP y que no es requisito que los contratos aportados estén asociados* *específicamente a alguno de los códigos mencionados.*	Se acepta observación. De acuerdo al numeral "Certificación de experiencia" de los estudios previos, establece que el "***Objeto de los contratos:*** *Los contratos acreditados deberán tener como objeto o alcance técnico la implementación de soluciones de ciberseguridad para la protección de infraestructura tecnológica y la implementación de soluciones de ciberseguridad y protección de datos*"
Juridica	*Pliego de Condiciones* *Experiencia requisitos técnicos*		No se acepta, no es clara la observación.

RESPUESTA DE LA UNIVERSIDAD: Cada observación de la tabla se responde en la columna "RESPUESTA DE LA UNIVERSIDAD"

OBSERVACIONES REALIZADAS POR LA EMPRESA SPECTRUM TECHNOLOGY SAS AVENIDA CALLE 26 No. 68C - 61 OFICINA 8 - 18. Gerencia@spectrumt.co Licitaciones@spectrumt.co 3118338799

OBSERVACIÓN No. 1

Con base en el numeral 1.33.4 se solicita aclaración, teniendo en cuenta que la Universidad divide el pago en dos momentos, se solicita aclarar el porcentaje del valor total en cada uno, para tenerlo claro en el momento de que se realicen.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, en apartado de "*FORMA DE PAGO*", se especifica que los pagos se realizarán de la siguiente manera:

"Pago 1: *Este pago corresponde a la entrega, instalación, configuración y puesta en correcto funcionamiento de la solución de detección, prevención y respuesta de red (…) Estos requerimientos corresponden a los ítems 1, 2, 3, 4 y 5 del ANEXO – PROPUESTA ECONÓMICA."*

"Pago 2: *Este pago corresponde a las actividades de pruebas de funcionamiento, estabilización de la plataforma y a los servicios de soporte de partner en esquema 7x24 por un periodo mínimo de (1) año, incluyendo actualizaciones (update y upgrade) de la solución de detección, prevención y respuesta de red. Este pago se realizará una vez la solución se encuentre en correcto funcionamiento y haya culminado el periodo de estabilización de la plataforma, el cual se estima entre treinta (30) y noventa (90) días calendario.*
Nota: Lo anterior mencionado corresponde a los ítems 6 del ANEXO - PROPUESTA ECONÓMICA"

Los pagos se realizarán contra el cumplimiento de los entregables definidos y la aprobación por parte de la supervisión del contrato, conforme a lo establecido en el pliego de condiciones. El valor correspondiente se calculará de acuerdo a lo definido en la oferta económica.

OBSERVACIÓN No. 2

Con respecto al Anexo Técnico de licencias, la Universidad sugiere en los ítems 1 y 4 que la solución esté configurada en ambiente on premises. Como primera medida, se solicita aclaración si es posible ofertar soluciones que se implementen y operen en las nubes de fabricantes.

En caso de que esto no sea posible, nos permitimos informar a la Universidad que la limitación a soluciones que operen exclusivamente de manera local desconoce la evolución técnica de las plataformas XDR/NDR y vulnera el principio de pluralidad de oferentes, al restringir la participación a un subconjunto de tecnologías que no representa el estado actual del mercado. Desde el punto de vista técnico, los fabricantes líderes posicionados por analistas han desarrollado estas soluciones bajo arquitecturas nativas en cloud, dado que su efectividad depende de la correlación centralizada de grandes volúmenes de telemetría, el uso de inteligencia de amenazas global y la actualización continua, capacidades que se optimizan en entornos cloud multi-tenant. En este contexto, el modelo que es posible ofertar por muchos fabricantes no solo no compromete la seguridad ni el control de los datos, sino que las fortalece mediante controles avanzados de cifrado, segmentación y cumplimiento, además de habilitar escalabilidad, analítica avanzada y menor tiempo de despliegue.

Desde la perspectiva jurídica, excluir este modelo constituye una condición desproporcionada y no relacionada directamente con el objeto contractual, que limita la libre concurrencia y favorece indirectamente a un grupo reducido de oferentes, contrariando los lineamientos de Colombia Compra Eficiente sobre selección objetiva. En consecuencia, se solicita permitir la oferta de soluciones de ambas modalidades, siempre que cumplan con los requisitos de seguridad, gobernanza y gestión de datos exigidos, evitando así un posible direccionamiento del proceso y garantizando condiciones reales de competencia.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. La Universidad ha definido que la solución requerida debe operar bajo una arquitectura On-Premise, de acuerdo a las necesidades institucionales de seguridad de la información, control de los datos y operación dentro de la infraestructura tecnológica de la entidad.

OBSERVACIÓN No. 3

Con base en lo indicado por la Universidad en cuanto al proceso, se solicita confirmar si las observaciones y las ofertas serán publicadas por la universidad y por qué medio, para garantizar los principios de transparencia, publicidad y selección objetiva que rigen la contratación pública, así como permitir el ejercicio efectivo del control social por parte de los interesados.

RESPUESTA DE LA UNIVERSIDAD: La Universidad aclara que, en cumplimiento de los principios de transparencia, publicidad y selección objetiva que rigen la contratación pública, todas las observaciones

presentadas por los interesados, así como sus respectivas respuestas, serán publicadas a través de https://contratacion.udistrital.edu.co/ en la sección convocatoria pública – 2026. SECOP II

Una vez sea publicada la evaluación inicial, las empresas que se encuentran participando pueden solicitar copia de las ofertas al correo contratacionud@udistrital.edu.co.

OBSERVACIONES REALIZADAS POR LA EMPRESA SOLUCIONES DE SOFTWARE INDTECH SAS NIT: 901432969 DEISY RODRIGUEZ CAMACHO REPRESENTANTE LEGAL SUPLENTE CORREO ELECTRÓNICO: Deisy.rodriguez@Indtech.io TELÉFONO: +57 3246761209

OBSERVACIÓN No. 1

En ejercicio del derecho consagrado en el numeral 1.14 del Proyecto de Pliego de Condiciones de la Convocatoria Pública No. 007 de 2026, y dentro del plazo establecido en el cronograma del proceso (del 24 de junio al 1 de julio de 2026), SOLUCIONES DE SOFTWARE INDTECH SAS con NIT 901.432.969-3, a través de su representante legal, respetuosamente presenta las siguientes observaciones al Proyecto de Pliego de Condiciones, específicamente en relación con los requisitos habilitantes financieros establecidos en la sección 2.2 "Capacidad Financiera" del documento.

Nuestra empresa es una compañía del sector de tecnologías de la información con amplia experiencia en el suministro, implementación y soporte de soluciones de ciberseguridad, y tiene un legítimo interés en participar en el presente proceso de selección. Las presentes observaciones se formulan con el ánimo constructivo de que los pliegos definitivos permitan la mayor pluralidad de oferentes, sin comprometer las garantías de capacidad financiera que la Universidad legítimamente requiere.:

OBSERVACIÓN PRIMERA: ÍNDICE DE LIQUIDEZ

Realidad del sector de tecnología y ciberseguridad *Las empresas del sector TI y ciberseguridad en Colombia operan con modelos de negocio basados en rotación rápida de inventario, contratos de prestación de servicios con ciclos cortos de cobro y alta conversión de activos operativos. Según datos sectoriales, la razón corriente promedio del sector se ubica entre 1.0 y 1.3 veces.*

Proporcionalidad con la naturaleza del contrato*. El objeto contractual corresponde a un contrato de compraventa de una solución de ciberseguridad, con una estructura de pagos dividida en dos hitos. No se trata de un contrato que exija al contratista financiar operaciones por largos periodos de tiempo. El primer pago se realiza contra entrega e instalación de los equipos y licenciamiento, y el segundo tras el periodo de estabilización (30-90 días). Esta estructura de pagos reduce significativamente el riesgo de liquidez del contratista durante la ejecución.*

Se solicita respetuosamente a la Universidad Distrital Francisco José de Caldas que, en los pliegos de condiciones definitivos, se ajuste el requisito de Índice de Liquidez de la siguiente manera:

Indicador	*Valor actual pre-pliego*	*Valor solicitado*
Liquidez	*≥ 1.5*	*≥ 1.1*

Este ajuste se encuentra alineado con las mejores prácticas de contratación pública, con los promedios sectoriales del mercado de tecnología y ciberseguridad, y garantiza la participación de empresas financieramente sanas sin exponer a la entidad contratante a riesgo alguno.

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 SEGUNDA: CAPITAL DE TRABAJO

Desproporcionalidad del requisito. *Exigir un capital de trabajo equivalente al 100% del presupuesto oficial implica que el proponente debe demostrar, en su balance general, la totalidad de los recursos del contrato como excedente de activos corrientes sobre pasivos corrientes. Este requisito es desproporcionado frente a la naturaleza del contrato, por las siguientes razones:*
El contrato es de compraventa, no de concesión ni de obra pública. El contratista no está obligado a financiar con recursos propios la totalidad del objeto contractual durante la ejecución. Los fabricantes de soluciones de ciberseguridad otorgan crédito y condiciones de pago a sus canales autorizados, lo cual reduce significativamente la necesidad de capital propio para la adquisición de los componentes.

Estructura de pagos del contrato. *La forma de pago prevista en el numeral 1.33.4 del pre-pliego establece dos pagos:*

- ***Pago 1:*** *Contra entrega, instalación, configuración y puesta en correcto funcionamiento de la solución (hardware, licenciamiento, mecanismos de visibilidad para 400 endpoints, y soporte de fábrica).*
- ***Pago 2:*** *Tras las pruebas de funcionamiento, estabilización de la plataforma y servicios de soporte 7x24 por un año (estimado entre 30 y 90 días calendario después del Pago 1).*

Esta estructura demuestra que la entidad paga contra entrega de resultados verificables, por lo que el contratista no necesita financiar el 100% del valor del contrato con capital propio. La exposición financiera real del contratista se limita al costo de adquisición de los equipos y licencias durante el periodo entre la orden de compra al fabricante y el primer pago, que en la práctica oscila entre el 35% y 50% del valor total del contrato.

Lineamientos de Colombia Compra Eficiente*. Colombia Compra Eficiente, en su Manual para la Determinación y Verificación de Requisitos Habilitantes, recomienda que el capital de trabajo requerido sea proporcional a las necesidades operativas del contrato. Para contratos de suministro de bienes con pago contra entrega, la práctica usual y recomendada es establecer requisitos de capital de trabajo entre el 30% y 50% del presupuesto oficial, lo cual refleja la real necesidad de financiamiento del contratista.*

Comparativo con procesos similares*. En procesos de contratación pública de naturaleza similar (adquisición de soluciones de seguridad informática, plataformas de monitoreo de red, soluciones NDR/IDS/IPS), las entidades estatales colombianas establecen típicamente requisitos de capital de trabajo entre el 30% y 50% del presupuesto oficial. Exigir el 100% se aparta de la práctica comúnmente aceptada y puede limitar injustificadamente la participación de empresas idóneas.*

Afectación a la pluralidad de oferentes*. Un requisito de capital de trabajo del 100% del PO restringe de manera significativa el universo de posibles oferentes, concentrando la participación en empresas de gran tamaño que, en muchos casos, no son las que mejor conocen ni operan directamente las soluciones de ciberseguridad especializadas que requiere la Universidad. Este tipo de barrera contraría los principios de libre concurrencia y selección objetiva consagrados en el Acuerdo 03 de 2015 del Consejo Superior Universitario y en las normas de contratación aplicables.*

Se solicita respetuosamente a la Universidad Distrital Francisco José de Caldas que, en los pliegos de condiciones definitivos, se ajuste el requisito de Capital de Trabajo de la siguiente manera:

Indicador	***Valor actual pre-pliego***	***Valor solicitado***
Capital de Trabajo	*≥ 100% del PO*	***≥ 30% del PO***

Con un capital de trabajo mínimo del 30% del presupuesto oficial (equivalente a $297.000.000), la Universidad mantendría una garantía adecuada de solvencia del contratista, al tiempo que ampliaría la base de posibles oferentes con empresas financieramente sanas y técnicamente idóneas para ejecutar el objeto contractual. Este porcentaje refleja con mayor precisión la exposición financiera real del contratista dada la estructura de pagos del contrato.

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. 3

3. OBSERVACIÓN TERCERA: EXPERIENCIA

Proporcionalidad con la naturaleza del contrato. *Los requisitos habilitantes deben ser "adecuados y proporcionales a la naturaleza y valor del contrato." El mercado de soluciones NDR (Network Detection and Response) en Colombia es un segmento especializado y de desarrollo reciente. Exigir que la sumatoria de contratos ejecutados equivalga al 100% del presupuesto oficial en un máximo de tres (3) contratos, restringidos además a un objeto específico de ciberseguridad, constituye una barrera que favorece únicamente a grandes integradores y excluye a empresas especializadas con capacidad demostrada.*

Lineamientos de Colombia Compra Eficiente*. El Manual establece que la experiencia es proporcional "cuando tiene relación con el alcance, la cuantía, riesgo y la complejidad del negocio a celebrar" y advierte que exigir condiciones idénticas a las del objeto "puede suponer una restricción injustificada a la pluralidad de oferentes." Adicionalmente, el Manual orienta a las entidades a preguntarse si los requisitos habilitantes "permiten la participación de la mayoría de los actores del mercado que ofrecen los bienes y servicios.*

Promoción de la participación de MiPyMEs (Ley 2069 de 2020, Arts. 31 y 33). *La Ley de Emprendimiento obliga a las entidades públicas a "definir reglas que promuevan y faciliten la participación" de las micro, pequeñas y medianas empresas en la contratación pública. El artículo 31 autoriza expresamente la fijación de requisitos diferenciales en "tiempo de experiencia" y "número de contratos para acreditación de experiencia." INDTECH, clasificada como Pequeña Empresa en el RUP, cuenta con experiencia real y verificable en ciberseguridad, pero el umbral del 100% impide su habilitación.*

Se solicita respetuosamente reducir el umbral del 100% al 70% del valor estimado de la contratación, de manera que la sumatoria de los contratos acreditados en el RUP sea igual o superior al setenta por ciento (70%) del presupuesto oficial.

De manera complementaria a los contratos acreditados mediante el RUP, se permita la presentación de certificaciones de contratos en ejecución con avance igual o superior al cincuenta por ciento (50%), expedidas por la entidad contratante, como medio de acreditación complementario de la experiencia. El valor acreditable de estos contratos correspondería al porcentaje efectivamente ejecutado.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. La Universidad estableció los requisitos habilitantes de experiencia con fundamento en el análisis del objeto contractual, su complejidad técnica, el nivel de riesgo asociado a la implementación de la solución de ciberseguridad y la necesidad de seleccionar un contratista que demuestre capacidad suficiente para ejecutar integralmente las obligaciones derivadas del contrato.

En este sentido, se considera razonable y proporcional exigir que la sumatoria de los contratos aportados para acreditar la experiencia sea igual o superior al cien por ciento (100 %) del presupuesto oficial, toda vez que este requisito permite verificar que el proponente ha ejecutado satisfactoriamente proyectos de magnitud equivalente a la contratación que se pretende celebrar.

Respecto de la solicitud de permitir la acreditación de experiencia mediante contratos en ejecución, la misma no es procedente, por cuanto la finalidad del requisito de experiencia es verificar la ejecución efectiva y satisfactoria de obligaciones similares a las del objeto contractual. En consecuencia, la experiencia exigida debe corresponder a contratos completamente ejecutados y recibidos a satisfacción, condición que permite a la Universidad verificar objetivamente el cumplimiento integral de las obligaciones contractuales y los resultados obtenidos.

OBSERVACIÓN No. 4

Observaciones Técnicas:

Observación No. 1
Documento: *27397 – Especificaciones Técnicas*
Numeral: *4. Requerimientos técnicos mínimos obligatorios*
Ítem 4 – Arquitectura y componentes físicos de la solución

Respetuosamente solicitamos a la Entidad revisar y precisar el alcance del siguiente requerimiento:

"La solución deberá permitir la creación e incorporación de nuevos sensores, los cuales podrán ser desplegados de manera física o virtual sobre la infraestructura tecnológica de la Universidad, sin que ello genere costos adicionales para la Universidad."

Al respecto, es importante considerar que, en este tipo de soluciones, la posibilidad de incorporar sensores físicos o virtuales se encuentra asociada al esquema de licenciamiento y a la capacidad de procesamiento o inspección contratada, normalmente medida en Gbps.

En ese sentido, si bien la solución propuesta permite desplegar nuevos sensores sin requerir licencias adicionales, dicha capacidad aplica siempre que el volumen de tráfico inspeccionado no exceda la capacidad licenciada adquirida por la Universidad. En caso de que la Entidad requiera procesar un volumen de tráfico superior al inicialmente contratado, será necesario ampliar la capacidad de licenciamiento correspondiente, situación que podría generar costos adicionales.

Por lo anterior, respetuosamente solicitamos que el requisito sea ajustado o aclarado, indicando que la incorporación de nuevos sensores físicos o virtuales no generará costos adicionales ***siempre que la capacidad total de inspección de tráfico permanezca dentro del licenciamiento adquirido por la Universidad****. Esta precisión permitirá que todos los oferentes interpreten el requerimiento de manera uniforme, evitará expectativas que excedan el alcance técnico del licenciamiento y contribuirá a una ejecución contractual transparente y acorde con las capacidades reales de la solución ofertada.*

RESPUESTA DE LA UNIVERSIDAD: Se acepta observación. Se ajusta el ítem 4 los requerimientos técnicos mínimos, quedando de la siguiente manera: "*La solución deberá permitir la creación e incorporación de nuevos sensores, los cuales podrán ser desplegados de manera física o virtual sobre la infraestructura tecnológica de la Universidad siempre y cuando no sobrepase las capacidades contratadas y sin que ello genere costos adicionales la Universidad.*"

OBSERVACIÓN No. 5

Observación No. 2
Documento: *27397 – Especificaciones Técnicas*
Numeral: *4. Requerimientos técnicos mínimos obligatorios*
Ítem 19 – Arquitectura y Diseño de la Plataforma

Respetuosamente solicitamos a la Entidad aclarar el alcance del siguiente requisito:

"Cada Centro de Análisis deberá soportar el procesamiento del volumen de tráfico de la red institucional, incluyendo enlaces troncales de alta capacidad (mínimo 6 Gbps de tráfico o superior), sin degradación del análisis ni pérdida de visibilidad."

Al respecto, se observa que la capacidad de procesamiento exigida constituye uno de los principales parámetros para el dimensionamiento de la solución NDR, ya que de ella dependen aspectos como el licenciamiento, la arquitectura propuesta, el dimensionamiento de los recursos de hardware y el valor económico de la oferta.

En procesos de consulta o ejercicios de análisis de mercado realizados previamente por la Universidad, se ha evidenciado la referencia a escenarios de dimensionamiento de ***4 Gbps*** *y* ***6 Gbps****, razón por la cual respetuosamente solicitamos precisar cuál corresponde a la capacidad de procesamiento que deberá ser considerada para efectos de la presentación de las ofertas.*

Esta aclaración permitirá que todos los oferentes estructuren sus propuestas bajo un mismo criterio técnico, garantizando condiciones homogéneas de evaluación, evitando interpretaciones diferentes sobre el alcance del proyecto y reduciendo posibles diferencias durante la etapa de ejecución contractual.

*En consecuencia, respetuosamente solicitamos a la Entidad confirmar si la solución requerida deberá dimensionarse para una capacidad de procesamiento de **4 Gbps** o de **6 Gbps**, o, en caso de corresponder a otro escenario, indicar expresamente la capacidad de procesamiento que deberá ser considerada por los oferentes.*

RESPUESTA DE LA UNIVERSIDAD: Se acepta la observación, se modifica el ítem 19 de la tabla de requisitos mínimos quedando de la siguiente manera "Cada Centro de Análisis deberá soportar el procesamiento del volumen de tráfico de la red institucional, incluyendo enlaces troncales de alta capacidad (mínimo 4 Gbps de tráfico o superior), sin degradación del análisis ni pérdida de visibilidad"

OBSERVACIÓN No. 6

Observación No. 3

Documento: *27397 – Especificaciones Técnicas*

Numeral: *5. Certificaciones técnicas solicitadas*

Literal b)

Respetuosamente solicitamos a la Entidad revisar el alcance del siguiente requisito:

"Los componentes de la solución no deberán encontrarse en estado de End of Support (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."

*Al respecto, consideramos pertinente diferenciar el comportamiento del ciclo de vida de los componentes de hardware frente al de las soluciones de software especializadas en ciberseguridad, tales como las plataformas de **Network Detection and Response (NDR)** y **Endpoint Detection and Response (EDR)**.*

En este tipo de soluciones, los fabricantes evolucionan continuamente sus plataformas mediante la liberación de nuevas versiones, incorporando capacidades funcionales, mejoras de rendimiento, nuevas técnicas de detección de amenazas y actualizaciones de seguridad.

*Como consecuencia, las políticas de **End of Life (EOL)** y **End of Support (EOS)** se administran normalmente sobre versiones específicas del software y no sobre el producto como tal, el cual continúa vigente y soportado mediante procesos de actualización tecnológica.*

Por lo anterior, exigir que una versión específica mantenga un ciclo de vida mínimo de cinco (5) años podría limitar la participación de soluciones líderes del mercado, cuyas políticas de soporte contemplan ciclos de actualización más dinámicos, sin que ello represente una disminución en la calidad, continuidad del servicio o compromiso de soporte por parte del fabricante.

En consecuencia, respetuosamente solicitamos que el requisito sea ajustado para distinguir los componentes de hardware de las soluciones de software de ciberseguridad, manteniendo el requisito de cinco (5) años para los componentes cuya naturaleza lo permita y estableciendo un período mínimo de soporte de dos (2) años para las versiones de software de ciberseguridad, tiempo durante el cual el fabricante garantice soporte técnico y actualizaciones de seguridad. Lo anterior permitiría una mayor pluralidad de oferentes, manteniendo plenamente protegidos los intereses de la Entidad y alineando el proceso con las prácticas habituales de la industria.

En este sentido, respetuosamente proponemos la siguiente redacción:

"Los componentes de la solución no deberán encontrarse en estado de End of Support (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. Para los componentes de software de ciberseguridad, tales como la solución de Network Detection and Response (NDR) y Endpoint Detection and Response (EDR), el fabricante deberá garantizar para la versión ofertada un período de soporte y actualizaciones de seguridad no inferior a dos (2) años, sin perjuicio de la posibilidad de actualización a versiones posteriores soportadas por el fabricante."

Agradecemos de antemano la atención a las presentes observaciones, las cuales permitirán estructurar una oferta económica competitiva y un cronograma de ejecución viable para el éxito del proyecto.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. El ítem b del punto 5. Certificaciones técnicas solicitadas, hace referencia a que la solución ofertada deberá contar con soporte y actualizaciones durante el tiempo exigido por la Universidad.

En el caso de las soluciones de software de ciberseguridad, se entiende que el fabricante podrá liberar nuevas versiones durante la vigencia del servicio, las cuales reemplazarán las versiones anteriores como parte de la evolución del producto, sin que ello afecte el cumplimiento del requisito de soporte establecido.

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

Observación No. 1

CONVOCATORIA PÚBLICA No. 005 DE 2026 - 3.2.2.1 CERTIFICACIÓN DE DISTRIBUCIÓN:

> **3.2.2.1 CERTIFICACIÓN DE DISTRIBUCIÓN:**
>
> 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 de la marca ofertada en el territorio colombiano. 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 acotar el alcance de la certificación. Teniendo en cuenta el numeral 1.2.2 ALCANCE TÉCNICO - PARA EL COMPONENTE 2: del documento CONVOCATORIA PÚBLICA No. 005 DE 2026, en el que se indica lo siguiente

> **Nota:** La presente adquisición se limita estrictamente al suministro, entrega física e instalación de hardware (componentes físicos) y garantías asociadas. Por lo tanto, quedan excluidos del alcance del proveedor los siguientes puntos:

*Respetuosamente se solicita a la entidad que, en la certificación de fabricante se indique que es distribuidor autorizado y que puede cumplir con las garantías. Es decir, se solicita que, dado el alcance del servicio, se elimine las palabras **"instalar, configurar, soportar y realizar mantenimiento"** dado que, por un lado, estos servicios no están incluidos en el alcance, y por otro lado, el contratista podría contratar servicios de fabricante, o contar con ingenieros certificados para esta labor, teniendo en cuenta que no todos los fabricantes de hardware lideres del mercado cuentan con canales de servicios, para lo cual está dirigida la certificación. Esto se solicita, con el fin de propender por la pluralidad de oferentes. Adicionalmente, el skill necesario para exigir proveedores de alto nivel se está solicitando en el numeral 3.2.2.2 CERTIFICACIÓN DE CANAL AUTORIZADO: en el que se solicita acreditar condición en nivel Advanced o equivalente, por lo que solicitar otra carta con esa especificidad sería redundante y en contravía de la pluralidad.*

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, se evidencia que la observación corresponde a la "CONVOCATORIA PÚBLICA No. 005 DE 2026" la cual no se encuentra vigente, el presente proceso corresponde a la "CONVOCATORIA PÚBLICA No. 007 DE 2026".

OBSERVACIÓN No. 2

Observación No. 2

CONVOCATORIA PÚBLICA No. 005 DE 2026 - 3.2.2.8 REQUERIMIENTOS TÉCNICOS MÍNIMOS OBLIGATORIOS EQUIPO SERVIDOR TIPO 1

Ítem	Característica técnica	Descripción
8	Almacenamiento	Como mínimo 480GB SSD SATA Mixed Use 6Gbps 512e 2.5in Hot-plug AG Drive, 3 DWPD + BOSS-N1 controller card + with 2 M.2 960GB (RAID 1) (22x80)
		Los discos ofertados deben ser de estado sólido con mínimo 3 DWPD

Se solicita muy amablemente a la entidad permitir controladoras de almacenamiento acorde a la marca de cada fabricante, dado que la BOSS-N1 controller card es una tarjeta exclusiva del fabricante DELL.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, se evidencia que la observación corresponde a la "CONVOCATORIA PÚBLICA No. 005 DE 2026" la cual no se encuentra vigente, el presente proceso corresponde a la "CONVOCATORIA PÚBLICA No. 007 DE 2026".

OBSERVACIÓN No. 3

Observación No. 3

CONVOCATORIA PÚBLICA No. 005 DE 2026 - 3.2.2.8 REQUERIMIENTOS TÉCNICOS MÍNIMOS OBLIGATORIOS EQUIPO SERVIDOR TIPO 1

Nota: El equipo servidor ofertado deberá cumplir con certificación ENERGY STAR vigente, contar con fuentes de poder certificadas 80 o superior de acuerdo a la calificación del fabricante, y cumplir con normativas ambientales RoHS y WEEE.

Se solicita a la entidad aclarar si la certificación Energy Star se deberá dar al equipo o al procesador, dado que, normalmente este tipo de certificaciones se entregan al procesador del equipo y no al servidor como tal.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, se evidencia que la observación corresponde a la "CONVOCATORIA PÚBLICA No. 005 DE 2026" la cual no se encuentra vigente, el presente proceso corresponde a la "CONVOCATORIA PÚBLICA No. 007 DE 2026".

OBSERVACIÓN No. 4

Observación No. 4

CONVOCATORIA PÚBLICA No. 005 DE 2026 - 3.2.2.8 REQUERIMIENTOS TÉCNICOS MÍNIMOS OBLIGATORIOS EQUIPO SERVIDOR TIPO 1

5	Procesador	El equipo debe poseer mínimo 2 SOCKETS para procesadores con las siguientes características: Procesador con un mínimo de 16 cores físicos, frecuencia base de 3,2 GHz, ancho de banda de interconexión de 24 GT/s y memoria caché de al menos 72 MB.

Se solicita a la entidad aclarar si requiere dos procesadores de 16 cores cada uno o que ambos procesadores sumen en total 16 cores (8 cores cada uno)

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, se evidencia que la observación corresponde a la "CONVOCATORIA PÚBLICA No. 005 DE 2026" la cual no se encuentra vigente, el presente proceso corresponde a la "CONVOCATORIA PÚBLICA No. 007 DE 2026".

OBSERVACIÓN No. 5

Observación No. 5

CONVOCATORIA PÚBLICA No. 005 DE 2026 - 3.2.2.8 REQUERIMIENTOS TÉCNICOS MÍNIMOS OBLIGATORIOS EQUIPO SERVIDOR TIPO 2

5	Procesador	El equipo debe poseer mínimo 2 SOCKETS para procesadores con las siguientes características: Procesador con un mínimo de 32 cores físicos, frecuencia base de 2.5 GHz, ancho de banda de interconexión 16 GT/s y memoria caché de al menos 72 MB

Se solicita a la entidad aclarar si requiere dos procesadores de 32 cores cada uno o que ambos procesadores sumen en total 32 cores (16 cores cada uno)

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, se evidencia que la observación corresponde a la "CONVOCATORIA PÚBLICA No. 005 DE 2026" la cual no se encuentra vigente, el presente proceso corresponde a la "CONVOCATORIA PÚBLICA No. 007 DE 2026".

OBSERVACIÓN No. 6

Observación No. 6

CONVOCATORIA PÚBLICA No. 005 DE 2026 - 3.2.2.8 REQUERIMIENTOS TÉCNICOS MÍNIMOS OBLIGATORIOS EQUIPO SERVIDOR TIPO 2

8	Almacenamiento	Como mínimo 2 TB Hard Drive SAS ISE 12Gbps 10K 512e 2.5in Hot-Plug + BOSS-N1 controller card

Se solicita muy amablemente a la entidad permitir controladoras de almacenamiento acorde a la marca de cada fabricante, dado que la BOSS-N1 controller card es una tarjeta exclusiva del fabricante DELL.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, se evidencia que la observación corresponde a la "CONVOCATORIA PÚBLICA No. 005 DE 2026" la cual no se encuentra vigente, el presente proceso corresponde a la "CONVOCATORIA PÚBLICA No. 007 DE 2026".

OBSERVACIÓN No. 7

Observación No. 7

CONVOCATORIA PÚBLICA No. 005 DE 2026 - 2.4.1.2 OFRECIMIENTOS TÉCNICOS ADICIONALES

ÍTEM	DESCRIPCIÓN	ASIGNACIÓN DE PUNTOS	TOTAL
1	Licencias adicionales sin costo para fortalecer la protección de Endpoints durante la vigencia del contrato.	Se otorgarán hasta 100 puntos al proponente que ofrezca la mayor cantidad de licencias	100
2	Ampliación del tiempo de licenciamiento y soporte técnico	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 2 de la propuesta económica), alineado al ítem 1?*
- *¿La ampliación es únicamente para la línea base de 400 licencias?*

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, se evidencia que la observación corresponde a la "CONVOCATORIA PÚBLICA No. 005 DE 2026" la cual no se encuentra vigente, el presente proceso corresponde a la "CONVOCATORIA PÚBLICA No. 007 DE 2026".

OBSERVACIÓN No. 8

Observación No. 8

4. ESPECIFICACIONES TÉCNICAS LICENCIAS

Ítem	Característica técnica	Descripción
6	Requisitos Generales	La solución deberá permitir una arquitectura distribuida, soportando la instalación de al menos un (1) nodo central de administración y análisis principal en la sede Calle 40, y al menos un (1) sensor de red adicional en la sede Bosa. La administración, configuración de políticas, correlación de eventos y generación de reportes deberá realizarse desde una única consola centralizada. La comunicación entre sensores y el nodo central deberá realizarse de forma segura y cifrada.

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: No se acepta la observación, se evidencia que la observación corresponde a la "CONVOCATORIA PÚBLICA No. 005 DE 2026" la cual no se encuentra vigente, el presente proceso corresponde a la "CONVOCATORIA PÚBLICA No. 007 DE 2026".

OBSERVACIÓN No. 9

Observación No. 9

4. ESPECIFICACIONES TÉCNICAS LICENCIAS

Ítem	Característica técnica	Descripción
1	Requisitos Generales	La solución deberá permitir configuraciones que garanticen que la información analizada permanezca bajo control de la entidad cuando se requiera, conforme a las políticas de seguridad institucional.

Se entiende que la entidad permite una solución que asegure que la información permanezca bajo control de la entidad con soluciones en modalidad SaaS. En la que toda la información propia está asegurada y disponible para la entidad con capacidades de seguridad, aislamiento y gobernanza de la información. Por favor, confirmar este entendimiento.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, se evidencia que la observación corresponde a la "CONVOCATORIA PÚBLICA No. 005 DE 2026" la cual no se encuentra vigente, el presente proceso corresponde a la "CONVOCATORIA PÚBLICA No. 007 DE 2026".

OBSERVACIÓN No. 10

Observación No. 10

4. ESPECIFICACIONES TÉCNICAS LICENCIAS

4	Requisitos Generales	La solución debe conservar todos los datos de telemetría de red y puntos finales localmente, con configuraciones de almacenamiento configurables para adaptarse a necesidades específicas de retención y gestión de datos.

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.

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, mas 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 continua 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, se evidencia que la observación corresponde a la "CONVOCATORIA PÚBLICA No. 005 DE 2026" la cual no se encuentra vigente, el presente proceso corresponde a la "CONVOCATORIA PÚBLICA No. 007 DE 2026".

OBSERVACIÓN No. 11

Observación No. 11

4. ESPECIFICACIONES TÉCNICAS LICENCIAS

31	Integración	La solución deberá permitir esquemas de integración segura unidireccional en entornos que requieran segmentación estricta entre redes.

Se entiende que el requerimiento de "esquemas de integración segura unidireccional" hace referencia a esquemas de flujos unidireccionales funcionales acorde a la arquitectura de cada fabricante e implementación segura. Por favor confirmar este entendimiento.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, se evidencia que la observación corresponde a la "CONVOCATORIA PÚBLICA No. 005 DE 2026" la cual no se encuentra vigente, el presente proceso corresponde a la "CONVOCATORIA PÚBLICA No. 007 DE 2026".

OBSERVACIÓN No. 12

Observación No. 12

4. ESPECIFICACIONES TÉCNICAS LICENCIAS

63	Capacidades ANTI-APT (APT / SANDBOX)	La solución debe ser capaz de procesar y analizar archivos adjuntos en mensajes de correo, incluidos archivos protegidos por contraseña y documentos de oficina.
65	Capacidades ANTI-APT (APT / SANDBOX)	La solución debe ser capaz de obtener contraseñas para desempaquetar archivos protegidos por contraseña y documentos de oficina del cuerpo del mensaje de correo.

Teniendo en cuenta que los ítems 63 y 65 hacen referencia a una solución de protección de correo, se solicita muy amablemente a la entidad aclarar el alcance de dichos requerimientos, es decir:

- *¿La entidad requiere adicionalmente una solución de protección de correo?*
- *¿La entidad requiere que la solución se integre con la solución de protección de correo implementada actualmente en la entidad para que pueda analizar adjuntos y archivos protegidos?*

De esta manera, teniendo en cuenta que estos ítems no tienen relación con protección de EndPoints y/o red, se solicita eliminar dichos ítems y/o aclarar el alcance de los mismos.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, se evidencia que la observación corresponde a la "CONVOCATORIA PÚBLICA No. 005 DE 2026" la cual no se encuentra vigente, el presente proceso corresponde a la "CONVOCATORIA PÚBLICA No. 007 DE 2026".

OBSERVACIÓN No. 13

Observación No. 13

CONVOCATORIA PÚBLICA No. 005 DE 2026 - 2.4.2.2 OFRECIMIENTOS TÉCNICOS ADICIONALES COMPONENTE 2

ítem	Descripción	Asignación de puntos	Total
1	Mayor capacidad en cores	Se otorgarán hasta 100 puntos al proponente que ofrezca este ítem	100
2	Mayor capacidad en memoria	Se otorgarán hasta 100 puntos al proponente que ofrezca este ítem	100

Se solicita muy amablemente a la entidad confirmar para cual de los tres servidores que se planean adquirir se debe ofrecer mayor capacidad en cores y en memoria para obtener los puntos del ofrecimiento técnico.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación, se evidencia que la observación corresponde a la "CONVOCATORIA PÚBLICA No. 005 DE 2026" la cual no se encuentra vigente, el presente proceso corresponde a la "CONVOCATORIA PÚBLICA No. 007 DE 2026".

OBSERVACIÓN No. 14

Observación No. 14

Con respecto al requerimiento que exige que las certificaciones acrediten el "valor del contrato y su equivalente en salarios mínimos legales mensuales vigentes (SMMLV) a la fecha de firma", respetuosamente solicitamos a la Entidad eliminar la exigencia de incluir el valor en SMMLV dentro de la certificación.

Lo anterior, teniendo en cuenta la mayoría de las certificaciones contractuales expedidas por las entidades públicas y privadas únicamente incluyen el valor del contrato en pesos, sin contemplar su equivalencia en SMMLV. Adicionalmente, el valor en SMMLV es un dato que puede ser fácilmente verificado y calculado por la Entidad a partir de la información registrada en el Registro Único de Proponentes (RUP), el cual constituye un documento oficial y válido para la acreditación de experiencia, conforme a lo establecido en la normativa de contratación pública.

RESPUESTA DE LA UNIVERSIDAD: Se acepta la observación. La Universidad ajustará el ítem *"d"* del "*Análisis de la experiencia*" quedando así "*d. Valor del contrato".* No obstante, la Entidad verificará la experiencia acreditada con base en la información registrada en el Registro Único de Proponentes (RUP) y, cuando resulte necesario, realizará la conversión del valor de los contratos a salarios mínimos legales mensuales vigentes (SMLMV), de conformidad con la normatividad aplicable y los criterios establecidos en el pliego de condiciones.

OBSERVACIÓN No. 15

Observación No. 15

Con respecto al siguiente requerimiento:

La propuesta económica inicial se presentará en el formato establecido en el Anexo No. 3, en medio impreso y en copia de medio magnético en formato Excel.

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

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

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

Respetuosamente solicitamos a la Entidad aclarar el alcance del requisito contenido en el numeral correspondiente a la presentación de la propuesta económica, en el cual se establece que esta deberá presentarse en "medio impreso y en copia de medio magnético en formato Excel".

En particular, agradecemos precisar si la expresión "medio impreso" hace referencia a la presentación del Anexo No. 3 en formato PDF, debidamente suscrito por el representante legal o si la entidad requiere algún otro formato específico.

RESPUESTA DE LA UNIVERSIDAD: La Universidad acepta la observación y ajustara lo pertinente en el pliego definitivo.

OBSERVACIÓN No. 16

Observación No. 16 – Arquitectura física, virtual o software 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 físico central en Calle 40, un sensor o colector físico en Bosa Porvenir, componentes físicos para la operación on-premise y posibilidad de incorporar nuevos sensores físicos o virtuales.

Observación:

Se solicita amablemente a la Entidad aclarar y permitir que la solución pueda ser implementada mediante appliance físico, appliance virtual del fabricante o software del fabricante instalado sobre servidor físico dedicado, siempre que se garantice la operación on-premise, el desempeño requerido, la retención, la seguridad, el soporte y la garantía durante la vigencia contractual.

Lo anterior teniendo en cuenta que en el mercado existen soluciones especializadas de detección y respuesta a nivel de red que pueden operar bajo esquemas físicos, virtuales o híbridos sobre infraestructura dedicada, sin que ello afecte el cumplimiento del objeto contractual ni la administración de la información por parte de la Universidad.

Solicitud:

Se solicita amablemente a la Entidad ajustar el requerimiento en los siguientes términos:

"La solución deberá contemplar los componentes físicos, virtuales o software sobre infraestructura física dedicada necesarios para su correcta implementación, operación, monitoreo y administración bajo arquitectura on-premise. El nodo central y los sensores podrán ser implementados como appliances físicos, appliances virtuales o componentes de software del fabricante sobre hardware dedicado, siempre que el oferente garantice el desempeño, capacidad, soporte, retención y disponibilidad requeridos."

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. La Universidad ha definido en los requerimientos técnicos que la solución deberá contemplar componentes físicos necesarios para la implementación y correcto funcionamiento bajo arquitectura on-premise, incluyendo el nodo central y los sensores asociados.

Lo anterior pensado en las condiciones de infraestructura, operación y seguridad definidas para el proyecto, por lo cual no se habilitan modalidades de despliegue basadas exclusivamente en componentes virtuales o software sobre infraestructura no provista por el fabricante. Por lo tanto, se mantiene el requisito.

OBSERVACIÓN No. 17

Observación No. 17 – Incorporación de sensores adicionales sin costo

Ubicación del requerimiento:

Numeral 1.2 – Alcance técnico, literal a, y Anexo 10 – Requerimientos técnicos, ítem 4, donde se indica que la solución debe permitir la incorporación de nuevos sensores físicos o virtuales sin generar costos adicionales para la Universidad.

Observación:
Se solicita amablemente a la Entidad aclarar el alcance de la expresión "sin que ello genere costos adicionales", toda vez que la incorporación futura de nuevos sensores puede requerir licenciamiento, capacidad de procesamiento, almacenamiento, interfaces, hardware o servicios adicionales, dependiendo del crecimiento real de la infraestructura y del modelo de licenciamiento del fabricante.

Solicitud:
Se solicita amablemente a la Entidad ajustar el requerimiento así:
"La solución deberá permitir la incorporación futura de nuevos sensores físicos o virtuales, de acuerdo con la arquitectura y capacidades ofertadas. La incorporación de sensores adicionales no deberá requerir el reemplazo total de la solución y podrá realizarse mediante ampliación de licenciamiento, capacidad, hardware o componentes adicionales cuando el crecimiento supere el dimensionamiento inicialmente contratado."

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. La incorporación de nuevos sensores podrá realizarse sobre la infraestructura tecnológica de la Universidad, sin generar costos adicionales, siempre y cuando se encuentren dentro de las capacidades y condiciones de la solución adquirida.

OBSERVACIÓN No. 18

Observación No. 18 – Integración con Kaspersky EDR mediante mecanismos estándar
Ubicación del requerimiento:

Numeral 1.2 – Alcance técnico, literal d, Integración, donde se solicita integración con EDR de Kaspersky versión 12.11 y agente 16.1 para correlación de eventos y ejecución de acciones de respuesta en endpoints.

Observación:

Se solicita amablemente a la Entidad permitir que la integración con la solución EDR existente pueda realizarse mediante mecanismos estándar de interoperabilidad, tales como API, syslog, conectores soportados, intercambio de indicadores de compromiso, integración con SIEM, integración con SOAR o mecanismos equivalentes.

Exigir una integración directa, nativa o propietaria con una marca específica puede restringir la pluralidad de oferentes y limitar la participación de fabricantes que cuentan con capacidades NDR, sandboxing, inteligencia de amenazas, correlación y automatización, pero que interoperan mediante estándares abiertos o mecanismos de integración soportados.

Solicitud:
Se solicita amablemente a la Entidad ajustar el requerimiento así:

"La solución deberá integrarse o interoperar con la solución EDR existente en la Universidad, actualmente Kaspersky, mediante mecanismos estándar de la industria tales como API, syslog, conectores soportados, intercambio de indicadores de compromiso, integración con SIEM, integración con SOAR o mecanismos equivalentes, permitiendo la correlación de eventos y acciones de respuesta asistidas o automatizadas, conforme a las capacidades técnicas disponibles de las plataformas involucradas."

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. La Universidad ha definido la necesidad de integración con la solución EDR existente (Kaspersky), con el fin de permitir la correlación de eventos y la ejecución de acciones de respuesta sobre endpoints.

La integración podrá realizarse mediante mecanismos estándar de la industria o aquellos soportados por las dos soluciones, tales como API, syslog, conectores o intercambio de indicadores de compromiso, siempre que se garantice la interoperabilidad funcional requerida en el pliego.

Esto se indica en las especificaciones técnicas, numeral 4. Requerimientos técnicos mínimos obligatorios

OBSERVACIÓN No. 19

Observación No. 19 – Integración con Palo Alto y SolarWinds mediante API, Syslog o mecanismos equivalentes

Ubicación del requerimiento:

Numeral 1.2 – Alcance técnico, literal d, Integración, donde se solicita integración con Palo Alto Networks NGFW 3420 para bloqueo automático de IPs maliciosas, integración con Kaspersky EDR e integración con SolarWinds SEM para correlación de eventos.

Observación:

Se solicita amablemente a la Entidad aclarar que las integraciones con Palo Alto Networks, Kaspersky y SolarWinds SEM podrán realizarse mediante mecanismos estándar o equivalentes, tales como API, syslog, CEF, LEEF, conectores soportados, listas dinámicas, intercambio de indicadores, integración con SIEM/SOAR, scripts de automatización o mecanismos certificados por el fabricante.
Esto permite mantener el objetivo funcional de la Entidad, sin restringir la participación a soluciones con conectores nativos específicos para cada marca.

Solicitud:

Se solicita amablemente a la Entidad ajustar el requerimiento así:

"La integración con las herramientas de seguridad y monitoreo existentes en la Universidad, incluyendo Palo Alto Networks NGFW 3420, Kaspersky EDR y SolarWinds Security Event Manager, podrá realizarse mediante API, syslog, CEF, LEEF, conectores soportados, listas dinámicas, integración SIEM/SOAR, intercambio de indicadores de compromiso, scripts de automatización o mecanismos equivalentes que permitan la correlación de eventos, generación de alertas y ejecución de acciones de respuesta asistidas o automatizadas."

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. En el alcance técnico se define la necesidad de integración con las herramientas de seguridad y monitoreo existentes, incluyendo Palo Alto Networks NGFW 3420, Kaspersky EDR y SolarWinds Security Event Manager, con el fin de habilitar capacidades de correlación de eventos, generación de alertas y ejecución de acciones de respuesta.

Las integraciones podrán realizarse mediante mecanismos estándar de la industria o equivalentes soportados por las plataformas involucradas, tales como API, syslog, CEF, LEEF, conectores soportados o intercambio de indicadores de compromiso, siempre que se garantice la funcionalidad requerida en el pliego, incluyendo la capacidad de respuesta asistida o automatizada.
Esto se indica en las especificaciones técnicas, numeral 4. Requerimientos técnicos mínimos obligatorios

OBSERVACIÓN No. 20

Observación No. 20 – Consola única o integración con consola central / SIEM

Ubicación del requerimiento:

Anexo 10 – Requerimientos técnicos, ítem 48, donde se indica que la gestión y visualización de la información recolectada deberá realizarse desde una consola centralizada que permita monitoreo, análisis, detección y respuesta desde una única interfaz.

Observación:

Se solicita amablemente a la Entidad permitir que la gestión, visualización y correlación se realice desde la consola centralizada de la solución NDR, desde una plataforma de administración del fabricante o mediante integración con el SIEM institucional, siempre que se garantice la consulta, trazabilidad, correlación y seguimiento de eventos.
Lo anterior teniendo en cuenta que el objeto contractual está orientado a fortalecer las capacidades de detección y respuesta a nivel de red, sin constituir una solución EDR independiente.

Solicitud:
Se solicita amablemente a la Entidad ajustar el requerimiento así:

"La gestión y visualización de la información recolectada podrá realizarse desde la consola centralizada de la solución NDR, desde una plataforma de administración del fabricante o mediante integración con el SIEM institucional, siempre que se permita la consulta, correlación, análisis, trazabilidad y seguimiento de eventos, alertas e indicadores de compromiso relacionados con la infraestructura monitoreada."

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. El ítem 48 establece que la gestión y visualización de la información recolectada deberá realizarse desde una consola centralizada de la solución NDR, la cual permita monitoreo, análisis, detección y respuesta desde una única interfaz.

Lo anterior no excluye la posibilidad de integración con el SIEM institucional para fines de correlación y análisis complementario, sin que este sustituya la consola central de operación de la solución.

OBSERVACIÓN No. 21

Observación No. 21 – Visibilidad de 400 endpoints mediante integración o telemetría equivalente

Ubicación del requerimiento:

Numeral 1.2 – Alcance técnico, literal b, donde se solicitan capacidades de visibilidad, monitoreo y correlación para cuatrocientos (400) endpoints; y Anexo 10, ítems 48, 49 y 50, donde se solicitan mecanismos de visibilidad, bajo impacto, despliegue selectivo hasta 400 equipos e integración con la plataforma central sin generar conflicto con antivirus o EDR existentes.

Observación:

Se solicita amablemente a la Entidad permitir que la visibilidad extendida sobre endpoints pueda ser cubierta mediante agentes ligeros, sensores, integración con el EDR existente, integración con SIEM, API, syslog, telemetría de red, logs, conectores soportados u otros mecanismos equivalentes.
Esto permitiría garantizar la convivencia operativa con las soluciones actualmente instaladas y evitar conflictos por la instalación obligatoria de agentes adicionales.

Solicitud:

Se solicita amablemente a la Entidad ajustar el requerimiento así:

"La solución deberá permitir ampliar las capacidades de visibilidad y correlación sobre hasta cuatrocientos (400) endpoints estratégicos mediante agentes, sensores ligeros, telemetría de red, integración con la solución EDR existente, integración con SIEM, API, syslog, conectores soportados, logs u otros mecanismos equivalentes, siempre que no se genere conflicto operativo con las soluciones de seguridad existentes."

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. Los ítems 48, 49 y 50 no exigen el uso obligatorio de agentes instalados en los equipos de cómputo, sino que permite ampliar las capacidades de visibilidad y correlación mediante agentes, sensores ligeros, telemetría de red u otros mecanismos soportados por el fabricante, es decir, la solución podrá emplear los mecanismos de integración que soporte el fabricante, siempre que cumpla con las capacidades funcionales requeridas y no genere conflictos con las soluciones de seguridad existentes.

OBSERVACIÓN No. 22

Observación No. 22 – Capacidad mínima de 6 Gbps

Ubicación del requerimiento:

Anexo 10 – Requerimientos técnicos, ítem 19, donde se solicita que cada Centro de Análisis soporte el procesamiento del volumen de tráfico de la red institucional, incluyendo enlaces troncales de mínimo 6 Gbps o superior, sin degradación del análisis ni pérdida de visibilidad.

Observación:

Se solicita amablemente a la Entidad aclarar si la capacidad mínima de 6 Gbps corresponde al tráfico agregado monitoreado, tráfico pico, throughput efectivo inspeccionado, capacidad de interfaz o tráfico espejo recibido por los sensores.
En soluciones NDR, el dimensionamiento depende del tráfico real a monitorear, cantidad de sensores, protocolos, objetos extraídos, retención, analítica aplicada y arquitectura propuesta por el fabricante.

Solicitud:

Se solicita amablemente a la Entidad ajustar el requerimiento así:
"La solución deberá ser dimensionada para soportar el volumen de tráfico espejo o monitoreado requerido por la Universidad, tomando como referencia una capacidad mínima agregada de hasta 6 Gbps o superior, de acuerdo con el diseño arquitectónico propuesto por el oferente. Dicha capacidad podrá ser alcanzada mediante uno o varios sensores, appliances, nodos de análisis o componentes equivalentes, sin pérdida de visibilidad sobre los segmentos definidos."

RESPUESTA DE LA UNIVERSIDAD: Se aclara que el ítem 19 se ajusta estableciendo una capacidad mínima de 4 Gbps. Esta capacidad corresponde al volumen de tráfico que la solución debe ser capaz de procesar y analizar en el Centro de Análisis, sin degradación del análisis ni pérdida de visibilidad.

El dimensionamiento de la solución, incluyendo la cantidad de sensores, nodos, appliances o componentes requeridos para cumplir dicho procesamiento, hará parte de la arquitectura propuesta por el oferente, siempre que garantice el cumplimiento de los requerimientos establecidos por la Universidad.

OBSERVACIÓN No. 23

Observación No. 23 – Sandboxing nativo, integrado o mediante componente adicional

Ubicación del requerimiento:

Anexo 10 – Requerimientos técnicos, ítems 65 al 76, donde se solicitan capacidades de análisis dinámico o sandboxing, análisis de artefactos

sospechosos, integración con agentes o EDR, resultados detallados, análisis de archivos protegidos por contraseña, análisis de objetos identificados en tráfico de red y enriquecimiento de procesos de correlación.

Observación:
Se solicita amablemente a la Entidad aclarar que las capacidades de sandboxing o análisis avanzado podrán ser prestadas de forma nativa, mediante componente adicional del mismo fabricante, appliance físico, appliance virtual, integración ICAP, API u otro mecanismo equivalente soportado por el fabricante.

Solicitud:
Se solicita amablemente a la Entidad ajustar el requerimiento así:
"El análisis de archivos u objetos sospechosos podrá realizarse mediante sandboxing nativo de la solución, componente adicional del mismo fabricante, appliance dedicado, appliance virtual, integración ICAP, API u otro mecanismo equivalente soportado por el fabricante, siempre que se garantice el análisis dinámico, generación de veredictos, enriquecimiento de alertas y trazabilidad de los resultados."

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. Los ítems del 65 al 76 no establecen un mecanismo específico para la implementación de las capacidades de análisis avanzado o sandboxing. Por lo tanto, dichas capacidades podrán ser prestadas de forma nativa, mediante integraciones, componentes o mecanismos soportados por el fabricante, siempre que se garantice el cumplimiento de las funcionalidades requeridas para el análisis dinámico, la generación de veredictos, el enriquecimiento de alertas y la trazabilidad de los resultados.

OBSERVACIÓN No. 24

Observación No. 24 – Captura de tráfico, PCAP, BPF y evidencia forense equivalente
Ubicación del requerimiento:

Anexo 10 – Requerimientos técnicos, ítems 100 al 105, donde se solicita capturar y registrar tráfico de red en bruto, formato PCAP, interfaz de descarga con filtros BPF y expresiones regulares, búsqueda de sesiones y exportación de tráfico para análisis posterior.

Observación:

Se solicita amablemente a la Entidad permitir que la capacidad forense pueda cumplirse mediante captura de paquetes asociada a eventos, descarga PCAP, metadatos de sesión, registros enriquecidos, objetos extraídos, evidencias de comunicación o mecanismos equivalentes que permitan soportar actividades de investigación y respuesta a incidentes.
La exigencia de registrar tráfico en bruto de forma amplia puede generar altos requerimientos de almacenamiento y puede limitar la participación de soluciones que realizan análisis forense mediante metadatos enriquecidos, sesiones, eventos y capturas asociadas a incidentes.

Solicitud:

Se solicita amablemente a la Entidad ajustar el requerimiento así:

"La solución deberá proporcionar capacidades de análisis forense mediante captura de paquetes, exportación PCAP asociada a eventos, metadatos de sesión, objetos extraídos, registros enriquecidos, evidencias de comunicación o mecanismos equivalentes que permitan soportar actividades de investigación, respuesta a incidentes y análisis posterior. La búsqueda y filtrado podrá realizarse mediante BPF, expresiones regulares, filtros de consola, consultas avanzadas o herramientas equivalentes soportadas por la solución."

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. La Universidad requiere que la solución cuente con capacidades de captura y registro del tráfico de red para soportar actividades de investigación forense y respuesta a incidentes.

Adicionalmente, durante el proceso de respuesta a observaciones fueron modificados los ítems 83 y 101, relacionados con la recuperación de evidencias, la exportación y el análisis del tráfico, permitiendo el uso de PCAP u otros mecanismos equivalentes soportados por el fabricante, así como mecanismos de filtrado y recuperación de información compatibles con la solución ofertada.

OBSERVACIÓN No. 25

Observación No. 25 – Reglas de detección en formatos abiertos, propietarios o equivalentes
Ubicación del requerimiento:

Anexo 10 – Requerimientos técnicos, ítem 51, donde se solicita la creación, ajuste e importación de reglas de detección utilizando formatos estructurados y estandarizados de uso común en la industria.

Observación:

Se solicita amablemente a la Entidad permitir que las reglas de detección puedan ser abiertas, estandarizadas, propietarias del fabricante o equivalentes, siempre que permitan adaptar la detección a las necesidades operativas de la Universidad.
Algunos fabricantes utilizan motores propietarios, inteligencia global de amenazas, machine learning, análisis de comportamiento y reglas propias que no necesariamente se exponen bajo formatos abiertos, pero que cumplen el objetivo funcional de detección y respuesta.

Solicitud:

Se solicita amablemente a la Entidad ajustar el requerimiento así:

"La solución deberá permitir la creación, ajuste, importación o administración de reglas de detección basadas en análisis de tráfico, comportamiento, anomalías, inteligencia de amenazas o motores propios del fabricante, utilizando formatos abiertos, estandarizados, propietarios o equivalentes, siempre que permitan adaptar la detección a las necesidades operativas de la Universidad."

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. El ítem 51 no impide que la solución incorpore motores de detección, inteligencia de amenazas o reglas propietarias del fabricante como capacidades complementarias, siempre que se dé cumplimiento al requisito establecido.

OBSERVACIÓN No. 26

Observación No. 26 – SFP+ Cisco o compatible certificado
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:

Se solicita amablemente a la Entidad permitir módulos SFP+ Cisco originales o compatibles certificados/homologados para infraestructura Cisco, siempre que el oferente garantice compatibilidad, operación, soporte y no afectación de la infraestructura existente.

Solicitud:

Se solicita amablemente a la Entidad ajustar el requerimiento así:
"Los módulos SFP+ deberán ser Cisco originales o compatibles certificados/homologados para operación con infraestructura Cisco, siempre que el oferente garantice compatibilidad, funcionamiento, soporte y no afectación de la operación de los equipos de red de la Universidad.

En caso de que la Universidad requiera preservar condiciones específicas de garantía del switch core, el oferente deberá suministrar los módulos originales o los que la supervisión apruebe técnicamente."

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. Las especificaciones técnicas del patch cord de fibra óptica corresponden a los elementos de conectividad requeridos para la integración de la solución con la infraestructura de red de la Universidad. El cumplimiento de estas características podrá ser verificado mediante la ficha técnica y/o documentación del fabricante del patch cord ofertado. Por tal razón, se mantienen el ítem 10 de la tabla de especificaciones técnicas mínimas, ya que, que son necesarias para garantizar la compatibilidad con la infraestructura de telecomunicaciones existente y las condiciones de soporte y garantía de los equipos de red de la Universidad.

OBSERVACIÓN No. 27

Observación No. 27 – Certificación del fabricante o canal autorizado
Ubicación del requerimiento:

Numeral 3.2.1 – Certificación del fabricante o canal autorizado, donde se solicita certificación expedida por el fabricante en la que conste que el oferente es distribuidor autorizado, está en capacidad de instalar, configurar, soportar, mantener y cumplir garantías en Colombia, en niveles superiores de certificación según la clasificación del fabricante.

Observación:

Se solicita amablemente a la Entidad ajustar el requisito para que no se limite exclusivamente a "niveles superiores", considerando que los programas de canal varían entre fabricantes y no todos utilizan la misma clasificación comercial o técnica.
Lo relevante para el proceso es que el oferente esté autorizado para comercializar, implementar y soportar la solución ofertada, y que cuente con respaldo del fabricante o mayorista autorizado.

Solicitud:

Se solicita amablemente a la Entidad ajustar el requerimiento así:

"El oferente deberá presentar certificación vigente expedida por el fabricante o mayorista autorizado, en la cual se acredite su condición de canal autorizado, partner oficial o integrador habilitado para comercializar, implementar y soportar la solución ofertada en Colombia. En caso de que el fabricante cuente con niveles de especialización, se aceptará el nivel que habilite formalmente al oferente para suministrar, implementar y soportar la solución objeto del proceso."

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. La Universidad mantiene el requisito de que el oferente cuente con niveles superiores de certificación, de acuerdo con la clasificación establecida por el fabricante, con el fin de garantizar que dispone de las capacidades técnicas, el respaldo y la experiencia necesarios para la implementación, configuración, soporte, mantenimiento y atención de garantías de la solución ofertada.

OBSERVACIÓN No. 28

Observación No. 28 – Reconocimiento de analistas en categorías equivalentes

Ubicación del requerimiento:

Numeral 5 – Certificaciones técnicas solicitadas, donde se solicita que el fabricante haya sido reconocido dentro de los últimos tres años en informes de analistas de industria como Gartner Magic Quadrant, Forrester Wave, ISG Provider Lens, SPARK Matrix, Radicati Market Quadrant u otros estudios equivalentes.

Observación:
Se solicita amablemente a la Entidad aclarar que el reconocimiento podrá corresponder al fabricante o a la familia de soluciones ofertadas en categorías relacionadas con NDR, XDR, protección de endpoint, seguridad de red, análisis avanzado de amenazas, sandboxing, threat intelligence o categorías equivalentes.
Esto permite mayor pluralidad y evita que el requisito se interprete de forma restrictiva frente a una única categoría de análisis.

Solicitud:

Se solicita amablemente a la Entidad adicionar la siguiente aclaración:
"Se aceptarán reconocimientos del fabricante o de la familia de soluciones ofertadas en estudios de analistas de industria relacionados con Network Detection and Response, Extended Detection and Response, Endpoint Protection, Threat Intelligence, Network Security, Advanced Threat Protection, Sandboxing, Email Security o categorías equivalentes, siempre que guarden relación funcional con el objeto del proceso."

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. El requisito tiene como finalidad acreditar el reconocimiento del fabricante mediante informes elaborados por analistas de la industria reconocidos, sin restringirse a un único estudio o entidad evaluadora. Adicionalmente, se verificará que dicho reconocimiento tenga relación con el objeto del presente proceso. Por lo anterior, no se considera necesario incorporar un listado adicional de categorías.

OBSERVACIÓN No. 29

Observación No. 29 – Retención mínima de 90 días
Ubicación del requerimiento:

Numeral 1.2 – Alcance técnico, literal a, y Anexo 10 – Requerimientos técnicos, ítem 6, donde se solicita almacenamiento y consulta de eventos, alertas, registros y telemetría histórica por un periodo mínimo de noventa (90) días.

Observación:

Se solicita amablemente a la Entidad aclarar que la retención mínima de noventa (90) días aplica sobre eventos, alertas, registros, metadatos y telemetría generada por la solución, de acuerdo con la arquitectura y el dimensionamiento ofertado, y no necesariamente sobre la totalidad del tráfico en bruto capturado.

Solicitud:

Se solicita amablemente a la Entidad ajustar el requerimiento así:

"La solución deberá permitir el almacenamiento y consulta de eventos, alertas, registros, metadatos y telemetría histórica por un periodo mínimo de noventa (90) días, conforme a la arquitectura ofertada. En caso de captura de paquetes o tráfico en bruto, su retención dependerá del dimensionamiento de almacenamiento contratado y de las políticas de captura configuradas por la Universidad."

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. El periodo mínimo de noventa (90) días aplica al almacenamiento y consulta de eventos, alertas, registros y telemetría histórica generada por la solución, conforme a la arquitectura ofertada. El requisito no establece que dicho periodo de retención deba aplicarse a la totalidad del tráfico en bruto capturado.

OBSERVACIONES REALIZADAS POR LA EMPRESA GLOBALTEK SECURITY SAS PEDRO JESUS MUÑOZ PULIDO REPRESENTANTE LEGAL

OBSERVACIÓN No. 1

Observación 1:

Se solicita a la Universidad Distrital confirmar si, en caso de requerirse el despliegue de un agente ligero del fabricante de la solución ofertada para cumplir con el envío de telemetría y metadatos, la Universidad facilitará las políticas de exclusión mutua (tanto en la consola de Kaspersky como en la consola de la solución adjudicada) durante la fase de implementación para garantizar la coexistencia operativa y evitar impactos en el rendimiento de los dispositivos.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. En caso de que la solución ofertada requiera el despliegue de agentes ligeros u otros mecanismos sobre los endpoints de la Universidad, esta facilitará las actividades de implementación que sean necesarias, incluyendo la definición de políticas de exclusión con las soluciones de seguridad existentes (como antivirus o firewall), siempre que dichas exclusiones sean técnicamente necesarias, no generen brechas de seguridad y sean previamente validadas de manera conjunta entre la Universidad y el contratista.

OBSERVACIÓN No. 2

Observación 2:

Teniendo en cuenta que Kaspersky Next EDR Optimum ejecuta sus acciones de aislamiento y contención de manera nativa mediante su propia consola de administración, se solicita a la entidad confirmar si la "integración para la ejecución de acciones de respuesta" solicitada se considerará cumplida mediante el envío/recepción de alertas cruzadas vía mecanismos estándar (como APIs del fabricante o reenvío de eventos Syslog/SIEM estructurados), permitiendo que la plataforma de red notifique al entorno institucional para detonar la respuesta de manera orquestada.

RESPUESTA DE LA UNIVERSIDAD: No se acepta la observación. El requisito de integración se considerará cumplido siempre que la solución permita el intercambio de información con las herramientas de seguridad existentes en la Universidad mediante APIs, conectores, Syslog u otros mecanismos soportados por el fabricante, facilitando la correlación de eventos y la ejecución de acciones de respuesta entre las plataformas integradas.

OBSERVACIONES REALIZADAS POR LA EMPRESA GROWTH – VALUE SALES LAURA CAROLINA NIÑO VARGAS CUSTOMER VALUE EXECUTIVE

OBSERVACIONES

No.	*Numeral*	*Texto Observado*	*Observación/Solicitud*	RESPUESTA DE LA UNIVERSIDAD
1	*1,5*	*Registro de proveedores de la Universidad.*	*Se solicita aclarar si la inscripción en el registro de proveedores constituye un requisito habilitante para presentar oferta o si podrá realizarse únicamente por el proponente adjudicatario antes de la suscripción del contrato.*	Se acepta observación. Se modifica el ítem E de las "CONDICIONES GENERALES" de los estudios previos, el cual queda de la siguiente manera "*Para la suscripción del contrato, el oferente ganador deberá estar inscrito en el Sistema Único de Registro de Personas y Banco de Proveedores AGORA de la Universidad Distrital* (…)"
2	*1,5*	*Referencia al Decreto 338 de 2022 sobre Seguridad Digital.*	*Se solicita precisar cuáles de los lineamientos del Decreto 338 de 2022 serán objeto de verificación durante la ejecución contractual y qué entregables deberán evidenciar su cumplimiento.*	No se acepta la observación. La referencia al Decreto 338 de 2022 corresponde al marco normativo aplicable en materia de seguridad digital y orienta los requerimientos establecidos en el presente proceso. Su cumplimiento se verificará mediante el cumplimiento de las especificaciones técnicas, las obligaciones contractuales y los entregables definidos en el pliego de condiciones y sus anexos. Por lo anterior, no se considera necesario establecer lineamientos o

No.	Numeral	Texto Observado	Observación/Solicitud	RESPUESTA DE LA UNIVERSIDAD
				entregables adicionales asociados específicamente al citado decreto.
3	*1,6*	*Riesgo No. 2: "Deficiencias en las especificaciones técnicas de los estudios previos o en sus anexos".*	*Se solicita realizar una revisión integral de las especificaciones técnicas antes de la publicación del pliego definitivo, garantizando que los requerimientos sean claros, medibles y no generen interpretaciones ambiguas durante la evaluación.*	No se acepta la observación. La Universidad realizó la revisión de las especificaciones técnicas durante la elaboración de los estudios previos y continuará efectuando los ajustes que considere pertinentes como resultado del análisis de las observaciones recibidas, con el fin de garantizar la claridad, coherencia y adecuada definición de los requerimientos del proceso.
4	*1,6*	*Riesgo No. 3: Deficiencia en la prestación del servicio.*	*Se solicita definir indicadores objetivos de aceptación del servicio (ANS, criterios de calidad y mecanismos de validación), con el fin de establecer parámetros verificables para el supervisor del contrato.*	No se acepta la observación. La Universidad precisa que el objeto del presente proceso corresponde a un contrato de compraventa que comprende el suministro, instalación, configuración, puesta en funcionamiento y demás actividades requeridas para la implementación de una solución de ciberseguridad, y no a la prestación de un servicio continuo administrado sujeto a Acuerdos de Niveles de Servicio (ANS). En consecuencia, la aceptación de los bienes y servicios objeto del contrato se realizará con base en el cumplimiento de las especificaciones técnicas, los requisitos funcionales, los entregables definidos en el pliego de condiciones y la verificación de su correcta instalación, configuración, integración, pruebas de funcionamiento y puesta en operación, según corresponda.
5	*1,6*	*Riesgo No. 5: Mala calidad o deficiencias del servicio.*	*Se solicita precisar cuáles serán los criterios técnicos mediante los cuales la Entidad determinará que un servicio presenta deficiencias, evitando apreciaciones subjetivas durante la supervisión contractual.*	No se acepta la observación. La aceptación de los bienes y servicios objeto del contrato se realizará con base en el cumplimiento de las especificaciones técnicas, los requisitos funcionales, los entregables definidos en el pliego de condiciones y la verificación de su correcta instalación, configuración, integración, pruebas de funcionamiento y puesta en operación, según corresponda.
6	*1,6*	*Riesgo No. 7: Retrasos en los pagos por demoras en la entrega de documentos.*	*Se solicita relacionar expresamente el listado de documentos requeridos para cada pago y establecer un plazo máximo para la revisión y aprobación por parte de la Entidad.*	No se acepta la observación. Los documentos requeridos para cada pago están establecidos en el ítem 12.1 FORMA DE PAGO. En cuanto a la solicitud de establecer un plazo máximo para la revisión y aprobación de la documentación presentada, la Universidad realizará dicho trámite conforme a sus procedimientos internos y dentro de los términos previstos en la normatividad aplicable y en las condiciones contractuales, una vez el contratista haya radicado la totalidad de la documentación requerida de manera completa y correcta.
7	*1,6*	*Riesgo No. 8: Errores en la planeación del contrato.*	*Se solicita aclarar el procedimiento que adoptará la Universidad en caso de identificarse durante la ejecución que el*	No se acepta la observación. El alcance, el plazo de ejecución y el presupuesto oficial fueron determinados con fundamento en el análisis técnico realizado por la Universidad, considerando las actividades requeridas,

No.	Numeral	Texto Observado	Observación/Solicitud	RESPUESTA DE LA UNIVERSIDAD
			alcance, plazo o presupuesto inicialmente definidos resultan insuficientes para el cumplimiento del objeto contractual.	las condiciones de ejecución y los recursos necesarios para garantizar el cumplimiento del objeto contractual. En consecuencia, la Entidad considera que estos son suficientes para atender la necesidad que dio origen al presente proceso de contratación. Cualquier situación que eventualmente pueda presentarse durante la ejecución contractual será analizada por la Entidad conforme a las circunstancias particulares del caso y en el marco de la normativa aplicable, sin que resulte procedente establecer de manera anticipada un procedimiento específico para escenarios hipotéticos.
8	*1.12*	*CRONOGRAMA DE LA CONVOCATORIA PÚBLICA No. 007 - 2026*	*Respetuosamente se solicita otorgar una prórroga de por lo menos cinco (5) días hábiles para la presentación de la oferta, con el fin de contar con el tiempo prudencial necesario para estructurar de manera adecuada la propuesta técnica y económica, especialmente en lo relacionado con la definición y validación de los precios. Lo anterior permitirá presentar una oferta integral, competitiva y alineada con los requerimientos del proceso.*	No se acepta la observación. La Universidad considera que el cronograma establecido para el presente proceso otorga un plazo suficiente para la preparación y presentación de las ofertas.

RESPUESTA DE LA UNIVERSIDAD: Cada observación de la tabla se responde en la columna "RESPUESTA DE LA UNIVERSIDAD"

COMITÉ ASESOR DE CONTRATACIÓN