Bogotá D.C., 26 de agosto de 2026

UDNET-202-2026

Doctora
IVETTE CATALINA MARTÍNEZ MARTÍNEZ
Vicerrectora Administrativa y Financiera
Universidad Distrital
Presente –

REF: Evaluación técnica final convocatoria pública 007-2026

Respetada doctora Ivette:

Atentamente se remite la evaluación técnica final de las propuestas recibidas en el marco de la convocatoria pública 007-2026 cuyo objeto es: "*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",* como resultado se presenta el siguiente resumen:

1. CONSOLIDADO DE EVALUACIÓN TÉCNICA

ÍTEM	PROPONENTE	EVALUACIÓN TÉCNICA
1	UNIÓN TEMPORAL INFOCOMUNICACIONES S.A.S - SOLUCIONES EN SEGURIDAD INFORMÁTICA S.A.S	No habilitada
2	SONDA DE COLOMBIA S.A.	No habilitada
3	COINSA S.A.S.	Habilitada
4	GRUPO MICROSISTEMAS COLOMBIA S.A.S.	No habilitada
5	HEIMCORE	No habilitada

La única empresa habilitada técnicamente es "COINSA S.A.S.", a continuación, se presenta la verificación de los requisitos habilitantes de la misma:

ÍTEM	DESCRIPCIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE
1	El oferente deberá dimensionar los equipos para el nodo central (Calle 40) y el sensor o colector de tráfico (Bosa Porvenir) garantizando que soporten la totalidad de la solución. Para la validación de	Hardware ofertado: Lenovo ThinkSystem SR650 V4. Links oficiales del fabricante:	CUMPLE

ÍTEM	DESCRIPCIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE
	este ítem se revisará la ficha técnica del hardware y software enviada por el oferente.	https://support.kaspersky.com/kata/7.1/247120 https://support.kaspersky.com/kata/7.1/247448 https://lenovopress.lenovo.com/lp2127-thinksystem-sr650-v4-server , Anexo Datasheet ds0194_ES Lenovo ThinkSystem Datasheet.pdf	
2	La solución deberá contemplar los componentes físicos necesarios para su correcta implementación, operación, monitoreo y administración bajo arquitectura On-Premise.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/194604 https://support.kaspersky.com/kata/7.1/247120 https://lenovopress.lenovo.com/lp2127-thinksystem-sr650-v4-server Anexo Datasheet ds0194_ES Lenovo ThinkSystem Datasheet.pdf	CUMPLE
3	La solución deberá incluir los componentes físicos necesarios para la implementación de un nodo central de administración, análisis y correlación de eventos, el cual deberá ser instalado en la sede Calle 40 y un sensor o colector de tráfico en la sede Bosa Porvenir	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247494 https://support.kaspersky.com/kata/7.1/247493 https://lenovopress.lenovo.com/lp2127-thinksystem-sr650-v4-server	CUMPLE
4	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 a la Universidad.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247493 https://support.kaspersky.com/kata/7.1/247179	CUMPLE
5	La solución deberá permitir escalabilidad para la incorporación futura de nuevos sensores, colectores o capacidades de procesamiento sin requerir el reemplazo total de la solución.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247179 https://support.kaspersky.com/kata/7.1/247448	CUMPLE
6	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.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/329325 https://support.kaspersky.com/kata/7.1/300871 Anexo Sizing (Dimensionamiento servers) .pdf	CUMPLE

ÍTEM	DESCRIPCIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE
7	Los componentes físicos suministrados deberán incluir los accesorios, interfaces, módulos, cableados y demás elementos necesarios para su correcta instalación y puesta en funcionamiento.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/242456 https://support.kaspersky.com/kata/7.1/266033	CUMPLE
8	La solución deberá soportar mecanismos de captura de tráfico mediante SPAN, port mirroring o tecnologías equivalentes compatibles con la infraestructura institucional.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/242456 https://support.kaspersky.com/kata/7.1/266033	CUMPLE
9	La arquitectura propuesta deberá permitir la integración y comunicación segura entre el nodo central y los sensores o colectores desplegados.	Links oficiales delfabricante:https://support.kaspersky.com/kata/7.1/252062https://support.kaspersky.com/kata/7.1/194604	CUMPLE
10	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	Se anexa Datasheet Ofical del fabircante: DSLPF13L10L1081L3M DataSheet Patch Cord.pdf Se anexa Certificacion de fabrica por 25 años CERTIFICACION LANPRO COMPANIA DE INGENIEROS DE SISTEMAS ASOCIADOS - COINSA SAS.pdf	CUMPLE

ÍTEM	DESCRIPCIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE
	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.		
11	Especificaciones técnicas - SFP + • Fabricante: Cisco – Se solicita de este fabricante teniendo en cuenta que el Switch Core es de esta marca y uno diferente podría traer complicaciones en la garantía del Switch Core. • Formato: SFP-10G-SR • Velocidad: 10 Gbps • Tipo de enlace: Ethernet 10 Gigabit (10GBASE-SR) • Fibra: Multimodo (MMF) • Conector: LC dúplex • Longitud de onda: 850 nm • Alcance típico: Hasta 400 m (OM4)	Referencia: Cisco SFP-10G-SR. Links oficiales del fabricante: https://www.cisco.com/c/en/us/products/collateral/interfacesmodules/transceivermodules/data_sheet_c78-455693.html Se anaxa datasheet data_sheet_c78-455693 SFP-10G-SR.pdf	CUMPLE
12	La solución deberá ser ofertada en su versión estable y soportada oficialmente por el fabricante al momento de la presentación de la oferta, incluyendo acceso a actualizaciones, parches y mejoras durante la vigencia del licenciamiento. Se debe presentar una certificación en donde se compruebe de lo solicitado.	Se Adjunta también la carta de fábrica: Kaspersky Representative Letter_EOS_EOL_Universidad Distrital.pdf (10/08/2026). Certificación: Kaspersky Representative Letter_EOS_EOL_Universidad Distrital.pdf, 10/08/2026. Links oficiales del fabricante: https://support.kaspersky.com/corporate/lifecycle?type=limited,full&program=kata&version=7.1&id=kata-7.1 https://support.kaspersky.com/kata/7.1	CUMPLE
13	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,	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/194604	CUMPLE

ÍTEM	DESCRIPCIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE
	conforme a las políticas institucionales de seguridad de la información.	https://support.kaspersky.com/kata/7.1/247461	
14	La solución deberá soportar el crecimiento progresivo de activos monitoreados dentro de la infraestructura institucional, garantizando capacidades de procesamiento, análisis y correlación acordes con las necesidades de la Universidad.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247448 https://support.kaspersky.com/kata/7.1/247179	CUMPLE
15	La solución deberá ser compatible con entornos tecnológicos que incluyan sistemas operativos Windows, Linux y MacOS, permitiendo capacidades de visibilidad, monitoreo, análisis o correlación sobre dichos entornos mediante los mecanismos soportados por la solución ofertada.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/246849 https://support.kaspersky.com/kata/7.1/247128	CUMPLE
16	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.	Links oficiales delfabricante:https://support.kaspersky.com/kata/7.1/194604https://support.kaspersky.com/kata/7.1/247325	CUMPLE
17	La solución debe contar con capacidades centralizadas de investigación y correlación de eventos que permitan analizar la telemetría de red y la información asociada a los activos monitoreados por la solución, incluyendo el análisis del tráfico de red relacionado con protocolos de correo electrónico cuando este sea visible a nivel de red.	fabricante: https://support.kaspersky.com/kata/7.1/247494 https://support.kaspersky.com/kata/7.1/247636	CUMPLE
18	La solución debe permitir la centralización lógica del análisis de información, garantizando una visión consolidada de eventos y alertas, pudiendo desplegar sus componentes en uno o varios nodos según el diseño arquitectónico propuesto por el fabricante.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247494 https://support.kaspersky.com/kata/7.1/247179	CUMPLE
19	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.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/211923 https://support.kaspersky.com/kata/7.1/328197	CUMPLE
20	La solución deberá permitir esquemas de alta disponibilidad (HA) para los componentes críticos	Hardware ofertado: Lenovo ThinkSystem SR650 V4.	CUMPLE

ÍTEM	DESCRIPCIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE
	de administración, análisis y procesamiento, incorporando mecanismos de redundancia, failover y continuidad operativa que minimicen la interrupción del servicio ante fallos de hardware o software.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247120 https://support.kaspersky.com/kata/7.1/247448 https://lenovopress.lenovo.com/lp2127-thinksystem-sr650-v4-server , Anexo Datasheet ds0194_ES Lenovo ThinkSystem Datasheet.pdf	
21	La solución debe incluir una interfaz web para que los administradores gestionen y analicen los datos del sistema, incluyendo el seguimiento de incidentes, la monitorización del rendimiento del sistema y la configuración de sistema.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1 https://support.kaspersky.com/kata/7.1/247507	CUMPLE
22	La solución debe soportar despliegues sobre entornos virtualizados VMware ESXi, HyperV, KVM o tecnologías de virtualización equivalentes, permitiendo la implementación futura de componentes adicionales de análisis, sensores o colectores en diferentes sedes o segmentos de red de la Universidad.	KATA 7.1 soporta KVM para Central Node y Sensor; Hipervisor soportador para la Solucion https://support.kaspersky.com/kata/7.1/247120?page=help Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247120 https://support.kaspersky.com/kata/7.1/303948	CUMPLE
23	La solución debe proporcionar notificaciones por correo electrónico a los administradores cuando los componentes del sistema experimenten problemas operativos, incluyendo baja capacidad de almacenamiento, para garantizar una atención y resolución rápidas.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247515 https://support.kaspersky.com/kata/7.1	CUMPLE
24	La solución deberá permitir la administración centralizada de políticas, eventos, tareas y reportes mediante una consola unificada de gestión.	fabricante:https://support.kaspersky.com/kata/7.1/247507https://support.kaspersky.com/kata/7.1/246747	CUMPLE
25	La solución debe soportar mecanismos controlados para la descarga de actualizaciones mediante conexión directa o a través de servidores proxy con autenticación.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1 https://support.kaspersky.com/kata/7.1/247577	CUMPLE
26	La solución deberá contar con un modelo de control de acceso basado en roles (RBAC), que	Links oficiales del fabricante:	CUMPLE

ÍTEM	DESCRIPCIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE
	permita: • La creación de roles personalizados. • La asignación granular de permisos por módulo, funcionalidad y alcance (por dominio o unidad organizacional). • La aplicación del principio de mínimo privilegio. • La delegación administrativa segmentada por unidades organizacionales. • La integración con servicios de directorio (LDAP/Active Directory). • El registro y auditoría de todas las acciones realizadas por los usuarios administradores. • La gestión centralizada de perfiles y políticas de acceso.	https://support.kaspersky.com/kata/7.1/247461 https://support.kaspersky.com/kata/7.1	
27	La solución debe utilizar un canal seguro para la comunicación entre la consola y el administrador. También debe permitir la importación del certificado digital utilizado para asegurar el canal de comunicación.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247521 https://support.kaspersky.com/kata/7.1/247571	CUMPLE
28	La solución debe soportar sincronización de tiempo con servidores NTP.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/273215 https://support.kaspersky.com/kata/7.1/247520	CUMPLE
29	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.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/271112	CUMPLE
30	La solución deberá registrar y auditar las acciones realizadas por los usuarios administradores sobre la plataforma, permitiendo su consulta y conservación para fines de trazabilidad y auditoría.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247576 https://support.kaspersky.com/kata/7.1/153523	CUMPLE
31	La solución debe soportar actualizaciones del Centro de Análisis preservando las configuraciones existentes, bases de datos de incidentes, políticas y demás información crítica de operación, sin requerir reinstalaciones completas desde cero y minimizando la interrupción del servicio.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1 https://support.kaspersky.com/kata/7.1/247577	CUMPLE
32	La solución debe integrarse con servicios de inteligencia de amenazas, ya sean en la nube o	Links oficiales del fabricante:	CUMPLE

ÍTEM	DESCRIPCIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE
	locales, proporcionados por el fabricante o por fuentes confiables de terceros, para realizar comprobaciones de reputación en tiempo real sobre indicadores de compromiso.	https://support.kaspersky.com/kata/7.1/247465 https://support.kaspersky.com/kata/7.1/247421	
33	La solución deberá permitir capacidades locales o híbridas de consulta y almacenamiento de información de inteligencia de amenazas, incluyendo reputación de indicadores de compromiso (IoC), hashes, URLs o dominios, con el fin de fortalecer las capacidades de análisis y correlación de eventos dentro de la infraestructura institucional.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247465 https://support.kaspersky.com/kata/7.1/247421	CUMPLE
34	La solución debe permitir el acceso a plataformas analíticas de inteligencia de amenazas que proporcionen contexto ampliado sobre indicadores, infraestructura asociada y relaciones entre objetos.	Links oficiales delfabricante:https://support.kaspersky.com/kata/7.1/247465https://support.kaspersky.com/kata/7.1/247421	CUMPLE
35	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.	Links oficiales del fabricante: https://support.kaspersky.com/KATA/7.1/KataAPI/PublicApi-v4.html https://support.kaspersky.com/KATA/7.1/en-US/227245.htm	CUMPLE
36	La solución deberá permitir integración con mecanismos estándar de inspección y análisis de contenido (por ejemplo, ICAP u otros métodos equivalentes como API o integración nativa con dispositivos de seguridad).	Links oficiales del fabricante: https://support.kaspersky.com/KATA/7.1/KataAPI/PublicApi-v4.html https://support.kaspersky.com/KATA/7.1/en-US/227245.htm	CUMPLE
37	La solución debe soportar el envío de alertas de ciberseguridad y la monitorización de información mediante syslog.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247568 https://support.kaspersky.com/kata/7.1/247573	CUMPLE
38	La solución deberá permitir mecanismos seguros de integración y segmentación entre componentes de la arquitectura, conforme a las políticas de seguridad institucional.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/194604 https://support.kaspersky.com/kata/7.1/252062	CUMPLE

ÍTEM	DESCRIPCIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE
39	La solución deberá contar con la capacidad de integrarse con plataformas SIEM y sistemas de gestión de registros.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247568 https://support.kaspersky.com/kata/7.1/153523	CUMPLE
40	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).	Links oficiales del fabricante: https://support.kaspersky.com/KATA/7.1/KataAPI/PublicApi-v4.html https://support.kaspersky.com/kata/7.1/247568 https://support.kaspersky.com/kata/7.1/207166	CUMPLE
41	La solución deberá proporcionar capacidades de análisis automatizado y generación de alertas en tiempos acordes con la operación y monitoreo continuo de la infraestructura institucional.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247494 https://support.kaspersky.com/kata/7.1/247636	CUMPLE
42	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.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247494 https://support.kaspersky.com/kata/7.1/247636	CUMPLE
43	La solución deberá permitir la generación de reportes personalizables basados en eventos, alertas, incidentes y demás información recopilada por la plataforma.	Links oficiales delfabricante:https://support.kaspersky.com/kata/7.1/247735	CUMPLE
44	La solución deberá permitir la configuración de notificaciones automáticas por correo electrónico ante la generación de alertas o eventos de seguridad, dirigidas a los administradores o responsables designados para la gestión y atención de incidentes.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/153523	CUMPLE
45	La solución deberá proporcionar capacidades de analítica, visualización y correlación de eventos orientadas a la identificación de amenazas internas y externas sobre la infraestructura monitoreada.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247494 https://support.kaspersky.com/kata/7.1/247636	CUMPLE
46	La solución debe tener la capacidad de crear informes ejecutivos diarios, semanales y mensuales y permitir la exportación de informes.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247735	CUMPLE

ÍTEM	DESCRIPCIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE
47	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.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247494 https://support.kaspersky.com/kata/7.1/247636	CUMPLE
48	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). La gestión y visualización de la información recolectada deberá realizarse desde una consola centralizada que permita capacidades de monitoreo, análisis, detección y respuesta desde una única interfaz.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/219777 https://support.kaspersky.com/kata/7.1/247325	CUMPLE
49	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	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247325 https://support.kaspersky.com/kata/7.1/219777	CUMPLE
50	Los mecanismos utilizados para la recolección de telemetría y visibilidad sobre los endpoints no deberán interferir ni generar conflictos con las soluciones de seguridad existentes en la infraestructura institucional, incluyendo antivirus, EDR u otras herramientas de protección de endpoints, garantizando la convivencia operativa sobre los equipos monitoreados.	Links oficiales delfabricante:https://support.kaspersky.com/kata/7.1/247325https://support.kaspersky.com/kata/7.1/219777	CUMPLE

ÍTEM	DESCRIPCIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE
51	La solución debe permitir la creación, ajuste e importación de reglas de detección basadas en el análisis de tráfico de red, comportamiento y anomalías, utilizando formatos estructurados y estandarizados de uso común en la industria, facilitando la interoperabilidad, reutilización y adaptación de reglas de detección existentes.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/137926 https://support.kaspersky.com/kata/7.1/247702	CUMPLE
52	La solución deberá permitir el análisis de archivos u objetos identificados dentro del tráfico de red mediante sandboxing, análisis dinámico u otros mecanismos equivalentes soportados por el fabricante permitiendo su inspección en entornos controlados para la detección de comportamientos maliciosos. Esta función debe permitir: • Identificación de archivos u objetos sospechosos a partir del análisis del tráfico de red. • Envío automatizado de dichos objetos al entorno de sandbox para su análisis. • Integración con mecanismos o motores de análisis avanzado para la detección de amenazas desconocidas. Generación de alertas y enriquecimiento de eventos a partir de los resultados del análisis avanzado realizado	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247495 https://support.kaspersky.com/kata/7.1/247475	CUMPLE
53	Los mecanismos de visibilidad utilizados sobre los endpoints deberán permitir la recolección de telemetría y contexto de seguridad desde los equipos monitoreados, con el fin de complementar las capacidades de visibilidad y correlación de la solución NDR.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247325 https://support.kaspersky.com/kata/7.1/219777	CUMPLE
54	La solución deberá proporcionar visibilidad sobre la propagación y relación de amenazas dentro de la infraestructura monitoreada, incluyendo correlación entre eventos de red, activos involucrados y endpoints donde se desplieguen mecanismos de visibilidad extendida.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/176734	CUMPLE
55	La solución deberá permitir la integración con fuentes externas de telemetría, con el fin de enriquecer la base de datos de eventos y permitir su consulta desde la consola de análisis.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/207166 https://support.kaspersky.com/KATA/7.1/KataAPI/PublicApi-v4.html	CUMPLE
56	La solución deberá permitir la búsqueda, consulta y correlación de indicadores de compromiso	Links oficiales del fabricante:	CUMPLE

ÍTEM	DESCRIPCIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE
	(IOC) sobre la telemetría centralizada recolectada, incluyendo información proveniente del tráfico de red y de los mecanismos de visibilidad extendida.	https://support.kaspersky.com/kata/7.1/247421 https://support.kaspersky.com/kata/7.1/247636	
57	La solución debe proporcionar una interfaz de búsqueda con funcionalidad avanzada que permita a los analistas realizar consultas sobre la telemetría y eventos recolectados.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247637 https://support.kaspersky.com/kata/7.1/247636	CUMPLE
58	La solución debe ser capaz de detectar comunicaciones sospechosas dentro del tráfico de red monitoreado, incluyendo conexiones hacia infraestructuras de comando y control (C&C).	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/137926 https://support.kaspersky.com/kata/7.1/247421	CUMPLE
59	Las alertas generadas deben enriquecerse automáticamente con información contextual relevante como descripciones, clasificación de amenazas y otros datos que faciliten el análisis.	Links oficiales delfabricante:https://support.kaspersky.com/kata/7.1/216715https://support.kaspersky.com/kata/7.1	CUMPLE
60	La solución deberá permitir el etiquetado de activos, equipos o segmentos de red, con el fin de facilitar la gestión y el análisis diferenciado.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/188133 https://support.kaspersky.com/kata/7.1/175616	CUMPLE
61	Las alertas y eventos generados deberán mapearse, cuando aplique, a tácticas, técnicas y procedimientos (TTP) de la matriz MITRE ATT&CK.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/249034	CUMPLE
62	La solución deberá permitir la gestión e incorporación de indicadores personalizados de compromiso (IOC) e indicadores de ataque (IOA), aplicables a los motores de análisis de red, sandbox y a las integraciones con otras herramientas de seguridad.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247421 https://support.kaspersky.com/kata/7.1/247702	CUMPLE
63	La solución propuesta debe contar con capacidades avanzadas de detección de amenazas, incluyendo la capacidad de identificar y alertar en: • Ataques Zero-Day: vulnerabilidades previamente desconocidas o no parcheadas. • Amenazas Persistentes Avanzadas (APT): ataques sofisticados y dirigidos por grupos estatales u organizados. Amenazas sofisticadas de red: incluyendo, pero	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247495 https://support.kaspersky.com/kata/7.1/247465	CUMPLE

ÍTEM	DESCRIPCIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE
	no limitándose a, malware, ransomware y otros tipos de actividades maliciosas que evaden los controles de seguridad tradicionales.		
64	La solución deberá contar con capacidades para la detección de malware avanzado, amenazas desconocidas y ataques de tipo zero-day, mediante técnicas de análisis avanzadas que permitan su identificación en tiempo cercano a real, incluso cuando no existan firmas previamente conocidas.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247495 https://support.kaspersky.com/kata/7.1/247465	CUMPLE
65	La solución deberá permitir capacidades de análisis dinámico o sandboxing sobre artefactos sospechosos identificados en el tráfico de red, utilizando entornos controlados compatibles con uno o varios sistemas operativos, ya sea de forma nativa o mediante integraciones soportadas por el fabricante.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247495 https://support.kaspersky.com/kata/7.1/159685	CUMPLE
66	La solución deberá permitir la recopilación y análisis de telemetría proveniente de sensores, agentes o mecanismos equivalentes, proporcionando información contextual sobre comportamientos sospechosos, indicadores de compromiso y posibles amenazas detectadas.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247493 https://support.kaspersky.com/kata/7.1/247325	CUMPLE
67	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.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247325 https://support.kaspersky.com/kata/7.1/219777	CUMPLE
68	La solución deberá proporcionar resultados detallados del análisis avanzado de amenazas o sandboxing, incluyendo información relacionada con procesos, comunicaciones de red, consultas DNS, comportamiento observado y demás indicadores relevantes que permitan a los analistas comprender las características y el impacto potencial de las amenazas detectadas.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/159685	CUMPLE
69	La solución deberá permitir que las capacidades de análisis avanzado o sandboxing puedan ser utilizadas por múltiples nodos, centros de análisis o componentes de la arquitectura, conforme al diseño propuesto por el fabricante.	Links oficiales delfabricante:https://support.kaspersky.com/kata/7.1/247475https://support.kaspersky.com/kata/7.1/247179	CUMPLE
70	La solución deberá permitir, cuando aplique, capacidades controladas y configurables de comunicación externa para enriquecer el análisis avanzado de amenazas, incluyendo la validación	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/159685	CUMPLE

ÍTEM	DESCRIPCIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE
	de comportamientos, reputación o descarga de componentes requeridos para el análisis.	https://support.kaspersky.com/kata/7.1	
71	La solución deberá permitir técnicas avanzadas de análisis dinámico orientadas a identificar comportamientos maliciosos asociados a ejecución controlada, interacción simulada o activación de comportamientos sospechosos durante el análisis de amenazas.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/159685 https://support.kaspersky.com/kata/7.1/247779	CUMPLE
72	La solución debe ser capaz de procesar y analizar archivos, incluidos archivos protegidos por contraseña y documentos de oficina, independientemente de su origen	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247580 https://support.kaspersky.com/kata/7.1/159685	CUMPLE
73	La solución deberá incorporar mecanismos orientados a mejorar la efectividad del análisis dinámico frente a amenazas que intenten detectar o evadir entornos de análisis automatizado.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247495 https://support.kaspersky.com/kata/7.1/159685	CUMPLE
74	La solución deberá proporcionar capacidades de análisis avanzado sobre objetos identificados en el tráfico de red, permitiendo obtener información relevante sobre su comportamiento, comunicaciones y posibles indicadores de compromiso.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247495 https://support.kaspersky.com/kata/7.1/150811	CUMPLE
75	La solución deberá permitir escalabilidad en las capacidades de análisis avanzado mediante mecanismos distribuidos o múltiples instancias de procesamiento, orientados a optimizar los tiempos de análisis y respuesta.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247180 https://support.kaspersky.com/kata/7.1/247179	CUMPLE
76	Los resultados obtenidos mediante las capacidades de análisis avanzado deberán poder enriquecer los procesos de correlación, reputación o detección utilizados por otras herramientas de seguridad integradas dentro de la infraestructura institucional.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247475 https://support.kaspersky.com/kata/7.1/247465	CUMPLE
77	La solución deberá permitir que múltiples componentes o nodos de análisis puedan utilizar capacidades centralizadas o compartidas de análisis avanzado de amenazas, conforme a la arquitectura propuesta por el fabricante.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247180 https://support.kaspersky.com/kata/7.1/247179	CUMPLE
78	La solución deberá proporcionar capacidades de análisis y visibilidad del tráfico de red,	Links oficiales del fabricante:	CUMPLE

ÍTEM	DESCRIPCIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE
	permitiendo como mínimo: • Visualización e inspección de eventos de tráfico de red en tiempo real. • Análisis de capturas de paquetes y/o flujos de red. • Identificación de amenazas, anomalías y comportamientos sospechosos en el tráfico monitoreado. Soporte a procesos de investigación y respuesta ante incidentes de seguridad.	https://support.kaspersky.com/kata/7.1/247507 https://support.kaspersky.com/kata/7.1/257980	
79	La solución deberá proporcionar recomendaciones de investigación, contención o remediación ante alertas de seguridad generadas por la plataforma, con el fin de apoyar a los administradores en la investigación y remediación de incidentes.	Links oficiales delfabricante:https://support.kaspersky.com/help/KATA/7.1/en-US/196721.htm	CUMPLE
80	La solución debe ser capaz de recibir entradas para indicadores personalizados de compromiso (IOC) e indicadores de ataque (IOA) para clasificar y analizar eventos.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247421 https://support.kaspersky.com/kata/7.1/247702	CUMPLE
81	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.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247702 https://support.kaspersky.com/kata/7.1/247424	CUMPLE
82	La solución deberá permitir habilitar, deshabilitar, ajustar o excluir reglas de detección de red, conforme a las necesidades operativas de la Universidad.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247774 https://support.kaspersky.com/kata/7.1/247702	CUMPLE
83	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.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/150811 https://support.kaspersky.com/KATA/7.1/KataAPI/PublicApi-v4.html	CUMPLE
84	La solución deberá soportar despliegues en modo de monitorización mediante SPAN, port mirroring o mecanismos equivalentes.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/242456 https://support.kaspersky.com/kata/7.1/266033	CUMPLE

ÍTEM	DESCRIPCIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE
85	La solución debe poder funcionar en modo de monitorización (fuera de banda), sin interferir con la comunicación entrante/saliente ni interrumpir los procesos empresariales.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/242456 https://support.kaspersky.com/kata/7.1/266033	CUMPLE
86	La solución deberá permitir el reanálisis de eventos, objetos o tráfico previamente almacenado utilizando inteligencia de amenazas, reglas o capacidades analíticas actualizadas, con el fin de identificar amenazas no detectadas inicialmente.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247636 https://support.kaspersky.com/kata/7.1/300871	CUMPLE
87	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.	Links oficiales del fabricante: https://support.kaspersky.com/KATA/7.1/en-US/227245.htm https://support.kaspersky.com/kata/7.1/281282	CUMPLE
88	Las acciones sospechosas detectadas deben relacionarse con fases de ataque, técnicas de hackers y métodos de la matriz MITRE ATT&CK.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/249034	CUMPLE
89	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.	Links oficiales delfabricante:https://support.kaspersky.com/kata/7.1/137926https://support.kaspersky.com/kata/7.1/247421https://support.kaspersky.com/kata/7.1/247465	CUMPLE
90	La solución deberá permitir la identificación de infraestructuras de comando y control (C2), incluyendo aquellas previamente desconocidas, mediante mecanismos de análisis, detección e inteligencia de amenazas actualizada proporcionada por el fabricante o fuentes integradas compatibles.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247465 https://support.kaspersky.com/kata/7.1/247421	CUMPLE
91	La solución deberá ser capaz de analizar y detectar en el tráfico los objetos que puedan contener patrones con técnicas como evasión, trafico malicioso asociado a comunicaciones de comando y control (C2).	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247465 https://support.kaspersky.com/kata/7.1/247421	CUMPLE
92	La solución proporcionará un inventario lógico de activos monitoreados, incluyendo: • Información de la cuenta de usuario registrada	Links oficiales del fabricante: https://support.kaspersky.com/kat	CUMPLE

ÍTEM	DESCRIPCIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE
	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).	a/7.1/175616 https://support.kaspersky.com/kata/7.1/257980	
93	La solución permitirá mostrar los riesgos asociados a los dispositivos, facilitando la gestión proactiva de amenazas.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/175616 https://support.kaspersky.com/kata/7.1/257980	CUMPLE
94	Para proporcionar una visibilidad completa de la actividad del endpoint, la solución deberá integrarse con los agentes endpoint protegidos por la solución EDR institucional desde los que enviar datos adicionales de telemetría de red, proporcionando contexto complementario, incluyendo, pero no limitado a: • Nombres de procesos del sistema que inician conexiones de red. Ruta del sistema de archivos al proceso del sistema que inicia la conexión de red.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247325 https://support.kaspersky.com/kata/7.1/219777	CUMPLE
95	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.	Links oficiales del fabricante: https://support.kaspersky.com/KATA/7.1/en-US/227245.htm https://support.kaspersky.com/kata/7.1/281282	CUMPLE
96	La solución debe soportar direccionamiento IP dinámico de los dispositivos, asegurando un seguimiento y monitorización precisos.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/175616 https://support.kaspersky.com/kata/7.1/257980	CUMPLE
97	La solución proporcionará monitorización en tiempo real de la actividad de red de los dispositivos mediante capacidades gráficas o visuales de representación de actividad y relaciones de red, permitiendo la visualización del tráfico de red y posibles amenazas de seguridad.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247507 https://support.kaspersky.com/kata/7.1/246747	CUMPLE

ÍTEM	DESCRIPCIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE
98	La solución permitirá un sondeo activo y configurable de dispositivos para enriquecer la información del dispositivo y construir un mapa topológico de red completo.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/236044 https://support.kaspersky.com/kata/7.1/176734	CUMPLE
99	La solución debe permitir el análisis de tráfico cifrado mediante técnicas de fingerprinting TLS u otros métodos equivalentes que faciliten la detección de comportamientos anómalos sin requerir descifrado del contenido.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247495 https://support.kaspersky.com/kata/7.1/159685	CUMPLE
100	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.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/237877 https://support.kaspersky.com/kata/7.1/266033	CUMPLE
101	El tráfico grabado puede capturarse en un formato que puede analizarse y reproducirse fácilmente, como PCAP (Captura de Paquetes) u otros mecanismos equivalentes soportados por el fabricante.	Links oficiales delfabricante:https://support.kaspersky.com/kata/7.1/150811https://support.kaspersky.com/kata/7.1/258283	CUMPLE
102	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.	la documentación KATA 7.1 de búsqueda de paquetes soporta ambos filtros y descarga de dumps. Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/292608 https://support.kaspersky.com/kata/7.1/150811	CUMPLE
103	La solución NDR deberá realizar inspección profunda de tráfico (Deep Packet Inspection – DPI), permitiendo identificar y analizar protocolos comunes y propietarios, sin limitarse a una lista cerrada de protocolos predefinidos.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/292608 https://support.kaspersky.com/kata/7.1/152739	CUMPLE
104	La solución permitirá la búsqueda y recuperación de sesiones de red basándose en capturas de paquetes en el almacenamiento de tráfico.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/150811 https://support.kaspersky.com/kata/7.1/258283	CUMPLE

ÍTEM	DESCRIPCIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE
105	La solución permitirá la exportación de tráfico de red para su análisis posterior, mediante paquetes, datos de sesión o una combinación de ambos	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/150811 https://support.kaspersky.com/kata/7.1/258283	CUMPLE

Así mismo, la empresa COINSA presentó la totalidad de requisitos técnicos habilitantes, los cuales fueron verificados, así:

- **a.** Certificación del fabricante o canal autorizado
- **b.** Certificación de vigencia y soporte del hardware
- **c.** Certificación de vigencia y soporte del licenciamiento
- **d.** Especificaciones técnicas
- **e.** Certificaciones de experiencia

2. VALORES DE LA OFERTA ECONÓMICA

ÍTEM	PROPONENTE	TOTAL COTIZACIÓN
1	UNIÓN TEMPORAL INFOCOMUNICACIONES S.A.S - SOLUCIONES EN SEGURIDAD INFORMÁTICA S.A.S	$ 993.400.000
2	SONDA DE COLOMBIA S.A.	$ 984.323.005
3	COINSA S.A.S.	$ 894.494.180
4	GRUPO MICROSISTEMAS COLOMBIA S.A.S.	$ 948.673.950
5	HEIMCORE	$ 889.427.612,78

La propuesta de la empresa COINSA S.A.S., está dentro del presupuesto del proceso y es la oferta de menor valor.

3. ASIGNACIÓN DE PUNTAJES

Dado que la empresa COINSA es la única habilitada técnicamente, se presenta el consolidado de asignación de puntajes:

Ítem	Criterio	COINSA S.A.S.
		Puntaje
1	Propuesta económica	700
2	Ampliación de las capacidades de visibilidad	100
3	Ampliación del tiempo de licenciamiento y soporte técnico	200
	Total	**1000**

Por las razones expuestas anteriormente, desde la Oficina Asesora de las tecnologías e Información y el programa RED UDNET se sugiere que el contrato sea adjudicado a la empresa COINSA S.A.S. ya que cumple técnicamente con la totalidad de los requerimientos técnicos.

Cordialmente,

Alejandro Daza Corredor
Jefe Oficina Asesora de las Tecnologías e Información
Gestor proyecto 8194

	Nombre	Cargo	Firma
VoBo	Yuleima Ortiz Zambrano	Líder Programa RED UDNET	
Proyectó	Stefany Arias	CPS OATI UDNET	