UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS

"CONTRATAR LA ADQUISICIÓN, INSTALACIÓN Y PUESTA EN CORRECTO FUNCIONAMIENTO DE UNA SOLUCIÓN DE SEGURIDAD PERIMETRAL COMPUESTA POR DOS EQUIPOS PARA GARANTIZAR LA ALTA DISPONIBILIDAD (HA) PARA LA UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS INCLUYENDO LICENCIAMIENTO, SOPORTE Y ACTUALIZACIONES (UPDATE Y UPGRADE)."

MATRIZ DE EVALUACION TECNICA

ITEM	DESCRIPCIÓN	UNIÓN TEMPORAL INFO COMUNICACIONES S.A.S - SOLUCIONES EN SEGURIDAD INFORMATICA S.A.S			SONDA DE COLOMBIA S.A.			COINSA S.A.S			GRUPO MICROSISTEMAS COLOMBIA SAS			HEIMCORE		
		UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
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 este ítem se revisará la ficha técnica del hardware y software enviada por el oferente.	https://support.kaspersky.com/kata/7.1/en-US/247176.htm https://support.kaspersky.com/kata/7.1/en-US/247193.htm Sensor: https://support.kaspersky.com/help/KATA/7.1/en-US/211923.htm Central Node: https://support.kaspersky.com/help/KATA/7.1/en-US/247136.htm Central Node component deployed on the KVM and VMware ESXi virtualization platforms: https://support.kaspersky.com/help/KATA/7.1/en-US/265697.htm Sandbox: https://support.kaspersky.com/help/KATA/7.1/en-US/247180.htm	CUMPLE		Propuesta Técnica: pág. 12, numeral 4.1.6 "Alcance configuración de la solución" (dos appliances NDR en dos sedes); pág. 13 "Monitoreo Inteligente del Tráfico de Red". REQUIERE AJUSTE en propuesta para identificar explícitamente Calle 40 y Bosa Porvenir y el modelo NX 6600 por sede. Fabricante: Trellix Network Security Technical Specifications, pág. 2 (NX 6600: rendimiento hasta 5 Gbps; puertos de monitoreo 10G/40G; TAP/SPAN). https://www.trellix.com/assets/data-sheets/trellix-network-security-tech-specifications-datasheet.pdf	CUMPLE		Hardware ofertado: Lenovo ThinkSystem SR650 V4. 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	CUMPLE		•Hardware and software requirements: https://support.kaspersky.com/kata/7.1/247120 •Sizing Guide: https://support.kaspersky.com/kata/7.1/247448 •Calculations for the Sensor component: https://support.kaspersky.com/kata/7.1/211923 •Calculations for the Central Node component when using KATA, NDR and KEDR functionality: https://support.kaspersky.com/kata/7.1/328197 •Calculations for the Sandbox component: https://support.kaspersky.com/kata/7.1/247180	CUMPLE		CUMPLE. DDI Datasheet, p. 2 del PDF Cómo cumple: Se dimensiona un DDI Series 4000 de 4 Gbps para Calle 40 y un DDI Series 1000 de 1 Gbps para Bosa Porvenir. Deep Discovery Director virtual en HA centraliza administración, correlación y visibilidad.	CUMPLE	
2	La solución deberá contemplar los componentes físicos necesarios para su correcta implementación, operación, monitoreo y administración bajo arquitectura On-Premise.	Central Node calle 40 Sensor calle 40 Sensor Bosa Sandbox calle 40 https://www.dell.com/es-es/shop/ipovw/poweredge-r670#techspecs_section https://www.delltechnologies.com/asset/es-es/products/servers/technical-support/poweredge-rack-series-spec-sheet.pdf	CUMPLE		Propuesta Técnica: pág. 6, numeral 3.2 "Alcance detallado" (arquitectura 100 % On-Premise); págs. 12-13, numeral 4.1.6. Fabricante: Trellix Network Security Technical Specifications, págs. 2-5 (appliances físicos NX y opciones de administración Air-gap/Cloud). https://www.trellix.com/assets/data-sheets/trellix-network-security-tech-specifications-datasheet.pdf	CUMPLE		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		•Architecture of the application: https://support.kaspersky.com/kata/7.1/194604 •Hardware and software requirements: https://support.kaspersky.com/kata/7.1/247120	CUMPLE		CUMPLE. DDI Datasheet, pp. 1–2 · DDD, pp. 25–29 Cómo cumple: Los appliances DDI y las dos instancias de Deep Discovery Director se despliegan en la infraestructura de la Universidad. La solución se integra de forma segura para XDR y Sandbox Analysis conforme al licenciamiento ofertado.	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	Central Node calle 40 Sensor calle 40: https://www.dell.com/es-es/shop/ipovw/poweredge-r670#techspecs_section https://www.delltechnologies.com/asset/es-es/products/servers/technical-support/poweredge-rack-series-spec-sheet.pdf	CUMPLE		Propuesta Técnica: pág. 6, numeral 3.2 "Alcance detallado" (arquitectura 100 % On-Premise); págs. 12-13, numeral 4.1.6. Fabricante: Trellix Network Security Technical Specifications, págs. 2-5 (appliances físicos NX y opciones de administración Air-gap/Cloud). https://www.trellix.com/assets/data-sheets/trellix-network-security-tech-specifications-datasheet.pdf	CUMPLE		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		•Central Node component: https://support.kaspersky.com/kata/7.1/247494 •Sensor component: https://support.kaspersky.com/kata/7.1/247493 •Architecture of the application: https://support.kaspersky.com/kata/7.1/194604	CUMPLE		CUMPLE. DDD, pp. 27–29 · DDI Datasheet, pp. 1–2 Cómo cumple: El nodo central de Calle 40 se implementa con DDI Series 4000 y Deep Discovery Director virtual en HA; Bosa Porvenir opera con el DDI Series 1000 como sensor de tráfico.	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.	https://support.kaspersky.com/kata/7.1/en-US/247176.htm https://support.kaspersky.com/kata/7.1/en-US/247529.htm https://support.kaspersky.com/kata/7.1/en-US/247493.htm https://support.kaspersky.com/kata/7.1/en-US/247445.htm	CUMPLE		Propuesta Técnica: pág. 6, numeral 3.1 (diseño modular y escalable); pág. 13, numeral 4.1.6. Fabricante: Trellix Network Security Technical Specifications, pág. 6 (Smart Node virtual VA-NXS y diferentes capacidades). https://docs.trellix.com/bundle/ndr_4.x_dg/page/UUID-ef56faf9-567b-b6a5-9fa0-3075c21f1ed5.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247493 https://support.kaspersky.com/kata/7.1/247179	CUMPLE		•Sensor component: https://support.kaspersky.com/kata/7.1/247493 •Scenario of deployment on four or more servers: https://support.kaspersky.com/kata/7.1/247179 •Deploying an application on virtualization platforms: https://support.kaspersky.com/kata/7.1/303948	CUMPLE		CUMPLE. XDR for Networks, pp. 2–3 · DDI IDG, pp. 111–112 Cómo cumple: La plataforma permite registrar appliances adicionales y desplegar sensores virtuales sobre VMware, Hyper-V o KVM, dentro de la capacidad y créditos licenciados, sin reemplazar los componentes existentes.	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.	https://support.kaspersky.com/kata/7.1/en-US/247193.htm https://support.kaspersky.com/kata/7.1/en-US/247176.htm https://support.kaspersky.com/kata/7.1/en-US/247177.htm https://support.kaspersky.	CUMPLE		Propuesta Técnica: pág. 6, numeral 3.1 (diseño modular y escalable que permite incorporar nuevas capacidades sin cambios estructurales); pág. 13. Fabricante: Trellix Network Security Technical Specifications, págs. 2-6 (familia de appliances físicos y virtuales con capacidades escalables).. https://docs.trellix.com/bundle/ndr_4.x_dg/page/UUID-ef56faf9-567b-b6a5-9fa0-3075c21f1ed5.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247179 https://support.kaspersky.com/kata/7.1/247448	CUMPLE		•Scenario of deployment on four or more servers: https://support.kaspersky.com/kata/7.1/247179 •Sizing Guide: https://support.kaspersky.com/kata/7.1/247448	CUMPLE		CUMPLE. DDI Datasheet, p. 2 · XDR for Networks, pp. 2–3 Cómo cumple: La familia DDI permite incorporar appliances físicos o virtuales y ampliar capacidad de análisis por licenciamiento, manteniendo la administración centralizada en Deep Discovery Director.	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.	https://support.kaspersky.com/kata/7.1/300871 https://support.kaspersky.com/kata/7.1/en-US/267995.htm	CUMPLE		Pagina 3 (Item 3.1) y 12 (Item 4.1.6) de la propuesta técnica. https://docs.trellix.com/bundle/nx_11.x_sag/page/UUID-a461e037-4c29-c171-100e-5d79f4ab4c7b.html	NO CUMPLE	El requerimiento no se puede verificar con la información adjuntada por la empresa.	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		•Calculating the size of the event database and Storage: https://support.kaspersky.com/kata/7.1/329325 •Configuring the retention period for logs, alerts and events: https://support.kaspersky.com/kata/7.1/300871	CUMPLE		CUMPLE. XDR for Networks, p. 2 · DDD, pp. 419–421 Cómo cumple: Se configura una política de conservación mínima de 90 días para eventos, alertas y telemetría en Deep Discovery Director, con el almacenamiento dimensionado en las máquinas virtuales de la solución.	NO CUMPLE	El requerimiento no puede ser verificado con la información suministrada por la empresa, dado que en el ítem 12 se oferta la versión 7.0, mientras que la documentación aportada corresponde a la versión 5.5.
7	Los componentes físicos suministrados deberán incluir los accesorios, interfaces, módulos, cableados y demás elementos necesarios para su correcta instalación y puesta en funcionamiento.	Central Node calle 40 Sensor calle 40 Sensor Bosa Sandbox calle 40 https://www.dell.com/es-es/shop/ipovw/poweredge-r670#techspecs_section https://www.delltechnologies.com/asset/es-es/products/servers/technical-support/poweredge-rack-series-spec-sheet.pdf	CUMPLE		Propuesta Técnica: pág. 7, numeral 3.2 (SONDA ejecutará suministro, instalación y puesta en producción) y pág. 17, numeral 4.3.9 (adquirir y coordinar instalación de componentes).. https://www.trellix.com/assets/docs/data-sheets/trellix-network-security-datasheet.pdf, https://docs.trellix.com/bundle/nx_11.x_sag/page/UUID-4e49b271-e8ae-23c1-5a60-5c3b55028869.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/242456 https://support.kaspersky.com/kata/7.1/266033	CUMPLE		•Hardware and software requirements: https://support.kaspersky.com/kata/7.1/247120	CUMPLE		CUMPLE. Cómo cumple: Se incluyen rieles y fuentes del fabricante, un Cisco SFP-10G-SR para el DDI 4000, un Cisco GLC-TE para el enlace del DDI 1000, una fibra OM4 LC-LC de 2 m, patch cords Cat6A, alimentación e identificación.	CUMPLE	
8	La solución deberá soportar mecanismos de captura de tráfico mediante SPAN, port mirroring o tecnologías equivalentes compatibles con la infraestructura institucional.	https://support.kaspersky.com/kata/7.1/en-US/247193.htm https://support.kaspersky.com/kata/7.1/en-US/266033.htm	CUMPLE		Propuesta Técnica: pág. 13, "Monitoreo Inteligente del Tráfico de Red". Fabricante: Trellix Network Security Technical Specifications, pág. 2 (modo de operación TAP/SPAN). https://www.trellix.com/assets/data-sheets/trellix-network-security-tech-specifications-datasheet.pdf	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/242456 https://support.kaspersky.com/kata/7.1/266033	CUMPLE		•Configuring receipt of mirrored traffic from SPAN ports: https://support.kaspersky.com/kata/7.1/242456 •Configuring recording of mirrored traffic from SPAN ports: https://support.kaspersky.com/kata/7.1/266033	CUMPLE		CUMPLE. DDI IDG, pp. 62–67 y 186–190 Cómo cumple: Los DDI reciben copias del tráfico mediante SPAN o port mirroring: enlace óptico 10G para el Series 4000 y enlace de cobre 1G para el Series 1000.	CUMPLE	
9	La arquitectura propuesta deberá permitir la integración y comunicación segura entre el nodo central y los sensores o colectores desplegados.	https://support.kaspersky.com/kata/7.1/en-US/247178.htm https://support.kaspersky.com/kata/7.1/283631 https://support.kaspersky.com/kata/7.1/283630 https://support.kaspersky.com/kata/7.1/303090	CUMPLE		Propuesta Técnica: pág. 8, diagrama de arquitectura de referencia e integración; pág. 13, Integración con el Ecosistema de Seguridad. https://docs.trellix.com/bundle/nx_11.x_sag/page/UUID-a461e037-4c29-c171-100e-5d79f4ab4c7b.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/252062 https://support.kaspersky.com/kata/7.1/194604	CUMPLE		•Connecting the Sensor component to the Central Node: https://support.kaspersky.com/kata/7.1/252062 •Architecture of the application: https://support.kaspersky.com/kata/7.1/194604	CUMPLE		CUMPLE. DDI IDG, pp. 239–241 · DDI AG, pp. 354–356 Cómo cumple: Los appliances se comunican con Deep Discovery Director mediante HTTPS/TLS y puertos controlados por ACL, utilizando certificados administrados por la Universidad.	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 un 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 l 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 s 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 form 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 parámetros de desempeño, a través de la página web del fabricante.	https://www.legrand.com.co/sites/g/files/ocwmcr491/files/2024-12/patch_cords_fibra_optica_legrand.pdf https://daga-sa.com/wp-content/uploads/2023/12/Ficha_Tecnica_Patch_Cord_Fibra_OM4_LC-SC_PC.pdf	CUMPLE		https://www.trellix.com/assets/data-sheets/trellix-network-security-tech-specifications-datasheet.pdf	NO CUMPLE	El requerimiento no se puede verificar con la información adjuntada por la empresa. Se adjunto la ficha tecnica de la solución y no del cableado.	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		Como parte de la solución ofertada, se suministrarán los patch cords de fibra óptica requeridos para la correcta conexión e integración de los equipos contemplados en el proyecto, cumpliendo con las especificaciones técnicas solicitadas por la Universidad. Los elementos serán suministrados nuevos, originales de fábrica, debidamente identificados. Garantizando su compatibilidad, calidad y adecuado funcionamiento dentro de la infraestructura tecnológica institucional.	NO CUMPLE	El requerimiento no se puede verificar con la información adjuntada por la empresa. Se adjunto la ficha tecnica de la solución y no del cableado.	CUMPLE. Panduit Certification Plus, garantía 25 años Cómo cumple: Se suministra un patch cord Panduit FZ2ELLNLNSNM002, OM4, LC-LC dúplex, 50/125 µm, LSZH y 2 m, dentro de un sistema elegible para garantía Panduit Certification Plus de 25 años.	CUMPLE	

ITEM	DESCRIPCIÓN	UNIÓN TEMPORAL INFO COMUNICACIONES S.A.S - SOLUCIONES EN SEGURIDAD INFORMATICA S.A.S			SONDA DE COLOMBIA S.A.			COINSA S.A.S			GRUPO MICROSISTEMAS COLOMBIA SAS			HEIMCORE		
		UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
11	Especificaciones técnicas - SFP + • Fabricante: Cisco – Se solicita de este fabricante teniendo en cuenta que el Switch Core es de esta marca y uno diferent 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)	Broadcom BCM57414 Ethernet 10/25Gb 2-port SFP28 Adapter for HPE (P26262-B21) https://www.hpe.com/psnow/doc/PSN1012926857VEES HPE BladeSystem c-Class 10Gb SFP+ SR Transceiver (455883-B21) https://www.hpe.com/psnow/doc/PSN3837815BOES	NO CUMPLE	El requisito solicita que los SFP + sean de fabricante Cisco	https://www.trellix.com/assets/data-sheets/trellix-network-security-tech-specifications-datasheet.pdf	NO CUMPLE	El requerimiento no se puede verificar con la información adjuntada por la empresa. Se adjunto la ficha tecnica de la solución del SFP+.	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		Se suministrarán los módulos SFP+ requeridos para la correcta interconexión de los equipos con la infraestructura de red de la Universidad, cumpliendo con las especificaciones técnicas solicitadas para enlaces de 10 Gbps sobre fibra multimodo. Los transceptores serán originales de fábrica, compatibles con la infraestructura existente.	NO CUMPLE	El requerimiento no se puede verificar con la información adjuntada por la empresa. Se adjunto la ficha tecnica de la solución del SFP+.	CUMPLE. Cisco 10GBASE-SR SFP+, ficha web · Cisco GLC-TE 1000BASE-T, ficha web Cómo cumple: Se instala un Cisco SFP-10G-SR original en el Core para el enlace 10GBASE-SR del DDI 4000, con fibra OM4 LC dúplex. Para el DDI 1000 se contempla Cisco GLC-TE 1000BASE-T y patch cord Cat6A.	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.	https://support.kaspersky.com/kata/7.1/en-US/226747.htm https://support.kaspersky.com/kata/7.1/en-US/272042.htm https://support.kaspersky.com/kata/7.1/en-US/247577.htm https://support.kaspersky.com/kata/7.1/en-US/246850.htm	CUMPLE		Propuesta Técnica: pág. 15, Centro de Servicios Especializados 24x7; pág. 16, gestión de configuración/mejora . https://docs.trellix.com/bundle/nx_11.x_rn/page/UUID-84e41c7a-680a-dfaa-5b0b-b0c1b2003d8c.html, https://www.trellix.com/support/end-of-life-products/ y Security Updates https://www.trellix.com/downloads/security-updates	CUMPLE		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		•Kaspersky Anti Targeted Attack Platform 7.1 Help: https://support.kaspersky.com/kata/7.1 •Hardware and software requirements: https://support.kaspersky.com/kata/7.1/247120	CUMPLE		CUMPLE. Documentación vigente de DDI 7.0 Cómo cumple: La oferta incluye versiones vigentes y soportadas de DDI, Deep Discovery Director, XDR for Endpoints, XDR for Networks y Sandbox Analysis, con soporte y actualizaciones durante la vigencia contractual; se adjunta carta de Trend Micro.	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, conforme a las políticas institucionales de seguridad de la información.	https://support.kaspersky.com/kata/7.1/en-US/247445.htm https://support.kaspersky.com/kata/7.1/en-US/247176.htm https://support.kaspersky.com/kata/7.1/en-US/247494.htm https://support.kaspersky.com/kata/7.1/en-US/159935.htm https://support.kaspersky.com/kata/7.1/en-US/247488.htm	CUMPLE		Propuesta Técnica: págs. 4-6 (arquitectura On-Premise y control de la información); pág. 12 (100 % On-Premise); pág. 13 (Administración y Gobierno de la Plataforma). Fabricante , https://docs.trellix.com/bundle/nx_11.x_rn/page/UUID-84e41c7a-680a-dfaa-5b0b-b0c1b2003d8c.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/194604 https://support.kaspersky.com/kata/7.1/247461	CUMPLE		•Architecture of the application: https://support.kaspersky.com/kata/7.1/194604 •Configuring integration with Active Directory: https://support.kaspersky.com/kata/7.1/247461	CUMPLE		CUMPLE. DDI Datasheet, pp. 1–2 · DDD, pp. 25–29 Cómo cumple: La inspección NDR, configuración y administración se ejecutan en los appliances y VMs controlados por la Universidad; los servicios XDR/Sandbox se conectan mediante canales seguros y políticas institucionales de tratamiento de datos.	NO CUMPLE	El requerimiento no puede ser verificado con la información suministrada por la empresa, dado que en el ítem 12 se oferta la versión 7.0, mientras que la documentación aportada corresponde a la versión 5.5.
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.	https://support.kaspersky.com/kata/7.1/en-US/247193.htm https://support.kaspersky.com/kata/7.1/en-US/247445.htm https://support.kaspersky.com/kata/7.1/en-US/247176.htm	CUMPLE		Propuesta Técnica: pág. 6, numeral 3.1 (diseño modular y escalable); pág. 13, alcance de configuración. Fabricante: Trellix Network Security Technical Specifications, págs. 2-6 (diferentes niveles de rendimiento físicos y virtuales). . https://docs.trellix.com/bundle/nx_11.x_sag/page/UUID-83d20d2a-29df-bad7-310b-beac50604f62.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247448 https://support.kaspersky.com/kata/7.1/247179	CUMPLE		•Sizing Guide: https://support.kaspersky.com/kata/7.1/247448 •Scenario of deployment on four or more servers: https://support.kaspersky.com/kata/7.1/247179	CUMPLE		CUMPLE. DDI Datasheet, p. 2 · XDR for Networks, pp. 2–3 Cómo cumple: La capacidad se amplía incorporando nuevos sensores, appliances o ancho de banda licenciado, y los 4.000 Endpoint Sensors aportan visibilidad adicional sin sustituir la plataforma central.	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.	https://support.kaspersky.com/kata/7.1/en-US/246849.htm https://support.kaspersky.com/kata/7.1/en-US/247128.htm https://support.kaspersky.com/kata/7.1/en-US/219777.htm	CUMPLE		Propuesta Técnica: pág. 6-7 (telemetría de endpoints estratégicos). Fabricante: Trellix Network Security Technical Specifications, pág. 2: OS Support Linux, macOS X y Microsoft Windows para NX 6600; pág. 6 para Smart Nodes virtuales . https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-d20d9dd9-87cc-37d7-d709-b2931aa25e17.html	NO CUMPLE	El requerimiento no se puede verificar con la información adjuntada por la empresa. No se encuentra en la propuesta tecnica o en el link suministrado información sobre los sistemas operativos soportados.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/246849 https://support.kaspersky.com/kata/7.1/247128	CUMPLE		•Compatibility of Kaspersky Endpoint Security for Windows with KATA: https://support.kaspersky.com/kata/7.1/246849 •Compatibility of Kaspersky Endpoint Security for Linux with KATA: https://support.kaspersky.com/kata/7.1/247128 •Compatibility of Kaspersky Endpoint Security for Mac with KATA: https://support.kaspersky.com/kata/7.1/252759	CUMPLE		CUMPLE. Endpoint Security, p. 3 Cómo cumple: Los Endpoint Sensors ofertados soportan Windows, Linux y macOS y envían telemetría de seguridad a la consola central para análisis y correlación.	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.	https://support.kaspersky.com/kata/7.1/en-US/247193.htm https://support.kaspersky.com/kata/7.1/en-US/247176.htm https://support.kaspersky.com/kedr-expert-on-premise/8.1/298639	CUMPLE		Propuesta Técnica: págs. 5-8, numerales 3.1 y 3.2; pág. 8 diagrama (NX, HX, capacidades de análisis e integración); pág. 13 (Integración con Ecosistema de Seguridad). . https://www.trellix.com/assets/solution-briefs/trellix-hyperautomation-solution-brief.pdf	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/194604 https://support.kaspersky.com/kata/7.1/247325	CUMPLE		•Architecture of the application: https://support.kaspersky.com/kata/7.1/194604 •Configuring integration of Endpoint Agent with the KEDR functional block: https://support.kaspersky.com/kata/7.1/247325 •Configuring integration of Endpoint Agent with the NDR functional block: https://support.kaspersky.com/kata/7.1/219777 •Sandbox component: https://support.kaspersky.com/kata/7.1/247495	CUMPLE		CUMPLE. DDI Datasheet, pp. 1–2 · XDR for Networks, pp. 1–2 · Conexión directa DDI–Trend Vision One, web Cómo cumple: DDI proporciona NDR; correlaciona red y 4.000 endpoints; Sandbox Analysis recibe automáticamente objetos sospechosos detectados por los appliances.	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.	https://support.kaspersky.com/kata/7.1/en-US/247193.htm https://support.kaspersky.com/kata/7.1/en-US/150806.htm https://support.kaspersky.com/kata/7.1/en-US/134912.htm https://support.kaspersky.com/kata/7.1/en-US/247484.htm	CUMPLE		Propuesta Técnica: pág. 6-8 (correlación centralizada, telemetría de red/endpoints, investigación); pág. 13 Analítica y Correlación Inteligente" e "Investigación Forense". Fabricante: Trellix Network Security aporta evidencia e inteligencia accionable para resolver incidentes y soporta análisis de tráfico . https://docs.trellix.com/bundle/nx_11.x_sag/page/UUID-83d20d2a-29df-bad7-310b-beac50604f62.html	CUMPLE		fabricante: https://support.kaspersky.com/kata/7.1/247494 https://support.kaspersky.com/kata/7.1/247636	CUMPLE		•Central Node component: https://support.kaspersky.com/kata/7.1/247494 •Events database threat hunting: https://support.kaspersky.com/kata/7.1/247636	CUMPLE		CUMPLE. DDD, pp. 27–29 y 171–173 · XDR for Networks, pp. 1–2 Cómo cumple: Deep Discovery Director consolida detecciones, telemetría de red, activos y protocolos visibles, incluidos los asociados al correo electrónico.	NO CUMPLE	El requerimiento no puede ser verificado con la información suministrada por la empresa, dado que en el ítem 12 se oferta la versión 7.0, mientras que la documentación aportada corresponde a la versión 5.5.
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.	https://support.kaspersky.com/kata/7.1/en-US/247176.htm https://support.kaspersky.com/kata/7.1/en-US/247193.htm	CUMPLE		Propuesta Técnica: pág. 6-8 (consola y correlación centralizada); pág. 8 diagrama; pág. 13 Analítica y Correlación Inteligente . https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-2a73cb36-b937-99fc-6a82-980ba1fa8c43.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247494 https://support.kaspersky.com/kata/7.1/247179	CUMPLE		•Central Node component: https://support.kaspersky.com/kata/7.1/247494 •Scenario of deployment on four or more servers: https://support.kaspersky.com/kata/7.1/247179	CUMPLE		CUMPLE. DDD, pp. 27–29 · Conexión directa DDI–Trend Vision One, web Cómo cumple: Dos instancias virtuales de Deep Discovery Director se implementan en HA y consolidan lógicamente la administración y el análisis de los DDI de Calle 40 y Bosa Porvenir.	NO CUMPLE	El requerimiento no puede ser verificado con la información suministrada por la empresa, dado que en el ítem 12 se oferta la versión 7.0, mientras que la documentación aportada corresponde a la versión 5.5.
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.	https://support.kaspersky.com/kata/7.1/en-US/247176.htm https://support.kaspersky.com/kata/7.1/en-US/247193.htm	CUMPLE		Propuesta Técnica: pág. 12-13 (dos appliances NDR. Fabricante: Trellix Network Security Technical Specifications, pág. 2: NX 6600 Performance hasta 5 Gbps y SmartVision hasta 10 Gbps; pág. 4: Smart Node NX 6600 hasta 10 Gbps. https://www.trellix.com/assets/data-sheets/trellix-network-security-tech-specifications-datasheet.pdf	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/211923 https://support.kaspersky.com/kata/7.1/328197	CUMPLE		•Calculations for the Sensor component: https://support.kaspersky.com/kata/7.1/211923 •Calculations for the Central Node component when using KATA, NDR and KEDR functionality: https://support.kaspersky.com/kata/7.1/328197	CUMPLE		CUMPLE. DDI Datasheet, p. 2 Cómo cumple: El Centro de Análisis de Calle 40 utiliza DDI Series 4000 con procesamiento licenciado de 4 Gbps. Bosa Porvenir opera como sensor remoto con Series 1000 y capacidad de 1 Gbps.	CUMPLE	
20	La solución deberá permitir esquemas de alta disponibilidad (HA) para los componentes críticos 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.	https://support.kaspersky.com/kata/7.1/en-US/247136.htm https://support.kaspersky.com/kata/7.1/en-US/247176.htm https://support.kaspersky.com/kata/7.1/en-US/247494.htm	CUMPLE		Propuesta Técnica: pág. 6 (continuidad operativa) y págs. 15-16 (modelo de operación), pero no describe HA técnica. Fabricante: Trellix Network Security Technical Specifications, pág. 4, tabla de Smart Nodes físicos: High Availability (HA) Available para NX 6600; fuentes de poder redundantes 1+1 . https://docs.trellix.com/bundle/nx_10.x_haug/page/UUID-68ad60bd-0060-5b3e-8121-5fc11cc70daa.html	CUMPLE		Hardware ofertado: Lenovo ThinkSystem SR650 V4. 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	CUMPLE		•Scenario of deployment on four or more servers: https://support.kaspersky.com/kata/7.1/247179 •Calculations for the Central Node component when using KATA, NDR and KEDR functionality: https://support.kaspersky.com/kata/7.1/328197	CUMPLE		CUMPLE. DDI Datasheet, p. 2 · Deep Discovery Director, pp. 25–29 y 426–427 Cómo cumple: La administración central se despliega con Deep Discovery Director virtual en HA. Los appliances incorporan RAID y fuentes redundantes, y se configuran respaldo, restauración y procedimiento documentado de continuidad operativa.	NO CUMPLE	El requerimiento no puede ser verificado con la información suministrada por la empresa, dado que en el ítem 12 se oferta la versión 7.0, mientras que la documentación aportada corresponde a la versión 5.5.
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.	https://support.kaspersky.com/kata/7.1/en-US/247454.htm https://support.kaspersky.com/kata/7.1/en-US/247506.htm	CUMPLE		Propuesta Técnica: pág. 7 (consola única); pág. 13 (administración centralizada). Fabricante: The Network Security appliance Web UI usa HTTPS y permite administración mediante interfaz web . https://docs.trellix.com/bundle/cm_11.x_sag/page/UUID-83edc610-abab-99d7-b901-daa514869e4f.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1 https://support.kaspersky.com/kata/7.1/247507	CUMPLE		•Kaspersky Anti Targeted Attack Platform 7.1 Help: https://support.kaspersky.com/kata/7.1 •Monitoring the performance of the application: https://support.kaspersky.com/kata/7.1/247507	CUMPLE		CUMPLE. DDI AG, pp. 33–37 · DDD, pp. 27–29 Cómo cumple: DDI, Deep Discovery Director dispone de consolas web para gestión, estado del sistema, configuración, investigación y seguimiento de detecciones.	CUMPLE	

ITEM	DESCRIPCIÓN	UNIÓN TEMPORAL INFO COMUNICACIONES S.A.S - SOLUCIONES EN SEGURIDAD INFORMATICA S.A.S			SONDA DE COLOMBIA S.A.			COINSA S.A.S			GRUPO MICROSISTEMAS COLOMBIA SAS			HEIMCORE		
		UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
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.	https://support.kaspersky.com/kata/7.1/en-US/247176.htm https://support.kaspersky.com/kata/7.1/en-US/247484.htm https://support.kaspersky.com/kata/7.1/en-US/247120.htm	CUMPLE		Propuesta Técnica: pág. 6 (arquitectura modular/escalable; futuras capacidades) y pág. 13. Fabricante: Trellix NDR Console soporta VMware ESXi https://docs.trellix.com/bundle/ndr_4.x_dg/page/UUID-46045f34-bdbd-9868-c695-5e5f5c876135.html ; KVM https://docs.trellix.com/bundle/ndr_4.x_dg/page/UUID-9d32dd55-9736-d90b-633f-cb6cdfbb7b06.html ; Hyper-V https://docs.trellix.com/bundle/ndr_4.x_dg/page/UUID-a63eeceb-61f1-2045-8044-649cc0c0c3c7.html , https://docs.trellix.com/bundle/td_dg/page/UUID-7c259792-76f2-d214-8e7d-f5ecd9314198.html	CUMPLE		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		•Hardware and software requirements: https://support.kaspersky.com/kata/7.1/247120 •Deploying an application on virtualization platforms: https://support.kaspersky.com/kata/7.1/303948 •Scenario of deployment on four or more servers: https://support.kaspersky.com/kata/7.1/247179	CUMPLE		CUMPLE. DDI IDG, pp. 111–112 · XDR for Networks, p. 3 Cómo cumple: Deep Discovery Director y los componentes virtuales se despliegan en hipervisores soportados; la solución admite futuros sensores virtuales en VMware, Hyper-V o KVM.	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.	https://support.kaspersky.com/kata/7.1/en-US/207166.htm https://support.kaspersky.com/kata/7.1/en-US/247786.htm https://support.kaspersky.com/kata/7.1/en-US/247787.htm	CUMPLE		Propuesta Técnica: pág. 13 (alertas y parámetros operativos); pág. 16 (gestión de informes/operación). Documentación Trellix de appliances contempla notificaciones de salud del sistema, incluida baja capacidad de disco, en componentes de la familia . https://docs.trellix.com/bundle/nx_10.x_ug/page/UUID-1fd9ea57-4809-123a-a69c-b2db5670e39a.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247515 https://support.kaspersky.com/kata/7.1	CUMPLE		•Monitoring the receipt and processing of incoming data: https://support.kaspersky.com/kata/7.1/247515 •Kaspersky Anti Targeted Attack Platform 7.1 Help: https://support.kaspersky.com/kata/7.1	CUMPLE		CUMPLE. DDI AG, pp. 184–192 · DDD, pp. 343–345 y 396 Cómo cumple: Se configuran SMTP y reglas de notificación para alertar por fallos operativos, interfaces, actualización, alta/baja de tráfico y condiciones de almacenamiento.	CUMPLE	
24	La solución deberá permitir la administración centralizada de políticas, eventos, tareas y reportes mediante una consola unificada de gestión.	https://support.kaspersky.com/kata/7.1/en-US/247443.htm https://support.kaspersky.com/kata/7.1/en-US/247506.htm https://support.kaspersky.com/kata/7.1/en-US/247454.htm	CUMPLE		Propuesta Técnica: pág. 7 (plataforma integra información y consolida en una única consola); pág. 13 "Analítica y Correlación Inteligente" y "Administración y Gobierno de la Plataforma . https://docs.trellix.com/bundle/nx_11.x_sag/page/UUID-83d20d2a-29df-bad7-310b-beac50604f62.html	CUMPLE		fabricante: https://support.kaspersky.com/kata/7.1/247507 https://support.kaspersky.com/kata/7.1/246747	CUMPLE		•Monitoring the performance of the application: https://support.kaspersky.com/kata/7.1/247507 •Managing user-defined Sandbox rules: https://support.kaspersky.com/kata/7.1/246747	CUMPLE		CUMPLE. DDD, pp. 27–29 y 257–263 · Conexión directa DDI–Trend Vision One, web Cómo cumple: Deep Discovery Director centraliza appliances, políticas, eventos, tareas y reportes; unifica la investigación XDR de red y endpoint.	NO CUMPLE	El requerimiento no puede ser verificado con la información suministrada por la empresa, dado que en el ítem 12 se oferta la versión 7.0, mientras que la documentación aportada corresponde a la versión 5.5.
25	La solución debe soportar mecanismos controlados para la descarga de actualizaciones mediante conexión directa o a través de servidores proxy con autenticación.	https://support.kaspersky.com/kata/7.1/en-US/247577.htm	CUMPLE		Propuesta Técnica: págs. 15-16 (gestión de configuración/mejora) . http://docs.trellix.com/bundle/nx_10.x_sag/page/UUID-2e77e182-5dcc-3a1e-c079-5ef867bdf8dd.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1 https://support.kaspersky.com/kata/7.1/247577	CUMPLE		•Kaspersky Anti Targeted Attack Platform 7.1 Help: https://support.kaspersky.com/kata/7.1 •Updating application databases: https://support.kaspersky.com/kata/7.1/247577	CUMPLE		CUMPLE. DDI AG, p. 176 · DDD, p. 395 Cómo cumple: Las actualizaciones se obtienen desde Trend Micro por conexión directa o proxy autenticado, con ventanas de mantenimiento y control de versiones.	CUMPLE	
26	La solución deberá contar con un modelo de control de acceso basado en roles (RBAC), que permita: •La creación de roles personalizados. •La asignación granular de permisos por módulo, funcionalidad y alcance (por dominio o unidad organizacional). •La aplicación del principio de mínimo privilegio. •La delegación administrativa segmentada por unidades organizacionales. •La integración con servicios de directorio (LDAP/Active Directory). •El registro y auditoría de todas las acciones realizadas por los usuarios administradores. •La gestión centralizada de perfiles y políticas de acceso.	https://support.kaspersky.com/kata/7.1/en-US/247453.htm https://support.kaspersky.com/kata/7.1/en-US/247458.htm	CUMPLE		Propuesta Técnica: pág. 13, numeral 4.1.6 "Administración y Gobierno de la Plataforma" (usuarios, perfiles, roles y políticas de acceso). Fabricante: Trellix Network Security – Overview of Network Security user interfaces (documenta controles de acceso basados en roles y reglas) . https://docs.trellix.com/bundle/iam_ag/page/UUID-e81089d5-4f08-e7f9-589a-d5bb49bd2010.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247461 https://support.kaspersky.com/kata/7.1	CUMPLE		•Configuring integration with Active Directory: https://support.kaspersky.com/kata/7.1/247461 •Kaspersky Anti Targeted Attack Platform 7.1 Help: https://support.kaspersky.com/kata/7.1 •Managing accounts of application administrators and users: https://support.kaspersky.com/kata/7.1/247453	CUMPLE		CUMPLE. DDD, pp. 405–408 · DDI AG, pp. 363–366 y 375–378 Cómo cumple: Se configuran roles de administrador/analista/consulta, integración con Active Directory/LDAP, mínimo privilegio, segregación de funciones y auditoría de acciones administrativas.	CUMPLE	
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.	https://support.kaspersky.com/kata/7.1/en-US/247521.htm https://support.kaspersky.com/kata/7.1/247806 https://support.kaspersky.com/kata/7.1/303090	CUMPLE		Propuesta Técnica: pág. 13, "Administración y Gobierno de la Plataforma". Fabricante: Trellix Network Security utiliza Web UI de administración segura y HTTPS; referencia de interfaz y administración . https://docs.trellix.com/bundle/nx_11.x_sag/page/UUID-83edc610-abab-99d7-b901-daa514869e4f.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247521 https://support.kaspersky.com/kata/7.1/247571	CUMPLE		•Generating or uploading a TLS certificate of the server: https://support.kaspersky.com/kata/7.1/247521 •Uploading a TLS certificate: https://support.kaspersky.com/kata/7.1/247571	CUMPLE		CUMPLE. DDI AG, pp. 354–355 Cómo cumple: La administración utiliza HTTPS y certificados digitales importados o emitidos por la PKI institucional para proteger el canal entre la consola y los administradores.	CUMPLE	
28	La solución debe soportar sincronización de tiempo con servidores NTP.	https://support.kaspersky.com/kata/7.1/en-US/247520.htm https://support.kaspersky.com/kata/7.1/en-US/273042.htm	CUMPLE		Propuesta Técnica: pág. 13, "Administración y Gobierno de la Plataforma" (parámetros operativos). Fabricante: Trellix Network Security – Date and time settings: permite configurar uno o más servidores NTP para sincronizar el appliance. https://docs.trellix.com/bundle/nx_11.x_sag/page/UUID-86252d5a-5fab-04fa-5f65-a910425b1fbb.html , https://docs.trellix.com/bundle/nx_11.x_sag/page/UUID-5049ead8-313f-78bf-f058-bc5242d3f279.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/273215 https://support.kaspersky.com/kata/7.1/247520	CUMPLE		•Step 10. Configuring time synchronization with an NTP server: https://support.kaspersky.com/kata/7.1/273215 •Configuring the date and time on the server: https://support.kaspersky.com/kata/7.1/247520	CUMPLE		CUMPLE. DDI AG, pp. 355–356 · DDD, p. 402 Cómo cumple: Todos los appliances y VMs se sincronizan con los servidores NTP institucionales para garantizar consistencia temporal de eventos y auditoría.	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.	https://support.kaspersky.com/kata/7.1/en-US/271112.htm https://support.kaspersky.com/kata/7.1/en-US/271365.htm https://support.kaspersky.com/kata/7.1/271114	CUMPLE		Propuesta Técnica: pág. 13, "Administración y Gobierno de la Plataforma" (respaldos). Fabricante: Trellix Network Security – Database backup and restore . https://docs.trellix.com/bundle/nx_10.x_sag/page/UUID-ff638f5e-0b5a-13c4-6579-ed5700c3cfd0.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/271112	CUMPLE		•Backing up and restoring the data of the Central Node server: https://support.kaspersky.com/kata/7.1/271112	CUMPLE		CUMPLE. DDI AG, pp. 381–382 · DDD, pp. 426–427 Cómo cumple: Se programan respaldos de configuración de DDI y Deep Discovery Director, se documentan restauración y recuperación y se incluyen pruebas dentro del plan de aceptación.	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.	https://support.kaspersky.com/kata/7.1/en-US/247574.htm https://support.kaspersky.com/kata/7.1/en-US/247575.htm https://support.kaspersky.com/kata/7.1/en-US/301483.htm https://support.kaspersky.com/kata/7.1/en-US/140034.htm	CUMPLE		Propuesta Técnica: pág. 13, "Administración y Gobierno de la Plataforma"; pág. 16, numeral 4.3.4 "Gestión de la configuración". Fabricante: la guía de Trellix Network Security contempla archivos de audit log y su administración; referencia: https://docs.trellix.com/bundle/nx_11.x_sag/page/UUID-e5355574-d1d7-0b4e-8939-e38686320faf.html. , https://docs.trellix.com/bundle/cli_cr/page/UUID-117dd1a2-f479-1827-5eae-7023d81d58c4.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247576 https://support.kaspersky.com/kata/7.1/153523	CUMPLE		•Records in the user activity log: https://support.kaspersky.com/kata/7.1/247576 •Sending events, application messages, and audit records to third-party systems: https://support.kaspersky.com/kata/7.1/153523	CUMPLE		CUMPLE. DDI AG, pp. 375–378 · DDD, pp. 419–421 Cómo cumple: Los registros de sistema y administración conservan usuario, acción y fecha; su retención y exportación se configuran para trazabilidad y auditoría institucional.	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.	https://support.kaspersky.com/kata/7.1/en-US/246850.htm https://support.kaspersky.com/kata/7.1/en-US/319319.htm https://support.kaspersky.com/kata/7.1/en-US/243480.htm	CUMPLE		Propuesta Técnica: pág. 16, numerales 4.3.4 y 4.3.5 (gestión de configuración y mejora continua). Fabricante: Trellix Network Security – Upgrading the appliance using the CLI: https://docs.trellix.com/bundle/nx_11.x_sag/page/UUID-b1cfe872-0b12-6cb0-e751-bdaa2690ebd5.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1 https://support.kaspersky.com/kata/7.1/247577	CUMPLE		•Kaspersky Anti Targeted Attack Platform 7.1 Help: https://support.kaspersky.com/kata/7.1 •Updating application databases: https://support.kaspersky.com/kata/7.1/247577	CUMPLE		CUMPLE. DDI AG, pp. 176–182 · DDI AG, pp. 381–382 Cómo cumple: Los upgrades se ejecutan con respaldo previo, validación de compatibilidad y procedimiento de reversión, conservando configuraciones, políticas e información operativa soportada por el producto.	CUMPLE	
32	La solución debe integrarse con servicios de inteligencia de amenazas, ya sean en la nube o 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/en-US/247466.htm https://support.kaspersky.com/kata/7.1/en-US/157533.htm https://support.kaspersky.com/kata/7.1/en-US/246848.htm	CUMPLE		Propuesta Técnica: págs. 6-8 (inteligencia de amenazas y enriquecimiento); pág. 13 "Inteligencia de Amenazas". Fabricante: Trellix Insights proporciona inteligencia global y análisis de campañas/IOC: https://docs.trellix.com/bundle/trellix-insights-product-guide/page/UUID-1ee12346-846f-1a91-c0f1-3f3cea77c65c.htm , https://docs.trellix.com/bundle/nx_10.0.0_smartvision/page/UUID-63ec3f17-f604-209c-6d3d-8beefda6a39a.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247465 https://support.kaspersky.com/kata/7.1/247421	CUMPLE		•Participation in Kaspersky Security Network and use of Kaspersky Private Security Network: https://support.kaspersky.com/kata/7.1/247465 •Managing user-defined IOC rules: https://support.kaspersky.com/kata/7.1/247421	CUMPLE		CUMPLE. DDI Datasheet, p. 1 · DDI AG, p. 299 · DDD, pp. 214–215 Cómo cumple: DDI consulta servicios de reputación Trend Micro e incorpora inteligencia mediante STIX/TAXII, objetos sospechosos y fuentes de terceros para validar IoC en tiempo real.	CUMPLE	
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.	https://support.kaspersky.com/kata/7.1/en-US/247466.htm https://support.kaspersky.com/kata/7.1/en-US/247465.htm https://opentip.kaspersky.com/Help/Doc_data/all-in-one.htm#Licensing	CUMPLE		Propuesta Técnica: pág. 7 (IOC e inteligencia global); pág. 13 "Inteligencia de Amenazas". Fabricante: Trellix Insights permite investigar IOCs e incluye MD5, SHA256, URLs, direcciones IP y hashes de archivo: https://docs.trellix.com/bundle/trellix-insights-product-guide/page/UUID-f40cc14b-cbc9-cbbd-cccb-7b6d2009747a.htm , https://docs.trellix.com/bundle/nx_11.x_sag/page/UUID-60eca20b-09ab-8f88-fe3c-350f96a70538.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247465 https://support.kaspersky.com/kata/7.1/247421	CUMPLE		•Participation in Kaspersky Security Network and use of Kaspersky Private Security Network: https://support.kaspersky.com/kata/7.1/247465 •Managing user-defined IOC rules: https://support.kaspersky.com/kata/7.1/247421	CUMPLE		CUMPLE. DDI AG, p. 299 · DDD, pp. 214–215 Cómo cumple: Deep Discovery Director conserva y distribuye objetos sospechosos, hashes, dominios y URL; agrega inteligencia global y contexto XDR.	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.	https://support.kaspersky.com/kata/7.1/en-US/246848.htm https://opentip.kaspersky.com/Help/Doc_data/all-in-one.htm#Licensing	CUMPLE		Propuesta Técnica: págs. 6-8; pág. 13 "Inteligencia de Amenazas". Fabricante: Trellix Insights permite buscar e investigar campañas, actores e IOCs y visualizar coincidencias/contexto: https://docs.trellix.com/bundle/trellix-insights-product-guide/page/UUID-506e10b0-2000-137a-63cc-cce187e512ed.html , https://docs.trellix.com/bundle/nx_11.x_sag/page/UUID-08fad756-bae5-2962-ab59-6da35be9a399.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247465 https://support.kaspersky.com/kata/7.1/247421	CUMPLE		•Participation in Kaspersky Security Network and use of Kaspersky Private Security Network: https://support.kaspersky.com/kata/7.1/247465 •Managing user-defined IOC rules: https://support.kaspersky.com/kata/7.1/247421	CUMPLE		CUMPLE. DDD, pp. 171–173 y 214–215 Cómo cumple: Deep Discovery Director ofrece gráficos de correlación e Intelligence Reports para consultar relaciones entre indicadores, infraestructura y objetos.	NO CUMPLE	El requerimiento no puede ser verificado con la información suministrada por la empresa, dado que en el ítem 12 se oferta la versión 7.0, mientras que la documentación aportada corresponde a la versión 5.5.

ITEM	DESCRIPCIÓN	UNIÓN TEMPORAL INFO COMUNICACIONES S.A.S - SOLUCIONES EN SEGURIDAD INFORMATICA S.A.S			SONDA DE COLOMBIA S.A.			COINSA S.A.S			GRUPO MICROSISTEMAS COLOMBIA SAS			HEIMCORE		
		UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
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.	https://support.kaspersky.com/kata/7.1/247805 https://support.kaspersky.com/kata/7.1/155163 https://support.kaspersky.com/kata/7.1/247807 https://support.kaspersky.com/help/KSC/16.2/KSCAPI/index.html https://support.kaspersky.com/kedr-expert-on-premise/8.1/211453	CUMPLE		Propuesta Técnica: pág. 8, diagrama de arquitectura (APIs, conectores y mecanismos soportados); pág. 13 “Automatización y Orquestación” e “Integración con el Ecosistema de Seguridad” , https://www.trellix.com/assets/solution-briefs/trellix-hyperautomation-solution-brief.pdf	CUMPLE		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		•Kaspersky Anti Targeted Attack Platform Public API: https://support.kaspersky.com/KATA/7.1/KataAPI/PublicApi-v4.html •Threat Response API: https://support.kaspersky.com/KATA/7.1/en-US/227245.htm •Managing user-defined Intrusion Detection rules: https://support.kaspersky.com/kata/7.1/137926	CUMPLE		CUMPLE. Trend Vision One Sandbox Analysis, web Cómo cumple: Las APIs permiten consultar alertas/telemetría, ejecutar acciones autorizadas y automatizar investigación; Sandbox Analysis recibe archivos y devuelve resultados.	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).	https://support.kaspersky.com/kata/7.1/247805 https://support.kaspersky.com/kata/7.1/155163 https://support.kaspersky.com/kata/7.1/247807	CUMPLE		Propuesta Técnica: pág. 8, diagrama de integración; pág. 13 “Integración con el Ecosistema de Seguridad”. Fabricante: Trellix Network Security soporta ICAP en su Web UI/guía de configuración; referencia oficial de búsqueda de documentación: https://docs.trellix.com/search?labelkey=prod-fe-network-security-v10-x&page=22 , https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-8c200134-b6f4-1c1c-44b0-c5165d599224.html	CUMPLE		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		•Kaspersky Anti Targeted Attack Platform Public API: https://support.kaspersky.com/KATA/7.1/KataAPI/PublicApi-v4.html •Threat Response API: https://support.kaspersky.com/KATA/7.1/en-US/227245.htm •Managing user-defined Intrusion Detection rules: https://support.kaspersky.com/kata/7.1/137926	CUMPLE		CUMPLE. Trend Vision One Sandbox Analysis, web Cómo cumple: La integración se realiza mediante APIs y conectores nativos: DDI envía objetos directamente a Sandbox Analysis, mecanismo equivalente al flujo ICAP solicitado.	CUMPLE	
37	La solución debe soportar el envío de alertas de ciberseguridad y la monitorización de información mediante syslog.	https://support.kaspersky.com/kata/7.1/en-US/247568.htm https://support.kaspersky.com/kata/7.1/en-US/247570.htm https://support.kaspersky.com/kata/7.1/en-US/207166.htm	CUMPLE		Propuesta Técnica: pág. 8, diagrama “Intercambio de eventos (Syslog/CEF)”; pág. 13 “Integración con el Ecosistema de Seguridad”. Fabricante: la familia de seguridad de red Trellix soporta perfiles/notificaciones syslog; referencia oficial: https://docs.trellix.com/bundle/intrusion-prevention-system-11.1.x-product-guide/page/UUID-ed0ef2a1-bf4b-992e-9eff-1d46368e05c3.html. , https://docs.trellix.com/bundle/nx_10.0.0_ips/page/UUID-deb5f26e-fa8b-11b2-e992-d1ad910efc3d.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247568 https://support.kaspersky.com/kata/7.1/247573	CUMPLE		•Configuring integration with an SIEM system: https://support.kaspersky.com/kata/7.1/247568 •Content and properties of syslog messages about detections: https://support.kaspersky.com/kata/7.1/247573 •Sending events, application messages, and audit records to third-party systems: https://support.kaspersky.com/kata/7.1/153523	CUMPLE		CUMPLE. DDI AG, pp. 343–345 Cómo cumple: DDI exporta alertas y registros mediante syslog en CEF, LEEF o formato Trend Micro hacia los sistemas institucionales de monitoreo.	CUMPLE	
38	La solución deberá permitir mecanismos seguros de integración y segmentación entre componentes de la arquitectura, conforme a las políticas de seguridad institucional.	https://support.kaspersky.com/kata/7.1/en-US/247193.htm https://support.kaspersky.com/kata/7.1/en-US/194604.htm	CUMPLE		Propuesta Técnica: pág. 8, arquitectura de referencia e integración; pág. 13 “Integración con el Ecosistema de Seguridad” y “Administración y Gobierno”. Fabricante: Trellix Network Security contempla rutas de administración y acceso seguro a sus interfaces; Management path: https://docs.trellix.com/bundle/nx_11.x_sag/page/UUID-6641b5e5-6eee-401b-c14b-3fe19cc522f5.html. , https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-d20d9dd9-87cc-37d7-d709-b2931aa25e17.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/194604 https://support.kaspersky.com/kata/7.1/252062	CUMPLE		•Architecture of the application: https://support.kaspersky.com/kata/7.1/194604 •Connecting the Sensor component to the Central Node: https://support.kaspersky.com/kata/7.1/252062	CUMPLE		CUMPLE. DDI IDG, pp. 239–241 Cómo cumple: Se separan gestión, monitoreo y servicios mediante VLAN/segmentos, ACL, HTTPS/TLS y únicamente los flujos documentados en la matriz de comunicaciones.	CUMPLE	
39	La solución deberá contar con la capacidad de integrarse con plataformas SIEM y sistemas de gestión de registros.	https://support.kaspersky.com/kata/7.1/247805 https://support.kaspersky.com/kata/7.1/en-US/247570.htm https://support.kaspersky.com/kata/7.1/247807	CUMPLE		Propuesta Técnica: pág. 8, diagrama (Syslog/CEF, integración e interoperabilidad); pág. 13. Fabricante: Trellix Security Platform correlaciona controles y terceros y dispone de consola/operaciones de seguridad: , https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-f056e83a-d9c9-aefb-edc7-7cfcca49df16.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247568 https://support.kaspersky.com/kata/7.1/153523	CUMPLE		•Configuring integration with an SIEM system: https://support.kaspersky.com/kata/7.1/247568 •Sending events, application messages, and audit records to third-party systems: https://support.kaspersky.com/kata/7.1/153523 •Managing connectors: https://support.kaspersky.com/kata/7.1/207166	CUMPLE		CUMPLE. DDI AG, pp. 343–345 Cómo cumple: SolarWinds SEM y cualquier SIEM compatible reciben eventos DDI mediante syslog CEF/LEEF, preservando fecha, severidad, activo e indicador.	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).	https://support.kaspersky.com/kata/7.1/247805 https://support.kaspersky.com/kata/7.1/247807 https://support.kaspersky.com/kedr-expert-on-premise/8.1/211453 https://support.kaspersky.com/kata/7.1/en-US/247570.htm https://support.kaspersky.com/kata/7.1/en-US/247568.htm	CUMPLE		Propuesta Técnica: pág. 13 “Integración con el Ecosistema de Seguridad” declara explícitamente Palo Alto Networks, Kaspersky Endpoint Security y SolarWinds SEM; pág. 8, diagrama de arquitectura , https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-f056e83a-d9c9-aefb-edc7-7cfcca49df16.html	CUMPLE		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		•Kaspersky Anti Targeted Attack Platform Public API: https://support.kaspersky.com/KATA/7.1/KataAPI/PublicApi-v4.html •Configuring integration with an SIEM system: https://support.kaspersky.com/kata/7.1/247568 •Managing connectors: https://support.kaspersky.com/kata/7.1/207166 •Threat Response API: https://support.kaspersky.com/KATA/7.1/en-US/227245.htm	CUMPLE		CUMPLE. DDI AG, pp. 326–327 · DDI AG, pp. 343–345 · Logs de terceros en Vision One, web Cómo cumple: Palo Alto se integra de forma nativa para respuesta; SolarWinds SEM recibe CEF/LEEF; Kaspersky convive con Endpoint Sensor y su interoperabilidad se valida mediante piloto y matriz de exclusiones.	NO CUMPLE	De acuerdo con el ítem 50, la convivencia del agente EDR Kaspersky con el endpoint ofrecido no demuestra por sí sola una integración funcional entre ambas plataformas, ya que esta debería ser validada mediante pruebas piloto.
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.	https://support.kaspersky.com/kata/7.1/en-US/247887.htm https://support.kaspersky.com/kata/7.1/en-US/216715.htm https://support.kaspersky.com/kata/7.1/en-US/247508.htm	CUMPLE		Propuesta Técnica: págs. 6-8 (monitoreo, correlación, detección y alertas); pág. 13 “Monitoreo Inteligente” y “Analítica y Correlación Inteligente”. Fabricante: Trellix Network Security analiza el tráfico recibido en puertos de monitoreo y genera alertas activas agregadas al Central Management System: https://docs.trellix.com/bundle/nx_11.x_sag/page/UUID-a461e037-4c29-c171-100e-5d79f4ab4c7b.html , https://docs.trellix.com/bundle/nx_11.x_sag/page/UUID-e39a6c8d-499c-7598-16f4-7ba87150bbc8.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247494 https://support.kaspersky.com/kata/7.1/247636	CUMPLE		•Central Node component: https://support.kaspersky.com/kata/7.1/247494 •Events database threat hunting: https://support.kaspersky.com/kata/7.1/247636 •Monitoring the receipt and processing of incoming data: https://support.kaspersky.com/kata/7.1/247515 •Monitoring the performance of the application: https://support.kaspersky.com/kata/7.1/247507	CUMPLE		CUMPLE. DDI AG, pp. 56–68 y 184–192 Cómo cumple: Los motores de detección analizan tráfico continuamente y generan alertas en tiempo cercano a real; se configuran umbrales, severidades y notificaciones operativas.	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.	https://support.kaspersky.com/kata/7.1/en-US/247508.htm https://support.kaspersky.com/kata/7.1/en-US/176134.htm https://support.kaspersky.com/kata/7.1/en-US/176554.htm	CUMPLE		Propuesta Técnica: pág. 13 “Monitoreo Inteligente del Tráfico de Red”. Fabricante: Trellix Network Security – Utilization and performance checks indica “Total Bandwidth (Mbps)” sobre puertos de monitoreo https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-9ac6ee37-fa41-217c-7851-f2f280dddbf0.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247494 https://support.kaspersky.com/kata/7.1/247636	CUMPLE		•Central Node component: https://support.kaspersky.com/kata/7.1/247494 •Events database threat hunting: https://support.kaspersky.com/kata/7.1/247636 •Monitoring the receipt and processing of incoming data: https://support.kaspersky.com/kata/7.1/247515 •Monitoring the performance of the application: https://support.kaspersky.com/kata/7.1/247507	CUMPLE		CUMPLE. DDI AG, pp. 56, 62 y 68 Cómo cumple: Los tableros DDI muestran tráfico y ancho de banda monitoreado, interfaces activas, estado de procesamiento y estadísticas por protocolo.	CUMPLE	
43	La solución deberá permitir la generación de reportes personalizables basados en eventos, alertas, incidentes y demás información recopilada por la plataforma.	https://support.kaspersky.com/kata/7.1/247732 https://support.kaspersky.com/kata/7.1/236181 https://support.kaspersky.com/kata/7.1/247734	CUMPLE		Propuesta Técnica: pág. 13 “Analítica y Correlación Inteligente”; pág. 16 “Gestión de informes”. Fabricante: Trellix Network Security appliance dashboard permite generar y programar reportes: https://docs.trellix.com/bundle/nx_11.x_sag/page/UUID-3cec7b44-d79b-24a3-293a-9b439f68cd24.html , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-9ac6ee37-fa41-217c-7851-f2f280dddbf0.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247735	CUMPLE		•Creating a report based on a template: https://support.kaspersky.com/kata/7.1/247735	CUMPLE		CUMPLE. DDI AG, pp. 159–168 Cómo cumple: Se crean reportes personalizados por severidad, evento, activo, protocolo, periodo e indicador, con programación y distribución a responsables.	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.	https://support.kaspersky.com/kata/7.1/247786 https://support.kaspersky.com/kata/7.1/en-US/216715.htm https://support.kaspersky.com/kata/7.1/en-US/247787.htm	CUMPLE		Propuesta Técnica: pág. 13 “Administración y Gobierno de la Plataforma” (alertas); pág. 16, gestión de informes/incidentes. Fabricante: Trellix Network Security – Configuring email recipients: los destinatarios pueden recibir notificaciones de eventos del sistema y reportes programados. https://docs.trellix.com/bundle/nx_11.x_sag/page/UUID-2003bc24-21e6-c051-189a-fe84aef726ed.html , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-9ac6ee37-fa41-217c-7851-f2f280dddbf0.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/153523	CUMPLE		•Sending events, application messages, and audit records to third-party systems: https://support.kaspersky.com/kata/7.1/153523	CUMPLE		CUMPLE. DDI AG, pp. 184–192 · DDD, pp. 343–345 Cómo cumple: Se configuran destinatarios, severidades y condiciones para envío automático de alertas por correo a administradores y responsables de incidentes.	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.	https://support.kaspersky.com/kata/7.1/en-US/247787.htm https://support.kaspersky.com/kata/7.1/en-US/247585.htm https://support.kaspersky.com/kata/7.1/en-US/216715.htm	CUMPLE		Propuesta Técnica: págs. 6-8 (analítica comportamental, correlación, movimientos laterales, amenazas); pág. 13 “Analítica y Correlación Inteligente” , https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-a3fdcef4-5c87-41fc-4916-be44ceef520f.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247494 https://support.kaspersky.com/kata/7.1/247636	CUMPLE		•Central Node component: https://support.kaspersky.com/kata/7.1/247494 •Events database threat hunting: https://support.kaspersky.com/kata/7.1/247636 •Monitoring the performance of the application: https://support.kaspersky.com/kata/7.1/247507 •Events database threat hunting: https://support.kaspersky.com/kata/7.1/247636	CUMPLE		CUMPLE. DDD, pp. 79–123 y 171–173 Cómo cumple: La solución correlaciona actividad interna, conexiones externas, C&C, movimiento lateral, activos y endpoint para identificar amenazas internas y externas.	CUMPLE	
46	La solución debe tener la capacidad de crear informes ejecutivos diarios, semanales y mensuales y permitir la exportación de informes.	https://support.kaspersky.com/kata/7.1/247732 https://support.kaspersky.com/kata/7.1/247734 https://support.kaspersky.com/kata/7.1/en-US/247735.htm https://support.kaspersky.com/kata/7.1/en-US/247733.htm	CUMPLE		Propuesta Técnica: pág. 16 “Gestión de informes”. Fabricante: Trellix Network Security appliance dashboard permite generar reportes individuales y programarlos hourly, daily, weekly o monthly: https://docs.trellix.com/bundle/nx_11.x_sag/page/UUID-3cec7b44-d79b-24a3-293a-9b439f68cd24.html. , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-9ac6ee37-fa41-217c-7851-f2f280dddbf0.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247735	CUMPLE		•Creating a report based on a template: https://support.kaspersky.com/kata/7.1/247735	CUMPLE		CUMPLE. DDI AG, pp. 159–168 Cómo cumple: Los reportes ejecutivos se programan con periodicidad diaria, semanal y mensual y se exportan desde la consola para entrega y archivo.	CUMPLE	

ITEM	DESCRIPCIÓN	UNIÓN TEMPORAL INFO COMUNICACIONES S.A.S - SOLUCIONES EN SEGURIDAD INFORMATICA S.A.S			SONDA DE COLOMBIA S.A.			COINSA S.A.S			GRUPO MICROSISTEMAS COLOMBIA SAS			HEIMCORE		
		UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
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.	https://support.kaspersky.com/kata/7.1/en-US/247583.htm https://support.kaspersky.com/kata/7.1/en-US/247513.htm https://support.kaspersky.com/kata/7.1/en-US/247887.htm	CUMPLE		Propuesta Técnica: pág. 13 “Analítica y Correlación Inteligente”; pág. 8, arquitectura centralizada. Fabricante: Trellix Network Security – Custom dashboards permite crear dashboards personales con widgets y periodos configurables: https://docs.trellix.com/bundle/nx_11.x_sag/page/UUID-94218be7-7898-8e5c-100e-dbe9e104db7b.html , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-9ac6ee37-fa41-217c-7851-f2f280dddbf0.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247494 https://support.kaspersky.com/kata/7.1/247636	CUMPLE		•Central Node component: https://support.kaspersky.com/kata/7.1/247494 •Events database threat hunting: https://support.kaspersky.com/kata/7.1/247636 •Monitoring the performance of the application: https://support.kaspersky.com/kata/7.1/247507 •Events database threat hunting: https://support.kaspersky.com/kata/7.1/247636	CUMPLE		CUMPLE. DDI AG, pp. 56–68 · DDD, pp. 79–123 Cómo cumple: DDI, Deep Discovery Director ofrece paneles de eventos, salud, tráfico, IoC, activos, alertas, MITRE y resultados de Sandbox Analysis.	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.	https://support.kaspersky.com/help/KESWin/12.5/en-US/236497.htm https://support.kaspersky.com/help/KESWin/12.5/en-US/236470.htm https://support.kaspersky.com/kata/7.1/247334	CUMPLE		Propuesta Técnica: pág. 6 (visibilidad sobre 400 endpoints estratégicos); págs. 7-8 (correlación centralizada); págs. 12-13, numeral 4.1.6 “Visibilidad sobre 400 Endpoints Estratégicos , https://www.trellix.com/assets/solution-briefs/trellix-hyperautomation-solution-brief.pdf https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-35ae97d9-8a1d-52c2-0f6e-6c5cf4e04ccf.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/219777 https://support.kaspersky.com/kata/7.1/247325	CUMPLE		•Configuring integration of the Endpoint Agent component with the NDR functional block: https://support.kaspersky.com/kata/7.1/219777 •Configuring integration of the Endpoint Agent component with the KEDR functional block: https://support.kaspersky.com/kata/7.1/247325 •Central Node component: https://support.kaspersky.com/kata/7.1/247494	CUMPLE		CUMPLE. Endpoint Security, pp. 1–3 · Endpoint Sensor: datos recolectados, web · Conexión directa DDI–Trend Vision One, web Cómo cumple: Se habilitan 4.000 Endpoint Sensors para complementar el NDR en usuarios remotos, tráfico cifrado y segmentos no instrumentados, con análisis central.	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	https://support.kaspersky.com/kata/7.1/247334 https://support.kaspersky.com/help/KESWin/12.5/en-US/236497.htm https://support.kaspersky.com/kata/7.1/269820	CUMPLE		Propuesta Técnica: pág. 6 declara cuatrocientos (400) endpoints estratégicos; pág. 13 “Visibilidad sobre 400 Endpoints Estratégicos”. Fabricante: Trellix HX aporta visibilidad/búsqueda sobre endpoints y generación de alertas/IOC: , https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-f056e83a-d9c9-aefb-edc7-7cfcca49df16.html	NO CUMPLE	El requerimiento no se puede verificar con la información adjuntada por la empresa	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247325 https://support.kaspersky.com/kata/7.1/219777	CUMPLE		•Configuring integration of Endpoint Agent with the KEDR functional block: https://support.kaspersky.com/kata/7.1/247325 •Configuring integration of Endpoint Agent with the NDR functional block: https://support.kaspersky.com/kata/7.1/219777 •Compatibility of Kaspersky Endpoint Security for Windows with KATA: https://support.kaspersky.com/kata/7.1/246849	CUMPLE		CUMPLE. Endpoint Security, pp. 2–3 · Endpoint Sensor: datos recolectados, web Cómo cumple: La oferta supera el mínimo de 400 y licencia 4.000 endpoints. El sensor recolecta contexto de procesos, archivos, usuarios y actividad con bajo impacto y envío seguro.	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.	https://support.kaspersky.com/help/KESWin/12.5/en-US/236470.htm https://support.kaspersky.com/kata/7.1/246849	CUMPLE		Propuesta Técnica: pág. 13 “Integración con el Ecosistema de Seguridad” , https://docs.trellix.com/bundle/trellix_hyperautomation/page/UUID-c7c720ab-7009-2fdd-6c61-815dab39466f.html	NO CUMPLE	El requerimiento no se puede verificar con la información adjuntada por la empresa	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247325 https://support.kaspersky.com/kata/7.1/219777	CUMPLE		•Configuring integration of Endpoint Agent with the KEDR functional block: https://support.kaspersky.com/kata/7.1/247325 •Configuring integration of Endpoint Agent with the NDR functional block: https://support.kaspersky.com/kata/7.1/219777 •Compatibility of Kaspersky Endpoint Security for Windows with KATA: https://support.kaspersky.com/kata/7.1/246849 •Compatibility of Kaspersky Endpoint Security for Linux with KATA: https://support.kaspersky.com/kata/7.1/247128 •Compatibility of Kaspersky Endpoint Security for Mac with KATA: https://support.kaspersky.com/kata/7.1/252759	CUMPLE		CUMPLE. Endpoint Security, pp. 2–3 Cómo cumple: Se ejecuta un piloto de convivencia con Kaspersky EDR, se definen exclusiones mutuas y se despliega progresivamente el Endpoint Sensor sin desactivar la protección institucional.	NO CUMPLE	Aunque un piloto puede ser adecuado, este no constituye por sí mismo evidencia verificable de que el requisito se cumpla al momento de la evaluación, por lo que no permite determinar de manera objetiva si, a futuro, existirá una adecuada coexistencia y compatibilidad entre el EDR Kaspersky actualmente implementado y la solución ofrecida. Adicionalmente, debido al cronograma del proceso, no resulta viable la ejecución de pilotos durante la etapa de evaluación, teniendo en cuenta que, una vez adjudicado el contrato, se dará inicio al proceso de implementación y no de pruebas.
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.	https://support.kaspersky.com/kata/7.1/en-US/247695.htm https://support.kaspersky.com/kata/7.1/en-US/137926.htm https://support.kaspersky.com/kata/7.1/en-US/247430.htm	CUMPLE		Propuesta Técnica: pág. 9, numeral 3.2.1 (Configuración y Parametrización: políticas y reglas de detección); pág. 13, numeral 4.1.6. Fabricante: Trellix Network Security soporta custom rules para malware analysis: , https://docs.trellix.com/bundle/nx_10.x_ug/page/UUID-e086f629-e9a2-2ce5-f3ac-13e734f4e0bd.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/137926 https://support.kaspersky.com/kata/7.1/247702	CUMPLE		•Managing user-defined Intrusion Detection rules: https://support.kaspersky.com/kata/7.1/137926 •Importing TAA (IOA) rules: https://support.kaspersky.com/kata/7.1/247702 •Managing user-defined IOC rules: https://support.kaspersky.com/kata/7.1/247421	CUMPLE		CUMPLE. DDI AG, pp. 263–264 · DDD, pp. 214–215 Cómo cumple: Se utilizan reglas configurables, YARA, STIX/TAXII, objetos sospechosos e inteligencia personalizada para ampliar la detección sobre tráfico, comportamiento y artefactos.	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	https://support.kaspersky.com/kata/7.1/en-US/176763.htm https://support.kaspersky.com/kata/7.1/en-US/247484.htm https://support.kaspersky.com/kata/7.1/en-US/247488.htm https://support.kaspersky.com/kata/7.1/en-US/181470.htm	CUMPLE		Propuesta Técnica: págs. 6-8 (investigación, análisis avanzado e inteligencia); pág. 13 “Investigación Forense” e “Inteligencia de Amenazas”. Fabricante: IVX realiza análisis dinámico, signature-less, en entorno seguro y detecta zero-day/multiflow/evasión , https://www.trellix.com/assets/docs/data-sheets/trellix-network-security-datasheet.pdf	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247495 https://support.kaspersky.com/kata/7.1/247475	CUMPLE		•Sandbox component: https://support.kaspersky.com/kata/7.1/247495 •Configuring connection between the Sandbox and Central Node components: https://support.kaspersky.com/kata/7.1/247475	CUMPLE		CUMPLE. Trend Vision One Sandbox Analysis, web Cómo cumple: Los DDI identifican objetos sospechosos y los envían automáticamente a Sandbox Analysis; el veredicto, comportamiento e IoC enriquecen la detección original.	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.	https://support.kaspersky.com/kata/7.1/283632 https://support.kaspersky.com/kata/7.1/en-US/266038.htm https://support.kaspersky.com/kedr-expert-on-premise/8.1/298639	CUMPLE		Propuesta Técnica: pág. 6 (400 endpoints estratégicos); pág. 7 (telemetría de endpoints); pág. 13 “Visibilidad sobre 400 Endpoints Estratégicos” , https://docs.trellix.com/bundle/helixconnect_ig/page/UUID-2cedcf4d-a4a6-b2bc-c2a1-630c01998f23.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247325 https://support.kaspersky.com/kata/7.1/219777	CUMPLE		•Configuring integration of the Endpoint Agent component with the KEDR functional block: https://support.kaspersky.com/kata/7.1/247325 •Configuring integration of the Endpoint Agent component with the NDR functional block: https://support.kaspersky.com/kata/7.1/219777	CUMPLE		CUMPLE. Endpoint Sensor: datos recolectados, web · Endpoint Security, pp. 2–3 Cómo cumple: Los Endpoint Sensors recolectan equipo, usuario, proceso, línea de comandos, archivo, ruta, URL, registro y eventos relevantes para correlación con el NDR.	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.	https://support.kaspersky.com/kata/7.1/en-US/134912.htm https://support.kaspersky.com/kata/7.1/en-US/196705.htm https://support.kaspersky.com/kata/7.1/en-US/247887.htm https://support.kaspersky.com/kedr-expert-on-premise/8.1/298639	CUMPLE		Propuesta Técnica: págs. 6-8 (correlación de red y endpoints, movimientos laterales y visión integral); pág. 13 “Analítica y Correlación Inteligente” , https://docs.trellix.com/es-ES/bundle/helix_pg/page/UUID-ade143dd-0b3d-813a-3b9d-bbc62dd54486.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/176734	CUMPLE		•Working with the network interaction map: https://support.kaspersky.com/kata/7.1/176734	CUMPLE		CUMPLE. XDR for Networks, pp. 1–2 · DDD, pp. 171–173 · Conexión directa DDI–Trend Vision One, web Cómo cumple: La solución correlaciona red y endpoint en el Workbench y representa relaciones entre activos, alertas, objetos y etapas del ataque	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.	https://support.kaspersky.com/kata/7.1/247805 https://support.kaspersky.com/kata/7.1/247807 https://support.kaspersky.com/kata/7.1/en-US/247887.htm https://support.kaspersky.com/kedr-expert-on-premise/8.1/211453	CUMPLE		Propuesta Técnica: pág. 7 (información proveniente de red, endpoints y diferentes fuentes de seguridad); pág. 8, diagrama de integraciones; pág. 13 “Integración con el Ecosistema de Seguridad”. , https://docs.trellix.com/bundle/trellix_hyperautomation/page/UUID-688bc5d4-2b19-01c8-7920-4d615d07a864.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/207166 https://support.kaspersky.com/KATA/7.1/KataAPI/PublicApi-v4.html	CUMPLE		•Managing connectors: https://support.kaspersky.com/kata/7.1/207166 •Kaspersky Anti Targeted Attack Platform Public API: https://support.kaspersky.com/KATA/7.1/KataAPI/PublicApi-v4.html	CUMPLE		CUMPLE. Logs de terceros en Vision One, web · Endpoint Security, p. 2 · Conexión directa DDI–Trend Vision One, web Cómo cumple: La solución admite fuentes y registros de terceros; durante la implementación se habilitan los conectores definidos en la matriz de integración institucional.	CUMPLE	
56	La solución deberá permitir la búsqueda, consulta y correlación de indicadores de compromiso (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/en-US/247887.htm https://support.kaspersky.com/kata/7.1/247585 https://support.kaspersky.com/kedr-expert-on-premise/8.1/211453	CUMPLE		Propuesta Técnica: pág. 7 (IOC, inteligencia global, MITRE ATT&CK); pág. 13 “Inteligencia de Amenazas” e “Investigación Forense”. Fabricante , https://docs.trellix.com/es-ES/bundle/helix_pg/page/UUID-ade143dd-0b3d-813a-3b9d-bbc62dd54486.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247421 https://support.kaspersky.com/kata/7.1/247636	CUMPLE		•Managing user-defined IOC rules: https://support.kaspersky.com/kata/7.1/247421 •Events database threat hunting: https://support.kaspersky.com/kata/7.1/247636	CUMPLE		CUMPLE. DDD, pp. 113–131 y 171–173 · APIs de alertas y eventos, web · Conexión directa DDI–Trend Vision One, web Cómo cumple: Los analistas buscan IoC y objetos sospechosos sobre telemetría de red y endpoint mediante Data Explorer, Workbench, detecciones DDI y APIs.	CUMPLE	
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.	https://support.kaspersky.com/kata/7.1/en-US/247887.htm https://support.kaspersky.com/kata/7.1/247585 https://support.kaspersky.com/kata/7.1/en-US/247583.htm	CUMPLE		Propuesta Técnica: pág. 13 “Investigación Forense y Búsqueda Avanzada” , https://docs.trellix.com/bundle/iocs_1-3-166_ug/page/UUID-787e58d2-a91b-88e0-43df-40e44b9ac097.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247637 https://support.kaspersky.com/kata/7.1/247636	CUMPLE		•Searching for events in source code mode: https://support.kaspersky.com/kata/7.1/247637 •Events database threat hunting: https://support.kaspersky.com/kata/7.1/247636 •Searching network packets: https://support.kaspersky.com/kata/7.1/292608	CUMPLE		CUMPLE. DDD, pp. 113–131 y 171–173 · Trend Vision One Automation Center, web · Conexión directa DDI–Trend Vision One, web Cómo cumple: Data Explorer y las vistas de investigación permiten consultas por tiempo, activo, IP, dominio, URL, hash, proceso, usuario, severidad y producto de origen.	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).	https://support.kaspersky.com/kata/7.1/en-US/247484.htm https://support.kaspersky.com/kata/7.1/en-US/247887.htm https://support.kaspersky.com/kata/7.1/en-US/247193.htm	CUMPLE		Propuesta Técnica: pág. 6 (comunicaciones maliciosas y movimientos laterales); pág. 7 (amenazas avanzadas); pág. 13 “Monitoreo Inteligente”. Fabricante , https://docs.trellix.com/bundle/nx_10.0.0_smartvision/page/UUID-e7459fa2-e134-6bf9-490a-b33f4c51cba7.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/137926 https://support.kaspersky.com/kata/7.1/247421	CUMPLE		•Managing user-defined Intrusion Detection rules: https://support.kaspersky.com/kata/7.1/137926 •Managing user-defined IOC rules: https://support.kaspersky.com/kata/7.1/247421 •Searching network packets: https://support.kaspersky.com/kata/7.1/292608	CUMPLE		CUMPLE. DDI Datasheet, p. 1 · DDI AG, pp. 23–27 Cómo cumple: DDI identifica conexiones C&C conocidas y desconocidas mediante reputación, patrones, comportamiento, aprendizaje automático e inteligencia correlacionada.	CUMPLE	
59	Las alertas generadas deben enriquecerse automáticamente con información contextual relevante como descripciones, clasificación de amenazas y otros datos que faciliten el análisis.	https://support.kaspersky.com/kata/7.1/en-US/247887.htm https://support.kaspersky.com/kata/7.1/247585 https://support.kaspersky.com/kata/7.1/en-US/247484.htm	CUMPLE		Propuesta Técnica: pág. 7 (enriquecimiento mediante inteligencia global, IOC y MITRE ATT&CK); pág. 13 “Inteligencia de Amenazas”. Fabricante , https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-10042859-4a01-393c-b553-39531146ea37.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/216715 https://support.kaspersky.com/kata/7.1	CUMPLE		•General information about an alert of any type: https://support.kaspersky.com/kata/7.1/216715 •Kaspersky Anti Targeted Attack Platform 7.1 Help - Viewing alert details: https://support.kaspersky.com/kata/7.1	CUMPLE		CUMPLE. DDI AG, pp. 85–97 y 134–145 Cómo cumple: Cada detección presenta descripción, severidad, activo afectado, conexiones, archivos, objetos, mitigación, MITRE y evidencia disponible.	CUMPLE	

ITEM	DESCRIPCIÓN	UNIÓN TEMPORAL INFO COMUNICACIONES S.A.S - SOLUCIONES EN SEGURIDAD INFORMATICA S.A.S			SONDA DE COLOMBIA S.A.			COINSA S.A.S			GRUPO MICROSISTEMAS COLOMBIA SAS			HEIMCORE		
		UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
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.	https://support.kaspersky.com/kata/7.1/en-US/283691.htm https://support.kaspersky.com/kata/7.1/en-US/247583.htm https://support.kaspersky.com/kata/7.1/en-US/247887.htm https://support.kaspersky.com/kata/7.1/en-US/247193.htm	CUMPLE		Propuesta Técnica: pág. 13 "Administración y Gobierno de la Plataforma" y capacidades de monitoreo. , https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-62202359-7f58-5fac-01c4-4080e26c7c77.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/188133 https://support.kaspersky.com/kata/7.1/175616	CUMPLE		•Adding and removing device labels: https://support.kaspersky.com/kata/7.1/188133 •Viewing the table of devices: https://support.kaspersky.com/kata/7.1/175616	CUMPLE		CUMPLE. DDI AG, pp. 268–269 Cómo cumple: Se crean Network Groups y etiquetas para diferenciar sedes, segmentos, criticidad y tipos de activo en reportes e investigaciones.	CUMPLE	
61	Las alertas y eventos generados deberán mapearse, cuando aplique, a tácticas, técnicas y procedimientos (TTP) de la matriz MITRE ATT&CK.	https://support.kaspersky.com/kata/7.1/en-US/272427.htm https://support.kaspersky.com/kata/7.1/247585 https://support.kaspersky.com/kata/7.1/en-US/247484.htm	CUMPLE		Propuesta Técnica: pág. 7 declara MITRE ATT&CK; pág. 8, arquitectura; pág. 13. Fabricante , https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-771b724b-87d5-65b4-dc3a-6b77beade20a.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/249034	CUMPLE		•Event search criteria: https://support.kaspersky.com/kata/7.1/249034	CUMPLE		CUMPLE. DDI AG, pp. 88, 94, 136 y 142 · DDD, pp. 27–28 Cómo cumple: Las detecciones aplicables se mapean a tácticas y técnicas MITRE ATT&CK en DDI, Deep Discovery Director.	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.	https://support.kaspersky.com/kata/7.1/247781 https://support.kaspersky.com/kata/7.1/247643_1 https://support.kaspersky.com/kata/7.1/247420 https://support.kaspersky.com/KATA/7.1/en-US/247421.htm https://support.kaspersky.com/KATA/7.1/en-US/247428.htm	CUMPLE		Propuesta Técnica: pág. 7 (IOC); pág. 13 "Inteligencia de Amenazas" y "Automatización y Orquestación" , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-23de1256-929a-49fc-60fe-1c983e211bac.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247421 https://support.kaspersky.com/kata/7.1/247702	CUMPLE		•Managing user-defined IOC rules: https://support.kaspersky.com/kata/7.1/247421 •Importing TAA (IOA) rules: https://support.kaspersky.com/kata/7.1/247702	CUMPLE		CUMPLE. DDD, pp. 214–215 · DDI AG, pp. 263–264 y 299 Cómo cumple: Los IoC personalizados se incorporan como objetos sospechosos/STIX-TAXII y las reglas YARA se aplican al análisis de artefactos; los IOA se administran desde la analítica XDR.	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 no limitándose a, malware, ransomware y otros tipos de actividades maliciosas que evaden los controles de seguridad tradicionales.	https://support.kaspersky.com/kata/7.1/en-US/247887.htm https://support.kaspersky.com/kata/7.1/en-US/247193.htm https://support.kaspersky.com/kata/7.1/en-US/246848.htm https://support.kaspersky.com/kata/7.1/en-US/247176.htm https://support.kaspersky.com/kata/7.1/en-US/176763.htm	CUMPLE		Propuesta Técnica: págs. 6-7 (amenazas conocidas/desconocidas, analítica comportamental, amenazas avanzadas); pág. 13. Fabricante: IVX detecta zero-day, multiflow y ataques evasivos mediante análisis dinámico sin firmas: , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-8e73bf06-fadf-e224-8795-cae94e69a368.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247495 https://support.kaspersky.com/kata/7.1/247465	CUMPLE		•Sandbox component: https://support.kaspersky.com/kata/7.1/247495 •Participation in Kaspersky Security Network and use of Kaspersky Private Security Network: https://support.kaspersky.com/kata/7.1/247465	CUMPLE		CUMPLE. DDI Datasheet, p. 1 · DDI AG, pp. 23–27 · Integración de DDI con Sandbox Analysis, web Cómo cumple: DDI combina reputación, heurística, patrones, aprendizaje automático y Sandbox Analysis para detectar zero-day, APT, ransomware, malware avanzado y evasión.	CUMPLE	
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.	https://support.kaspersky.com/kata/7.1/en-US/176763.htm https://support.kaspersky.com/kata/7.1/en-US/246848.htm https://support.kaspersky.com/kata/7.1/en-US/247176.htm https://support.kaspersky.com/kata/7.1/en-US/247484.htm https://support.kaspersky.com/kata/7.1/en-US/247887.htm	CUMPLE		Propuesta Técnica: págs. 6-7; pág. 13 "Monitoreo Inteligente" e "Inteligencia de Amenazas". Fabricante: IVX engine proporciona análisis dinámico signature-less y detecta zero-day/multiflow/evasive attacks: https://docs.trellix.com/bundle/intrusion-prevention-system-11.1.x-product-guide/page/UUID-b4e4f438-af02-fb20-760e-6d2e0d6fd53a.html , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-8e73bf06-fadf-e224-8795-cae94e69a368.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247495 https://support.kaspersky.com/kata/7.1/247465	CUMPLE		•Sandbox component: https://support.kaspersky.com/kata/7.1/247495 •Participation in Kaspersky Security Network and use of Kaspersky Private Security Network: https://support.kaspersky.com/kata/7.1/247465	CUMPLE		CUMPLE. Trend Vision One Sandbox Analysis, web Cómo cumple: Los objetos desconocidos se inspeccionan estática y dinámicamente en Sandbox Analysis, generando veredictos y alertas sin depender únicamente de firmas.	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.	https://support.kaspersky.com/kata/7.1/en-US/247176.htm https://support.kaspersky.com/kata/7.1/en-US/247193.htm https://support.kaspersky.com/kata/7.1/en-US/247484.htm https://support.kaspersky.com/kata/7.1/en-US/176763.htm	CUMPLE		Propuesta Técnica: págs. 6-8; pág. 13 "Investigación Forense y Búsqueda Avanzada". Fabricante: IVX guest images permiten detonar malware en un entorno controlado donde no puede dañar activos: https://docs.trellix.com/bundle/ivx_10.x_sag/page/UUID-d34ba141-9a0d-9cb1-7f10-187f9ed6aa7f.html ; , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-adc83507-3c64-5294-2ce8-4ee8d794747d.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247495 https://support.kaspersky.com/kata/7.1/159685	CUMPLE		•Sandbox component: https://support.kaspersky.com/kata/7.1/247495 •Managing the Sandbox component through the web interface: https://support.kaspersky.com/kata/7.1/159685	CUMPLE		CUMPLE. Trend Vision One Sandbox Analysis, web Cómo cumple: DDI extrae artefactos del tráfico y los remite a Sandbox Analysis, que ejecuta las muestras en entornos controlados y devuelve el análisis a la consola central.	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.	https://support.kaspersky.com/kata/7.1/en-US/246848.htm https://support.kaspersky.com/kata/7.1/en-US/247887.htm https://support.kaspersky.com/kata/7.1/en-US/266038.htm https://support.kaspersky.com/kata/7.1/en-US/247334.htm https://support.kaspersky.com/help/KESWin/12.12/en-US/236862.htm	CUMPLE		Propuesta Técnica: págs. 6-7 (NX + 400 endpoints + correlación); pág. 13. Fabricante: EDRF Historical Search recolecta procesos, archivos/registro, DNS y conexiones: https://docs.trellix.com/bundle/endsec-edrf-docs/page/UUID-98a84779-ac14-ed95-a83b-c5de74bb2d4f.html ; , https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-d20d9dd9-87cc-37d7-d709-b2931aa25e17.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247493 https://support.kaspersky.com/kata/7.1/247325	CUMPLE		•Sensor component: https://support.kaspersky.com/kata/7.1/247493 •Configuring integration of Endpoint Agent with the KEDR functional block: https://support.kaspersky.com/kata/7.1/247325	CUMPLE		CUMPLE. Endpoint Sensor: datos recolectados, web · XDR for Networks, pp. 1–2 · Conexión directa DDI–Trend Vision One, web Cómo cumple: La telemetría de los DDI y de los 4.000 Endpoint Sensors se centraliza y correlaciona para aportar comportamiento, IoC y contexto de los activos.	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.	https://support.kaspersky.com/kata/7.1/en-US/247334.htm https://support.kaspersky.com/kedr-expert-on-premise/8.1/211453 https://support.kaspersky.com/help/KESWin/12.12/en-US/257252.htm https://support.kaspersky.com/help/KESWin/12.12/en-US/236470.htm	CUMPLE		Propuesta Técnica: pág. 8, arquitectura de referencia; pág. 13 "Integración con el Ecosistema de Seguridad". Fabricante: IVX acepta submissions desde endpoints y herramientas NDR; T , https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-9ded1756-65aa-374b-8644-93eea14e28e0.html	NO CUMPLE	El requerimiento no se puede verificar con la información adjuntada por la empresa	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247325 https://support.kaspersky.com/kata/7.1/219777	CUMPLE		•Configuring integration of Endpoint Agent with the KEDR functional block: https://support.kaspersky.com/kata/7.1/247325 •Configuring integration of Endpoint Agent with the NDR functional block: https://support.kaspersky.com/kata/7.1/219777 •Configuring connection between the Sandbox and Central Node components: https://support.kaspersky.com/kata/7.1/247475	CUMPLE		CUMPLE. Trend Vision One Sandbox Analysis, web Cómo cumple: La solución recibe objetos sospechosos desde DDI y Endpoint Sensor y los somete a Sandbox Analysis mediante conectores y flujos nativos.	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.	https://support.kaspersky.com/kata/7.1/en-US/176763.htm https://support.kaspersky.com/kata/7.1/en-US/247484.htm https://support.kaspersky.com/kata/7.1/en-US/247887.htm https://support.kaspersky.com/kata/7.1/en-US/181470.htm	CUMPLE		Propuesta Técnica: pág. 7 (investigación forense, IOC y contexto); pág. 13 "Investigación Forense". Fabricante: IVX Web UI permite revisar detailed reports de análisis: https://docs.trellix.com/bundle/11.x_sag/page/UUID-9f97ea4b-7d0b-7687-4d3c-9d88d927679e.html , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-bf98fd6e-60c8-c057-7505-48479b980e9c.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/159685	CUMPLE		•Managing the Sandbox component through the web interface: https://support.kaspersky.com/kata/7.1/159685	CUMPLE		CUMPLE. Trend Vision One Sandbox Analysis, web Cómo cumple: Sandbox Analysis entrega procesos, archivos modificados, comunicaciones, DNS, URL, comportamiento, capturas, IoC y clasificación de la muestra.	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.	https://support.kaspersky.com/kata/7.1/en-US/176763.htm https://support.kaspersky.com/kata/7.1/en-US/247176.htm https://support.kaspersky.com/kata/7.1/en-US/247193.htm	CUMPLE		Propuesta Técnica: pág. 8, arquitectura centralizada; pág. 13. Fabricante: IVX cluster deployment soporta compute nodes compartidos y múltiples appliances , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-348d97e6-bf7a-8d8e-b112-4988dd192071.html	NO CUMPLE	El requerimiento no se puede verificar con la información adjuntada por la empresa	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247475 https://support.kaspersky.com/kata/7.1/247179	CUMPLE		•Configuring connection between the Sandbox and Central Node components: https://support.kaspersky.com/kata/7.1/247475 •Scenario of deployment on four or more servers: https://support.kaspersky.com/kata/7.1/247179	CUMPLE		CUMPLE. Trend Vision One Sandbox Analysis, web Cómo cumple: El servicio central de Sandbox Analysis es utilizado por los DDI de Calle 40 y Bosa Porvenir y por los flujos autorizados de endpoint.	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 de comportamientos, reputación o descarga de componentes requeridos para el análisis.	https://support.kaspersky.com/kata/7.1/en-US/246848.htm https://support.kaspersky.com/help/KATA/7.1/en-US/247577.htm https://support.kaspersky.com/help/KATA/7.1/en-US/247479.htm https://support.kaspersky.com/help/KATA/7.1/en-US/161840.htm	CUMPLE		Propuesta Técnica: pág. 8, inteligencia de amenazas e integración; pág. 13. , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-7858f86e-385a-8f9a-822d-22ebf8c6fb76.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/159685 https://support.kaspersky.com/kata/7.1	CUMPLE		•Managing the Sandbox component through the web interface: https://support.kaspersky.com/kata/7.1/159685 •Kaspersky Anti Targeted Attack Platform 7.1 Help - Configuring a network interface used for Internet access of processed objects: https://support.kaspersky.com/kata/7.1	CUMPLE		CUMPLE. Trend Vision One Sandbox Analysis, web Cómo cumple: Las conexiones externas del sandbox se controlan por la plataforma y permiten resolver DNS, consultar reputación y descargar componentes necesarios para observar el comportamiento.	CUMPLE	
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.	https://support.kaspersky.com/kata/7.1/en-US/246848.htm https://support.kaspersky.com/kata/7.1/en-US/247484.htm https://support.kaspersky.com/kata/7.1/en-US/176763.htm https://support.kaspersky.com/kata/7.1/en-US/181470.htm	CUMPLE		Propuesta Técnica: págs. 6-7 (analítica avanzada e investigación); pág. 13. Fabricante: IVX realiza análisis dinámico en entorno seguro y signature-less: https://docs.trellix.com/bundle/intrusion-prevention-system-11.1.x-product-guide/page/UUID-b4e4f438-af02-fb20-760e-6d2e0d6fd53a.html , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-50cf1629-b04c-3b1f-a587-7fc96c84a7e2.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/159685 https://support.kaspersky.com/kata/7.1/247779	CUMPLE		•Managing the Sandbox component through the web interface: https://support.kaspersky.com/kata/7.1/159685 •Managing TAA exclusions: https://support.kaspersky.com/kata/7.1/247779	CUMPLE		CUMPLE. Trend Vision One Sandbox Analysis, web Cómo cumple: Sandbox Analysis ejecuta dinámicamente las muestras y utiliza interacción/emulación controlada para activar y observar comportamientos sospechosos.	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	https://support.kaspersky.com/kata/7.1/en-US/176763.htm https://support.kaspersky.com/kata/7.1/en-US/181470.htm https://support.kaspersky.com/kata/7.1/en-US/181471.htm https://support.kaspersky.com/kata/7.1/en-US/181469.htm https://support.kaspersky.com/kata/7.1/247484	CUMPLE		Propuesta Técnica: no evidencia este nivel de detalle. Fabricante: IVX soporta múltiples tipos de archivo para análisis estático/dinámico: https://docs.trellix.com/bundle/11.x_sag/page/UUID-a9e18256-3162-b4f9-2e70-62c40eceb551.html. , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-fc8c1262-5b2f-273c-1d45-4bf952e99f58.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247580 https://support.kaspersky.com/kata/7.1/159685	CUMPLE		•Creating a list of passwords for archives: https://support.kaspersky.com/kata/7.1/247580 •Managing the Sandbox component through the web interface: https://support.kaspersky.com/kata/7.1/159685	CUMPLE		CUMPLE. Trend Vision One Sandbox Analysis, web Cómo cumple: Se configuran contraseñas conocidas para desempaquetado y se analizan documentos Office, ejecutables, scripts, archivos comprimidos y demás formatos soportados.	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.	https://support.kaspersky.com/kata/7.1/en-US/246848.htm https://support.kaspersky.com/kata/7.1/en-US/181470.htm https://support.kaspersky.com/kata/7.1/en-US/176763.htm https://support.kaspersky.com/KATA/7.1/en-US/245731.htm https://www.kaspersky.com/enterprise-security/wiki-section/products/sandbox	CUMPLE		Propuesta Técnica: págs. 6-7 (amenazas avanzadas/desconocidas); pág. 13. Fabricante: IVX está diseñado para detectar ataques evasivos mediante análisis dinámico sin firmas: https://docs.trellix.com/bundle/intrusion-prevention-system-11.1.x-product-guide/page/UUID-b4e4f438-af02-fb20-760e-6d2e0d6fd53a.html , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-50cf1629-b04c-3b1f-a587-7fc96c84a7e2.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247495 https://support.kaspersky.com/kata/7.1/159685	CUMPLE		•Sandbox component: https://support.kaspersky.com/kata/7.1/247495 •Managing the Sandbox component through the web interface: https://support.kaspersky.com/kata/7.1/159685 •Kaspersky Anti Targeted Attack 7.0 Technical presentation.pdf	CUMPLE		CUMPLE. Trend Vision One Sandbox Analysis, web Cómo cumple: Los entornos de análisis, imágenes y técnicas de observación de comportamiento están diseñados para detectar muestras que intentan identificar o evadir el sandbox.	CUMPLE	

ITEM	DESCRIPCIÓN	UNIÓN TEMPORAL INFO COMUNICACIONES S.A.S - SOLUCIONES EN SEGURIDAD INFORMATICA S.A.S		
		UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
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.	https://support.kaspersky.com/kata/7.1/en-US/181471.htm https://support.kaspersky.com/kata/7.1/en-US/247887.htm https://support.kaspersky.com/kata/7.1/en-US/176763.htm https://support.kaspersky.com/kata/7.1/247484	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.	https://support.kaspersky.com/kata/7.1/en-US/247176.htm https://support.kaspersky.com/kata/7.1/en-US/176763.htm https://support.kaspersky.com/kata/7.1/en-US/247193.htm	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.	https://support.kaspersky.com/kata/7.1/en-US/181470.htm https://support.kaspersky.com/kata/7.1/en-US/247887.htm https://support.kaspersky.com/kata/7.1/247805 https://support.kaspersky.com/kata/7.1/247807 https://support.kaspersky.com/kata/7.1/247570	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.	https://support.kaspersky.com/kata/7.1/en-US/176763.htm https://support.kaspersky.com/kata/7.1/en-US/247176.htm https://support.kaspersky.com/kata/7.1/en-US/247193.htm	CUMPLE	
78	La solución deberá proporcionar capacidades de análisis y visibilidad del tráfico de red, 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/help/kata/7.1/en-US/247582.htm https://support.kaspersky.com/kata/7.1/en-US/247484.htm https://support.kaspersky.com/kata/7.1/en-US/247887.htm https://support.kaspersky.com/help/KATA/7.1/en-US/216715.htm	CUMPLE	
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.	https://support.kaspersky.com/kata/7.1/en-US/247887.htm https://support.kaspersky.com/kata/7.1/247585 https://support.kaspersky.com/kata/7.1/216715 https://support.kaspersky.com/kedr-expert-on-premise/8.1/211453	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.	https://support.kaspersky.com/kata/7.1/en-US/246848.htm https://support.kaspersky.com/kata/7.1/247420 https://support.kaspersky.com/help/KATA/7.1/en-US/247430.htm https://support.kaspersky.com/help/KATA/7.1/en-US/247695.htm https://support.kaspersky.com/KATA/7.1/en-US/247421.htm https://support.kaspersky.com/KATA/7.1/en-US/247428.htm	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.	https://support.kaspersky.com/help/KATA/7.1/en-US/137926.htm https://support.kaspersky.com/help/KATA/7.1/en-US/134913.htm https://support.kaspersky.com/help/KATA/7.1/en-US/247719.htm https://support.kaspersky.com/help/KATA/7.1/en-US/196718.htm https://support.kaspersky.com/help/KATA/7.1/en-US/189671.htm	CUMPLE	
82	La solución deberá permitir habilitar, deshabilitar, ajustar o excluir reglas de detección de red, conforme a las necesidades operativas de la Universidad.	https://support.kaspersky.com/help/KATA/7.1/en-US/134913.htm https://support.kaspersky.com/help/KATA/7.1/en-US/189671.htm https://support.kaspersky.com/help/KATA/7.1/en-US/247719.htm https://support.kaspersky.com/help/KATA/7.1/en-US/196718.htm https://support.kaspersky.com/help/KATA/7.1/en-US/137926.htm	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.	https://support.kaspersky.com/help/KATA/7.1/en-US/150811.htm https://support.kaspersky.com/help/KATA/7.1/en-US/258283.htm https://support.kaspersky.com/help/KATA/7.1/en-US/294209.htm https://support.kaspersky.com/help/KATA/7.1/en-US/266038.htm https://support.kaspersky.com/help/KATA/7.1/en-US/267995.htm	CUMPLE	
84	La solución deberá soportar despliegues en modo de monitorización mediante SPAN, port mirroring o mecanismos equivalentes.	https://support.kaspersky.com/help/KATA/7.1/en-US/247193.htm https://support.kaspersky.com/help/KATA/7.1/en-US/266033.htm https://support.kaspersky.com/help/KATA/7.1/en-US/247176.htm	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.	https://support.kaspersky.com/help/KATA/7.1/en-US/247193.htm https://support.kaspersky.com/help/KATA/7.1/en-US/266033.htm https://support.kaspersky.com/help/KATA/7.1/en-US/247176.htm https://support.kaspersky.com/help/KATA/7.1/en-US/283631.htm	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.	https://support.kaspersky.com/help/KATA/7.1/en-US/247269.htm https://support.kaspersky.com/help/KATA/7.1/en-US/266033.htm https://support.kaspersky.com/help/KATA/7.1/en-US/292608.htm https://support.kaspersky.com/help/KATA/7.1/en-US/237877.htm	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.	https://support.kaspersky.com/kata/7.1/247805 https://support.kaspersky.com/kata/7.1/247807 https://support.kaspersky.com/kata/7.1/155163 https://support.kaspersky.com/kedr-expert-on-premise/8.1/211453 https://support.kaspersky.com/help/KSC/16.2/KSCAPI/index.html	CUMPLE	

ITEM	SONDA DE COLOMBIA S.A.			COINSA S.A.S		
	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
74	Propuesta Técnica: pág. 7 (preservación, análisis retrospectivo, IOC y contexto); pág. 13 "Investigación Forense". Fabricante: IVX permite submit/review files y URLs y revisar detailed reports: https://docs.trellix.com/bundle/11.x_sag/page/UUID-9f97ea4b-7d0b-7687-4d3c-9d88d927679e.html , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-50cf1629-b04c-3b1f-a587-7fc96c84a7e2.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247495 https://support.kaspersky.com/kata/7.1/150811	CUMPLE	
75	Propuesta Técnica: pág. 6 (diseño modular/escalable); pág. 13. Fabricante: IVX cluster deployment utiliza múltiples compute nodes y permite escalar el análisis: https://docs.trellix.com/bundle/11.x_sag/page/UUID-b23f743e-3302-c3d8-e4b8-171ffad6efdf.html , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-348d97e6-bf7a-8d8e-b112-4988dd192071.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247180 https://support.kaspersky.com/kata/7.1/247179	CUMPLE	
76	Propuesta Técnica: pág. 7, numeral 3.2 (inteligencia global, IOC, correlación y contexto); pág. 8, diagrama de arquitectura (inteligencia de amenazas, enriquecimiento de contexto e integración); pág. 13, "Inteligencia de Amenazas" e "Integración con el Ecosistema de Seguridad" , https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-9e3c706b-445a-cbeb-520e-17fd83923503.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247475 https://support.kaspersky.com/kata/7.1/247465	CUMPLE	
77	Propuesta Técnica: pág. 8, diagrama de arquitectura centralizada; pág. 13. , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-348d97e6-bf7a-8d8e-b112-4988dd192071.html	NO CUMPLE	El requerimiento no se puede verificar con la información adjuntada por la empresa	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247180 https://support.kaspersky.com/kata/7.1/247179	CUMPLE	
78	Propuesta Técnica: págs. 5-8, numerales 3.1 y 3.2 (monitoreo NDR, análisis de tráfico, anomalías, investigación y respuesta); pág. 13 "Monitoreo Inteligente" e "Investigación Forense , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-8e73bf06-fadf-e224-8795-cae94e69a368.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247507 https://support.kaspersky.com/kata/7.1/257980	CUMPLE	
79	Propuesta Técnica: pág. 7 (investigación y respuesta informada); pág. 13 "Automatización y Orquestación"; pág. 15-16 (gestión de incidentes y ciberseguridad). Fabricante ,+G83+G85+G84:G85	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/help/KATA/7.1/en-US/196721.htm	CUMPLE	
80	Propuesta Técnica: pág. 7 (IOC); pág. 13 "Inteligencia de Amenazas" , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-7ae3a720-f92f-3d8a-30e4-2772000f8425.html	NO CUMPLE	El requerimiento no se puede verificar con la información adjuntada por la empresa. En la documentación se encuentra información sobre indicadores personalizados de compromiso (IOC) pero no sobre indicadores de ataque (IOA)	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247421 https://support.kaspersky.com/kata/7.1/247702	CUMPLE	
81	Propuesta Técnica: pág. 9, numeral 3.2.1 (políticas y reglas de detección); pág. 13. Fabricante: YARA es una herramienta open-source y Trellix permite cargar/configurar reglas YARA personalizadas: https://docs.trellix.com/bundle/ax_10.x_ug/page/UUID-b3edfd29-55b9-e7fe-025d-9c44edd72364.html , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-9643de8a-071b-381d-f70a-d6626e2c6b99.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247702 https://support.kaspersky.com/kata/7.1/247424	CUMPLE	
82	Propuesta Técnica: pág. 9 "Configuración y Parametrización"; pág. 13. Fabricante: Trellix permite habilitar/deshabilitar reglas YARA personalizadas mediante CLI: https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-b5151261-1e35-b0f4-8707-9e1886cf15be.html , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-0ca6d03c-8291-158c-1d66-e49e1ccaf7c9.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247774 https://support.kaspersky.com/kata/7.1/247702	CUMPLE	
83	Propuesta Técnica: pág. 7 (preservación y consulta de evidencia técnica, investigaciones retrospectivas); pág. 8, diagrama"; pág. 13 "Investigación Forense y Búsqueda Avanzada". Fabricante: Trellix NDR Console permite recuperar PCAP de flujos capturados por appliances. https://docs.trellix.com/es-ES/bundle/ndr_4.x_console_pg/page/UUID-79212d6a-3933-149f-470a-0ab2248e9615.html, https://docs.trellix.com/es-ES/bundle/nx_11.x_ug/page/UUID-3dca2471-6953-554a-7b17-3570694c9990.html	CUMPLE		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	Propuesta Técnica: pág. 13 "Monitoreo Inteligente del Tráfico de Red". Fabricante: Trellix Network Security Technical Specifications documenta operación TAP/SPAN y puertos de monitoreo; https://www.trellix.com/assets/data-sheets/trellix-network-security-tech-specifications-datasheet.pdf , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-6b116089-4839-2ddb-ffbc-d771870a2c42.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/242456 https://support.kaspersky.com/kata/7.1/266033	CUMPLE	
85	Propuesta Técnica: pág. 13 "Monitoreo Inteligente", con sensores NDR para análisis del tráfico. Fabricante: el modo TAP/SPAN de Network Security permite monitorización pasiva/fuera de banda: https://www.trellix.com/assets/data-sheets/trellix-network-security-tech-specifications-datasheet.pdf , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-6b116089-4839-2ddb-ffbc-d771870a2c42.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/242456 https://support.kaspersky.com/kata/7.1/266033	CUMPLE	
86	Propuesta Técnica: pág. 7 declara investigaciones retrospectivas sobre tráfico de red y enriquecimiento con inteligencia; pág. 13 "Investigación Forense" , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-940c4aa9-7f08-399e-d4c5-137fda5f956f.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247636 https://support.kaspersky.com/kata/7.1/300871	CUMPLE	
87	Propuesta Técnica: pág. 8, diagrama (automatización de respuestas e integraciones); pág. 13 "Automatización y Orquestación". , https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-8c200134-b6f4-1c1c-44b0-c5165d599224.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/KATA/7.1/en-US/227245.htm https://support.kaspersky.com/kata/7.1/281282	CUMPLE	

ITEM	GRUPO MICROSISTEMAS COLOMBIA SAS			HEIMCORE		
	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
74	•Sandbox component: https://support.kaspersky.com/kata/7.1/247495 •Downloading traffic for events: https://support.kaspersky.com/kata/7.1/150811	CUMPLE		CUMPLE. Trend Vision One Sandbox Analysis, web Cómo cumple: DDI extrae objetos del tráfico y Sandbox Analysis informa comportamiento, procesos, comunicaciones, DNS, archivos e IoC asociados.	CUMPLE	
75	•Calculations for the Sandbox component: https://support.kaspersky.com/kata/7.1/247180 •Scenario of deployment on four or more servers: https://support.kaspersky.com/kata/7.1/247179	CUMPLE		CUMPLE. Trend Vision One Sandbox Analysis, web Cómo cumple: La capacidad de Sandbox Analysis se escala mediante créditos por ancho de banda y procesamiento, sin desplegar infraestructura adicional.	CUMPLE	
76	•Configuring connection between the Sandbox and Central Node components: https://support.kaspersky.com/kata/7.1/247475 •Participation in Kaspersky Security Network and use of Kaspersky Private Security Network: https://support.kaspersky.com/kata/7.1/247465	CUMPLE		CUMPLE. Trend Vision One Sandbox Analysis, web Cómo cumple: Los resultados del sandbox actualizan objetos sospechosos, inteligencia, detecciones y correlaciones disponibles para DDI, endpoint e integraciones de terceros.	CUMPLE	
77	•Calculations for the Sandbox component: https://support.kaspersky.com/kata/7.1/247180 •Scenario of deployment on four or more servers: https://support.kaspersky.com/kata/7.1/247179 •Configuring connection between the Sandbox and Central Node components: https://support.kaspersky.com/kata/7.1/247475	CUMPLE		CUMPLE. Trend Vision One Sandbox Analysis, web Cómo cumple: Los dos DDI y los Endpoint Sensors utilizan la capacidad centralizada de Sandbox Analysis conforme a los créditos ofertados.	CUMPLE	
78	•Monitoring the performance of the application: https://support.kaspersky.com/kata/7.1/247507 •Monitoring network sessions: https://support.kaspersky.com/kata/7.1/257980 •Searching network packets: https://support.kaspersky.com/kata/7.1/292608	CUMPLE		CUMPLE. DDI Datasheet, pp. 1–2 · XDR for Networks, p. 1 Cómo cumple: DDI inspecciona tráfico en tiempo real, conexiones, protocolos, objetos y PCAP de evidencia, generando detecciones de amenazas, anomalías y comportamiento para investigación	CUMPLE	
79	•Recommendations for processing alerts: https://support.kaspersky.com/help/KATA/7.1/en-US/196721.htm	CUMPLE		CUMPLE. DDI AG, pp. 85–89 · Conexión directa DDI–Trend Vision One, web Cómo cumple: Las detecciones incluyen información de investigación, mitigación y respuesta; los playbooks de la solución permiten ejecutar acciones asistidas o automatizadas.	CUMPLE	
80	•Managing user-defined IOC rules: https://support.kaspersky.com/kata/7.1/247421 •Importing TAA (IOA) rules: https://support.kaspersky.com/kata/7.1/247702	CUMPLE		CUMPLE. DDD, pp. 214–215 · DDI AG, pp. 263–264 · Conexión directa DDI–Trend Vision One, web Cómo cumple: Los IoC se ingresan mediante objetos sospechosos/STIXTAXII y los IOA se aplican desde las capacidades analíticas XDR para clasificar y correlacionar eventos.	NO CUMPLE	El requerimiento no puede ser verificado con la información suministrada por la empresa, dado que en el ítem 12 se oferta la versión 7.0, mientras que la documentación aportada corresponde a la versión 5.5.
81	•Importing TAA (IOA) rules: https://support.kaspersky.com/kata/7.1/247702 •Uploading an IOC file: https://support.kaspersky.com/kata/7.1/247424 •Information in the IDS rule section: https://support.kaspersky.com/kata/7.1/196718	CUMPLE		CUMPLE. DDI AG, pp. 263–264 · DDD, pp. 214–215 Cómo cumple: La solución incorpora/importa inteligencia y reglas en formatos abiertos como YARA y STIX/TAXII para complementar la detección predeterminada.	CUMPLE	
82	•Managing Intrusion Detection rule exclusions: https://support.kaspersky.com/kata/7.1/247774 •Importing TAA (IOA) rules: https://support.kaspersky.com/kata/7.1/247702	CUMPLE		CUMPLE. DDI AG, pp. 246–248 y 263–264 Cómo cumple: Los administradores gestionan reglas, excepciones, listas de confianza, grupos de red y criterios de envío a análisis conforme a la política operativa.	CUMPLE	
83	•Downloading traffic for events: https://support.kaspersky.com/kata/7.1/150811 •Kaspersky Anti Targeted Attack Platform Public API: https://support.kaspersky.com/KATA/7.1/KataAPI/PublicApi-v4.html	CUMPLE		CUMPLE. DDI AG, pp. 85–87 y 227–228 Cómo cumple: DDI conserva y permite descargar PCAP relacionado con detecciones y reglas de captura para análisis forense e investigación.	CUMPLE	
84	•Configuring receipt of mirrored traffic from SPAN ports: https://support.kaspersky.com/kata/7.1/242456 •Configuring recording of mirrored traffic from SPAN ports: https://support.kaspersky.com/kata/7.1/266033	CUMPLE		CUMPLE. DDI IDG, pp. 62–67 y 186–190 Cómo cumple: Los appliances reciben tráfico desde puertos SPAN o port mirroring de los switches Cisco, sin quedar en el camino de producción.	CUMPLE	
85	•Configuring receipt of mirrored traffic from SPAN ports: https://support.kaspersky.com/kata/7.1/242456 •Configuring recording of mirrored traffic from SPAN ports: https://support.kaspersky.com/kata/7.1/266033	CUMPLE		CUMPLE. DDI IDG, pp. 62–67 Cómo cumple: DDI opera de forma pasiva y fuera de banda, por lo que una falla del sensor no interrumpe las comunicaciones de la Universidad.	CUMPLE	
86	•Events database threat hunting: https://support.kaspersky.com/kata/7.1/247636 •Configuring the retention period for logs, alerts and events: https://support.kaspersky.com/kata/7.1/300871	CUMPLE		CUMPLE. DDI AG, pp. 122–125 · XDR for Networks, p. 2 Cómo cumple: Retro Scan reevalúa eventos históricos con inteligencia actualizada; Sandbox Analysis permite reanalizar objetos.	CUMPLE	
87	•Threat Response API: https://support.kaspersky.com/KATA/7.1/en-US/227245.htm •Automatic network access control for devices via Cisco Switch connectors: https://support.kaspersky.com/kata/7.1/281282 •Managing connectors: https://support.kaspersky.com/kata/7.1/207166	CUMPLE		CUMPLE. DDI AG, pp. 326–327 · Trend Vision One Automation Center, web · Conexión directa DDI–Trend Vision One, web Cómo cumple: DDI se integra con Palo Alto para contención y ejecuta acciones sobre endpoints mediante playbooks/ APIs; Kaspersky se incorpora al procedimiento validado de respuesta.	CUMPLE	

ITEM	DESCRIPCIÓN	UNIÓN TEMPORAL INFO COMUNICACIONES S.A.S - SOLUCIONES EN SEGURIDAD INFORMATICA S.A.S		
		UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
88	Las acciones sospechosas detectadas deben relacionarse con fases de ataque, técnicas de hackers y métodos de la matriz MITRE ATT&CK.	https://support.kaspersky.com/kata/7.1/247585 http://support.kaspersky.com/kata/7.1/247584 https://support.kaspersky.com/kata/7.1/272427	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.	https://support.kaspersky.com/kata/7.1/137926 https://support.kaspersky.com/kata/7.1/249006 http://support.kaspersky.com/kata/7.1/247584 https://opentip.kaspersky.com/Help/Doc_data/all-in-one.htm	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.	https://support.kaspersky.com/kata/7.1/134912 https://support.kaspersky.com/kata/7.1/152004 https://support.kaspersky.com/kata/7.1/247465 https://support.kaspersky.com/kata/7.1/159935	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).	https://support.kaspersky.com/kata/7.1/247193 https://support.kaspersky.com/kata/7.1/246848 https://support.kaspersky.com/kata/7.1/272427 https://support.kaspersky.com/kata/7.1/196705	CUMPLE	
92	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).	https://support.kaspersky.com/kata/7.1/209940 https://support.kaspersky.com/kata/7.1/176134 https://support.kaspersky.com/kata/7.1/247506 https://support.kaspersky.com/kata/7.1/196705 https://support.kaspersky.com/kata/7.1/219821	CUMPLE	
93	La solución permitirá mostrar los riesgos asociados a los dispositivos, facilitando la gestión proactiva de amenazas.	https://support.kaspersky.com/kata/7.1/209940 https://support.kaspersky.com/kata/7.1/247506 https://support.kaspersky.com/kata/7.1/196705 https://support.kaspersky.com/kata/7.1/247887 https://support.kaspersky.com/kata/7.1/176134	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.	https://support.kaspersky.com/kata/7.1/219821 https://support.kaspersky.com/kes-for-windows/12.12/236862 https://support.kaspersky.com/kes-for-linux/12.4.0/314118 https://support.kaspersky.com/kata/7.1/246853	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.	https://support.kaspersky.com/kata/7.1/294072 https://support.kaspersky.com/kes-for-windows/12.12/236862 https://support.kaspersky.com/kata/7.1/227245 https://support.kaspersky.com/kata/7.1/247443 https://support.kaspersky.com/kata/7.1/196705	CUMPLE	
96	La solución debe soportar direccionamiento IP dinámico de los dispositivos, asegurando un seguimiento y monitorización precisos.	https://support.kaspersky.com/kata/7.1/209959 https://support.kaspersky.com/kata/7.1/269820 https://support.kaspersky.com/kata/7.1/247443 https://support.kaspersky.com/kata/7.1/210010	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.	https://support.kaspersky.com/kata/7.1/176134 https://support.kaspersky.com/kata/7.1/196705 https://support.kaspersky.com/kata/7.1/247443 https://support.kaspersky.com/kata/7.1/247887	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.	https://support.kaspersky.com/kata/7.1/234108 https://support.kaspersky.com/kata/7.1/176884 https://support.kaspersky.com/kata/7.1/292608 https://support.kaspersky.com/kata/7.1/262106 https://support.kaspersky.com/kata/7.1/236044	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.	https://support.kaspersky.com/kata/7.1/247610 https://support.kaspersky.com/kata/7.1/247193 https://support.kaspersky.com/kata/7.1/171092 https://support.kaspersky.com/kata/7.1/252086	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.	https://support.kaspersky.com/kata/7.1/300871 https://support.kaspersky.com/kata/7.1/303090 https://support.kaspersky.com/kata/7.1/266034 https://support.kaspersky.com/kata/7.1/258283 https://support.kaspersky.com/kata/7.1/292608	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.	https://support.kaspersky.com/kata/7.1/258283 https://support.kaspersky.com/kata/7.1/266034 https://support.kaspersky.com/kata/7.1/292608	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.	https://support.kaspersky.com/kata/7.1/258283 https://support.kaspersky.com/kata/7.1/266034 https://support.kaspersky.com/kata/7.1/292608	CUMPLE	

ITEM	SONDA DE COLOMBIA S.A.			COINSA S.A.S		
	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
88	Propuesta Técnica: pág. 7 menciona MITRE ATT&CK; pág. 8 arquitectura; pág. 13. Fabricante: Trellix NDR Console mapea detecciones basadas en comportamiento a MITRE ATT&CK: https://docs.trellix.com/bundle/ndr_4.x_console_pg/page/UUID-79212d6a-3933-149f-470a-0ab2248e9615.html , https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-771b724b-87d5-65b4-dc3a-6b77beade20a.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/249034	CUMPLE	
89	Propuesta Técnica: pág. 9 (reglas de detección); pág. 13. Fabricante: Trellix Network Security permite custom YARA rules aplicables a tipos de archivo soportados: https://docs.trellix.com/bundle/11.x_sag/page/UUID-553293e2-ce62-f308-4542-1763f93312c5.html , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-98944cc4-6f1a-3d1a-1475-d382457c38b8.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/137926 https://support.kaspersky.com/kata/7.1/247421 https://support.kaspersky.com/kata/7.1/247465	CUMPLE	
90	Propuesta Técnica: pág. 6 (comunicaciones maliciosas, amenazas conocidas/desconocidas); pág. 7 (inteligencia global); pág. 13. Fabricante: IVX proporciona análisis dinámico sin firmas para zero-day y ataques evasivos: https://docs.trellix.com/bundle/intrusion-prevention-system-11.1.x-product-guide/page/UUID-b4e4f438-af02-fb20-760e-6d2e0d6fd53a.html , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-bf98fd6e-60c8-c057-7505-48479b980e9c.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247465 https://support.kaspersky.com/kata/7.1/247421	CUMPLE	
91	Propuesta Técnica: págs. 6-7 (amenazas desconocidas, comunicaciones maliciosas y análisis avanzado); pág. 13. Fabricante: IVX detecta ataques evasivos y zero-day mediante análisis dinámico sin firma , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-bf98fd6e-60c8-c057-7505-48479b980e9c.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247465 https://support.kaspersky.com/kata/7.1/247421	CUMPLE	
92	Propuesta Técnica: pág. 6-7 (activos estratégicos y telemetría de endpoints); pág. 13 “Visibilidad sobre 400 Endpoints Estratégicos , https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-4b986d93-1879-3767-94fc-7358765437b0.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/175616 https://support.kaspersky.com/kata/7.1/257980	CUMPLE	
93	Propuesta Técnica: pág. 6-8 (priorización de incidentes, contexto de activos); pág. 13 “Analítica y Correlación Inteligente , https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-bbf811fb-0eb3-d543-cf5b-e1a6cdfdda24.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/175616 https://support.kaspersky.com/kata/7.1/257980	CUMPLE	
94	Propuesta Técnica: pág. 6 (400 endpoints); pág. 7 (telemetría de endpoints); pág. 13. Fabricante: EDRF Historical Search recolecta ejecución de procesos y conexiones de red: https://docs.trellix.com/bundle/endsec-edrf-docs/page/UUID-98a84779-ac14-ed95-a83b-c5de74bb2d4f.htm , https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-c72abb85-fc29-3b91-705f-64a8ebdba816.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247325 https://support.kaspersky.com/kata/7.1/219777	CUMPLE	
95	Propuesta Técnica: pág. 8 (integraciones y automatización); pág. 13 “Automatización y Orquestación” e “Integración con Ecosistema , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-6b116089-4839-2ddb-ffbc-d771870a2c42.html	NO CUMPLE	El requerimiento no se puede verificar con la información adjuntada por la empresa	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	Propuesta Técnica: pág. 6-8 describe monitoreo de activos , https://docs.trellix.com/bundle/nx_11.x_ug/page/UUID-50cf1629-b04c-3b1f-a587-7fc96c84a7e2.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/175616 https://support.kaspersky.com/kata/7.1/257980	CUMPLE	
97	Propuesta Técnica: pág. 6-8 (monitoreo, visualización y correlación); pág. 13 “Monitoreo Inteligente” y “Analítica y Correlación , https://docs.trellix.com/bundle/helixconnect_pg/page/UUID-a3fdcef4-5c87-41fc-4916-be44ceef520f.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247507 https://support.kaspersky.com/kata/7.1/246747	CUMPLE	
98	Pagina 8 Alcance soluciòn, https://www.trellix.com/assets/events/partner-tech-summit-2024-emea-ltam/trellix-ndr-detecting-unknown-and-merging-threats-emea-ltam-partner-tech-summit-2024.pdf?, https://chatgpt.com/g/g-p-6a74a7adbd708191baf69269224fb50e/c/6a74a7ba-1630-83e9-a2ec-740fcc4775ea	NO CUMPLE	El requerimiento no se puede verificar con la información adjuntada por la empresa.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/236044 https://support.kaspersky.com/kata/7.1/176734	CUMPLE	
99	Propuesta Técnica: págs. 6-8 análisis comportamental , https://www.trellix.com/products/network-security/	NO CUMPLE	El requerimiento no se puede verificar con la información adjuntada por la empresa.	Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/247495 https://support.kaspersky.com/kata/7.1/159685	CUMPLE	
100	Propuesta Técnica: pág. 7 (preservación de evidencia e investigación); pág. 8 incorpora Network Forensics, https://docs.trellix.com/bundle/nx_10.x_ug/page/UUID-eb79d06b-9159-bcda-f106-b2d7ffb98aa8.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/237877 https://support.kaspersky.com/kata/7.1/266033	CUMPLE	
101	Propuesta Técnica: Pág. 8 (Diagrama de Arquitectura – Network Forensics PX); Pág. 13 'Investigación Forense y Búsqueda Avanzada', https://docs.trellix.com/bundle/nx_10.x_ug/page/UUID-eb79d06b-9159-bcda-f106-b2d7ffb98aa8.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/150811 https://support.kaspersky.com/kata/7.1/258283	CUMPLE	
102	Propuesta Técnica: Pág. 7, 13 'Investigación Forense y Búsqueda Avanzada'. Fabricante: Trellix NDR Console permite búsqueda, filtrado y recuperación de sesiones y PCAP almacenados. https://docs.trellix.com/bundle/ndr_4.x_console_pg/page/UUID-79212d6a-3933-149f-470a-0ab2248e9615.html, https://docs.trellix.com/es-ES/bundle/ndr_4.x_console_pg/page/UUID-79212d6a-3933-149f-470a-0ab2248e9615.html, https://docs.trellix.com/es-ES/bundle/nx_11.x_ug/page/UUID-3dca2471-6953-554a-7b17-3570694c9990.html	CUMPLE		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	

ITEM	GRUPO MICROSISTEMAS COLOMBIA SAS			HEIMCORE		
	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
88	•Event search criteria: https://support.kaspersky.com/kata/7.1/249034	CUMPLE		CUMPLE. DDI AG, pp. 88, 94, 136 y 142 Cómo cumple: Las detecciones se relacionan con tácticas, técnicas y fases de MITRE ATT&CK para orientar investigación, priorización y respuesta.	CUMPLE	
89	•Managing user-defined Intrusion Detection rules: https://support.kaspersky.com/kata/7.1/137926 •Importing TAA (IOA) rules: https://support.kaspersky.com/kata/7.1/247702 •Managing user-defined IOC rules: https://support.kaspersky.com/kata/7.1/247421 •Participation in Kaspersky Security Network and use of Kaspersky Private Security Network: https://support.kaspersky.com/kata/7.1/247465	CUMPLE		CUMPLE. DDI AG, pp. 263–264 y 299 · DDI Datasheet, p. 1 Cómo cumple: YARA, objetos sospechosos, listas de reputación y fuentes STIX/TAXII complementan la detección de archivos, dominios y comunicaciones C2.	CUMPLE	
90	•Participation in Kaspersky Security Network and use of Kaspersky Private Security Network: https://support.kaspersky.com/kata/7.1/247465 •Managing user-defined IOC rules: https://support.kaspersky.com/kata/7.1/247421	CUMPLE		CUMPLE. DDI Datasheet, p. 1 · DDI AG, pp. 23–27 Cómo cumple: DDI combina reputación global, patrones, analítica y Sandbox Analysis para identificar infraestructura C2 conocida y desconocida.	CUMPLE	
91	•Participation in Kaspersky Security Network and use of Kaspersky Private Security Network: https://support.kaspersky.com/kata/7.1/247465 •Managing user-defined IOC rules: https://support.kaspersky.com/kata/7.1/247421 •Searching network packets: https://support.kaspersky.com/kata/7.1/292608	CUMPLE		CUMPLE. DDI Datasheet, p. 1 · DDI AG, pp. 23–27 Cómo cumple: La inspección de protocolos, heurística y comportamiento identifica objetos evasivos y tráfico malicioso asociado con C2.	CUMPLE	
92	•Viewing the table of devices: https://support.kaspersky.com/kata/7.1/175616 •Monitoring network sessions: https://support.kaspersky.com/kata/7.1/257980	CUMPLE		CUMPLE. DDI AG, pp. 75–78 · Endpoint Sensor: datos recolectados, web Cómo cumple: DDI aporta IP, MAC y nombre de host; Endpoint Sensor agrega usuario, proceso, ruta y archivo, formando un inventario lógico correlacionado.	CUMPLE	
93	•Viewing the table of devices: https://support.kaspersky.com/kata/7.1/175616 •Monitoring network sessions: https://support.kaspersky.com/kata/7.1/257980	CUMPLE		CUMPLE. DDI AG, pp. 75–89 · Endpoint Security, p. 2 Cómo cumple: Los activos muestran severidad, detecciones, exposición y contexto de riesgo para priorización y gestión proactiva.	CUMPLE	
94	•Configuring integration of the Endpoint Agent component with the KEDR functional block: https://support.kaspersky.com/kata/7.1/247325 •Configuring integration of the Endpoint Agent component with the NDR functional block: https://support.kaspersky.com/kata/7.1/219777	CUMPLE		CUMPLE. Endpoint Sensor: datos recolectados, web Cómo cumple: Endpoint Sensor, desplegado junto con Kaspersky, aporta nombre y ruta del proceso, línea de comandos y contexto de actividad para relacionar conexiones y eventos.	CUMPLE	
95	•Threat Response API: https://support.kaspersky.com/KATA/7.1/en-US/227245.htm •Automatic network access control for devices via Cisco Switch connectors: https://support.kaspersky.com/kata/7.1/281282	CUMPLE		CUMPLE. DDI AG, pp. 326–327 · Trend Vision One Automation Center, web · Conexión directa DDI–Trend Vision One, web Cómo cumple: La integración con Palo Alto y los playbooks/APIs de la solución habilitan aislamiento, bloqueo y respuesta asistida, conservando el contexto del activo.	CUMPLE	
96	•Viewing the table of devices: https://support.kaspersky.com/kata/7.1/175616 •Monitoring network sessions: https://support.kaspersky.com/kata/7.1/257980	CUMPLE		CUMPLE. DDI AG, pp. 75–78 Cómo cumple: La identidad del activo se correlaciona mediante IP, MAC, hostname y telemetría de endpoint, permitiendo continuidad de seguimiento cuando cambia la dirección DHCP	CUMPLE	
97	•Monitoring the performance of the application: https://support.kaspersky.com/kata/7.1/247507 •Managing user-defined Sandbox rules: https://support.kaspersky.com/kata/7.1/246747 •Working with the network interaction map: https://support.kaspersky.com/kata/7.1/176734	CUMPLE		CUMPLE. DDI AG, pp. 56–68 · DDD, pp. 171–173 Cómo cumple: Los dashboards DDI y los gráficos de correlación muestran actividad, conexiones, hosts, amenazas y relaciones de eventos en tiempo cercano a real.	CUMPLE	
98	•Active device polling jobs: https://support.kaspersky.com/kata/7.1/236044 •Working with the network interaction map: https://support.kaspersky.com/kata/7.1/176734	CUMPLE		CUMPLE. DDI AG, pp. 268–269 La solución ofertada realiza descubrimiento pasivo mediante análisis de tráfico y Network Groups.	CUMPLE	
99	•Sandbox component: https://support.kaspersky.com/kata/7.1/247495 •Managing the Sandbox component through the web interface: https://support.kaspersky.com/kata/7.1/159685 •Kaspersky Anti Targeted Attack 7.0 Technical presentation.pdf	CUMPLE		CUMPLE. DDD, p. 118 Cómo cumple: Deep Discovery Director registra fingerprints JA3/JA3S de sesiones TLS para identificar comportamientos anómalos sin descifrar el contenido.	CUMPLE	
100	•Managing the settings for saving traffic dump files: https://support.kaspersky.com/kata/7.1/237877 •Configuring recording of mirrored traffic from SPAN ports: https://support.kaspersky.com/kata/7.1/266033	CUMPLE		CUMPLE. DDI AG, pp. 85–87 y 227–228 Cómo cumple: Las reglas de Packet Capture de DDI permiten capturar tráfico bruto asociado a criterios y detecciones definidos para investigación forense y respuesta.	CUMPLE	
101	•Downloading traffic for events: https://support.kaspersky.com/kata/7.1/150811 •Kaspersky Anti Targeted Attack Platform Public API: https://support.kaspersky.com/KATA/7.1/KataAPI/PublicApi-v4.html •Downloading network session traffic: https://support.kaspersky.com/kata/7.1/258283	CUMPLE		CUMPLE. DDI AG, pp. 85–87 y 227–228 Cómo cumple: La evidencia capturada se entrega en formato PCAP estándar, compatible con Wireshark y demás herramientas de análisis forense.	CUMPLE	
102	•Searching network packets: https://support.kaspersky.com/kata/7.1/292608 •Downloading traffic for events: https://support.kaspersky.com/kata/7.1/150811	CUMPLE		CUMPLE. DDI AG, pp. 85–87 y 227–228 Cómo cumple: La consola permite localizar detecciones mediante filtros y descargar el PCAP relacionado, recuperando subconjuntos de tráfico relevantes para la investigación.	CUMPLE	

ITEM	DESCRIPCIÓN	UNIÓN TEMPORAL INFO COMUNICACIONES S.A.S - SOLUCIONES EN SEGURIDAD INFORMATICA S.A.S			SONDA DE COLOMBIA S.A.			COINSA S.A.S			GRUPO MICROSISTEMAS COLOMBIA SAS			HEIMCORE		
		UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN	UBICACIÓN EN LA PROPUESTA (N° PÁGINA) Y OBSERVACIONES	CUMPLE / NO CUMPLE	OBSERVACIÓN
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.	https://support.kaspersky.com/kata/7.1/155163 https://support.kaspersky.com/kata/7.1/176734 https://support.kaspersky.com/kata/7.1/176838 https://support.kaspersky.com/kata/7.1/247193 https://support.kaspersky.com/kata/7.1/247430	CUMPLE		Propuesta Técnica: Pág. 13 'Monitoreo Inteligente del Tráfico de Red' e 'Investigación Forense'. Fabricante , https://docs.trellix.com/bundle/nx_10.x_ug/page/UUID-9515094a-e255-58f4-7ac0-fa182b0ea2c4.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/292608 https://support.kaspersky.com/kata/7.1/152739	CUMPLE		•Searching network packets: https://support.kaspersky.com/kata/7.1/292608 •Configuring automatic saving of traffic for system event types: https://support.kaspersky.com/kata/7.1/152739	CUMPLE		CUMPLE. DDI Datasheet, p. 1 Cómo cumple: DDI inspecciona contenido y más de 100 protocolos, aplicando decodificación, reputación, heurística y análisis de objetos sobre el tráfico monitoreado.	CUMPLE	
104	La solución permitirá la búsqueda y recuperación de sesiones de red basándose en capturas de paquetes en el almacenamiento de tráfico.	https://support.kaspersky.com/kata/7.1/300871 https://support.kaspersky.com/kata/7.1/303090 https://support.kaspersky.com/kata/7.1/258283 https://support.kaspersky.com/kata/7.1/292608 https://support.kaspersky.com/kata/7.1/266033	CUMPLE		Propuesta Técnica: Pág. 7, 13 'Investigación Forense y Búsqueda Avanzada'. Fabricante: Trellix NDR Console permite búsqueda, filtrado y recuperación de sesiones y PCAP almacenados. https://docs.trellix.com/bundle/ndr_4.x_console_pg/page/UUID-79212d6a-3933-149f-470a-0ab2248e9615.html, https://docs.trellix.com/es-ES/bundle/ndr_4.x_console_pg/page/UUID-79212d6a-3933-149f-470a-0ab2248e9615.html, https://docs.trellix.com/es-ES/bundle/nx_11.x_ug/page/UUID-3dca2471-6953-554a-7b17-3570694c9990.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/150811 https://support.kaspersky.com/kata/7.1/258283	CUMPLE		•Downloading traffic for events: https://support.kaspersky.com/kata/7.1/150811 •Kaspersky Anti Targeted Attack Platform Public API: https://support.kaspersky.com/KATA/7.1/KataAPI/PublicApi-v4.html •Downloading network session traffic: https://support.kaspersky.com/kata/7.1/258283	CUMPLE		CUMPLE. DDI AG, pp. 85–87 y 227–228 Cómo cumple: Los analistas buscan sesiones por IP, host, protocolo, tiempo y detección y recuperan el PCAP asociado desde la evidencia conservada por DDI.	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	https://support.kaspersky.com/kata/7.1/258283 https://support.kaspersky.com/kata/7.1/292608 https://support.kaspersky.com/kata/7.1/266034 https://support.kaspersky.com/kata/7.1/266033	CUMPLE		Propuesta Técnica: Pág. 13 'Investigación Forense y Búsqueda Avanzada'. Fabricante: Trellix Network Forensics permite exportar PCAP y sesiones para análisis forense, https://docs.trellix.com/bundle/nx_10.x_ug/page/UUID-eb79d06b-9159-bcda-f106-b2d7ffb98aa8.html	CUMPLE		Links oficiales del fabricante: https://support.kaspersky.com/kata/7.1/150811 https://support.kaspersky.com/kata/7.1/258283	CUMPLE		•Downloading traffic for events: https://support.kaspersky.com/kata/7.1/150811 •Kaspersky Anti Targeted Attack Platform Public API: https://support.kaspersky.com/KATA/7.1/KataAPI/PublicApi-v4.html •Downloading network session traffic: https://support.kaspersky.com/kata/7.1/258283	CUMPLE		CUMPLE. DDI AG, pp. 85–87 y 227–228 Cómo cumple: DDI exporta PCAP y datos de detección/sesión para análisis posterior en herramientas forenses o SIEM institucionales.	CUMPLE	
	EVALUACIÓN TÉCNICA	NO HABILITADA			NO HABILITADA			HABILITADA			NO HABILITADA			NO HABILITADA		

	NOMBRE	CARGO	FIRMA	FECHA
Responsable de la elaboración técnica	Santiago Lopez Gomez	CPS Programa Red UDNET - Area de Plataformas computacionales	SLg	14/08/2026
Aprobó	Yuleima Ortiz Zambrano	Lider Red de Datos UDNET	[illegible]	12/08/2026