



ASPECTOS ECONOMICOS

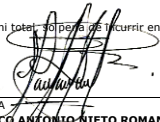
 Corporación Agencia Nacional de Gobierno Digital 							
Procedimiento para la selección de Aliados Estratégicos para la Ejecución de Proyectos.							
IPA-AND-004-2026							
Por favor diligenciar la propuesta económica sobre este formato							
PROPONENTE:	REDCOMPUTO LTDA						
DESCRIPCION DEL OBJETO:	Prestar servicios tecnológicos especializados para el fortalecimiento de la infraestructura tecnológica del ColCERT, mediante la actualización de licenciamiento especializado en seguridad digital, así como la prestación de servicios técnicos asociados a dicho licenciamiento, incluyendo el monitoreo, detección y respuesta ante incidentes de seguridad digital (MDR), y el soporte y mantenimiento del sistema de videowall, de conformidad con las condiciones y alcances definidos en el Anexo Técnico, en el marco de la ejecución del Componente 1 del contrato interadministrativo suscrito entre la Corporación Agencia Nacional de Gobierno Digital – AND y el Fondo Único de Tecnologías de la Información y las Comunicaciones – FUTIC.						
DESCRIPCION DEL ELEMENTO/BIEN/ SERVICIO	UNIDAD DE MEDIDA	CANTIDAD	VALOR UNITARIO ESTIMADO	VALOR UNITARIO	IVA	VALOR UNITARIO INCLUIDO IVA	SUBTOTAL
1- MDR (CrowdStrike Falcon® Enterprise) Para garantizar un esquema de defensa robusto y permanente en las entidades beneficiarias, el proyecto implementará un servicio de monitoreo continuo 24/7 basado en la solución CrowdStrike Falcon® Enterprise. Esta plataforma nativa en la nube unifica en un único agente funciones de antivirus de nueva generación, detección y respuesta extendida, inteligencia de amenazas y cacería gestionada, permitiendo identificar y neutralizar ataques conocidos y desconocidos en tiempo real. Plataforma nativa en la nube que unifica NGAV, EDR, inteligencia de amenazas y cacería gestionada en un único agente ligero, facilitando despliegues rápidos y operación centralizada. ➤ Antivirus de nueva generación alimentado por IA y machine learning que bloquea malware conocido, desconocido, ransomware, ataques sin archivos y amenazas de Estado-nación en tiempo real. ➤ Capacidades avanzadas XDR/EDR con captura de eventos sin procesar, visibilidad histórica y reconstrucción detallada de incidentes mediante CrowdScore™ e Incident Workbench. ➤ Servicio de cacería gestionada 24/7 (Falcon OverWatch) ejecutado por expertos que investigan actividades sigilosas, priorizan amenazas críticas y reducen falsos positivos. ➤ Control granular de dispositivos USB con políticas avanzadas para evitar fugas de información y refuerzo adicional mediante un firewall de host administrado centralmente. ➤ Inteligencia integrada que analiza tácticas, técnicas y procedimientos (TTP) de adversarios, apoyada en Threat Graph para correlación histórica y análisis contextual del entorno. ➤ Agente multiplataforma de mínimo impacto compatible con Windows, macOS, Linux, ChromeOS, iOS y Android, ofreciendo protección online y offline bajo un modelo de actualización continua. ➤ Capacidades de respuesta remota que permiten contener, investigar y remediar endpoints comprometidos con acciones guiadas desde la plataforma Falcon. ➤ Visibilidad unificada del entorno con análisis en tiempo real y datos contextualizados que aceleran la toma de decisiones y reducen significativamente MTTO/MTTR. ➤ Soporte técnico especializado 24/7 provisto por expertos de CrowdStrike, con recursos educativos avanzados para despliegue, operación y modernización automatizada. Actualización de licenciamientos El proyecto contempla la renovación y gestión de licencias de las soluciones identificadas por ColCERT por un periodo no menor a 12 meses, así como la integración de nuevas funcionalidades que optimicen la prestación del servicio y la infraestructura disponible. Se fortalecerá la colaboración a través de la afiliación al FIRST, fomentando el intercambio de información, la participación en ejercicios globales de ciberseguridad y el acceso a alertas y mejores prácticas internacionales. Se prevé un proceso sistemático para la actualización de configuraciones, capacitación del personal en el uso de herramientas y mantenimiento preventivo y correctivo, tales como: - Cloudflare DNS - Gestión y administración de DNS para colcert.gov.co Parte de actualización de licenciamientos; vigencia mínima ≥ 12 meses. - Trellix Intelligent Sandbox (DoD) - Grant Number: 17971347-NAI - Modernización de sandbox para análisis automatizado de malware. - La actualización del sistema Sandbox DoD a la última versión de Trellix Intelligent Sandbox (Grant Number: 17971347-NAI) representa un avance significativo para la capacidad del ColCERT de ofrecer servicios de análisis automatizado de malware. Esta modernización optimizará la detección y el análisis de amenazas sofisticadas, proporcionando información crucial a entidades públicas, privadas y a la ciudadanía en general. - La continuidad de este servicio automatizado es fundamental para la respuesta proactiva ante incidentes de seguridad y para la mejora continua de la postura defensiva del país. - Requisitos: Licenciamiento para una base mínima de 250 usuarios donde cada usuario dispone de una capacidad de 20 envíos mensuales para análisis en Sandbox, garantizando un volumen total de 60,000 procesamientos anuales como requerimiento mínimo. - Mailchimp – Standard - Plan hasta 10.000 correos electrónicos - Una plataforma de automatización de marketing digital, enfocada en el envío masivo de correos electrónicos y campañas de email marketing directamente desde los buzones del CSIRT Gobierno y ColCERT, se constituye como un canal estratégico para la difusión de comunicaciones esenciales. Esta herramienta permitirá la distribución eficiente de piezas informativas cruciales, tales como alertas tempranas, advertencias sobre amenazas, informes técnicos detallados y boletines informativos, emanados principalmente de la línea de análisis situacional. Al utilizar los canales de correo electrónico oficiales del CSIRT Gobierno y ColCERT, se asegura una mayor credibilidad y alcance de la información, facilitando que las entidades públicas y privadas en Colombia estén oportunamente informadas sobre el panorama de ciberseguridad y puedan tomar las acciones preventivas necesarias. - Tenable One (Web y On-premise) - Plan de actualización integral para asegurar la máxima visibilidad de vulnerabilidades en los activos tecnológicos. Ayuda a Activación de la membresía FIRST	UNIDAD	GLOBAL	\$ 778.500.000	\$ 778.500.000	\$ 0	\$ 778.500.000	\$ 778.500.000
Cloudflare DNS Gestión y administración de DNS para colcert.gov.co Parte de actualización de licenciamientos; vigencia mínima ≥ 12 meses. Trellix Intelligent Sandbox (DoD) Grant Number: 17971347-NAI Modernización de sandbox para análisis automatizado de malware. La actualización del sistema Sandbox DoD a la última versión de Trellix Intelligent Sandbox (Grant Number: 17971347-NAI) representa un avance significativo para la capacidad del ColCERT de ofrecer servicios de análisis automatizado de malware. Esta modernización optimizará la detección y el análisis de amenazas sofisticadas, proporcionando información crucial a entidades públicas, privadas y a la ciudadanía en general. La continuidad de este servicio automatizado es fundamental para la respuesta proactiva ante incidentes de seguridad y para la mejora continua de la postura defensiva del país. Requisitos: Licenciamiento para una base mínima de 250 usuarios donde cada usuario dispone de una capacidad de 20 envíos mensuales para análisis en Sandbox, garantizando un volumen total de 60,000 procesamientos anuales como requerimiento mínimo. Mailchimp – Standard Plan hasta 10.000 correos electrónicos Una plataforma de automatización de marketing digital, enfocada en el envío masivo de correos electrónicos y campañas de email marketing directamente desde los buzones del CSIRT Gobierno y ColCERT, se constituye como un canal estratégico para la difusión de comunicaciones esenciales. Esta herramienta permitirá la distribución eficiente de piezas informativas cruciales, tales como alertas tempranas, advertencias sobre amenazas, informes técnicos detallados y boletines informativos, emanados principalmente de la línea de análisis situacional. Al utilizar los canales de correo electrónico oficiales del CSIRT Gobierno y ColCERT, se asegura una mayor credibilidad y alcance de la información, facilitando que las entidades públicas y privadas en Colombia estén oportunamente informadas sobre el panorama de ciberseguridad y puedan tomar las acciones preventivas necesarias. Tenable One (Web y On-premise) Plan de actualización integral para asegurar la máxima visibilidad de vulnerabilidades en los activos tecnológicos. Ayuda a	UNIDAD	GLOBAL	\$ 1.070.000.000	\$ 1.070.000.000	\$ 203.300.000	\$ 1.273.300.000	\$ 1.273.300.000
Plan de actualización integral para asegurar la máxima visibilidad de vulnerabilidades en los activos tecnológicos. Ayuda a Activación de la membresía FIRST	UNIDAD	GLOBAL	\$ 14.000.000	\$ 14.000.000	\$ 0	\$ 14.000.000	\$ 14.000.000
MAGNET AXIOM Cyber Licenciamiento RI/Forense digital (móvil, PC y nube) Incluye transferencia de conocimiento (4 h) y soporte 12 meses. Solución DFIR – Torre Forense 1) (9-14900K5 CPU Procesador Tetracosa-core (24 núcleos) a 3.20 GHz - 36MB de caché L3 - 32MB de caché L2 Velocidad de overlocking de 6.20 GHz - Socket LGA-1700 - Intel UHD Graphics 770 (Si, gráficos integrados) - 150 W - 32 hilos 1) MEMORIA DDR5 128GB RAM 1) TARJETA RTX NVIDIA 4070 SUPER GPU 1) Realtek S1220A 7.1 Surround Sound, Códec de audio de alta definición, 5 jacks de audio 1) DISCO SSD M.2 NVMe 1TB 1) DISCO SSD M.2 NVMe 2TB 1) DISCO SSD M.2 NVMe 4TB PG/DB 1) CONTROLADOR SAS BI RAID 5) DISCOS 18TB SAS raid-5 1) Monitor 34 " Dispositivos externos de evidencia forense y almacenamiento adicional: 1) Caja para discos 5.25" (hot-swap) bahías intercambiables en caliente, interfaz SATA/600 1) Rack miniSAS 5.25" a 4x2.5"Adaptador SATA/SAS 12Gb/s, intercambio en caliente 5) DISCO HDD 18TB 3.5" SAS 7200rpmDiscos12Gb/s SAS, 7200 rpm, para arreglo RAID-51 1) DISCO SSD 8TB 2.5" (QVO) 2.5" SATA serie QVO 1) DISCO SSD 2TB 2.5" (EVO) 2.5" SATA serie EVO 2) Bahías abiertas bahías Slots libres para expansión 1) Cajón de disco SATA / rack móvil 3.5"Bahía 5.25" extraible para disco 3.5" HARDWARE FORENSE 1) Grabadora 16X DVD/CD/Blu-Ray Unidad óptica triple 16X 1) Logcube WriteProtect-BAY Bloqueador forense de escritura SAS/SATA/USB3/FW 1) Cooling Bay con Hub USB y lector forense Módulo de ventilación con hub USB 3.x y lector de tarjetas 1) Tarjeta expansión USB PCIe Puertos USB 3.x adicionales (ranura PCIe) 1)Teclado 1) raton Sistema operativo: Windows 11 Pro de alta gama (Español) Capacitación: ➤ Capacitación certificada de 4 horas por el canal o Fabricante	UNIDAD	GLOBAL	\$ 205.000.000	\$ 205.000.000	\$ 38.950.000	\$ 243.950.000	\$ 243.950.000
Garantizar la operatividad continua del sistema videowall de 3x6 mediante revisiones técnicas periódicas para prevenir fallos y la corrección inmediata de averías en sus paneles o controladores. Incluye el soporte técnico especializado para la calibración de imagen y la actualización de software y firmware de los procesadores de video para asegurar la compatibilidad con nuevas fuentes de señal. El objetivo es mantener una visualización óptima y sin interrupciones para el monitoreo situacional, optimizando la vida útil de los componentes electrónicos del sistema	UNIDAD	GLOBAL	\$ 43.000.000	\$ 43.000.000	\$ 8.170.000	\$ 51.170.000	\$ 51.170.000
Gestión proactiva de incidentes y remediación Se debe establecer un procedimiento de gestión de incidentes alineado al estándar NIST 800-61 R3, garantizando la contención, erradicación y recuperación de los sistemas comprometidos. La gestión eficiente y oportuna de los incidentes, incluyendo la entrega de informes preliminares y finales, es clave para minimizar el impacto y fortalecer la resiliencia operativa.	UNIDAD	GLOBAL	\$ 129.000.000	\$ 129.000.000	\$ 24.510.000	\$ 153.510.000	\$ 153.510.000

SopORTE 24/7 La continuidad operativa depende de la provisión de soporte técnico y mantenimiento directo por parte del fabricante, bajo la modalidad 24/7. Esto incluye la entrega de protocolos de escalamiento, manuales técnicos y legales, y la actualización constante de las herramientas y plataformas utilizadas. SOPORTE TÉCNICO, MANTENIMIENTO Y ACTUALIZACIÓN DE LICENCIAMIENTOS El servicio de soporte técnico constituye un componente transversal que garantiza la continuidad operativa, estabilidad funcional y aprovechamiento pleno de las soluciones tecnológicas desplegadas durante los doce (12) meses de vigencia del contrato. El proveedor será responsable de proporcionar soporte técnico especializado de primer, segundo y tercer nivel, articulado con el fabricante de cada solución y sujeto a los acuerdos de niveles de servicio establecidos en el Anexo Técnico. El soporte incluirá actividades de mantenimiento preventivo y correctivo, atención de incidentes, gestión de actualizaciones, aplicación de parches, acompañamiento en ajustes de configuración, análisis de fallas y validación de funcionamiento posterior a cada intervención. Cada licenciamiento entregado deberá acompañarse del servicio de soporte oficial del fabricante, garantizando acceso directo a documentación especializada, bases de conocimiento, actualizaciones, matrices de compatibilidad y gestión de casos técnicos que requieran intervención experta. El proveedor deberá establecer un plan de escalamiento formal, que contemple los tiempos máximos de respuesta y resolución, los flujos de comunicación entre niveles técnicos y los responsables de cada instancia. Este plan incluirá la interacción directa con el fabricante para la resolución de casos complejos, asegurando que los problemas críticos se escalen sin demoras y que la supervisión del proyecto disponga de visibilidad total sobre el estado de cada requerimiento. Asimismo, el proyecto contará con una mesa de servicios dedicada para la recepción, registro, clasificación y seguimiento de incidentes o solicitudes técnicas derivadas del uso de las soluciones adquiridas. Esta mesa deberá operar con disponibilidad acorde al nivel de criticidad de las herramientas (incluyendo atención 24/7 cuando la herramienta lo requiera), registrar cada caso en un sistema de atención con trazabilidad completa y garantizar la generación de reportes periódicos para la supervisión. Durante la vigencia del contrato, el proveedor deberá asegurar que todas las soluciones, plataformas y licencias se mantengan actualizadas a sus versiones más recientes, incluyendo parches de seguridad, mejoras funcionales y actualizaciones críticas del fabricante. Cualquier actualización deberá ser previamente validada en coordinación con el equipo técnico del CoICERT, confirmando su compatibilidad y evitando interrupciones operacionales. Finalmente, al término del proyecto, el contratista deberá entregar a la supervisión toda la documentación relacionada con el soporte prestado, los reportes de incidentes atendidos, las actualizaciones aplicadas, los certificados de soporte del fabricante y las recomendaciones para asegurar la continuidad operativa posterior a la finalización del contrato Desarrollar y entregar un plan completo de soporte, mantenimiento, actualizaciones, escalamiento y evidencia documental.	UNIDAD	GLOBAL	\$ 129.000.000	\$ 129.000.000	\$ 24.510.000	\$ 153.510.000	\$ 153.510.000
* Se debe verificar el % de IVA a aplicar por ítem cotizado según corresponda.	TOTAL						\$ 2.667.940.000

NOTAS:

- a) El presente formato es inmodificable so pena de incurrir en causal de rechazo.
- b) El proponente no podrá superar el valor estimado del presupuesto oficial por ítem ni total, so pena de incurrir en causal de rechazo.

NOMBRE DEL REPRESENTANTE LEGAL
C.C. REP LEGAL
NOMBRE DE LA EMPRESA
NIT
DIRECCION
CORREO ELECTRONICO
TELEFONO



FIRMA
MARCO ANTONIO NIETO ROMAN
79.288.025 DE BOGOTA
REDCOMPUTO LTDA
830.016.004-0
CRA. 31 A No 25 B 55
mmieto@redcomputo.com.co, comercial@redcomputo.com.co
2688655