ORDEN DE SERVICIO No. 2 AL CONTRATO MARCO No. 202500142_1

CONTRATO No:	**202500142_1**
CONTRATISTA:	**NSIT**
NIT:	**900.449.084-1**
OBJETO DEL CONTRATO MARCO:	Aunar esfuerzos de equipo para la ejecución de proyectos relacionados con servicios de TI, SOLUCIONES INTEGRALES DE CIBERSEGURIDAD Y SEGURIDAD DIGITAL donde se puedan sincronizar herramientas tecnológicas, capacidad instalada, y la infraestructura física existente.
PLAZO DEL CONTRATO MARCO:	El plazo es de doce (12) meses, contados desde la suscripción del contrato marco de alianza estratégica.
FECHA DE INICIO CONTRATO MARCO:	11 de agosto de 2025
VALOR CONTRATO MARCO:	**Cuantía Indeterminada**
OBJETO DE LA ORDEN DE SERVICIO 2:	servicio especializado de diagnóstico integral de ciberseguridad, para los Sistemas Inteligentes de Transporte (ITS) de la Secretaría de Movilidad del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín.
PLAZO ORDEN DE SERVICIOS No. 2:	Hasta el 31 de diciembre de 2026
VALOR ORDEN DE SERVICIOS No.2:	**SEISCIENTOS CINCO MILLONES DOSCIENTOS SETENTA Y OCHO MIL SETECIENTOS VEINTISIETE PESOS CON TREINTA Y CUATRO CENTAVOS ($605.278.727,34)** impuestos incluidos

La presente constituye la Orden de Servicio N° 2 al Contrato Marco 202500142_1 suscrito entre la Empresa para la Seguridad y Soluciones Urbanas ESU y NSIT SAS, cuyo objeto es "servicio especializado de diagnóstico integral de ciberseguridad, para los Sistemas Inteligentes de Transporte (ITS) de la Secretaría de Movilidad del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín." previas las siguientes:

CONSIDERACIONES:

ALCANCE DE LA ORDEN Y DESCRIPCIÓN DEL SERVICIO: En desarrollo del Acuerdo Marco de la referencia, el alcance del objeto será la satisfacción de las necesidades que requieran nuestros clientes en materia de servicios de soluciones de tecnologías de información y de las comunicaciones identificadas como herramientas que pueden aportar al control para mitigar riesgos de seguridad

informática frente a ciberamenazas y servicios especializados de seguridad informática que podrían aportar a mejorar la postura de Seguridad Informática frente a Ciberamenazas.

ESPECIFICACIONES TÉCNICAS SERVICIO ESPECIALIZADO DE DIAGNÓSTICO INTEGRAL DE CIBERSEGURIDAD

El presente componente se desarrollará conforme a lo establecido en el **"Anexo Componente de Ciberseguridad"**, documento complementario que detalla las fases, metodologías, entregables y alcances técnicos definidos para el fortalecimiento de la infraestructura tecnológica de los centros CITRA y CIOS. Dicho anexo hace parte integral del contrato y deberá ser consultado para la ejecución detallada de las actividades técnicas y la validación de los resultados.

Este componente comprende la ejecución de un servicio especializado de diagnóstico integral de ciberseguridad, orientado a evaluar, fortalecer y asegurar la postura de seguridad digital de la infraestructura tecnológica de los centros CITRA y CIOS de la Secretaría de Movilidad de Medellín.

El propósito es identificar vulnerabilidades técnicas, brechas de configuración, deficiencias en controles y riesgos asociados al procesamiento y transmisión de información crítica, a fin de definir un plan de fortalecimiento integral que garantice la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas tecnológicos bajo estándares internacionales de seguridad de la información.

El diagnóstico deberá abarcar la infraestructura física y lógica de ambos centros, sus plataformas y redes de comunicaciones, así como los procesos de gestión, operación y administración tecnológica que intervienen en el ciclo de vida de la información.

El mandatario y sus aliados deberá aplicar metodologías alineadas con los marcos ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework (CSF), MITRE ATT&CK, CIS Controls, OWASP, y las directrices establecidas por el Equipo de Respuesta a Incidentes del Distrito (CSIRT Medellín).

7.1 EVALUACIÓN DE SEGURIDAD DE INFRAESTRUCTURA Y REDES

Este subcomponente comprende la revisión técnica y diagnóstica de la infraestructura de hardware, redes y comunicaciones que soportan los servicios operativos y administrativos de CITRA y CIOS, con el fin de verificar la robustez, segmentación y eficacia de los controles de seguridad implementados.

Actividades

- Evaluación de la topología y segmentación de la red CITRA–CIOS.

- Análisis de configuraciones en switches, routers y firewalls (Brocade, Aruba, HP, Altheon, Radware, Ahnlab).
- Revisión de políticas de NAT, VPN, VLAN y ACLs.
- Escaneo interno y externo de redes para identificación de puertos y servicios abiertos.
- Validación de redundancia, alta disponibilidad y mecanismos de failover.
- Revisión de cumplimiento de CIS Benchmarks y NIST 800-53.

Productos y entregables

- Informe de arquitectura y segmentación de red.
- Inventario de equipos vulnerables o configuraciones inseguras.
- Informe de estado de firewalls y políticas perimetrales.
- Plan de mejora para segmentación y endurecimiento de la red.

Condiciones técnicas generales

- Las pruebas no deben alterar la disponibilidad de los sistemas en producción.
- Coordinación obligatoria con responsables de red y seguridad.
- No se permitirá captura de tráfico real sin autorización de la supervisión.

7.2 ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN

Este subcomponente cubre la ejecución de análisis de vulnerabilidades y pruebas de penetración controladas (PenTesting) sobre las redes, servidores, equipos y plataformas de CITRA y CIOS, con el fin de identificar debilidades explotables y medir la efectividad de los controles implementados.

Actividades

- Ejecución de escaneos automatizados sobre redes internas y externas.
- Validación manual de vulnerabilidades críticas (eliminación de falsos positivos).
- Ejecución de pruebas de penetración controladas (white-box / gray-box).
- Evaluación de exposición en servicios web, APIs y plataformas analíticas.
- Clasificación de vulnerabilidades conforme a CVSS v3.
- Validación de detección y respuesta ante ataques simulados.

Productos y entregables

- Reporte de vulnerabilidades con evidencia técnica y nivel de riesgo.
- Informe de pruebas de penetración (Pentest Report).
- Análisis comparativo de riesgo residual posterior a la mitigación.
- Condiciones técnicas generales

- Pruebas no intrusivas y con impacto controlado.
- Comunicación inmediata de hallazgos críticos.
- Entrega de evidencias cifradas (AES-256 o superior).

7.3 ASSESSMENT DE CONFIGURACIÓN, ENDPOINTS Y CONTROLES DE ACCESO

Este subcomponente abarca la evaluación de configuraciones seguras, gestión de accesos, endpoints, antivirus y respaldos, verificando el cumplimiento de políticas de seguridad y estándares internacionales.

Actividades

- Evaluación de configuraciones seguras (hardening) en RHEL, Ubuntu y Windows Server.
- Revisión de políticas de autenticación, bloqueo, privilegios y MFA.
- Verificación del estado del antivirus TrendMicro.
- Revisión de respaldos Arcserve UDP y NetBackup.
- Validación de logs, alertas y auditorías de acceso.
- Comprobación de cumplimiento CIS Controls y OWASP ASVS.

Productos y entregables

- Informe de Assessment de Configuración.
- Informe de Controles de Acceso y Seguridad de Endpoints.
- Plan de acción para mejora de políticas y controles.

Condiciones técnicas generales

- Las evaluaciones se realizarán sin alterar los sistemas en producción.
- Permisos temporales y auditables para el equipo auditor.
- Validación previa de cambios recomendados con la supervisión.

7.4 REVISIÓN DE SEGURIDAD DE PLATAFORMAS Y APLICATIVOS

Este subcomponente tiene por objetivo evaluar la seguridad lógica de las plataformas ITS, Big Data, IA y aplicativos web operativos en CITRA y CIOS, identificando debilidades en arquitectura, código o integración.

Actividades

- Revisión de arquitectura, dependencias y capas de seguridad.
- Ejecución de análisis estático y dinámico (SAST/DAST).
- Validación de cumplimiento OWASP Top 10.
- Revisión de certificados SSL/TLS y cabeceras de seguridad.
- Evaluación de exposición de APIs y endpoints.
- Pruebas de control de sesión y autenticación.

Productos y entregables

- Informe de Seguridad de Aplicaciones Web.
- Informe de Vulnerabilidades Lógicas y Riesgos.
- Plan de Mitigación y Ajuste de Configuración.

Condiciones técnicas generales

- Pruebas en entornos de staging o controlados.
- Ejecución bajo confidencialidad y control de impacto.
- Resultados compartidos únicamente con personal autorizado.

7.5 GESTIÓN DE RIESGOS, PLAN DE FORTALECIMIENTO Y SENSIBILIZACIÓN

Este subcomponente consolida los resultados del diagnóstico para elaborar el Plan Integral de Fortalecimiento de Ciberseguridad de CITRA y CIOS, incluyendo el análisis de riesgos, definición de controles, estrategias de mitigación y actividades de sensibilización y capacitación.

Actividades mínimas

- Identificación y valoración de riesgos según ISO 31000 e ISO 27005.
- Elaboración del Mapa de Riesgos y Matriz de Controles.
- Formulación del Plan de Fortalecimiento y Cierre de Brechas.
- Definición de KPIs/KRIs de seguimiento.
- Ejecución de talleres de sensibilización en ciberseguridad.
- Entrega de lineamientos para la futura implementación de un SGSI.

Productos y entregables

- Mapa de Riesgos y Matriz de Priorización.
- Plan de Fortalecimiento y Cierre de Brechas.
- Material de Capacitación y Sensibilización.
- Informe final consolidado y hoja de ruta de madurez.

Condiciones técnicas generals

- Tratamiento confidencial de la información analizada.
- Capacitaciones registradas y evaluadas.
- Alineación con las políticas institucionales de seguridad de la información.

VALOR DE LA ORDEN DE SERVICIO: El valor de la presente orden de servicios es de **SEISCIENTOS CINCO MILLONES DOSCIENTOS SETENTA Y OCHO MIL SETECIENTOS VEINTISIETE PESOS CON TREINTA Y CUATRO CENTAVOS ($605.278.727,34)** impuestos incluidos.

La ESU pagará al Contratista los servicios que efectivamente hayan sido prestados, cuyos valores hayan sido aprobados por la Supervisión, por lo que procederá una vez vencido el plazo, a liberar los valores que no hayan sido ejecutados.

INFORMACIÓN PRESUPUESTAL ORDEN DE SERVICIO:

Contrato Interadministrativo:	**4600106117 de 2025**
Certificado de Disponibilidad Presupuestal:	2026000401
Certificado de Registro Presupuestal:	2026000385
Centro de costos:	33416
Rubro al presupuesto:	23202020080481-2
Descripción al Rubro:	SERVICIO ESPECIALIZADO DE DIAGNOSTICO INTEGRAL DE CIBERSEGURIDAD
Requerimiento N°:	**20251006720**

Para efectos de consecutivo en la parte presupuestal, esta orden hace las veces de la No. 2

FORMA DE PAGO: La ESU cancelará el valor de la orden de servicio mediante pagos parciales; previa/o aprobación de las garantías expedida por la Unidad de Gestión Jurídica y recibo de cumplimiento de la prestación del servicio por parte del

supervisor del Contrato del cual se deriva la Orden de Servicio. Acorde a los siguientes parámetros:

- La respectiva factura debe cumplir con los requisitos de las normas fiscales establecidas en el artículo 617 del Estatuto Tributario. La fecha de la factura debe corresponder al mes de su elaboración, y en ella constará el número del contrato y, el concepto del bien o servicio que se está cobrando.

- El proveedor deberá acreditar la efectiva prestación del servicio por medio de una constancia de recibo firmada por el beneficiario. Una vez aprobada la constancia de recibo por parte del supervisor del contrato, éste emitirá el recibo a entera satisfacción del servicio contratado.

- Las retenciones en la fuente a que hubiere lugar y todo impuesto, tasa o contribución directa o indirecta, Nacional, Departamental o Municipal que se cause por razón de la celebración, ejecución y pago de este Contrato serán a cargo exclusivo del Aliado.

  Nota: Si la propuesta presentada supera los 6.000 UVT, el contrato resultante será gravado con el impuesto de timbre de conformidad con lo establecido en el Estatuto Tributario, las normas que lo modifican o complementan y el contrato.

- Una vez recibida a satisfacción la factura o cuenta de cobro correspondiente, la ESU tendrá treinta (30) días calendario para proceder a su pago. En caso de incurrir en mora en los pagos, la ESU reconocerá al Contratista un interés equivalente al DTF anual de manera proporcional al tiempo de retraso.

- Al momento de entregar la factura, ésta deberá estar acompañada con el certificado de pago de aportes de sus empleados al Sistema de Seguridad Social Integral y a las entidades que administran recursos de naturaleza parafiscal; y la carta donde se especifique la entidad y el número de cuenta bancaria a la cual se le deberá realizar el pago.

PLAZO DE LA ORDEN DE SERVICIO: Hasta el TREINTA Y UNO (31) de diciembre de 2026 contados a partir de la aprobación de la garantía única de cumplimiento por la Unidad de Gestión Jurídica.

PLAZO PARA LA SUSCRIPCIÓN DE LA PRESENTE ORDEN DE SERVICIO: Al recibo del presente documento, el CONTRATISTA, contará con máximo de dos (2) días hábiles para la suscripción y legalización del mismo, y si es del caso para allegar las pólizas modificadas, so pena de que se declare el incumplimiento y que se puedan hacer efectiva las garantías constituidas a favor del CONTRATANTE.

SUPERVISIÓN: El seguimiento técnico, administrativo, financiero, contable y jurídico del cumplimiento a satisfacción del presente objeto contractual se realizará por Profesional universitario, o quien sea designado por la Subgerente de servicios. En todo caso la designación podrá hacerse directamente por la Gerencia.

GARANTÍAS: El Contratista se obliga a constituir a favor de "La Empresa para la Seguridad y Soluciones Urbanas - ESU Y Secretaría de Innovación del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín", una garantía única de las expedidas para Entidades estatales que ampare el cumplimiento de las obligaciones contractuales, otorgada por una compañía de seguros autorizada para operar en Colombia por la Superintendencia Financiera y preferiblemente con poderes decisorios en la Ciudad de Medellín:

Garantías y Mecanismos de cobertura del riesgo: El Contratista se obliga a garantizar el cumplimiento de las obligaciones surgidas a favor de la ESU, con ocasión de la ejecución del contrato, de acuerdo con lo siguiente:

- ✓ **Cumplimiento:** Por el veinte por ciento (20%) del valor del mismo, con una vigencia igual a la duración del contrato y seis (6) meses más.
- ✓ **Calidad del servicio:** Por el diez por ciento (10%) del valor del mismo, con una vigencia igual a la duración del contrato y seis (6) meses más.
- ✓ **Salarios, prestaciones sociales e indemnizaciones al personal: hasta** Por el diez por ciento (10%) del valor del mismo, con una vigencia igual a la duración del contrato y tres (3) años más.
- ✓ **Responsabilidad civil extracontractual:** Doscientos (200) SMMLV con una vigencia igual al plazo del contrato.

PARÁGRAFO 1: El contratista deberá modificar el monto de la garantía cada vez que sea necesario, debido al incremento del contrato, la afectación por reclamaciones o por el cambio de vigencia y actualización de aquellos valores que estén tasados en SMMLV. Si el contratista se negare a constituir o a reponer la garantía exigida, la ESU directamente solicitará a la Compañía de Seguros la modificación de la misma, además podrá dar por terminado el contrato en el estado en que se encuentre, sin que haya lugar a reconocer o pagar indemnización alguna.

PARÁGRAFO 2: Al recibo del contrato, el contratista contará con máximo dos (2) días hábiles para la constitución de la póliza única de cumplimiento y entrega de la documentación respectiva.

DOCUMENTOS INTEGRALES: Hacen parte de la presente orden de servicio el Contrato Marco 202500142_1 y demás documentos emanados con ocasión de esta. Las estipulaciones pactadas mediante el presente documento no constituyen novación al contrato marco del cual se derivan, el cual encuentra vigente.

ACEPTACIÓN ORDEN DE SERVICIO: En aceptación de lo anterior, la fecha de suscripción será el 30 de enero de 2026

POR LA ESU,

MATEO GONZÁLEZ BENÍTEZ
Gerente

POR EL CONTRATISTA,

MÓNICA MARÍA GIRALDO GÓMEZ
Representante Legal

Aprobó	Kamal Abdul Nassar	Secretario General	
Aprobó	Angélica López	Subgerente de Servicios	
Aprobó	Nathalia Restrepo Caro	Subgerente Administrativa y Financiera	
Revisó	Ana Cristina Pérez Gil	Profesional Especializado - Unidad de Gestión Jurídica	
Proyectó	Tatiana Silva Pulido	Profesional Universitario - Unidad de Compras y Contratación	

Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes, por tanto, bajo nuestra responsabilidad lo presentamos para firma.