Radicado: 20250005613

JUSTIFICACIÓN DE CONTRATO MARCO DE ALIANZA ESTRATÉGICA

1. NECESIDAD:

La Empresa para la Seguridad y Soluciones Urbanas – ESU, es una empresa industrial y comercial del Estado, orientada a brindar soluciones integrales de seguridad, tecnología, servicios de redes y telecomunicaciones, gestión urbana y del riesgo a entidades del orden nacional e internacional, a través de la comercialización y prestación de bienes y servicios, mediante alianzas, convenios, contratos, cooperación intersectorial y aquellas actividades permitidas por la ley, para contribuir a la transformación social, la innovación, la investigación, el desarrollo económico y ambiental de las ciudades y territorios.

En cinco años, la ESU será una empresa reconocida por su operación rentable, estable y sostenible, con una fuerte alianza estratégica con el Distrito de Ciencia, Tecnología e Innovación de Medellín. Nos destacaremos por nuestra innovación tecnológica, procesos automatizados y un equipo especializado, ofreciendo soluciones apoyadas por IA y análisis de datos tanto para el sector público como privado, logrando la expansión a nivel nacional e internacional; contribuyendo activamente al desarrollo de ciudades inteligentes.

Ahora bien, frente a los servicios ofrecidos, en la actualidad la ESU brinda los siguientes:

Con el objetivo de consolidar las líneas definidas para alcanzar la visión proyectada, especialmente para este caso la línea estratégica de seguridad digital, se requiere contar con aliados estratégicos cuyo objeto social se encuentre en sintonía con el objeto social de la ESU, con el fin de generar sinergias para brindar soluciones integrales en seguridad, mediante instrumentos tecnológicos y logísticos de avanzada que permitan el cumplimiento de las misiones institucionales de las partes, como agente que aporta a la política de seguridad nacional, departamental o municipal.

En este sentido, se hace necesario contar con aliados estratégicos que aporten a la diversificación, cooperación técnica, consolidación y apertura de nuevos mercados tanto a nivel nacional como internacional y que permitan a la ESU afrontar retos tecnológicos, soluciones en telecomunicaciones, informática e innovación, buscando generar valor en el largo plazo a nuestros clientes potenciales y existentes, en aras del fortalecimiento de los mercados actuales y la apertura de nuevos con la dinamización de nuestro portafolio y contratación y oferta de nuevos servicios especializados.

Conforme lo anterior, la ESU en su trayectoria de más de 40 años ha generado grandes hitos para el desarrollo de la ciudad y de la región, principalmente en las Líneas estratégicas de Seguridad, Logística y Tecnología; actualmente la entidad se encuentra interesada en explorar nuevas temáticas de interés en la línea estratégica de Seguridad Digital, apoyada en su capacidad de estructuración, ejecución y cierre efectivo de proyectos, la cual contempla la implementación o prestación de servicios en el marco de las siguientes temáticas:

- Ciberinteligencia e identificación de amenazas.
- Ethical Hacking.
- Análisis de seguridad en los sistemas de Información
- Centro de Operaciones SOC y NOC - Seguridad Digital.

La Empresa para la Seguridad y Soluciones Urbanas -ESU, tiene un proyecto institucional llamado SOC360, el cual tiene como objetivo fortalecer la capacidad institucional de respuesta ante ciber amenazas, garantizar la continuidad de los servicios públicos y proteger los datos ciudadanos frente a ciberataques, que adicionalmente se alinea con la meta de convertir a la ESU en el proveedor exclusivo del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín en sistemas de seguridad integrales para 2027.

En consideración a la magnitud del proyecto SOC360 y su impacto tanto en la seguridad digital del Distrito de Medellín como de su conglomerado, se contrató un estudio financiero y de costos para analizar la viabilidad del proyecto y establecer la hoja de ruta para su

desarrollo, el cual se formalizó mediante el contrato 202500028, cuyo objeto es "Prestación de servicios profesionales para el análisis de viabilidad técnica financiera del Proyecto SOC 360".

El análisis de viabilidad técnica financiera fue realizado para cuatro modelos de negocio:

- Modelo 1: ESU tiene el SOC como Propio. El aliado solo presta servicios de consultoría profesional y apoyo en la implementación
- Modelo 2: ESU tiene el SOC como Propio y contrata a el aliado como operador del servicio
- Modelo 3: ESU se junta con el aliado y reparten las cargas e ingresos 50-50
- Modelo 4: ESU contrata al aliando bajo el Modelo AS-A-SERVICE

Arrojando como conclusión, que la implementación del proyecto SOC360 es viable y estratégica, tanto desde la perspectiva económica como institucional, así como altamente pertinente para fortalecer la gobernanza digital y la resiliencia tecnológica del sector público territorial. Adicionalmente, que de acuerdo con la evaluación de los diferentes escenarios, el modelo que permite un crecimiento más controlado de conformidad con las necesidades de los clientes y del proyecto, es el Modelo 4: AS-A-SERVICE, el cual no requiere inversión inicial.

En virtud de lo anterior, se requiere constituir una alianza estratégica mediante la cual la ESU, pueda ingresar al mercado de Soluciones en SOC con la participación de una empresa experta que cuente con trayectoria en este tipo de soluciones, con amplia experiencia en ejecución de contratos a nivel nacional, tanto con entidades públicas como privadas, además, que cuente con solidez económica y un equipo humano capacitado para afrontar de manera conjunta con la ESU los retos que fueron trazados en la visión proyectada para consolidación de nuestros clientes actuales y para la apertura de nuevos mercados. Así, se aporta experticia y demás beneficios como son: generación de conocimiento en sus colaboradores, inmersión en mercados no explorados por la entidad hasta ahora, reconocimiento en este tipo de soluciones, entre otros.

Según Kaliyaperumal (2021)*, un ***SOC (Security Operatión Center)*** *es una* ***instalación centralizada****, o unidad organizacional, que agrupa* ***personas, procesos y tecnología*** *para* ***monitorizar****,* ***detectar****,* ***investigar*** *y* ***responder*** *continuamente a incidentes y amenazas de ciberseguridad, con el objetivo de fortalecer la postura de seguridad digital de una organización.*

En el contexto de la aceleración digital (Digital Acceleration), con amenazas y actores maliciosos en constante evolución (APT – Advanced Persistent Threats), un SOC no es opcional sino una necesidad para la organización. Lo anterior, debido a que hoy en día es

clave en la estrategia de ciberseguridad para una empresa u organización (MinTIC para entidades públicas – modelo MSPI[1]), por factores como:

- *Ataques sofisticados*: Los ciberdelincuentes evolucionan constantemente sus tácticas y técnicas (TTPs). Utilizan herramientas automatizadas, métodos avanzados de ingeniería social y vulnerabilidades de día cero, lo que hace que sus ataques sean más difíciles de detectar con las medidas de seguridad tradicionales. Un SOC ofrece la experiencia y la supervisión continua necesarias para contrarrestar estas amenazas avanzadas.
- *Crecimiento exponencial de las superficies de ataque:* Las tendencias de aceleración digital como el trabajo remoto, la adopción de la nube y el IoT (Internet de las cosas) amplían significativamente la superficie de ataque de una organización. Esto crea más puntos de acceso que los atacantes pueden explotar. La visibilidad centralizada de un SOC ayuda a gestionar este panorama de riesgos más amplio.
- *Sensibilidad de los datos y normativa*: Muchas organizaciones manejan datos sensibles, ya sea información de clientes, datos financieros o propiedad intelectual. Un SOC demuestra un firme compromiso con la protección de estos datos y el cumplimiento de normativas como GDPR, HIPAA y PCI DSS, donde la supervisión de la seguridad puede ser un requisito.
- *Costo e impacto*: Las violaciones de datos pueden ser increíblemente costosas para las empresas. Aparte de las pérdidas financieras directas, una violación también daña la reputación de la organización, provoca la pérdida de clientes y puede dar lugar a multas legales.

Si bien la solución de tipo SOC es crucial para el sector público debido a que éste demanda cada vez más **servicios tecnológicos especializados en protección de datos y ciberseguridad**, especialmente en el contexto de ciudades inteligentes, digitalización de trámites y gobiernos digitales, contar con una alianza para operar un SOC robusto y profesionalizado permitiría a ESU ofrecer una **propuesta de valor diferencial** basada en la **seguridad como servicio (SECaaS)**, apalancando su experiencia local y credibilidad institucional.

Los SOC en entidades gubernamentales funcionan 24/7 para monitorear, detectar y responder ante ataques que podrían comprometer la infraestructura crítica (salud, energía, transporte) y poner en riesgo datos de los ciudadanos. En Estonia, España y otros países, se

---

1 * **Kaliyaperumal, R.** (2021). *The evolution of security operations and strategies for building an effective SOC*. ISACA Journal, **Volume 5**. Recuperado de https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-evolution-of-security-operations-and-strategies-for-building-an-effective-soc

demuestra que un SOC redujo significativamente interrupciones operativas. Además de lo anterior, mediante un SOC se puede garantizar:

- Defensa del dato ciudadano y cumplimiento normativo: El SOC protege la información personal de los ciudadanos y garantiza el cumplimiento de reglamentos como la Ley de Protección de Datos. Además, actúa como garante de transparencia, fundamental en un gobierno digitalizado.
- Visión integral de ciberseguridad y reducción de costos de brechas: Integrando herramientas como *SIEM, EDR, threat intelligence y hunting*, un SOC no solo detecta amenazas, sino que anticipa ataques, lo que previene brechas costosas y mejora la reputación institucional.
- Según un estudio en agencias públicas, esto reduce los costos de incidentes y minimiza tiempos de interrupción.
- Fortalecimiento del factor humano: La efectividad de un SOC depende de sus analistas. Un estudio reciente (2021) resalta que la capacitación, el diseño de procesos y la gestión del talento humano son tan críticos como la tecnología ACM Digital Library

En Colombia, el avance hacia un gobierno digital ha potenciado el uso de plataformas y datos abiertos, exigiendo a las entidades robustecer su ciberseguridad con SOC como componente clave. Actualmente se identifican barreras como la falta de personal altamente especializado, personas rotativas, restricciones presupuestales y la complejidad de procesos en sistemas de SOC públicos, con la entrega de conocimiento del sector privado en este tema se podría subsanar dicha brecha.

Ahora bien, el Apoyo gubernamental e institucional aporta al garantizar el respaldo presupuestal y estratégico desde lo más alto. El modelo híbrido público-privado, permite evaluar outsourcing controlado para cubrir capacidades especializadas, manteniendo control estatal, dichas sinergias aportan en el crecimiento de las entidades del estado para temas de Ciber seguridad y buena administración de la información.

En síntesis, implementar un SOC en el sector público no es una opción, es una necesidad estratégica en el contexto actual de gobiernos digitales. Protege datos, y fortalece la confianza ciudadana; todo bajo un modelo integrado que combina personas, procesos y tecnología, adaptado a la realidad y retos del Estado colombiano.
Finalmente, es importante rescatar el éxito y consideraciones de la implementación de este tipo de solución:

Modelo PPT + apoyo adicional (Majid & Ariffin, 2021)

"Based on prior studies…and the analysis…this study proposes a model…based on the critical factors of SOC, namely human, process, and technology, with support from external factors such as top management support, financial, and continuous improvement."

El estudio sugiere que para implementar un SOC de forma efectiva es crucial integrar tres componentes básicos: personas, procesos y tecnología. Además, debe existir respaldo de la alta dirección, recursos financieros adecuados y un mecanismo continuo de mejora. El modelo resultante permite a las instituciones –incluyendo al Estado– fortalecer sus capacidades defensivas al garantizar que cada elemento esté alineado y respaldado institucionalmente.[2]

Coordinación PPT para defensa sólida

"Coordination between humans, processes, and technologies is essential…to create strong cyber defences."

Una defensa cibernética robusta depende de la sinergia entre el personal que opera el SOC, los procedimientos que regulan su funcionamiento y las herramientas tecnológicas que lo soportan. Solo al operar en conjunto estos tres elementos se logra una protección efectiva frente a ataques.

SOC Nacional de Colombia (ColCERT) – Enero de 2025

En enero de 2025 se inauguró en Colombia el ***Centro de Operaciones de Seguridad Nacional***, gestionado por el grupo ColCERT, con una inversión cercana a USD 3.7 millones. Equipa herramientas avanzadas como Mandiant, ThreatQ, Trellix EDR y Tenable IO, para monitoreo continuo, detección proactiva y respuesta automatizada ante ciberamenazas, beneficiando inicialmente a más de 6.400 entidades públicas y extendiendo soporte a más de 300.000 organizaciones privadas.[3]

Centro Nacional de Seguridad Digital de Perú – 2023-2024

El Centro Nacional de Seguridad Digital (NDSC) del Perú integró en 2021 un CSIRT y un SOC dentro de su esquema de seguridad. En 2023-2024, se aplicó una hoja de ruta para madurar capacidades en monitoreo, SIEM y respuesta a incidentes, así como para robustecer infraestructura física y talento humano especializado.[4]

---

[2] Model for successful development and implementation of Cyber Security Operations Centre (SOC) - PMC

3 Ventas de Seguridad. (2025, 29 de enero). Colombia's National Security Operations Center inaugurated. Ventas de Seguridad.

4 Lee, C. (2025). Adapting cybersecurity maturity models for resource-constrained settings: A case study of Peru. The Electronic Journal of Information Systems in Developing Countries.

Agencia Gubernamental Malaya – Estudio Majid & Ariffin (2021)
Un estudio con 25 entidades federales de Malasia reveló que el éxito de un SOC no solo requiere tecnología y procesos robustos, sino que depende en un **principal lugar** del respaldo de la alta dirección. El análisis confirmó que, tras el compromiso político, la tecnología tuvo mayor impacto que los procesos, que a su vez influían más que las capacidades individuales del personal.[5]

Estos ejemplos muestran cómo diferentes niveles de gobierno desde entidades nacionales e internacionales han consolidado SOC efectivos combinando inversión, gobernanza, tecnología y talento humano, lo que ha resultado en mejoras reales en detección, respuesta y resiliencia cibernética.

Desde una perspectiva de crecimiento, esta alianza permitiría a ESU **acelerar el tiempo de salida al mercado** en un sector altamente competitivo, ofreciendo servicios de SOC como solución a alcaldías, hospitales, universidades y otras instituciones del Estado. Esto incluye desde la **consultoría inicial, el despliegue técnico, la operación y el soporte**, todo con una estructura escalable y eficiente. Las entidades públicas están cada vez más expuestas a amenazas cibernéticas (ransomware, ataques a infraestructuras críticas, fuga de datos). La alianza permitiría a ESU brindar **soluciones de cumplimiento con normativas locales (como la Ley 1581, Habeas Data, Decretos TIC)**, así como estándares internacionales como ISO 27001, NIST y GDPR, aumentando la confianza del cliente y reduciendo los riesgos legales.

La alianza también abriría la puerta a la **formación y transferencia de conocimiento**, lo cual es vital para una entidad como ESU que tiene una responsabilidad con el desarrollo tecnológico de Medellín. Esto se podría traducir en **entrenamiento del personal, formación de talento local en ciberseguridad**, y el fortalecimiento de un ecosistema digital resiliente en la ciudad.

Finalmente, esta colaboración estratégica puede posicionar a la ESU no solo como líder local, sino como una empresa con capacidad para **comercializar servicios especializados en ciberseguridad** a otras regiones de Colombia o incluso a nivel internacional, aprovechando su reputación como proveedor de confianza en el ámbito tecnológico y público.

Por lo anterior y soportado en el artículo 53, del acuerdo 090 de 2019, “Reglamento de contratación” de la ESU, y teniendo en cuenta lo indicado a continuación se justifica la Alianza estratégica a celebrar con NSIT:

[5] Majid, M. A., & Zainol Ariffin, K. A. (2021). *Model for successful development and implementation of Cyber Security Operations Centre (SOC)*. *PLOS ONE*, 16(11), e0260157.

- NSIT S.A.S. es una empresa especializada en servicios de TI y soluciones integrales de ciberseguridad

- NSIT S.A.S es una empresa que tienes experiencia en el acompañamiento a las organizaciones de la protección de sus activos digitales, el fortalecimiento de su infraestructura tecnológica y la prevención de amenazas que puedan comprometer el negocio.

- NSIT S.A.S cuentan con la tecnología, personal especializado y las soluciones avanzadas.

- Cuentan con certificaciones de Fortinet, cisco, Acronis, karpesky, eset, lo que quiere decir que cuentan con el respaldo de fabricantes, lo que permite entregar soluciones integrales y servicios de calidad.

- Cuentan con experiencia en el sector público, servicios como educación, financiero y salud.

- NSIT S.A.S. cuenta con certificado de Fortinet (Fortipartner) autorizado para vender productos y servicios de Fortinet con nivel Expert y como socio de servicios: Engage preferred services partner, El Ecosistema Abierto de Fortinet es uno de los ecosistemas de ciberseguridad más grandes de la industria, compuesto por socios de alianza tecnológica Fabric-Ready, colaboración con organizaciones que comparten amenazas y otras integraciones de Fabric. Proporciona soluciones de seguridad integradas con **Security Fabric** para que los clientes logren una seguridad avanzada de extremo a extremo en toda su infraestructura digital.

- Las condiciones (conocimiento, experiencia, tecnología, infraestructura, etc.) que posee NSIT S.A.S en ejercicio de su actividad económica, sumadas a las condiciones (conocimiento, experiencia, tecnología, infraestructura, naturaleza jurídica, relaciones comerciales en el sector público, etc.) que posee la ESU en ejercicio de su actividad económica, permiten el desarrollo conjunto y complementario de proyectos tecnológicos (principalmente asociados a las soluciones integrales en materia de seguridad digital, así como la provisión de bienes y servicios tecnológicos y de innovación), relacionados directa o indirectamente con el objeto social de esta última, con el fin de ser sometidos a prueba, ofrecidos y comercializados a terceros para el beneficio mutuo de los aliados estratégicos, optimizando de este modo las funciones comerciales de cada aliado para obtener ventajas competitivas en el mercado.

Conforme lo mencionado anteriormente, generar alianza con NSIT S.A.S., le permita a la ESU ofrecer servicios más completos, con mayor calidad y eficiencia.

2. ESPECIFICACIONES DEL CONTRATO MARCO DE ALIANZA ESTRATÉGICA:

2.1. OBJETO:

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.

2.2. ALCANCE DEL OBJETO:

Las Partes realizarán una exploración donde se podrán, sin excluir otras posibilidades, las siguientes actividades:

- Comercialización y prestación de bienes y servicios vinculados con los objetos de las partes.
- Gestión de proyectos (planeación, diseño, formulación y ejecución).
- Gestión de soluciones integrales para proyectos de *servicios de TI, SOLUCIONES INTEGRALES DE CIBERSEGURIDAD Y SEGURIDAD DIGITAL*, entre otros de conformidad con servicios vinculados con los objetos de las partes.
- Actividades de fortalecimiento y transferencia de conocimiento tecnológico dentro de las cuales se incluyen también asesoría y consultoría.

3. IDENTIFICACIÓN DEL TIPO DE CONTRATO A CELEBRAR:

Contrato Marco de Alianza Estratégica de acuerdo con lo establecido en el artículo 24 literal L y Articulo 53 del Acuerdo 090 de 2019 – Reglamento de Contratación de la Empresa para la Seguridad y Soluciones Urbanas-ESU.

4. VALOR DEL CONTRATO MARCO DE ALIANZA ESTRATÉGICA:

El valor del presente contrato es de cuantía indeterminada, cuyo valor será determinable a través de las ordenes de servicio que sean generadas durante su vigencia.

5. PLAZO DEL CONTRATO MARCO DE ALIANZA ESTRATÉGICA:

El plazo del contrato marco de alianza estratégica será contado desde la suscripción del contrato hasta, por doce (12) meses. En todo caso el plazo del contrato podrá ampliarse, antes de su vencimiento mediante documento suscrito por las partes.

6. FORMALIZACIÓN DEL CONTRATO MARCO DE ALIANZA ESTRATÉGICA:

Por tratarse de un contrato de cuantía indeterminada, el valor y formalización de este será dado mediante Ordenes de Servicios, las cuales deberán ser suscritas durante su vigencia, dentro de éstas serán dadas las especificaciones del servicio, alcance, así como el porcentaje de gestión comercial, comercialización, informes, plazo de ejecución, asignación presupuestal, obligaciones de las partes, aportes de las partes, derechos de comercialización, imagen corporativa (si aplica), entregables, matriz de riesgos, propiedad intelectual, garantías y todas las consideraciones que sean necesarias para el adecuado cumplimiento.

7. GESTIÓN COMERCIAL:

La gestión comercial será acordada en cada una de las ordenes de servicio derivadas en el desarrollo del contrato marco de alianza estratégica.

8. MATRIZ DE RIESGOS:

Entendiendo que el objeto del contrato pretende aunar esfuerzos, identificar mercados con intereses conjuntos entre las partes del contrato, se realizará matriz de riesgos para cada Orden de Servicios que sea suscrita durante la vigencia de la alianza estratégica.

9. OBLIGACIONES DE LA ALIANZA:

Para el cumplimiento de la presente Alianza, las partes se comprometen a:

1) Por parte de EL ALIADO ESTRATÉGICO: a) Informar sobre las propuestas y/o decisiones relacionadas con el desarrollo de la Alianza, b) Aportar el personal, equipos e infraestructura, que sean necesarios para el desarrollo de la presente Alianza, c) Prestar el apoyo y acompañamiento requerido para desarrollar los objetivos de la presente Alianza y de los contratos específicos que se llegasen a suscribir, d) Brindar la información y asesoría requerida para el desarrollo de los proyectos, e) Fomentar el intercambio de información y documentos entre las partes, f) Aplicar las medidas de seguridad necesarias y responder por el debido manejo de los instrumentos, instalación, materiales y equipos que se utilicen en LA ESU, así como por los daños que se puedan causar por negligencia o mala utilización, g) Las demás que sean necesarias para alcanzar los objetivos de la presente Alianza.

2) Por parte de **LA ESU**: a) Informar al Aliado sobre las decisiones y/o propuestas relacionadas con el desarrollo de la Alianza, b) Prestar el apoyo necesario para desarrollar los objetivos de la presente Alianza, c) Aportar el personal, equipos e infraestructura, que sean necesarios para el desarrollo de la presente Alianza, d) Facilitar los conocimientos y capacidades tecnológicas en proyectos conjuntos e) Velar por la correcta utilización de los equipos y demás elementos puestos por el Aliado en sus instalaciones, al servicio de las

actividades necesarias para el desarrollo de los proyectos conjuntos de diseño, comercialización, implementación y mantenimiento de las soluciones contratadas, f) Facilitar el uso de sus instalaciones y demás recursos técnicos, conforme a los planes de trabajo establecidos en cada contrato específico, g) Disponer de los medios, metodologías y tiempos necesarios para poder celebrar en debida forma las ordenes de servicios, contratos o acuerdo de voluntades, necesarios para materializar esta alianza. h) Las demás que sean necesarias para alcanzar los objetivos de la presente Alianza.

3) Por las partes: a) Designar un responsable de evaluar oportunidades, quien actuará como interlocutor ante la otra Parte. b) Poner a disposición un equipo de profesionales que acompañe el desarrollo de las actividades establecidas en la presente alianza. c) Presentar la información sobre funcionalidades, componentes y características de las Soluciones. d) Informar sobre los avances y resultados de las actividades realizadas. e) Respetar los derechos de propiedad intelectual y/o industrial de cada Parte, incluidos derechos de marca, secretos industriales y derechos de autor. La celebración de la presente alianza no constituye cesión y/o licenciamiento o autorización de uso o explotación de derechos patrimoniales. f) Cada Parte garantizará la confidencialidad de la información recibida, incluyendo información estratégica, técnica o comercial a la que llegare a tener acceso directamente o a través de sus dependientes o empleados, la cual se considera posee naturaleza confidencial. g) Actuar con buena fe en el desarrollo de las actividades propias de la presente alianza.

Para la ejecución de proyectos y/o negocios enmarcados bajo la vigencia de esta Alianza, las partes establecerán bilateralmente, en documento, las precisas condiciones comerciales de participación económica por el desarrollo de estos.

Toda la información respecto de la participación económica y/o gestión comercial en el desarrollo de esta Alianza será objeto de reserva, por lo que ninguna de las partes podrá revelar esta información, salvo que se trate de requerimiento de autoridad competente, para lo cual se informará previamente a la otra parte.

10. SEGUIMIENTO:

Para el seguimiento de esta alianza las partes celebrarán reuniones a necesidad de la alianza o de acuerdo con los negocios que surjan a partir de ella, que tengan como finalidad darle ejecución a través de la materialización de órdenes de servicio, de estas reuniones se levantarán actas que darán cuenta del seguimiento, ejecución y materialización de la alianza y que serán vinculantes para las partes en caso de que se establezcan compromisos por las personas facultadas para ello. La periodicidad, medio de convocatoria, asistentes y responsables para establecer compromisos serán definidos por las partes.

11. SUPERVISIÓN DEL CONTRATO MARCO DE ALIANZA ESTRATÉGICA:

La Supervisión de la Alianza Estratégica estará a cargo del Profesional Universitario o especializado o quien haga sus veces o quien sea designado por la ESU, el cual ejercerá las obligaciones y responsabilidades de acuerdo con lo establecido en el Manual de Supervisión de la Entidad.

Cordialmente,

ANGÉLICA MARÍA LÓPEZ
Subgerente de Servicios
Aprobó: Laura Alexandra Sepúlveda - Secretaría General
Aprobó: Nathalia Restrepo Caro-Subgerente Administrativo y Financiero
Revisó: Melisa María Mejía Román - Profesional Universitario - Unidad de Gestión Jurídica
Proyectó: Juliana Aguilar Duque - 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.