



## ESTUDIOS PREVIOS Y JUSTIFICACIÓN DE CONTRATACIÓN

Código: FT-M6-GC-12

Versión: 03

Página 1 de 32

### ESTUDIOS PREVIOS Y JUSTIFICACIÓN DE CONTRATACIÓN

#### ESTUDIOS Y DOCUMENTOS PREVIOS DE LA SOLICITUD PÚBLICA DE OFERTA PARA LA SELECCIÓN DE EMPRESAS COMERCIALIZADORAS DE BIENES Y SERVICIOS DE SOLUCIONES DE SEGURIDAD DIGITAL, SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD COMO ALIADOS PROVEEDORES PARA LA FIRMA DE ACUERDOS MARCO CON LA EMPRESA PARA LA SEGURIDAD Y SOLUCIONES URBANAS - ESU

##### 1. DESCRIPCIÓN DE LA NECESIDAD QUE LA ENTIDAD PRETENDE SATISFACER CON LA CONTRATACIÓN

La Empresa para la Seguridad y Soluciones Urbanas - ESU, es una Empresa Industrial y Comercial del Estado, del orden municipal, que tiene por objeto brindar soluciones integrales de seguridad, tecnología, servicios de redes y telecomunicaciones para la 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 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.

Adicionalmente tiene como misión la de contribuir a la transformación social, económica y ambiental de las ciudades y territorios, a través de soluciones integrales de seguridad, tecnología y gestión urbana.

Como forma de desarrollo de su objeto, la entidad tiene dentro de sus líneas estratégicas, la de seguridad digital, dentro de la cual se encuentra la comercialización, consultoría y desarrollo de soluciones para enfrentar las amenazas informáticas en el ciberespacio, que afectan significativamente al país.

De conformidad con los estatutos de la Empresa para la Seguridad y Soluciones Urbanas ESU, compilado mediante el Acuerdo número 102 del 8 de marzo de 2021, y específicamente según el Artículo 6° Formas de Desarrollo del Objeto, la ESU definió, entre otras, la línea Estratégica de Tecnología, la cual consiste en “Soluciones tecnológicas, innovadoras y eficientes que contribuyen al mejoramiento de procesos de nuestros clientes”. De igual forma, para poder ofrecer las líneas estratégicas definidas, en dicho artículo se determinó que la empresa desarrollará, entre otras, las siguientes actividades: a. Asesoría y consultoría; b. Comercialización y prestación de bienes y servicios; Gestión de proyectos (planeación, formulación, ejecución, evaluación e interventoría); Proveer redes y Servicios de Telecomunicaciones; e. Suministro y gestión de equipos, sistemas, redes e infraestructura tecnológica; f. Promover la investigación aplicada la innovación y la transferencia de conocimiento; g. Provisión de equipos, software y personal especializado en la identificación y prevención de ataques cibernéticos; h. Diseño, desarrollo, integración, licenciamiento y gestión de software y servicios informáticos; i. Diseño, construcción, gerencia y mantenimiento de obras públicas y privadas necesarias para el desarrollo de los proyectos de seguridad, logística, tecnología y/o sostenibilidad.



## ESTUDIOS PREVIOS Y JUSTIFICACIÓN DE CONTRATACIÓN

Código: FT-M6-GC-12

Versión: 03

Página 2 de 32

De acuerdo con lo expresado en ítem g, donde se expresa que la ESU tiene en sus principales actividades la “Provisión de equipos, software y personal especializado en la identificación y prevención de ataques cibernéticos”, implicando el desarrollo de proyectos donde se promueven y despliegan soluciones tecnológicas en apoyo a las labores de Seguridad Digital, Seguridad de la Información y Ciberseguridad, los presentes estudios previos se requieren para seleccionar aliados proveedores que permitan la atención de las necesidades de nuestros clientes en cuanto los aspectos técnicos mencionados, y una mejor oferta de mercado, toda vez que la ESU no suministra directamente los bienes y servicios que requieren en estos temas. Por ende, se hace necesario iniciar un proceso de selección de Aliados Proveedores para la línea de servicios de ciberseguridad y seguridad Digital mediante Solicitud Pública de Oferta.

Entiéndase seguridad Digital, seguridad de la información y ciberseguridad como las actividades asociadas a la protección de la información y la privacidad de datos, en el almacenamiento, uso y transporte de la información digital, establecimiento de controles de seguridad, diseño de procesos de ciberseguridad, monitoreo de la seguridad entre otros. Abarcando actividades de ingeniería y desarrollo en marco de la protección de la información que día a día crece en marco de la transformación digital

De allí que la ESU deba desarrollar proyectos donde se promuevan y desplieguen soluciones tecnológicas en apoyo a las labores de Seguridad Digital, Seguridad de la Información y Ciberseguridad, motivo por el cual requiere seleccionar aliados proveedores para esta línea de servicios, logrando así una mejor oferta de mercado.

### 2. OBJETO A CONTRATAR

Selección de empresas comercializadoras de bienes y servicios de Soluciones de Seguridad Digital, Seguridad de la Información y Ciberseguridad como aliados proveedores para la firma de acuerdos marco con la Empresa para la Seguridad y Soluciones Urbanas – ESU.

### 3. ESPECIFICACIONES DEL BIEN O SERVICIO A CONTRATAR:

El alcance del objeto del acuerdo marco de aliado proveedor será el suministro, implementación, mantenimiento y cualquier otro tipo de servicio para la satisfacción de las necesidades que requieran nuestros clientes en materia de bienes y servicios de soluciones de seguridad digital, seguridad de la información y ciberseguridad tales como: Gestión, Riesgo y Cumplimiento – GRC, Consultoría especializada (Establecimiento de Sistemas de Gestión de Seguridad SGSI basado en la norma ISO27001:2013 y los lineamientos de Gobierno en Línea, Acompañamiento a la certificación ISO27001:2013, Auditorías de Terceros), Centro de Operaciones de Seguridad SOC-NOC, Servicios de Atención de Incidentes de Seguridad y Ciberseguridad, Monitoreo de Productividad y Ciberseguridad de los usuarios, Ciclo de Vida de desarrollo seguro – S-SDLC, Análisis de Código Estático y Dinámico, Gestión continua de Vulnerabilidades, Hacking Ético, Servicios de Resolución de Vulnerabilidades, Monitoreo de Marca Empresarial, Ejercicios de RedTeam, Pruebas de Ingeniería Social, Pruebas de Intrusión Física, Protección Integral de Correo Electrónico, Control de Acceso a la Red, Protección Integral de Estaciones de Trabajo, Control de Navegación – Proxy,



## ESTUDIOS PREVIOS Y JUSTIFICACIÓN DE CONTRATACIÓN

Código: FT-M6-GC-12

Versión: 03

Página 3 de 32

Control de seguridad Perimetral, Firewalls y NGFW, Sandbox, Herramientas de Identificación y control de Amenazas Persistentes Avanzadas – APTs, capacitación, todo lo relacionado con las tecnologías e infraestructura que permita tener la Seguridad digital de nuestros clientes y que se encuentren dentro de los criterios técnicos y de cuantía que establezca la ESU.

#### 4. IDENTIFICACIÓN DEL CONTRATO A CELEBRAR:

El contrato a celebrar será un acuerdo marco de aliado proveedor, el cual es una modalidad contractual que permite disponer y pactar unas condiciones administrativas, técnicas, jurídicas y/o económicas generales, que regirán unas relaciones contractuales particulares que serán complementadas para cada bien o servicio específico, y cuyas condiciones se complementarán con aquellas generales. Esto permite hacer eficiente la prestación de los servicios y la operación administrativa interna, y además constituye un soporte contractual importante para las proyecciones de ventas y crecimiento comercial y de servicios de la entidad.

Esta condición de contrato marco ha permitido otorgarle un manejo presupuestal ágil a la relación contractual, en la medida que su celebración no ha requerido de la incorporación directa de recursos por parte de la ESU, sino que su movimiento de recursos precede de una comercialización efectiva del producto y a partir de allí se procede a definir márgenes de rentabilidad y condiciones de operación.

En conclusión será necesario realizar tantas Solicitudes Públicas de Oferta cuyo objeto sea la “SELECCIÓN DE EMPRESAS COMERCIALIZADORAS DE BIENES Y SERVICIOS DE SOLUCIONES DE SEGURIDAD DIGITAL, SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD COMO ALIADOS PROVEEDORES PARA LA FIRMA DE ACUERDOS MARCO CON LA EMPRESA PARA LA SEGURIDAD Y SOLUCIONES URBANAS - ESU”, con el fin de tener tres (3) Aliados Proveedores, con el fin de no perder la posibilidad de generar economías de escala para nuestros clientes, que se logran con la agregación de la demanda por parte de los aliados proveedores, de conformidad con lo dispuesto en el Reglamento de Contratación de la ESU.

Una vez seleccionados los aliados proveedores, se realizarán solicitudes privadas de ofertas entre los mismos de acuerdo a las políticas de la ESU y su Manual de Contratación, para que presenten ofertas que permitan proveer los bienes y servicios requeridos por nuestros clientes; o por los demás mecanismos dispuestos en la normativa interna de contratación de la ESU. Realizada la selección de la oferta ganadora, bastará el respectivo contrato con el aliado seleccionado para formalizar la contratación.

Al adquirir la calidad de aliado proveedor se obtiene el derecho a participar en las solicitudes privadas de ofertas entre aliados proveedores que compiten entre sí para la adjudicación de contratos, pero el hecho de ser aliado proveedor no implica por sí mismo la adjudicación de algún contrato, sino la expectativa de contratar con la ESU de conformidad con lo dispuesto en el Reglamento Interno de Contratación.

## **5. MODALIDAD DE SELECCIÓN DEL CONTRATISTA:**

Según el Reglamento de Contratación de la ESU, Acuerdo 090 de 2019 en su Artículo 25, prevé que la selección de aliados proveedores se hará mediante Solicitud Pública de Oferta, con el fin de suministrar con eficiencia y eficacia los bienes y servicios que requieran los clientes. Los términos y condiciones de contratación para la selección serán generales y tendrán en cuenta la capacidad financiera, operativa, experiencia, trayectoria, capacidad de contratación, y de acuerdo a las necesidades que se pretende suplir.

En el proceso podrán participar solo las personas jurídicas que cumplan los requisitos que se indican en el pliego de condiciones y que se encuentren en condiciones legales, económicas y técnicas de cumplir con el objeto aquí señalado.

La persona jurídica nacional debe encontrarse debidamente constituida por un término no menor a diez (10) años contados a partir de la fecha de cierre del proceso de selección.

No podrán participar en el presente proceso de selección, quienes se encuentren en cualquiera de las siguientes situaciones: Cesación de pagos; Concurso de acreedores; y cualquiera otra circunstancia que permita presumir incapacidad o imposibilidad jurídica, económica o técnica para cumplir con el objeto de los contratos que eventualmente pudieran suscribirse.

Todas las personas jurídicas interesadas, independientemente de que en la actualidad tengan alguna relación comercial con la ESU, deberán cumplir con la totalidad de los requisitos exigidos para la participación, so pena de rechazo.

## **6. VALOR ESTIMADO DEL CONTRATO Y JUSTIFICACIÓN DEL MISMO:**

Los servicios que se soliciten en el marco de esta alianza serán con destino a los diferentes clientes con los que cuenta la ESU, en virtud de los Contratos Interadministrativos que la ESU tenga suscritos o a suscribir.

El presente proceso de selección de aliados proveedores no conlleva ejecución presupuestal, toda vez que el objeto del mencionado es la escogencia de aliados proveedores para firma de acuerdos marco, el cual tendrá una cuantía indeterminada pero determinable de acuerdo al valor de los contratos que haya ejecutado los aliados proveedores durante la vigencia de los acuerdos.

En todo caso en los contratos y/u órdenes de servicio resultantes que se deriven del acuerdo marco se indicará la imputación presupuestal de conformidad con el requerimiento allegado por el cliente.

## **7. JUSTIFICACIÓN DE LOS FACTORES DE SELECCIÓN:**

Los proponentes deberán acreditar dentro de la propuesta presentada, los siguientes requisitos y documentos habilitantes, además de los de carácter técnico que serán evaluados conforme a las reglas siguientes:

	<b>ESTUDIOS PREVIOS Y JUSTIFICACIÓN DE CONTRATACIÓN</b>	<b>Código:</b> FT-M6-GC-12
		<b>Versión:</b> 03
		Página 5 de 32

### 7.1. Requisitos habilitantes

Con respecto a los requisitos habilitantes las personas jurídicas interesadas deben cumplir la totalidad de estos, so pena de rechazo.

La ESU verificará los requisitos habilitantes de cada oferta presentada, de acuerdo con la Ley y las exigencias establecidas en el pliego de condiciones, los cuales serán de carácter técnico, jurídico, financiero y de experiencia, con el fin de establecer las ofertas que posteriormente serán objeto de calificación, así:

**Información Jurídica:** Después de la apertura de las propuestas, la ESU realizará el análisis jurídico de las mismas, con el fin de determinar cuáles se encuentran ajustadas a la Ley y a los requisitos del Pliego de Condiciones, solicitando las aclaraciones que considere pertinentes, las cuales serán resueltas por el proponente en el término concedido por la ESU para ello, de lo contrario, dicha información se tendrá por no presentada y la propuesta será rechazada.

La ESU, con la finalidad de fortalecer los procedimientos y buenas prácticas para identificación y clasificación de riesgos operativos y legales, y evitar especialmente riesgos reputacionales o éticos, se reserva el derecho de solicitar aleatoriamente información sobre el proponente, su representante legal, junta directiva y socios, con el fin de validar sus condiciones jurídicas y económicas, a efectos de verificar directamente o a través de terceros, vinculaciones con el terrorismo, contrabando, actividades ilícitas. Lo anterior se hará mediante la consulta de listas restrictivas, listas vinculantes, listas sancionatorias, y demás bases de datos pertinentes. El resultado de estas verificaciones podrá dar lugar a la suscripción condicionada de acuerdos marco, a la no consideración de la propuesta presentada o la terminación inmediata y unilateral de los Acuerdos Marco y contratos derivados, ante situaciones conocidas con posterioridad.

**Información financiera:** Los oferentes nacionales deberán anexar el respectivo Certificado del Registro Único de Proponentes -RUP- expedido por la Cámara de Comercio correspondiente, con una fecha de expedición no mayor a treinta (30) días calendario contados a la fecha de cierre del proceso.

#### Clasificación RUP

Clasificación UNSPSC: El objeto del presente contrato está codificado en el Clasificador de Bienes y Servicios UNSPSC como se indica a continuación:

<b>Clasificador de Bienes y Servicios de Naciones Unidas (UNSPSC)</b>	<b>Descripción</b>
43211500	Difusión de Tecnologías de Información y Telecomunicaciones Computadores / Equipo informático y accesorios / Computadores
43222500	Difusión de Tecnologías de Información y Telecomunicaciones / Equipos o plataformas y accesorios de redes multimedia o de voz y datos / Equipo de seguridad de red
43233200	Difusión de Tecnologías de Información y Telecomunicaciones Computadores / Software / Software de seguridad y protección
80101600	Servicios de Gestión, Servicios Profesionales de Empresa y Servicios Administrativos / Servicios de asesoría de gestión / Gerencia de proyectos
81111800	Servicios Basados en Ingeniería, Investigación y Tecnología / Servicios informáticos / Servicios de sistemas y administración de componentes de sistemas
81112200	Servicios Basados en Ingeniería, Investigación y Tecnología / Servicios informáticos / Mantenimiento y soporte de software
81112300	Servicios Basados en Ingeniería, Investigación y Tecnología / Servicios informáticos / Mantenimiento y soporte de hardware de computador
81161500	Servicios Basados en Ingeniería, Investigación y Tecnología / Servicios informáticos / Entrega de servicios de tecnología de información / Servicios de administración de acceso

Los proponentes deberán cumplir mínimo los siguientes indicadores para considerarse habilitados financiera y organizacionalmente por cada uno de los alcances definidos en el pliego de condiciones así:

**Indicadores de capacidad financiera.**

INDICADOR	CÁLCULO	VALOR HABILITANTE
Indicador de Liquidez	$\frac{\text{Activo corriente}}{\text{Pasivo Corriente}}$	Mayor o igual a uno punto noventa y cinco (1.95)
Indicador de Endeudamiento	$\frac{\text{Pasivo total}}{\text{Activo Total}}$	Menor o igual al cincuenta y tres por ciento (53%)
Capital de trabajo	Activo Corriente - Pasivo Corriente	Mayor o igual a seis mil ochocientos ochenta millones de pesos M.L (\$6.880.000.000)
Cobertura de Intereses	$\frac{\text{Utilidad operacional}}{\text{Gastos intereses}}$	Mayor o igual a dos punto cinco (2.5)

**Indicadores de capacidad organizacional:**

Indicador	Cálculo	Valor Habilitante
Rentabilidad del Patrimonio	$\frac{\text{Utilidad operacional}}{\text{Total Patrimonio}}$	<u>Mayor o igual a cero punto diez (0.10)</u>
Rentabilidad del Activo	$\frac{\text{Utilidad operacional}}{\text{Total Activo}}$	<u>Mayor o igual al cero punto cero cuatro (0.04)</u>

**Experiencia Habilitante:**

Teniendo en cuenta las actividades que se deben ejercer para adquirir bienes y servicios de Soluciones de Seguridad Digital, Seguridad de la Información y Ciberseguridad, es importante contar con aliados que demuestren una adecuada experiencia en este tipo de contrataciones, donde se debe verificar la idoneidad requerida.

La experiencia requerida se deberá acreditar con la suma de contratos que se encuentren en el Registro Único de Proponentes - RUP, inscritos en al menos tres de los códigos estipulados a continuación:



**ESTUDIOS PREVIOS Y JUSTIFICACIÓN DE  
CONTRATACIÓN**

**Código:** FT-M6-GC-12

**Versión:** 03

Página 8 de 32

<b>Clasificador de Bienes y Servicios de Naciones Unidas (UNSPSC)</b>	<b>Descripción</b>
43211500	Difusión de Tecnologías de Información y Telecomunicaciones Computadores / Equipo informático y accesorios / Computadores
43222500	Difusión de Tecnologías de Información y Telecomunicaciones / Equipos o plataformas y accesorios de redes multimedia o de voz y datos / Equipo de seguridad de red
43233200	Difusión de Tecnologías de Información y Telecomunicaciones Computadores / Software / Software de seguridad y protección
80101600	Servicios de Gestión, Servicios Profesionales de Empresa y Servicios Administrativos / Servicios de asesoría de gestión / Gerencia de proyectos
81111800	Servicios Basados en Ingeniería, Investigación y Tecnología / Servicios informáticos / Servicios de sistemas y administración de componentes de sistemas
81112200	Servicios Basados en Ingeniería, Investigación y Tecnología / Servicios informáticos / Mantenimiento y soporte de software
81112300	Servicios Basados en Ingeniería, Investigación y Tecnología / Servicios informáticos / Mantenimiento y soporte de hardware de computador
81161500	Servicios Basados en Ingeniería, Investigación y Tecnología / Servicios informáticos / Entrega de servicios de tecnología de información / Servicios de administración de acceso

El proponente en su oferta deberá adjuntar certificación, en la cual se consignará la información sobre su experiencia en relación con el objeto de la presente Solicitud Pública de Oferta.

Deberá demostrar experiencia en los últimos ocho (8) años, con máximo seis (6) contratos, cuya sumatoria del monto total de estos sea igual o superior a nueve mil quinientos (9.500) SMMLV; y cada uno de los contratos certificados, no sea inferior a novecientos noventa (990) SMMLV.

Los contratos deben estar ejecutados y reportados en el RUP vigente, no se aceptan contratos en ejecución.

No se permiten certificaciones emitidas entre los miembros de un proponente plural, deben ser certificaciones emitidas directamente por el cliente final.

Las certificaciones se evaluarán a partir de la información que suministre el oferente, las cuales deben ser expedidas por la entidad o empresa contratante y deben contener como mínimo la siguiente información: la razón social de la entidad o empresa contratante, dirección, teléfono, número de contrato, fecha del contrato, objeto del contrato, alcances, valor del contrato, fecha de inicio y de terminación del contrato. Las certificaciones deberán estar firmadas por el representante legal de la empresa que las expide o por la persona autorizada para ello.

Las certificaciones deberán contener al menos uno de los siguientes alcances:

- Gestión, Riesgo y Cumplimiento – GRC.
- Consultoría especializada - Establecimiento de Sistemas de Gestión de Seguridad SGSI basado en la norma ISO27001:2013 y los lineamientos de Gobierno en Línea.
- Consultoría especializada - Acompañamiento a la certificación ISO27001:2013.
- Consultoría especializada - Auditorías de Terceros.
- Centro de Operaciones de Seguridad SOC-NOC.
- Servicios de Atención de Incidentes de Seguridad y Ciberseguridad.
- Monitoreo de Productividad y Ciberseguridad de los usuarios.
- Ciclo de Vida de desarrollo seguro – S-SDLC
- Análisis de Código Estático y Dinámico.
- Gestión continua de Vulnerabilidades.
- Hacking Ético.
- Servicios de Resolución de Vulnerabilidades.
- Monitoreo de Marca Empresarial.
- Ejercicios de RedTeam.
- Pruebas de Ingeniería Social.
- Pruebas de Intrusión Física.
- Protección de Integral de Correo Electrónico.
- Control de Acceso a la Red.
- Protección de Integral de Estaciones de Trabajo.
- Control de Navegación – Proxy.



## ESTUDIOS PREVIOS Y JUSTIFICACIÓN DE CONTRATACIÓN

Código: FT-M6-GC-12

Versión: 03

Página 10 de 32

- Control de seguridad Perimetral.
- Firewalls y NGFW.
- Sandbox de Ciberseguridad.
- Herramientas de Identificación y control de Amenazas Persistentes Avanzadas – APTs.
- Implementación de sistemas de correlación o detección de eventos o análisis comportamental.
- Prestación de servicios de seguridad

En el caso que las certificaciones expedidas por el contratante no contengan la información mínima requerida, la ESU podrá solicitar las respectivas aclaraciones.

### Habilitación Técnica:

El oferente debe proveer directamente los servicios y soluciones enumerados en el Anexo 8 - “Relación de Alcances Bienes, Servicios y Soluciones Requeridos” y debe dar respuesta punto a punto a cada uno de los requerimientos indicando los documentos donde da cumplimiento a cada uno de los ítems.

La ESU verificará los requisitos habilitantes de cada oferta presentada, de acuerdo con la Ley y las exigencias establecidas en el pliego de condiciones, con el fin de establecer las ofertas que posteriormente serán objeto de calificación.

Los proponentes deberán presentar con la oferta cada uno de los documentos que a continuación se relacionan, con el fin de cumplir con los requisitos habilitantes y ser admitidos, y poder continuar en el proceso de evaluación y selección del aliado proveedor.

No se aceptarán ofertas presentadas en Unión Temporal o Consorcio.

### 7.2. Documentos de la propuesta

Para facilitar la correcta integración de la propuesta por parte del proponente, su estudio y evaluación por parte de la ESU, se solicita al proponente que presente los documentos de la propuesta en el mismo orden en que se relaciona en este numeral.

Si en el listado que a continuación se indica no aparece enunciado un documento o información solicitada en el Pliego de Condiciones, ello no implica que desaparezca el requisito de aportarlo con la propuesta.

- a) Copia de la cédula de ciudadanía del representante legal de la persona jurídica.
- b) Copia del Certificado de Existencia y Representación Legal. Si el proponente es persona jurídica, expedido por la Cámara de Comercio de la jurisdicción o por autoridad competente para ello, expedido con una anterioridad no mayor a un (1) mes a la fecha de cierre de esta Solicitud Pública de Oferta. El objeto social del proponente debe estar relacionado con el objeto de la presente Solicitud Pública de oferta. La persona jurídica debe estar legalmente constituida y su duración no podrá ser inferior al plazo del contrato y un año más.

Si del certificado de existencia y representación legal se desprende que el representante legal requiere de una autorización previa de la Junta de Socios o Junta Directiva para celebrar contratos de determinada cuantía, se deberá anexar a la propuesta copia del acta correspondiente en donde se le autorice.

- c) Copia del Registro Único Tributario (RUT) actualizado, y expedido por la Dirección de Impuestos y Aduanas Nacionales - DIAN, donde aparezca claramente el NIT del proponente.
- d) Registro Único de Proponentes, expedido con una anterioridad no mayor a un (1) mes a la fecha de cierre de esta Solicitud Pública de Oferta, en firme.
- e) Certificado expedido por la Procuraduría General de la Nación de la persona jurídica y del representante legal, el cual podrá consultarse en la página web [www.procuraduria.gov.co](http://www.procuraduria.gov.co)
- f) Certificado expedido por la Contraloría General de la Nación de la persona jurídica y del representante legal, el cual podrá consultarse en la página web [www.contraloria.gov.co](http://www.contraloria.gov.co) (NOTA: Para la Consulta del Certificado de Antecedentes Fiscales de Persona Jurídica, deberá generarse el certificado incluyendo el dígito de verificación, sin puntos ni guiones).
- g) Certificado de antecedentes judiciales del representante legal de la persona jurídica el cual puede consultarse en la página web [www.antecedentes.policia.gov.co](http://www.antecedentes.policia.gov.co). <https://antecedentes.policia.gov.co:7005/WebJudicial/>.
- h) Certificado del registro nacional de medidas correctivas, donde conste que el representante legal no le han sido impuestas multas por infracción del Código de Policía o, si presenta multas, que no hayan transcurrido más de seis (6) meses sin pagarlas, el cual puede consultarse en el link [https://svcnpc.policia.gov.co/PSC/frm\\_cnp\\_consulta.aspx](https://svcnpc.policia.gov.co/PSC/frm_cnp_consulta.aspx).
- i) Certificado de la Consulta de Inhabilidades de la Ley 1918 de 2018 y Decreto 753 de 2019 del representante legal de la empresa.
- j) Sistema de Gestión de Seguridad y Salud en el Trabajo. El oferente deberá aportar los siguientes documentos:
  - ✓ Certificación de la Administradora de Riesgos Laborales (ARL) donde se evidencie el porcentaje de cumplimiento de migración a las normas en materia del Sistema de Gestión en Seguridad y Salud en el Trabajo-SGSST deberá presentar dicha certificación emitida por su ARL. El certificado debe estar vigente y no podrá superar los 90 días calendario de haber sido expedido por la respectiva ARL.
  - ✓ Copia de la designación del responsable del Sistema de Gestión de Seguridad y Salud en el Trabajo.
  - ✓ Copia de la licencia vigente de seguridad y salud en el trabajo del responsable del Sistema de Gestión de Seguridad y Salud en el Trabajo, de acuerdo con la clasificación de empresas de la Resolución 0312 de 2019, que expresa:

N° Trabajadores	Riesgo	Formación	Experiencia
De 0 a 10	I, II, III	Técnico SST	1 año
De 11 a 50	I, II, III	Tecnólogo SST	2 años
Más de 50	I, II, III, IV, V	Profesional en SST o Profesional con especialización en SST.	N/A
Cualquier número de trabajadores	IV, V		

- ✓ Certificado de pago de aportes parafiscales de los últimos seis (6) meses del proponente, el cual deberá estar firmado por el Representante Legal o por el Revisor Fiscal, si está obligado a tenerlo. La certificación suscrita por revisor fiscal deberá ir acompañada de la Tarjeta profesional y Certificado de la Junta Central de Contadores vigente.

**k) Documentación soporte según lo requerido en el Capítulo N° 4 del pliego de condiciones**

Los documentos que hacen parte de los Pliegos de Condiciones constituyen la única fuente de información que el proponente tiene para la preparación de la oferta, a su vez éste podrá solicitar las aclaraciones o presentar los comentarios y observaciones que considere necesarios sobre los pliegos de condiciones, hacerla llegar al correo [propuestas@esu.com.co](mailto:propuestas@esu.com.co) con copia a [mpatino@esu.com.co](mailto:mpatino@esu.com.co), [eosorio@esu.com.co](mailto:eosorio@esu.com.co), [lgraciano@esu.com.co](mailto:lgraciano@esu.com.co), dentro del plazo fijado para estas presentar estas observaciones en el cronograma que rige este proceso.

### **7.3. Factores de Evaluación**

Una vez realizadas las verificaciones jurídica y financiera, la ESU efectuará la evaluación y calificación de las propuestas teniendo en cuenta los siguientes factores de evaluación:

<b>FACTOR</b>	<b>PUNTAJE TOTAL</b>
Portafolio de Bienes Servicios y Soluciones	700
Recurso Humano	150
Experiencia Adicional Proponente	50
Elementos de Calidad	100
<b>PUNTAJE TOTAL</b>	<b>1000</b>

#### **7.3.1 PORTAFOLIO DE BIENES, SERVICIOS Y SOLUCIONES (700 PUNTOS)**

El oferente debe proveer directamente los bienes, servicios y soluciones enumerados en el ANEXO 8 - RELACIÓN DE ALCANCES BIENES SERVICIOS Y SOLUCIONES REQUERIDOS y debe dar respuesta punto a punto a cada uno de los requerimientos y entregar la información y documentos solicitados en caso de que aplique. Lo anterior para obtener el puntaje citado en la tabla siguiente, de no cumplirlos obtendrá cero (0) puntos en cada bien, servicios y/o soluciones a prestar.

El oferente podrá presentarse a uno o varios de los servicios a prestar, sin embargo deberá cumplir con el 100% de los requerimientos para el que aplique y deberá relacionar la documentación técnica de soporte de cumplimiento de los puntos solicitados.

La documentación técnica podrá entregarse en medio magnético y en idioma castellano o inglés, cualquier otro idioma deberá estar acompañado por una traducción simple del documento al idioma castellano.

La ESU podrá solicitar en caso de aclaraciones la traducción oficial de los documentos presentados como soporte para los siguientes ítems.

	Requerimiento
<b>Requerimientos Generales</b>	Manejar la Gestión del contrato bajo una metodología de Gestión de Proyectos como los lineamientos dados por el PMI y estos deben ser realizados por personal Certificado en Gestión de Proyectos
	Todos los servicios se deben prestar en el idioma español
	El oferente debe contar con un centro de operaciones de ciberseguridad propio en el territorio nacional colombiano desde el cual se deben brindar todos los servicios y soluciones
	El oferente debe contar con experiencia mínima de diez (10) años brindando soluciones de seguridad y ciberseguridad, se debe acreditar con experiencia comprobable de clientes
	Todos los servicios deben ser brindados en modalidad 7x24x365
	El oferente debe estar en capacidad de ofrecer todos los servicios, bienes y soluciones enunciados a continuación, no se aceptan servicios y soluciones parciales.

SERVICIOS A PRESTAR	SERVICIO PONDERACIÓN	PUNTAJE	PUNTAJE MÁXIMO
Gestión, Riesgo y Cumplimiento – GRC.	Dar cumplimiento a los requerimientos y entrega de la documentación solicitada	115	700
Centro de Operaciones de Seguridad SOC-NOC.		110	
Herramientas de Identificación y control de Amenazas Persistentes Avanzadas – APTs.		110	
Protección de Integral de Correo Electrónico.		40	

Control de Acceso a la Red.	40
Protección de Integral de Estaciones de Trabajo.	40
Control de Navegación – Proxy.	40
Control de seguridad Perimetral - Firewalls y NGFW	40
Sandbox de Ciberseguridad.	40
Análisis de Código Estático y Dinámico.	30
Gestión continua de Vulnerabilidades.	20
Monitoreo de Productividad y Ciberseguridad de los usuarios.	15
Monitoreo de Marca Empresarial.	10
Consultoría especializada - Establecimiento de Sistemas de Gestión de Seguridad SGSI basado en la norma ISO27001:2013 y los lineamientos de Gobierno en Línea.	5
Consultoría especializada - Acompañamiento a la certificación ISO27001:2013.	5
Consultoría especializada -Auditorías de Terceros.	5
Servicios de Atención de Incidentes de Seguridad y Ciberseguridad.	5
Ciclo de Vida de desarrollo seguro – S-SDLC	5
Hacking Ético.	5
Servicios de Resolución de Vulnerabilidades.	5
Ejercicios de RedTeam.	5
Pruebas de Ingeniería Social.	5
Pruebas de Intrusión Física.	5

### **7.3.2 RECURSO HUMANO (150 PUNTOS)**

El oferente deberá asignar los recursos y perfiles necesarios para cumplir con los servicios a prestar, sin embargo, deberá adjuntar con su propuesta las hojas de vida y las certificaciones de experiencia de los recursos mínimos con los cuales ejecutaran los servicios.

	<b>ESTUDIOS PREVIOS Y JUSTIFICACIÓN DE CONTRATACIÓN</b>	<b>Código:</b> FT-M6-GC-12
		<b>Versión:</b> 03
		Página 15 de 32

Para que una certificación de experiencia se considere válida, deberá cumplir las siguientes condiciones:

- ✓ Nombre y NIT de la empresa contratante
- ✓ Fecha de inicio del contrato.
- ✓ Fecha de terminación del contrato.
- ✓ Cargo y funciones desarrolladas.
- ✓ Fecha de expedición de la certificación.

El Oferente deberá adjuntar con la propuesta, la siguiente documentación para cada uno de los profesionales propuestos:

- ✓ Hoja de vida
- ✓ Actas de grado y/o diplomas de pregrado y postgrado (según la formación académica solicitada para cada perfil)
- ✓ Tarjeta profesional y/o matrícula profesional y certificado de vigencia de la matrícula
- ✓ Certificaciones técnicas mínimas requeridas
- ✓ Carta de compromiso del profesional. El modelo de esta se encuentra en el ANEXO N° 9 - CARTA DE COMPROMISO
- ✓ Fotocopias de las constancias o certificaciones de experiencia laboral y/o de prestación de servicios. En todos los casos donde se requiera ser profesional, sólo se contabilizará la experiencia posterior a la expedición de la tarjeta o matrícula profesional para lo cual es indispensable adjuntar este documento.

La ESU podrá solicitar a los proponentes aclaración de las certificaciones o la presentación de los documentos que conduzcan a ello, conforme con lo establecido en el pliego de condiciones. En ejercicio de esta facultad, los proponentes no podrán adicionar, modificar o mejorar sus propuestas.

La ESU, se reserva el derecho de verificar, cuando lo considere necesario, la información que suministren los oferentes sobre el personal requerido. La ESU verificará que la documentación presentada por el oferente se ajuste a lo exigido en los pliegos de condiciones, además se reserva el derecho de confirmar la veracidad de dichas certificaciones.

Para efecto del presente proceso de selección, el oferente podrá con miras a obtener el puntaje correspondiente a este criterio, ofrecer las condiciones descritas a continuación de los Recursos Humanos para lo cual debe acreditar los requisitos allí exigidos como concepto para obtener los respectivos puntajes.

ROL	DEDICACIÓN	OFRECIMIENTO	PUNTAJE MÁXIMO	PUNTAJE MÁXIMO TOTAL
UN (1) GERENTE DE SERVICIOS DE CIBERSEGURIDAD	100%	Recurso que cumple con los requerimientos solicitados	15	150
UN (1) LÍDER TÉCNICO DE SERVICIOS DE CIBERSEGURIDAD	100%	Recurso que cumple con los requerimientos solicitados	25	
UN (1) ARQUITECTO Y ASEGURADOR DE CALIDAD DE CIBERSEGURIDAD	50%	Recurso que cumple con los requerimientos solicitados	20	
UN (1) CONSULTOR CIBERSEGURIDAD Y SEGURIDAD DE LA INFOMACION	80%	Recurso que cumple con los requerimientos solicitados	15	
UN (1) ANALISTA SOC/NOC	70%	Recurso que cumple con los requerimientos solicitados	15	
UN (1) OPERADOR SOC/NOC	100%	Recurso que cumple con los requerimientos solicitados	15	
UN (1) LÍDER SOC/NOC	100%	Recurso que cumple con los requerimientos solicitados	15	
UN (1) IMPLEMENTADOR EXPERTO EN SOLUCIONES CIBERSEGURIDAD	50%	Recurso que cumple con los requerimientos solicitados	15	
UN (1) EXPERTO EN RESPUESTA A INCIDENTES	50%	Recurso que cumple con los requerimientos solicitados	15	

A continuación se relacionan los perfiles requeridos:

ROL / DESCRIPCIÓN	REQUERIMIENTO		PUNTAJE	PUNTAJE MÁXIMO
<b>UN (1) GERENTE DE SERVICIOS DE CIBERSEGURIDAD</b>  <b>Alta experiencia en gerencia / liderazgo de proyectos asociados a seguridad de la información teniendo en cuenta las mejores prácticas de seguridad</b>	Educación mínima requerida	Profesional universitario en Ingeniería de Sistemas y/o Electrónica y/o Telecomunicaciones y/o afines  Debe contar con especialización en Seguridad Informática o Gerencia de Tecnología o Gerencia de Sistemas de Información o Administración financiera o MBA - Master of Business Administration	10	15
	Experiencia profesional mínima requerida	Mínimo ocho (8) años de experiencia profesional contados a partir de la expedición de la tarjeta profesional		
	Experiencia específica mínima requerida	Experiencia específica igual o superior a cinco (5) años en gerencia y/o liderazgo de proyectos de seguridad de la información		
	Formación mínima requerida	Debe tener las siguientes certificaciones: * Certificación PMP o estudios en Gerencia de Proyectos		
	Experiencia Adicional	De uno a dos años adicionales de Experiencia Profesional a partir de la experiencia mínima requerida	2	
De tres a cuatro años adicionales de Experiencia Profesional a partir de la experiencia mínima requerida		3		
<b>UN (1) LÍDER TÉCNICO DE SERVICIOS DE CIBERSEGURIDAD</b>  <b>Alta experiencia coordinando proyectos asociados a seguridad de la información teniendo en cuenta las mejores prácticas de seguridad , así</b>	Educación mínima requerida	Profesional universitario en Ingeniería de Sistemas y/o Electrónica y/o Telecomunicaciones y/o afines  Debe contar con especialización en seguridad informática o Gerencia de Tecnología o Gerencia de Sistemas de Información o Maestría Informática o Administración de riesgos informáticos o Gestión de informática y telecomunicaciones o Administración Financiera	21	25
	Experiencia profesional mínima requerida	Mínimo ocho (8) años de experiencia profesional contados a partir de la expedición de la tarjeta profesional		

ROL / DESCRIPCIÓN	REQUERIMIENTO		PUNTAJE	PUNTAJE MÁXIMO
<b>como también alta experiencia en gestión de riesgos e incidentes de seguridad de la información</b>	Experiencia específica mínima requerida	Experiencia específica igual o superior a cinco (5) años como líder técnico en servicios de ciberseguridad o como oficial de seguridad		
	Formación mínima requerida	Debe tener las siguientes certificaciones: * CISM * Certificación auditor líder ISO27001:2013 * CRISC		
	Certificaciones Adicionales	Si ofrece las siguientes certificaciones adicionales (2 puntos adicionales por cada certificación adicional que se presente): * CISSP * CEH * CSX * Auditor líder ISO27032:2012 * ITIL Foundation v3 * Cobit 5 Foundation * Certificación en Protección de Datos Personales * Risk Manager ISO31000 * Certificación Auditor interno ISO27001:2013  Se otorgará puntaje para máximo dos certificaciones de las que presente dentro de las que se están requiriendo.	4	

ROL / DESCRIPCIÓN	REQUERIMIENTO		PUNTAJE	PUNTAJE MÁXIMO
<b>UN (1) ARQUITECTO Y ASEGURADOR DE CALIDAD DE CIBERSEGURIDAD</b>  <b>Experiencia liderando proyectos de seguridad de la información teniendo en cuenta buenas prácticas de seguridad, y en las cuales se vea reflejada la gestión de activos, riesgos, incidentes, continuidad de negocio.</b>	Educación mínima requerida	Profesional universitario en Ingeniería de Sistemas y/o Electrónica y/o Telecomunicaciones y/o software o afines.  Debe contar con maestría o especialización en Seguridad de la Información y/o Seguridad Informática  Debe contar con alguna las siguientes especializaciones Gerencia integral de proyectos y/o especialización en Administración de riesgos informáticos y/o Especialización en Telecomunicaciones y/o Gerencia de Proyectos Informáticos	16	20
	Experiencia profesional mínima requerida	Mínimo seis (6) años de experiencia profesional contados a partir de la expedición de la tarjeta profesional		
	Experiencia específica mínima requerida	Experiencia específica igual o superior a tres (3) años en proyectos relacionados con aseguramiento de calidad en proyectos de seguridad de la información y/o seguridad de la información y/o gestión de vulnerabilidades y/o líder, coordinador y/o especialista en seguridad informática.		
	Formación mínima requerida	Debe tener las siguientes certificaciones: * ITIL Foundation v3 o superior * Auditor interno ISO 27001:2013		
	Certificaciones Adicionales	Si ofrece las siguientes certificaciones adicionales (2 puntos adicional por cada certificación adicional que se presente): * ITIL® Intermediate Examination in Planning Protection and Optimization * Auditor interno o líder ISO 22301:2013 * Certificación Auditor Líder ISO27001:2013 * CEH  Se otorgará puntaje para máximo dos certificaciones de las que presente dentro de las que se están requiriendo.	4	

ROL / DESCRIPCIÓN	REQUERIMIENTO		PUNTAJE	PUNTAJE MÁXIMO
<b>UN (1) CONSULTOR CIBERSEGURIDAD Y SEGURIDAD DE LA INFOMACION</b>  <b>Experiencia en consultoría de seguridad de la información, continuidad de negocio y manejo de herramientas de Gobierno, Riesgo y Cumplimiento, Experiencia en gestión de incidentes de seguridad, análisis de vulnerabilidades, herramientas en herramientas informáticas como lo son: firewall, Análisis estático, escaneo de vulnerabilidades, Antivirus, seguridad de la información, SIEM.</b>	Educación mínima requerida	Profesional universitario en Ingeniería de Sistemas y/o Electrónica y/o Telecomunicaciones o afines.  Debe contar con alguna de las siguientes especializaciones o maestrías: Seguridad informática y/o de la información y/o especialización tecnológica y/o gerencia de proyectos informáticos y/o Gerencia de Sistemas	11	15
	Experiencia profesional mínima requerida	Mínimo un (1) año de experiencia profesional contados a partir de la expedición de la tarjeta profesional		
	Experiencia específica mínima requerida	Experiencia específica igual o superior a cuatro (4) años en proyectos relacionados con seguridad de la información y/o DRP y/o continuidad del negocio y/o análisis de vulnerabilidades y/o análisis de código		
	Formación mínima requerida	Debe tener las siguientes certificaciones:  * Certificación Auditor interno ISO27001:2013 o Líder ISO27001:2013 * Certified Ethical Hacker - CEH * Certificaciones de fabricante de soluciones de Análisis de Vulnerabilidades		
	Certificaciones Adicionales	Si ofrece las siguientes certificaciones adicionales (2 puntos adicionales por cada certificación adicional que se presente): * Certificación Implementador Líder ISO27001:2013 * CHFI * Certificaciones de fabricante de soluciones de Análisis de Código * Certificación en Protección de Datos Personales * AWS Security, Identity and Compliance  Se otorgará puntaje para máximo dos certificaciones de las que presente dentro de las que se están requiriendo.	4	

ROL / DESCRIPCIÓN	REQUERIMIENTO		PUNTAJE	PUNTAJE MÁXIMO
<b>UN (1) ANALISTA SOC/NOC</b>  <b>Experiencia en gestión de incidentes de seguridad, herramientas informáticas como los son: Control de navegación, protección a estaciones de trabajo, SIEM, firewall, protección de correo electrónico, metodología ITL.</b>	Educación mínima requerida	Profesional universitario en Ingeniería de Sistemas y/o Electrónica y/o Telecomunicaciones y/o software o afines  Debe contar con diplomados o Cursos en Administración de bases de datos	11	15
	Experiencia profesional mínima requerida	Mínimo dos (2) años de experiencia profesional contados a partir de la expedición de la tarjeta profesional		
	Experiencia específica mínima requerida	Experiencia igual o superior a dos (2) años en proyectos relacionados con funciones en SOC/NOC y/o administración de soluciones de ciberseguridad o seguridad digital		
	Formación mínima requerida	Debe tener las siguientes certificaciones: * ITIL Foundation v3 o superior		
	Certificaciones Adicionales	Si ofrece las siguientes certificaciones adicionales (2 puntos adicionales por cada certificación adicional que se presente): * Auditor Líder ISO 27001:2013 * Certificado Auditor o Risk Manager ISO 31000 * Certificaciones de fabricante de soluciones ofertadas  Se otorgará puntaje para máximo dos certificaciones de las que presente dentro de las que se están requiriendo.	4	
<b>UN (1) OPERADOR SOC/NOC</b>  <b>Alta experiencia en manejo de diferentes plataformas de SIEM, email Gateway , gestión de incidentes, firewall adicionalmente metodologías en</b>	Educación mínima requerida	Profesional universitario o estudiante de mínimo octavo semestre en Ingeniería de Sistemas y/o Electrónica y/o Telecomunicaciones y/o software o afines	11	15
	Experiencia profesional mínima requerida	N/A		
	Experiencia específica mínima requerida	Experiencia igual o superior a dos (2) años en proyectos relacionados con funciones en SOC/NOC		
	Formación mínima requerida	Debe tener las siguientes certificaciones: * Auditor interno ISO 27001:2013 * ITIL Foundation		

ROL / DESCRIPCIÓN	REQUERIMIENTO		PUNTAJE	PUNTAJE MÁXIMO
<b>seguridad de la información e ITIL</b>	Certificaciones Adicionales	Si ofrece las siguientes certificaciones adicionales (2 puntos adicionales por cada certificación adicional que se presente): * Certificaciones de fabricante de soluciones ofertadas  Se otorgará puntaje para máximo dos certificaciones fabricante.	4	
<b>UN (1) LÍDER SOC/NOC</b>  <b>Contar con experiencia en implementación y coordinación de servicios SOC, debe tener conocimiento y experiencia en administración de herramientas de seguridad de la información, como lo son: firewall, SIEM, Análisis de código estático, gestión de incidentes, metodología ISO27001 y metodología ITIL</b>	Educación mínima requerida	Profesional universitario en Ingeniería de Sistemas y/o Electrónica y/o Telecomunicaciones o afines  Debe contar con especialización Gerencia de Telecomunicaciones y/o en Seguridad Informática	11	15
	Experiencia profesional mínima requerida	Mínimo siete (7) años de experiencia profesional contados a partir de la expedición de la tarjeta profesional		
	Experiencia específica mínima requerida	Experiencia igual o superior a cinco (5) años en gestión de equipos de respuesta a incidentes, centro de operaciones de seguridad (SOC), pruebas de intrusión.		
	Formación mínima requerida	Debe tener las siguientes certificaciones: * Certificación en Manejo de Incidentes de Seguridad CIH - EC-COUNCIL CERTIFIED INCIDENT HANDLER * Certificación Auditor Líder ISO27001:2013 * Una Certificación ITIL * Auditor interno ISO 20000		
	Certificaciones Adicionales	Si ofrece las siguientes certificaciones adicionales (2 puntos adicionales por cada certificación adicional que se presente): * Certificaciones de fabricante de soluciones ofertadas * Certificación de ITIL Adicionales		
<b>UN (1) IMPLEMENTADOR EXPERTO EN SOLUCIONES</b>	Educación mínima requerida	Profesional universitario en Ingeniería de Sistemas y/o Electrónica y/o Telecomunicaciones o afines.	11	15

ROL / DESCRIPCIÓN	REQUERIMIENTO		PUNTAJE	PUNTAJE MÁXIMO
<b>CIBERSEGURIDAD</b>  <b>Experiencia en implementación de equipos de seguridad informática.</b>	Experiencia profesional mínima requerida	Mínimo tres (3) años de experiencia profesional contados a partir de la expedición de la tarjeta profesional		
	Experiencia específica mínima requerida	Experiencia específica igual o superior a dos (2) años en implementación de equipos de seguridad informática		
	Formación mínima requerida	Debe tener las siguientes certificaciones del fabricante de seguridad perimetral ofertado: * Certificación Profesional * Certificación Analista * Certificación Arquitecto		
	Certificaciones Adicionales	Si ofrece las siguientes certificaciones adicionales (2 puntos adicionales por cada certificación adicional que se presente): * Certificación CEH * Auditor Interno ISO 22301	4	
<b>UN (1) EXPERTO EN RESPUESTA A INCIDENTES</b>  <b>Experiencia en seguridad informática o seguridad de la información</b>	Educación mínima requerida	Profesional universitario en Ingeniería de Sistemas y/o Electrónica y/o Telecomunicaciones o afines.	11	15
	Experiencia profesional mínima requerida	Mínimo cinco (5) años de experiencia profesional contados a partir de la expedición de la tarjeta profesional		
	Experiencia específica mínima requerida	Experiencia específica igual o superior a cuatro (4) años en seguridad informática o seguridad de la información		
	Formación mínima requerida	Debe tener las siguientes certificaciones: * Certificación en Respuesta de Incidentes del fabricante ofertado en Herramientas de Identificación y control de Amenazas Persistentes Avanzadas - APTs		
	Certificaciones Adicionales	Si ofrece las siguientes certificaciones adicionales (2 puntos adicionales por cada certificación adicional que se presente): * Certificación ITIL Foundation * Certificación Auditor interno ISO27001:2013	4	

El oferente que no cumpla el mínimo solicitado tendrá cero puntos.

### 7.3.3 EXPERIENCIA ADICIONAL PROPONENTE (50 PUNTOS)

El oferente deberá demostrar experiencia mediante certificados suscritos por el cliente, donde demuestre haber ejecutado contratos de seguridad de la información que involucre el estándar ISO 27001, Instalaciones de Soluciones de Seguridad o consultorías adicionales, los contratos deberán ser por un valor mínimo de cada contrato 300 SMLMV, ejecutados en los últimos 5 años, en el sector público o privado. Los contratos relacionados en este numeral deberán ser distintos a los presentados en la experiencia técnica habilitante.

Descripción	Puntaje	Puntaje Máximo
1 contrato	10	50
2 a 3 contratos	30	
4 contratos en adelante	50	

El oferente que no cumpla el mínimo solicitado tendrá cero puntos.

### 7.3.4 ELEMENTOS DE CALIDAD (100 PUNTOS)

SERVICIO PONDERACIÓN	OFRECIMIENTO	Puntaje	Puntaje Máximo
Certificación ISO27001:2013	Oferente en proceso de Certificarse en la norma ISO27001:2013. El oferente que desee aplicar a este puntaje deberá anexar el contrato del proceso de certificación con la entidad certificadora; Contrato que deberá estar suscrito antes de la fecha de inicio del presente proceso.	5	25
	Oferente certificado en la norma ISO27001:2013 para todos sus productos y servicios	25	
Relacionamiento del SOC con fuentes de inteligencia de amenazas e incidentes	Servicio de SOC es miembro activo del FIRST.	10	25
	SOC con asociaciones con entidades de Inteligencia como el MISP.	10	
	Hace parte del CSIRT de la Policía Nacional.	5	

SERVICIO PONDERACIÓN	OFRECIMIENTO	Puntaje	Puntaje Máximo
Membresías de Fabricante	Oferente que cuente con el máximo nivel de membresía con el fabricante de la solución SIEM con la que prestan el servicio de SOC	20	20
	Oferente que cuente con el nivel de membresía por encima del nivel básico del fabricante de la solución SIEM con la que prestan el servicio de SOC	5	
Certificación ISO9001	Oferente que cuente con certificación vigente en la norma ISO 9001/2015	30	30

El oferente que no cumpla el mínimo solicitado tendrá cero puntos en cualquiera de los ítems calificables.

### **7.3.5 ALIADOS PROVEEDORES Y CRITERIOS DE DESEMPATE**

Agotado el análisis comparativo de las ofertas, se establecerá una lista de elegibilidad de la siguiente manera: se consideran elegibles aquellos proponentes que hayan obtenido un puntaje acumulado de (800 puntos) en la calificación total, y con quienes hayan acreditado todas las condiciones habilitantes. En dicha lista, el primer lugar de elegibilidad estará ocupado por el proponente que acumule la mayor cantidad de puntos y así sucesivamente hasta terminar la lista de elegibilidad de tres (3) aliados proveedores.

Se considerará aliado proveedor de la ESU los tres (3) proponentes que hayan obtenido el mayor puntaje. En caso de empate en el puntaje total de dos o más ofertas, la ESU aplicará los criterios de desempate establecidos en el artículo 35 de la Ley 2069 de 2020, de forma sucesiva y excluyente conforme se establece en el pliego de condiciones.

Con el Aliado Proveedor seleccionado se formalizará su condición mediante la suscripción del respectivo Acuerdo Marco, que se regirá por lo aquí dispuesto. En el evento que producto de esta Solicitud Pública de Oferta no se seleccione el oferente requerido, la ESU podrá adelantar nueva (s)



## ESTUDIOS PREVIOS Y JUSTIFICACIÓN DE CONTRATACIÓN

Código: FT-M6-GC-12

Versión: 03

Página 26 de 32

convocatoria (s) hasta tanto se complete el rango de aliados requerido. Los servicios que se deban prestar bajo el marco de estas Alianzas se podrán ejecutar mediante los Aliados seleccionados y complementar con otro mecanismo de adjudicación, de considerarse necesario.

### **8. EL SOPORTE QUE PERMITE LA TIPIFICACIÓN, ESTIMACIÓN Y ASIGNACION DE LOS RIESGOS PREVISIBLES.**

Se entienden como riesgos involucrados en la contratación todas aquellas circunstancias que, de presentarse durante el desarrollo y ejecución del contrato, pueden alterar el equilibrio financiero del mismo.

Teniendo en cuenta la modalidad bajo la cual se suscribirá el contrato marco, se verifica que las condiciones económicas, técnicas y financieras de los servicios, objeto de estos estudios, mantienen el equilibrio contractual y se analizarán puntualmente en cada Solicitud Privada de Ofertas que se adelante con los Proveedores con los cuales se suscriba el Acuerdo Marco. Sin embargo, se advierte que como base para futuras Solicitudes Privadas de Oferta con los Aliados Proveedores que resulten de esta Solicitud Pública de ofertas, que a partir de la fecha de suscripción del Contrato y en todas las etapas del mismo el Contratista asume los efectos derivados de todos y cada uno de los riesgos asociados a cada Contrato, al igual que respecto a los que logre determinar, salvo los casos en que expresamente se ha determinado lo contrario.

Por lo tanto, no procederán reclamaciones del contratista basadas en el suceso de alguno de los riesgos asumidos por el contratista y -consecuentemente- la ESU no hará reconocimiento alguno, ni se entenderá que ofrece garantía alguna al contratista, que permita eliminar o mitigar los efectos causados por la ocurrencia de alguno de estos riesgos, salvo que dicho reconocimiento o garantía se encuentren expresamente pactados en el contrato.

En este sentido el contratista asumirá los siguientes riesgos derivados de los efectos, favorables o desfavorables, producto de las variaciones de la tasa de cambio y de la evolución de la devaluación real observada frente a la estimada inicialmente por el Contratista.

Se recomienda que para cada contrato que se suscriba con los Aliados Proveedores seleccionados, EL CONTRATISTA constituya a favor de LA ESU y tercero una garantía única a favor de 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, tomada por el oferente a su costa y en favor de LA ESU. La garantía deberá detallar: objeto, número del contrato, vigencia, cuantía y firmas del tomador y de la aseguradora que la expide, así como acompañarse del respectivo comprobante de pago del valor de la prima y de los demás anexos o cláusulas generales que hagan parte de la garantía. La garantía deberá ser aceptable para LA ESU en su procedencia, contenido y forma. LA ESU se reservará el derecho de rechazar la Garantía Única si ésta es expedida por una entidad que a criterio de LA ESU no constituya una seguridad al cumplimiento de las obligaciones que se garantizan. Así mismo, LA ESU se reservará el derecho de revelar los motivos por los cuales la póliza no es aceptada. Las garantías deberán estar vigentes durante todo el término del contrato,

tal como se explica más adelante. Cuando haya modificación del plazo o del valor del contrato, EL CONTRATISTA deberá ampliar las garantías del contrato para conservar el monto porcentual y las vigencias; también lo hará cuando se haga efectiva total o parcialmente la garantía por cualquiera de los riesgos que ampara.

Se anexa matriz de riesgos del proceso.

## 9. EL ANÁLISIS QUE SUSTENTA LA EXIGENCIA DE GARANTÍAS

**GARANTIA DE SERIEDAD DE LA PROPUESTA:** Equivalente al diez por ciento (10%) calculado sobre la base de \$500.000.000 (Quinientos millones de pesos) y una vigencia de dos (2) meses contados a partir de la fecha de cierre del proceso contractual, donde el tomador y/o afianzado sea el proponente. Si el proponente es una persona jurídica, la garantía deberá tomarse con el nombre o razón social que figura en el Certificado de Existencia y Representación Legal expedido por la Cámara de Comercio.

Teniendo en cuenta que se trata de un proceso para la selección de Aliados Proveedores bajo modalidad de Solicitud Pública de ofertas, con quienes se celebrarán contratos marcos abiertos en cuantía, no se exigirá la constitución de garantías contractuales para la suscripción de dichos contratos marco. Sin embargo, para la suscripción de los contratos derivados de las Solicitudes Privadas de Ofertas, la ESU requerirá al futuro Aliado Proveedor la Garantía de cumplimiento a que haya lugar para la ejecución del contrato con observancia de lo dispuesto en el Acuerdo 090 de 2019, y garantía que cubrirá los amparos referenciados en la siguiente tabla, cuyas suficiencias y vigencias procederán conforme apliquen según las necesidades de cada SPVA:

AMPARO	SUFICIENCIA	VIGENCIA
Cumplimiento: (si aplica)	20%	Con una vigencia igual a la duración del contrato y seis (6) meses más
Calidad del servicio / bienes y/o equipos (si aplica)	20%	Con una vigencia igual a la duración del contrato y seis (6) meses más
Estabilidad de obra: (si aplica)	10%	Con una vigencia igual a la duración del contrato y cinco (5) años más.
Salarios, prestaciones sociales e indemnizaciones al personal: (si aplica)	10%	Con vigencia igual al plazo del contrato y tres (3) años más

<p>Responsabilidad civil extracontractual: (si aplica)</p>	<ol style="list-style-type: none"> <li>1. Doscientos (200) SMMLV para contratos cuyo valor no exceda de (1.500) SMMLV.</li> <li>2. Trescientos (300) SMMLV para contratos cuyo valor sea superior a mil quinientos (1.500) SMMLV e inferior o igual a dos mil quinientos (2.500) SMMLV.</li> <li>3. Cuatrocientos (400) SMMLV para contratos cuyo valor sea superior a dos mil quinientos (2.500) SMMLV e inferior o igual a cinco mil (5.000) SMMLV.</li> <li>4. Quinientos (500) SMMLV para contratos cuyo valor sea superior a cinco mil (5.000) SMMLV e inferior o igual a diez mil (10.000) SMMLV.</li> <li>5. El cinco por ciento (5%) del valor del contrato cuando este sea superior a diez mil (10.000) SMMLV, caso en el cual el valor asegurado debe ser máximo setenta y cinco mil (75.000) SMMLV. (aplicar acorde a la cuantía del contrato)</li> </ol>	<p>Su vigencia será igual al plazo del contrato.</p>
--	--	--

El asegurado será la Empresa para la Seguridad y Soluciones Urbanas -LA ESU- y el contratista, y serán beneficiarios tanto la Empresa para la Seguridad y Soluciones Urbanas -LA ESU- como los terceros que puedan resultar afectados por la responsabilidad extracontractual del contratista o sus subcontratistas.

En atención a los respectivos análisis de riesgos específicos de cada uno de los proyectos, estos amparos podrán variar en cuantía, vigencia y nuevos amparos.



## ESTUDIOS PREVIOS Y JUSTIFICACIÓN DE CONTRATACIÓN

Código: FT-M6-GC-12

Versión: 03

Página 29 de 32

### 10. INDICACIÓN DE SI LA CONTRATACIÓN RESPECTIVA ESTÁ COBIJADA POR UN ACUERDO INTERNACIONAL O UN TRATADO DE LIBRE COMERCIO VIGENTE PARA EL ESTADO COLOMBIANO:

La contratación no está cobijada con un acuerdo internacional y tampoco con tratado de libre comercio para el Estado colombiano, en atención a la exclusión que de ello tiene la contratación celebrada por las Empresas Industriales y Comerciales del Estado, como lo es la ESU.

### 11. CONDICIONES CONTRACTUALES:

#### 11.1 OBLIGACIONES DEL CONTRATO

##### 11.1.1 OBLIGACIONES DE LA ESU:

La ESU en desarrollo del presente contrato tendrá los siguientes deberes: 1) Pagar al aliado proveedor por la prestación de bienes y servicios de soluciones de seguridad digital, seguridad de la información y ciberseguridad, en virtud de los contratos asignados por la ESU mediante solicitudes privadas de oferta, conforme a los términos convenidos, previo recibo a satisfacción del supervisor. 2) Realizar la supervisión del contrato y recibir la prestación del servicio a satisfacción a través de éste. 3) Evaluar el desempeño del aliado proveedor de acuerdo a la periodicidad establecida en el pliego de condiciones del proceso de Solicitud Pública de Ofertas, o según sea requerido por parte de la Supervisión del contrato 4) Suministrar la información necesaria para la ejecución satisfactoria del objeto contractual.

##### 11.1.2 OBLIGACIONES ESPECIFICAS DEL CONTRATISTA:

El contratista en desarrollo del presente contrato tendrá las siguientes obligaciones: 1) Prestación de bienes y servicios de soluciones de seguridad digital, seguridad de la información y ciberseguridad, de acuerdo con lo dispuesto en la Solicitud Pública de Oferta, la oferta presentada por el aliado proveedor y los respectivos contratos u ordenes de servicio que se llegaren a suscribir, las cuales forman parte integral y vinculante de este contrato, con la diligencia y eficiencia requerida dentro de los términos establecidos, según las instrucciones que para el efecto le sean dadas por el supervisor. 2) Designar un representante para efectos de facilitar y agilizar el manejo de la información entre las partes. 3) Cumplir con la ejecución de los contratos que obtenga en calidad de aliado proveedor. 4) Informar inmediatamente sobre cualquier circunstancia que afecte o pueda afectar la ejecución del contrato. 5) Prestar los bienes y servicios de soluciones de seguridad digital, seguridad de la información y ciberseguridad de acuerdo a las indicaciones dadas por la ESU en los contratos que se llegaren a suscribir. 6) Garantizar la reserva profesional sobre la información que en virtud del desarrollo del Contrato llegare a conocer; se debe comprometer así mismo, a no hacer uso directo, próximo ni remoto, de ningún dato concreto o referencial que pudiese comprometer la seguridad de la ESU o de sus clientes, ni dar ventajas competitivas a terceras personas. 7) Presentar informes sobre el servicio prestado cada vez que así sea requerido por el supervisor del contrato. 8) Garantizar durante la ejecución del contrato domicilio, sucursal o agencia en algún municipio del área metropolitana. 9) Presentar la documentación y el cumplimiento de requisitos específicos que



## ESTUDIOS PREVIOS Y JUSTIFICACIÓN DE CONTRATACIÓN

Código: FT-M6-GC-12

Versión: 03

Página 30 de 32

se exijan para las selecciones de los proyectos que se desarrollen en el marco de esta Alianza. 10) Acreditar el pago de aportes parafiscales y seguridad social para cada uno de los pagos. 11) Considerar que las relaciones contractuales están basadas en el reconocimiento, seguimiento de las reglas, principios de la ética y la buena fe contractual; en un ambiente de respeto y de confianza que genere valor para las partes y para la sociedad en general. 12) Rechazar las prácticas corruptas y delictivas en general; se prevendrá y combatirá el fraude, el soborno, la extorsión y otras formas de corrupción. 13) Tanto en el desarrollo de los proyectos y procesos, como en su área de influencia, el contratista promoverá prácticas que reflejen la protección y conservación del medio ambiente, el respeto al pluralismo democrático, a las minorías étnicas, a la equidad de género y a los derechos humanos en general. 14) Velar por el respeto de la dignidad en las condiciones de trabajo por parte de sus contratistas y subcontratistas, por lo que no se avalarán prácticas discriminatorias, trabajo forzado o de menores. 15) Cumplir con las políticas de prevención que eviten la utilización y explotación sexual de niños, niñas y adolescentes en el desarrollo de sus actividades comerciales, así como a no contratar menores de edad en cumplimiento de los pactos, convenios y convenciones internacionales ratificados por Colombia, según lo establece la Constitución Política de 1991 y demás normas vigentes sobre la materia, en particular aquellas que consagran los derechos de los niños. 16) Las demás que tengan relación directa con la naturaleza y objeto del presente contrato.

**11.1.3 PRODUCTOS Y/O SERVICIOS:** En desarrollo de las anteriores obligaciones, el contratista se obliga a suministrar los siguientes productos y/o servicios:

Suministro, implementación, mantenimiento y cualquier otro tipo de servicio para la satisfacción de las necesidades que requieran nuestros clientes en materia de bienes y servicios de soluciones de seguridad digital, seguridad de la información y ciberseguridad tales como Gestión, Riesgo y Cumplimiento – GRC, Consultoría especializada (Establecimiento de Sistemas de Gestión de Seguridad SGSI basado en la norma ISO27001:2013 y los lineamientos de Gobierno en Línea, Acompañamiento a la certificación ISO27001:2013, Auditorías de Terceros), Centro de Operaciones de Seguridad SOC-NOC, Servicios de Atención de Incidentes de Seguridad y Ciberseguridad, Monitoreo de Productividad y Ciberseguridad de los usuarios, Ciclo de Vida de desarrollo seguro – S-SDLC, Análisis de Código Estático y Dinámico, Gestión continua de Vulnerabilidades, Hacking Ético, Servicios de Resolución de Vulnerabilidades, Monitoreo de Marca Empresarial, Ejercicios de RedTeam, Pruebas de Ingeniería Social, Pruebas de Intrusión Física, Protección de Integral de Correo Electrónico, Control de Acceso a la Red, Protección de Integral de Estaciones de Trabajo, Control de Navegación – Proxy, Control de seguridad Perimetral, Firewalls y NGFW, Sandbox, Herramientas de Identificación y control de Amenazas Persistentes Avanzadas – APTs, capacitación, todo lo relacionado con las tecnologías e infraestructura que permita tener la Seguridad digital de nuestros clientes y que se encuentren dentro de los criterios técnicos y de cuantía que establezca la ESU.

**11.1.4 FORMA DE PAGO:** La ESU pagará al Contratista así:

El contrato de Acuerdo Marco de Aliado Proveedor producto de esta Solicitud Pública de Oferta no conlleva pago alguno al Aliado porque no implica por sí mismo la prestación de servicio alguno. Los aliados proveedores que resulten seleccionados en esta Solicitud Pública de Oferta, serán invitados a participar posteriormente en Solicitudes Privadas de Ofertas o cualquier otro mecanismo



## ESTUDIOS PREVIOS Y JUSTIFICACIÓN DE CONTRATACIÓN

**Código:** FT-M6-GC-12

**Versión:** 03

Página 31 de 32

establecido en la normativa de contratación interna de la ESU, y para cada una de estas se establecerá por parte de la ESU la forma de pago aplicable y el procedimiento para el mismo.

No obstante, para el cobro de cada orden de servicio producto de una Solicitud Privada de Oferta o cualquier otra forma de selección, el eventual Aliado Proveedor deberá presentar la factura o documento equivalente en el Centro De Información Documental (CID) de la ESU, ubicado en la Carrera 48 #20 -114 Torre 3 Piso 5 Edificio Centro Empresarial Ciudad del Río, Medellín y deberá anexar los soportes que aseguren que el servicio o el bien fue recibido a entera satisfacción por el supervisor y la constancia de pago al Sistema de Seguridad Social Integral y aportes parafiscales del personal empleado para la ejecución de la orden de servicio o contrato (lo anterior en cumplimiento de lo dispuesto en el artículo 50 de la ley 789 de 2002). La ESU realizará la transferencia electrónica a la cuenta informada por el aliado proveedor o contratista.

El Aliado Proveedor deberá cumplir con los tiempos estipulados por la ESU para la recepción de facturas. La 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 de Acuerdo Marco y la orden de servicio, el concepto del bien o servicio que se está cobrando, la dependencia responsable y el nombre del supervisor del contrato designado o funcionario responsable. La ESU recibe facturas conforme a lo establecido en la circular 01 de 2021 o en el documento que lo modifique por la cual se definen las fechas de corte mensual para recepción de facturas en la entidad. Facturas posteriores a estas fechas no se reciben y el contratista deberá presentar una nueva factura dentro del mes siguiente a la prestación del servicio.

Al momento de entregar la factura, ésta deberá estar acompañada con el certificado de pago de aporte 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.

Para el caso de proveedores que se encuentren obligados a facturar electrónicamente, la facturación deberá ser remitida al correo electrónico [facturacion@esu.com.co](mailto:facturacion@esu.com.co) y la fecha límite para la recepción de las mismas por parte de la entidad estará sujeta a las fechas definidas en la circular 001 de 2021, documento donde adicionalmente se define la elaboración del recibo a satisfacción por parte del supervisor designado y el proceso de cierre contable en calidad de empresa industrial y comercial del estado.

Todo impuesto, tasa o contribución directa o indirecta, Nacional, Departamental o Municipal o costo administrativo por concepto de recursos a administrar a que hubiere lugar y que se cause por razón de la celebración, ejecución y pago de este Contrato serán a cargo exclusivo del Aliado Proveedor. Los servicios serán cancelados conforme lo establecido en los diferentes contratos y/u órdenes de servicio derivadas del acuerdo marco en los cuales se determinará la forma de pago, y en todo caso el valor final a reconocer corresponderá a los servicios efectivamente recibidos en cada una de éstas; previa recepción de recibo de cumplimiento de la prestación del servicio por parte del supervisor del contrato.



## ESTUDIOS PREVIOS Y JUSTIFICACIÓN DE CONTRATACIÓN

Código: FT-M6-GC-12

Versión: 03

Página 32 de 32

Una vez recibida a satisfacción la factura o cuenta de cobro correspondiente, la ESU tendrá hasta treinta (30) días calendario para proceder a su pago.

### 11.1.5 SUPERVISIÓN DEL CONTRATO:

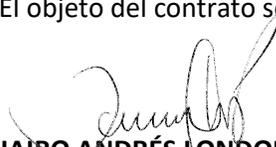
La Supervisión del Contrato estará a cargo del líder de programa de la unidad estratégica de tecnología o quien haga sus veces o por quien designe el Ordenador del Gasto; el cual ejercerá las obligaciones y responsabilidades de acuerdo con lo establecido en el artículo 44 y del Manual de Contratación y el Manual de Supervisión de la Entidad.

### 11.1.6 PLAZO DE EJECUCIÓN:

El plazo del presente contrato será de doce (12) meses a partir de la firma del Acuerdo Marco, previo cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato, prorrogable hasta por otros doce (12) meses más, previa aprobación del Comité de Gerencia. Estos Acuerdos podrán prorrogarse de conformidad con lo señalado en los artículos 28 y 29 del Reglamento de Contratación y la política de evaluación de proveedores de la ESU.

### 11.1.7 LUGAR DE EJECUCIÓN DEL CONTRATO:

El objeto del contrato se ejecutará en cualquier ciudad de Colombia.

  
**JAIRO ANDRÉS LONDOÑO PARDO**  
Subgerente de Servicios

Aprobó: Juan Felipe Hernández Giraldo- Secretario General

Aprobó: Jairo Andrés Londoño Pardo - Subgerente de Servicios

Aprobó: Marelbi Verbel Peña- Subgerente Administrativa y Financiera.

Revisó: Edison Osorio Hernández. Profesional Especializado Unidad de Gestión Jurídica

Proyectó: Mauricio Alejandro Patiño Restrepo. Líder de Programa. Unidad Estratégica de Servicios SIS