RESPUESTAS A LAS OBSERVACIÓNES PRESENTADAS
PROCESO No. SSF-SASI-003-2024

IDENTIFICACIÓN: SSF-SASI-003-2024 - SOC

OBJETO: *PRESTAR SERVICIOS DE MONITOREO Y ATENCIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (ID: OTIC-756)*

OBSERVACIÓNES INTERESADO OPEN GROUP

OBSERVACIÓN No.1

Se solicita a la entidad en el ROL Gerente de Proyecto no considerar como requisito que este perfil se encuentre certificado como SCRUM MASTER, toda vez que por la naturaleza de la labor a ejecutar es justificada con las Certificaciones: PMP - Project Management Professional o Prince, se solicita a la entidad solicitar la certificación SCRUM FUNDAMENTALS.

RESPUESTA:

Se acoge parcialmente la solicitud del interesado, en tal sentido respecto de los requisitos para el rol del Gerente de Proyectos, se realizará la inclusión de la certificación Project Management Professional (PMP). De esta manera se modifica el acápite 4.3.3 del pliego de condiciones, se establecerá lo siguiente:

Rol	Profesión en Colombia (Carreras Afines según SNIES)
Gerente de proyecto	Profesión: Título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines. Posgrado: posgrado en Gerencia de Proyectos o Gerencia de Proyectos en Ingeniería de Telecomunicaciones o Administración de Empresas con Especialidad en Dirección de Proyectos. Certificaciones: PMP - Project Management Professional o Prince. Experiencia mínima: 10 años como profesional ejecutando proyectos y/o labores como director o gerente de proyectos en el sector de tecnología Experiencia especifica: 5 años en Ciberseguridad, Seguridad informática, Seguridad de la Informacióny.

Rol	Profesión en Colombia (Carreras Afines según SNIES)
	Certificaciones: Auditor Lider ISO 27001:2022, Cobit 5 o ITIL v4, CISM Certified Information Security Manager o CISSP Certified Information Systems Segurity Professional, Scrum Master, Project Management Professional (PMP)

OBSERVACIÓN No.2

Se solicita a la entidad considerar como requisito habilitante los documentos de talento humano, es decir, para los 5 perfiles requeridos para la ejecución del contrato y el cumplimiento de los niveles de servicio solicitados, lo anterior por que aseguraría la capacidad de ejecución por parte del oferente y la facilidad para migrar los servicios contratados desde el actual operador del servicio a contratar, todo lo anterior redunda en la estabilidad del proyecto en su fase inicial de empalme por la madurez que puede llegar a tener un equipo profesional que hace parte del nuevo operador de SOC

RESPUESTA:

La Superintendencia del Subsidio Familiar, aclara que como se menciona en el numeral 4.3.3 certificación equipo de trabajo, este es un requisito que conllevará una verificación técnica y tendrá como resultado CUMPLE o NO CUMPLE y que el proponente que no cumpla alguno de los requisitos técnicos habilitantes será declarado NO HABILITADO, lo anterior obedece a que la entidad requiere validar la experiencia e idoneidad del proponente y el recurso humano con el que cuenta con el fin de minimizar la materialización de riesgos de incumplimiento en la ejecución del contrato, toda vez que las actividades asociadas a la cobertura del contrato resultante, es de factor crítico para la operación de la Entidad.

OBSERVACIÓN No.3

Se le solicita a la entidad aclarar el tamaño de los LOGS según su capacidad de tiempo de almacenamiento del Firewall y del WAF.

RESPUESTA:

La Superintendencia del Subsidio Familiar, aclara que en lo referente al tiempo de almacenamiento y como se evidencia en el numeral 1.5 Requerimientos Específicos Almacenamiento de Logs, el almacenamiento y disponibilidad de los LOGs se debe

asegurar por parte del contratista por la ejecución del servicio contratado, igualmente se indica que en el anexo técnico en el numeral 1.3 Especificaciones Técnicas Generales del SOC, se indica que como mínimo se debe tener considerar como mínimo 4500 EPS (Eventos por segundo).

OBSERVACIÓNES INTERESADO: PASSWORD CONSULTING SERVICES SAS

OBSERVACIÓN No.1

Solicitamos amablemente a la entidad proporcionar claridad con respecto a los requerimientos mencionados entre las páginas 27 y 42 del pliego. En el primer requerimiento de esta sección, se menciona que la entidad dispondrá de una herramienta SIEM, específicamente ArcSight (logger y ArcMC) del fabricante MicroFocus, para el servicio SOC. Sin embargo, los requerimientos posteriores hacen referencia a funcionalidades propias de un SIEM adicional. ¿Por lo tanto, agradeceríamos que se nos aclare si se debe contemplar la implementación de un SIEM adicional al que la entidad tiene en sus premisas?

RESPUESTA:

La Superintendencia del Subsidio Familiar desea aclarar que, efectivamente, cuenta con el SIEM ArcSight para el cumplimiento del objeto contractual. Sin embargo, el futuro adjudicatario podrá disponer del SIEM de su preferencia para el correcto funcionamiento del servicio y la cobertura, es necesario aclarar al respecto que el SIEM ArcSight estará disponible únicamente hasta el 31 de diciembre de 2024, por lo tanto, para el periodo de servicio posterior a esta fecha, el contratista deberá proporcionar su propio SIEM.

OBSERVACIÓN No.2

Los requerimientos solicitados desde la página 27 a la 42 están específicamente relacionados con funcionalidades de un SIEM y no de un SOC ¿La herramienta que la entidad propone cubre completamente este alcance?

RESPUESTA:

La Superintendencia del Subsidio Familiar se permite dar claridad sobre el uso del SIEM en la entidad La herramienta está diseñada para gestionar y analizar eventos de seguridad, pero es necesario tener en cuenta que su fecha máxima de uso es hasta el 31 de diciembre de 2024. Esto significa que se deben planificar acciones para la continuidad del servicio, sin embargo, como se menciona en los pliegos el contratista y en la respuesta a la observación No. 1 del interesado PASSWORD CONSULTING SERVICES SAS el adjudicatario podrá implementar su SIEM desde el inicio de la vigencia del contrato.

OBSERVACIÓN No.3

¿En el caso que se deba contemplar un SIEM adicional, cual es el propósito de tener 2 SIEM?

RESPUESTA:

Ver respuesta a la observación No. 1 y No. 2 del interesado PASSWORD CONSULTING SERVICES SAS

OBSERVACIÓN No.4

¿Solicitamos se confirme si bien el plazo de ejecución es hasta el 31 de diciembre, cuanto tiempo se debe desplegar las soluciones de que trata el anexo técnico?

RESPUESTA:

Se aclara al interesado que de acuerdo con lo descrito en el acápite 1.7 del pliego de condiciones se describen claramente las condiciones del plazo de ejecución del contrato

OBSERVACIÓNES INTERESADO: ITELCA

OBSERVACIÓN No.1

Forma de Pago (página 55): Solicitamos una aclaración sobre el segundo pago, equivalente al 40% del valor adjudicado, que se efectuaría tras la aprobación del Plan de Gestión de Seguridad del SOC. Se menciona que el servicio tendrá una duración de un año, pero el

contrato se ejecutará en tres meses, hasta el 31 de diciembre de 2024, según el numeral 1.7.

RESPUESTA:

Amablemente le solicitamos remitirse al numeral 1.11 del pliego de condiciones

OBSERVACIÓN No.2

Condiciones de la Experiencia Específica (página 93): Solicitamos eliminar el requisito de certificaciones para herramientas específicas, ya que dicha información es confidencial y no es certificada por los clientes. Además, este tipo de certificaciones de experiencia reduce la objetividad del proceso y lo sesga, limitándolo a ciertos oferentes que cumplen con esos criterios específicos. Proponemos que los contratos sean considerados válidos si han sido ejecutados en los últimos dos años, lo cual permitiría ampliar la pluralidad de oferentes y fomentar una competencia más justa.

RESPUESTA:

No se acepta la solicitud del interesado ya que las certificaciones requeridas son esenciales para garantizar la idoneidad del oferente y su experiencia para la ejecución de actividades asociadas al objeto establecido. Para el caso específico del presente proceso, el requisito del que trata la solicitud de certificaciones representa un indicador clave de la capacidad del proveedor para cumplir con los requisitos del servicio, por tal motivo se mantiene el requisito con el fin de asegurar que los oferentes cumplan con los estándares necesarios para la correcta ejecución del contrato.

OBSERVACIÓN No.3

Certificación del Equipo de Trabajo (páginas 96-98):

Solicitamos que no se requieran hojas de vida y soportes académicos con la oferta, proponiendo en su lugar una carta de compromiso del representante legal. Cabe señalar que, de acuerdo con el Manual de Contratación de Colombia Compra Eficiente, específicamente en la norma que regula el Decreto 1082 de 2015, está prohibido utilizar las hojas de vida como factores habilitantes en los procesos de contratación. Por lo tanto, la exigencia de presentar hojas de vida como requisito de participación iría en contra de esta normativa.

Para el Gerente de Proyecto, solicitamos que se admitan posgrados en áreas relacionadas, como seguridad informática. En el campo de la seguridad de la información y especialistas en SOC, las maestrías y especializaciones en seguridad informática son el estándar común, mientras que certificaciones como PMP, COBIT 5, ITIL 4 o Scrum están más enfocadas en modelos ágiles de ejecución o metodologías de gestión que, aunque útiles, están fuera del contexto específico de la seguridad. Por lo tanto, solicitamos que estas certificaciones también sean removidas, ya que no son acordes a los requerimientos específicos establecidos por la entidad.

Para el Consultor Senior de Despliegue, sugerimos que la experiencia pueda acreditarse con proyectos en SIEM o contratos que incluyan herramientas como SOAR, Honeypot, protección de marca o gestión de vulnerabilidades.

En cuanto al Líder SOC, pedimos aceptar una combinación de certificaciones como Auditor ISO o Ethical Hacking.

Para el Consultor Técnico SOC y el Analista Nivel 2 de SOC, solicitamos una mayor flexibilidad en la acreditación de experiencia y certificaciones.

RESPUESTA:

Frente a la inquietud en la cual se solicita la no exigencia de las hojas de vida para determinar si el proponente cumple o no cumple, ver respuesta a la observación No. 2 del interesado OPEN GROUP

Frente a la inquietud relacionada con el perfil de Gerente de Proyecto, la entidad no acoge la solicitud del interesado toda vez que el perfil en mención obedece a un rol especifico en el cual tanto las diferentes opciones de posgrado, como las certificaciones garantizan el conocimiento para llevar acabo el rol requerido, y para garantizar que la persona asignada para este rol sea idóneo para este proceso se solicita una experiencia de 5 años en Ciberseguridad, Seguridad Informática, Seguridad de la Información.

Frente a la inquietud relacionada con el perfil Consultor Senior de Despliegue, se permite aclarar que como se menciona en la experiencia específica para este perfil se deberá acreditar por medio de la certificación de 4 proyectos en despliegue de la herramienta propuesta para SIEM y uno de estos contratos que contenga despliegue de mínimo 2 de las siguientes herramientas SOAR, HONEYPOT, PROTECCION DE MARCA, GESTION DE VULNERABILIDADES para el sector gobierno.

Frente a la inquietud relacionada con el perfil de Líder SOC la entidad no acoge la solicitud del interesado puesto que en las consideraciones del perfil se estableció que las certificaciones solicitadas apoyan de manera clave el perfil solicitado y por tal motivo desistir de alguna de estas certificaciones desmejoraría el perfil solicitado.

Frente a la inquietud relacionada con el perfil de Consultor Técnico SOC y el Analista Nivel 2 de SOC la entidad no acoge la solicitud del interesado puesto que la experiencia solicitada en la documentación del proceso, garantiza que la cobertura del servicio se dé en la calidad esperada con el personal idóneo para tal fin.

OBSERVACIÓN No.4

Oferta Económica (página 1): Solicitamos una aclaración en el anexo económico, ya que la columna 'Valor Total Ofertado Incluido IVA' podría generar confusión. Solicitamos también confirmar el periodo de monitoreo del SOC, la integración con el SIEM de ArcSight, y si los 4500 EPS aplican mensualmente o a lo largo del contrato.

RESPUESTA:

Se acoge la solicitud presentada por el interesado y en tal sentido se realiza la modificación correspondiente al formato N° 11 Oferta económica, el cual será publicado de la siguiente manera:

Ítem	Descripción Necesidad	Valor ofertado incluido IVA
1	Servicio SOC	
2	Servicio de gestión de vulnerabilidades	
3	Servicio de ethical hacking	
TOTAL PROPUESTA ECONÓMICA		

Con relación al a la duración de cobertura del servicio, ver respuesta a la observación No. 4 del interesado PASSWORD CONSULTING SERVICES SAS

Con relación a la integración del SIEM, ver respuesta a la observación No. 1 y No. 2 del interesado PASSWORD CONSULTING SERVICES SAS

Con relación a los EPS, la entidad se permite aclarar que esta cantidad hace referencia a que en un segundo existan al menos 4500 EPS Eventos.

OBSERVACIÓN No.5

Con respecto a la referencia *"...El contratista deberá tener un SOC propio..."* el requerimiento establecido por la entidad en el pliego de condiciones, en el cual se solicita que los oferentes cuenten con un SOC (Security Operations Center) propio en sus instalaciones y en territorio nacional, se considera pertinente proponer la inclusión de un listado específico de certificaciones y auditorías que garanticen la calidad y capacidad operativa del SOC. Sugerimos que se tomen en cuenta las siguientes certificaciones internacionales, ampliamente reconocidas, para validar el cumplimiento de los estándares de seguridad requeridos:

Certificaciones específicas para el SOC:

- ISO/IEC 27001: Garantiza que el SOC posee un sistema de gestión de seguridad de la información (SGSI) adecuado, con controles implementados para proteger la confidencialidad, integridad y disponibilidad de la información.
- ISO/IEC 27032: Proporciona directrices específicas para la ciberseguridad, enfocándose en mejorar la seguridad de la información y la infraestructura en entornos cibernéticos.
- ISO/IEC 22301: Certifica que la entidad cuenta con un sistema de gestión de continuidad del negocio, asegurando que el SOC puede mantener la operatividad en situaciones de emergencia.
- SOC 2 Tipo II: Auditado por un tercero independiente, este informe proporciona evidencia de que el SOC cumple con los principios de seguridad, disponibilidad, integridad en el procesamiento, confidencialidad y privacidad. Es un estándar para evaluar la madurez y la calidad de las operaciones del SOC.

Cualquiera de estas certificaciones permitirá a la entidad validar de manera objetiva que el SOC propuesto cumple con los niveles de seguridad requeridos y cuenta con las capacidades necesarias para operar de forma efectiva dentro del territorio nacional. Por lo tanto, se recomienda especificar estos requerimientos en el pliego de condiciones para asegurar la calidad y el cumplimiento de los oferentes.

RESPUESTA:

La Superintendencia del Subsidio Familiar no acoge la observación realizada, puesto que como lo indica Colombia Compra, las certificaciones de gestión de calidad no se pueden

exigir como requisitos habilitantes o puntuables, esto según el artículo 5, parágrafo 2, de la Ley 1150 de 2007 normativa que establece que las «certificaiones de sistemas de gestión de calidad no serán objetos de calificación ni establecerse como documento habilitante para participar en licitaciones o concursos»

OBSERVACIÓNES INTERESADO: COINSA SAS

OBSERVACIÓN No.1

1.1 Especificaciones Técnicas Generales del Servicio SOC

Para la ejecución del contrato y el cumplimiento de los niveles de servicio solicitados, el contratista dispondrá del talento humano que él considere necesario, sin embargo, debeincluir mínimo lo siguiente:

Rol	Profesión en Colombia (Carreras Afines según SNIES)
Gerente de proyecto	Profesión: Título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines. Posgrado: posgrado en Gerencia de Proyectos o Gerencia de Proyectos en Ingeniería de Telecomunicaciones o Administración de Empresas con Especialidad en Dirección de Proyectos. Certificaciones: PMP - Project Management Professional o Prince. Experiencia mínima: 10 años como profesional ejecutando proyectos y/o labores como director o gerente de proyectos en el sector de tecnología Experiencia especifica: 5 años en Ciberseguridad, Seguridad informática, Seguridad de la Informacióny.
	Certificaciones: Auditor Lider ISO 27001:2022, Cobit 5 o ITIL v4, CISM Certified Information Security Manager o CISSP Certified Information Systems Segurity Professional, Scrum Master

Solicitamos amablemente a la entidad modificar dicho requerimiento de la siguiente manera: Un (1) Gerente de proyectos, Ingeniero en Sistemas, Informática, Telemática, Electrónico o carreras afines. Con especialización o Maestría en Gerencia de Proyectos o Gerencia de Tecnología o Gerencia Estratégica o Maestría en Seguridad Informática con experiencia mínima de cinco (5) años en proyectos de TI y/o mínimo cuatro (4) años en

proyectos de seguridad. Deberá contar con estas certificaciones: Certificación PMP vigente o ITIL V4.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA

OBSERVACIÓN No.2

Consultor Senior despliegue	Profesión: Título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines. Posgrado: Posgrado en Seguridad de la información o Seguridad informática o Seguridad de Redes Telemáticas o Seguridad Física y de la informática, Certificaciones: Certificación dada por el fabricante de la herramienta SIEM propuesta. Auditor Líder ISO 27001:2013 Auditor Lider ISO 27001:2022, CEH - Certified Ethical Hacker o CISM - Certified Information Security Manager o CISSP - Certified Information Systems Segurity Professional, Lead Cybersegurity Manager ISO/IEC 27032:2012 o Lead Cybersegurity Professional Certificate (LCSPC), Introductorio de Seguridad en Redes LACNIC o Seguridad en BGP con RPKI e IRR LACNIC Experiencia mínima: 5 años como profesional ejecutando proyectos y/o labores consultor especialista en seguridad de la información o Ciberseguridad Experiencia especifica: 4 proyectos en Despliegue de la herramienta propuesta para SIEM y uno de estos contratos que contenga despliegue de mínimo 2 de las siguientes herramientas SOAR, HONEYPOT, PROTECCION DE MARCA, GESTION DE VULNERABILIDADES para el sector gobierno

Solicitamos amablemente a la entidad modificar dicho requerimiento de la siguiente manera: Mínimo Un (1) Ingeniero de Sistemas, Informática, Telemática, Electrónico o carreras afines, con especialización o maestría en seguridad de la información y/o informática. Con experiencia mínima de cinco (4) años en proyectos de ciberseguridad y/o experiencia mínima de (5) años como auditor, coordinador, oficial de seguridad, Gestor de disponibilidad y Continuidad o profesional en seguridad informática. Deberá contar con CEH (Certified Ethical Hacker) y con al menos una (1) de las siguientes certificaciones: CISA (Certification - Information Systems Auditor), OSCP (Offensive Security Certified Professional), CISM (Certified Information Security Management), CPTE (Certified Penetration Testing Engineer), CISSP (Certified Information Systems Security Professional).

Sesgar la experiencia especifica 4 años a la implementación de herramientas tecnológicas de ciberseguridad como: SIEM , SOAR o protección de marca no garantiza que las competencias del profesional sean las idóneas y las que busca la entidad para el equipo humano durante la ejecución del contrato, en la industria existen diferentes compañías o empresas que se dedican al despliegue de herramientas de seguridad pero esto no quiere decir que entiendan a profundidad de las reglas de para la seguridad de la información y la protección de los activos digitales , dicho lo anterior las competencias de este profesional consultor deberían estar más orientadas a experiencias en la participación de este tipo de proyectos de acuerdo al objeto del contrato. Es importante también complementar en cuanto la solicitud del consultor que las competencias de este profesional antes mencionadas nos permiten garantizar que se implementen los controles de seguridad asociados a las buenas prácticas y marcos de referencias de seguridad como: NIST, ISO: 27001, ISO:27032, ISO:27035 entre otros. A continuación, se listan algunos de los controles más importantes que tienen que ver y están relacionados con el objeto de este proceso y que el profesional sugerido es el idóneo y que garantizan la implementación de estos bajo las buenas prácticas.

1. Inteligencia de amenazas. 2. seguridad de la información para el uso de servicios en la nube 3. Preparación de las TIC para la continuidad del negocio.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA

OBSERVACIÓN No.3

Líder SOC	Profesión: título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines Posgrado: Posgrado en seguridad de la información o Seguridad de Redes Telemáticas o Seguridad Física y de la informática o Seguridad informática Certificaciones: CHFI - Computer Hacking Forensic Investigator, Auditor Interno ISO 27001:2013 o Auditor Líder ISO 27001:2013, Auditor Lider ISO 27001:2022, CEH - Certified Ethical Hacker, ITIL v3 o superior, Introductorio de Seguridad en Redes LACNIC o Seguridad en BGP con RPKI e IRR LACNIC

Solicitamos amablemente a la entidad que para el profesional solicitado, Líder de SOC se modifique dicho requerimiento de la siguiente manera: Mínimo Un (1) Ingeniero de Sistemas, Informática, Telemática, Electrónico o carreras afines, con especialización en seguridad informática y/o en seguridad de la información y/o ciberseguridad y/o Redes

Telemáticas y/o Seguridad Física y de la Informática y/o maestría en seguridad informática y/o maestría en seguridad de la información y/o ciberseguridad. Con experiencia mínima de tres (3) años en proyectos de TI y mínimo dos (2) años como coordinador líder de SOC. En las certificaciones mínimas solicitadas del profesional en mención podemos identificar que solicitan: CHFI - Computer Hacking Forensic Investigator , CEH - Certified Ethical Hacker, Introductorio de Seguridad en Redes LACNIC o Seguridad en BGP con RPKI e IRR LACNIC , estas certificaciónes estan mas relacionas con el perfil de un arquitecto o especialista de seguridad y ciberseguridad de nivel 3. Requerir estas certificaciones para el líder de SOC que dentro de sus actividades más relevantes están encaminadas a la operación, las buenas prácticas en los procesos implementados para el servicio, la auditoria de los informes, la verificación de las actividades y el seguimiento entre otras, podemos evidenciar que sesga el proceso y no esta dando la oportunidad a que los demás oferentes puedan cumplir con estos requerimientos solicitados para el perfil. Mencionado lo anterior solicitamos amabelemente a la entidad retirar del requerimiento estas certifiaciones para el perfil solicitado Líder de SOC: CHFI - Computer Hacking Forensic Investigator , CEH - Certified Ethical Hacker, Introductorio de Seguridad en Redes LACNIC o Seguridad en BGP con RPKI e IRR LACNIC Y QUE la experiencia especifica mínima requerida para el profesional sea de tres (3) años en proyectos de TI y Mínimo dos (2) años como coordinador líder de SOC

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA

OBSERVACIÓN No.4

Se solicita amablemente a la entidad que de acuerdo con el requerimiento Especificaciones Técnicas Generales Herramienta SIEM, incluir el siguiente requerimiento: Se requiere que el servicio sea prestado con una plataforma SIEM que sea del tipo Security Information and Event Manager que permita colectar, retener y correlacionar los eventos de seguridad de la infraestructura IT de la entidad. Se requiere que la solución de SIEM tenga integración de CMDB, a nivel de security mesh, customización de playbooks y reportes con SOAR.

RESPUESTA:

Se acoge la solicitud del interesado y de acuerdo con lo propuesto se establecerá en los documentos definitivos del proceso lo siguiente:

Especificaciones técnicas del SIEM: Se requiere que el servicio sea prestado con una plataforma SIEM que sea del tipo Security Information and Event Manager que permita colectar, retener y correlacionar los eventos de seguridad de la infraestructura IT de la entidad. Se requiere que la solución de SIEM tenga integración de CMDB, a nivel de security mesh, customización de playbooks y reportes con SOAR.

OBSERVACIÓN No.5

Consultor Técnico SOC	Profesión: Título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines Certificaciones: Auditor Lider ISO 27001:2022, Seguridad en BGP con RPKI e IRR LACNIC. Curso o Certificación dada por el fabricante de la herramienta SIEM propuesta, Auditor Lider ISO 27001:2013, Cybersecurity Manager ISO/IEC 27032:2012 o Cyber Security Foundation Professional Certificate (CSFPC) Experiencia mínima: 4 años como profesional ejecutando proyectos y/o labores como consultor en Seguridad o Ciberseguridad Experiencia especifica: 3 proyectos en Ciberseguridad, Seguridad informática, Seguridad de la Información o SOC

Solicitamos amablemente a la entidad que, para el profesional solicitado, consultor técnico SOC se modifique dicho requerimiento de la siguiente manera: Profesión: Título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines, Certificaciones: Auditor Lider ISO 27001:2022, Certificación dada por el fabricante de la herramienta SIEM propuesta. Experiencia mínima: cinco (5) años como profesional ejecutando proyectos y/o labores como consultor en Seguridad o Ciberseguridad, Experiencia especifica: cinco (5) proyectos de implementación en Ciberseguridad y cinco (5) años en administración de herramientas de Seguridad informática o SOC.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA

OBSERVACIÓN No.6

Se solicita amablemente a la entidad que de acuerdo incluir para la herramienta tipo SIEM CERTIFIACIONES DE FABRICANTE. Solicitar que la certificación de la solucion de

Security Information (SIEM) and Event Management, el oferente este autorizado para comercializar servicios sobre las soluciones de SIEM y se encuentre en uno de los dos (2) niveles más altos de la membresía del fabricante de la herramienta SIEM propuesta. Además que en la carta se evidencie que cuenta con una especialización de SOC para la operación del servicio.

RESPUESTA:

Frente a la observación relacionada con el SIEM, ver respuesta a la Observación No. 4 interesado COINSA SAS.

Frente a los niveles de membresía del fabricante y la especificación en la carta del fabricante en la que se exprese que cuenta con una especialización de SOC, la entidad no acoge la solicitud del interesado toda vez que este requisito limita el proceso a un espectro pequeño de posibles proponentes.

OBSERVACIÓN No. 7

Según el numeral 4.3.1 EXPERIENCIA DEL PROPONENTE, se requiere que los proponentes acrediten experiencia de la siguiente manera:

> **4.3. REQUISITOS TÉCNICOS HABILITANTES**
> **4.3.1. EXPERIENCIA DEL PROPONENTE Y DEL EQUIPO DE TRABAJO**
>
> Con el fin de garantizar la calidad del servicio, el cumplimiento en la ejecución del contrato y mitigar el riesgo de incumplimientos en la ejecución del mismo, el proponente o al menos uno de los miembros del consorcio o unión temporal, deberán acreditar experiencia en el objeto, alcance y/o actividades en prestación de servicios de ciberseguridad, mediante la presentación de **máximo dos (2) certificaciones** /o actas de liquidación de contratos ejecutados en los últimos dos (2) años y hasta la fecha de la presentación de la oferta en al menos tres (3) de los siguientes códigos, registrados en el Registro Único de Proponentes RUP en las siguientes clasificaciones:

Solicitamos amablemente a la entidad que dicha experiencia sea solicitada de la siguiente manera: Con el fin de garantizar la calidad del servicio, el cumplimiento en la ejecución del contrato y mitigar el riesgo de incumplimientos en la ejecución del mismo, el proponente o al menos uno de los miembros del consorcio o unión temporal, deberán acreditar

experiencia en el objeto, alcance y/o actividades en prestación de servicios de Monitoreo y/o SOC, mediante la presentación de máximo dos (2) certificaciones /o actas de liquidación de contratos ejecutados en los últimos cuatro (4) años y hasta la fecha de la presentación de la oferta en al menos tres (3) de los siguientes códigos, registrados en el Registro Único de Proponentes RUP en las siguientes clasificaciones: Condiciones de la experiencia específica relacionada: a) La sumatoria de la cuantía de las certificaciones deberá ser mayor o igual al 100% del presupuesto oficial asignado para el presente proceso. b) Haber entregado licenciamiento con transferencia de propiedad a cliente final de las herramientas de amenazas de la red, y herramienta de suplantación de marca, dichas entregas deben estar certificadas por los respectivos fabricantes. Las certificaciones de experiencia deben contener los servicios de configuración y parametrización o implementación de dichas herramientas. c) Haber sido ejecutada para entidades públicas, mixtas, organismos multilaterales, o privados. d) Haber sido iniciada y terminada en los últimos cuatro (4) años. e) Las certificaciones y/o copias de minutas y/o actas de liquidación, de los contratos tendrán como mínimo la siguiente información y deben estar registrados en el RUP: f) Entidad Contratante g) Contratista h) Objeto del contrato i) Número de contrato (si registra) j) Valor del Contrato k) Fecha de inicio (día, mes y año) l) Fecha de terminación del contrato (día, mes y año) m) Nombre, firma y cargo de la persona que expide la certificación (representante legal o persona autorizada de la empresa que expide la certificación) Esta solicitud se fundamenta en la necesidad de que la experiencia exigida esté alineada con el objeto a contratar, considerando que, conforme a la ficha técnica del presente proceso, el componente principal es el SOC, siendo este el aspecto más relevante que los proponentes deberían acreditar.

Adicionalmente, solicitamos que el requisito de experiencia sea ajustado para que las certificaciones exigidas puedan corresponder a contratos ejecutados en los últimos cuatro (4) años y no en los últimos dos (2) años.

En atención a lo dispuesto en el artículo 5 de la Ley 1150 de 2007, que establece que la experiencia debe ser exigida en términos proporcionales y razonables, teniendo en cuenta la naturaleza y complejidad del objeto contractual. Esta modificación permitirá ampliar la concurrencia de oferentes sin comprometer la calidad de los servicios a contratar, en conformidad con los principios de selección objetiva y de transparencia consagrados en la Ley 80 de 1993 y la Ley 1150 de 2007.

RESPUESTA:

No se acoge la solicitud del interesado toda vez que en aspectos relacionados con ciberseguridad se requiere que el adjudicatario cuente con experiencia reciente en la

gestión de monitoreo de amenazas, gestión de incidentes y reacción frente a los mismos, ya que los ciberataques cuentan con un alto nivel de madurez y despliegue continuo, que requiere experticia reciente para su gestión.

PRESENTADA POR: YAK TILL S.A.S

OBSERVACIÓN No.1

Documento: "10 PROYECTO DE PLIEGO DE CONDICIONES SOC" Tema: "ESPECIFICACIONES TÉCNICAS GENERALES" Página(s): 23 Texto: "El contratista deberá realizar mensualmente, según lo establezcan las mejores prácticas de seguridad, análisis de tendencias sobre los eventos y plataformas monitoreadas por el servicio SOC". Por lo anterior solicitamos a la Superintendencia aclarar:

- ¿Qué tipo de eventos de seguridad deben ser analizados en las tendencias?
- ¿Qué herramientas específicas de análisis se deben utilizar para realizar el análisis de tendencias?
- ¿El análisis mensual debe incluir comparaciones con los meses anteriores para observar patrones de largo plazo?

RESPUESTA:

La Superintendencia del Subsidio Familiar, se permite informar que el tipo de amenazas a analizar se enlistan a continuación sin embargo se aclara que no se deben limitar a las mencionadas a continuación:

- Malware y ransomware.
- Phishing.
- Ataques DDoS.
- Violencia de datos.
- Vulnerabilidades y parches: Seguimiento de sistemas que no están actualizados y que pueden ser objetivos fáciles para atacantes
- Tendencias en amenazas emergentes

En general las nuevas tácticas, técnicas y procedimientos (TTP) utilizados por atacantes, y los incidentes relacionados con la falta de cumplimiento de regulaciones y su impacto en la seguridad.

Las herramientas dispuestas para realizar el análisis podrán ser establecidas por el contratista según considere.

El análisis deberá permitir realizar comparativos mensuales que permitan identificar patrones en el tiempo.

OBSERVACIÓN No.2

Documento: "10 PROYECTO DE PLIEGO DE CONDICIONES SOC" Tema: "ESPECIFICACIONES TÉCNICAS GENERALES" Página(s): 23 Texto: "El contratista deberá generar y entregar boletines sobre alertas de seguridad que afecten la infraestructura". Por lo anterior solicitamos a la Superintendencia aclarar:

- ¿Qué tipo de alertas de seguridad deben ser incluidas en los boletines?
- ¿Es necesario emitir boletines fuera de los ciclos regulares en caso de incidentes críticos?

RESPUESTA:

La Superintendencia del Subsidio Familiar se permite informar que las alertas de seguridad que se deben incluir en los boletines podrán ser, pero no limitarse a los siguientes:

- Nuevas tácticas, técnicas y procedimientos (TTP) utilizados por atacantes.
- Incidentes relacionados con la falta de cumplimiento de regulaciones y su impacto en la seguridad.

Los boletines podrán ser entregados fuera de los ciclos regulares según la criticidad de los mismos.

OBSERVACIÓN No.3

Documento: "10 PROYECTO DE PLIEGO DE CONDICIONES SOC" Tema: "ESPECIFICACIONES TÉCNICAS GENERALES" Página(s): 23 Texto: "El SOC deberá realizar análisis del comportamiento de la infraestructura monitoreada para correlacionar incidentes y determinar proactivamente problemas en la operación". Por lo anterior solicitamos a la Superintendencia aclarar:

- ¿Qué indicadores o métricas se deben monitorear para identificar problemas operativos proactivamente?
- ¿Con qué frecuencia se deben realizar estos análisis de comportamiento? (diario, semanal, mensual)?

RESPUESTA:

La Superintendencia del Subsidio Familiar, se permite dar respuesta a la observación del interesado indicando que los indicadores o métricas que se deben monitorear podrán ser, pero no limitarse a las que se mencionan a continuación:

- Tasa de Incidentes.
- Tiempo de Respuesta a Incidentes.
- Falsos Positivos.
- Eventos por Tipo.
- Actualizaciones y Parches.

De igual manera, la frecuencia de análisis de comportamiento podría darse según la criticidad del análisis del comportamiento al igual que algunos análisis que según su frecuencia e importancia podrían hacerse según corresponda. Una posible frecuencia del análisis del comportamiento podría ser, pero no limitarse ah, Diario, monitoreo de eventos críticos y alertas, análisis de la tasa de incidentes y tiempos de respuesta, semanal, falsos positivos, disponibilidad del sistema, mensual, análisis más profundo de tendencias, comparación de métricas a lo largo de la prestación del servicio, entre otros.

OBSERVACIÓN No.4

Documento: “10 PROYECTO DE PLIEGO DE CONDICIONES SOC” Tema: “1.3. Especificaciones Técnicas Generales del SOC” Página(s): 27 Texto: ““El SOC deberá tener la capacidad de integrarse con el SIEM de propiedad de la Superintendencia del Subsidio Familiar, el cual es ArcSight (logger y ArcMC) del fabricante MicroFocus, así mismo deberá contar con la capacidad de configurar, parametrizar y gestionar dicho SIEM.”. Por lo anterior solicitamos a la Superintendencia aclarar:

- ¿Qué datos o eventos del SOC deben ser enviados al SIEM y viceversa?
- ¿Cómo se configurarán las alertas en el SIEM en base a los eventos detectados por el SOC?

- ¿El equipo del SOC recibirá inducción específica en el uso y la gestión de ArcSight?

RESPUESTA:

La Superintendencia del Subsidio Familiar, informa en respuesta de la observación del interesado que la configuración de las alertas en el SIEM, específicamente ArcSight, estará a cargo del contratista. Esto implica que el contratista deberá asegurarse de que las alertas estén correctamente definidas y ajustadas a la necesidad de la entidad, igualmente se informa que el equipo del SOC no recibirá inducción especifica en el uso y la gestión de ArcSight.

Para más información ver respuesta a la observación No. 1 y No. 2 del interesado PASSWORD CONSULTING SERVICES SAS

OBSERVACIÓN No.5

Documento: “10 PROYECTO DE PLIEGO DE CONDICIONES SOC” Tema: “1.3. Especificaciones Técnicas Generales del SOC” Página(s): 27 Texto: “Las instalaciones del SOC deben contar con procedimientos, políticas de seguridad física para oficinas, recintos e instalaciones donde se encuentran los equipos con los cuales prestan el servicio, garantizando el esquema de seguridad sobre todos los componentes que lo integren, en el caso de utilizar herramientas basadas en nube deberán estar soportadas y garantizar el modo de alta disponibilidad.”. Por lo anterior solicitamos a la Superintendencia aclarar:

- ¿Cuáles son los procedimientos específicos que deben implementarse para garantizar la seguridad física de las instalaciones del SOC?
- ¿Se requiere la instalación de sistemas de monitoreo y vigilancia, como cámaras de seguridad o sensores de movimiento, en las instalaciones del SOC?

RESPUESTA:

La Superintendencia del Subsidio Familiar, informa en respuesta a su observación, que los procedimientos de seguridad física en las instalaciones podrán ser, pero no limitarse a control de acceso, zonas de seguridad y diferentes procedimientos que se alinean con las buenas prácticas en seguridad física para los SOC, de igual manera se indica que la

instalación de diferentes aspectos de seguridad y monitoreo estarán a disposición del contratista, siempre y cuando estas se alineen con las mejores prácticas.

OBSERVACIÓN No.6

Documento: “10 PROYECTO DE PLIEGO DE CONDICIONES SOC” Tema: “1.3. Especificaciones Técnicas Generales del SOC” Página(s): 28 Texto: “El servicio debe permitir la integración del envío de alarmas automáticas vía correo electrónico...”. Por lo anterior solicitamos a la Superintendencia aclarar:

- ¿Qué tipos de alarmas deben enviarse automáticamente a través del correo electrónico? (por ejemplo, alertas críticas, advertencias, incidentes de seguridad)
- ¿Se deben implementar mecanismos de seguimiento para asegurar que los correos de alarmas han sido recibidos y leídos?

RESPUESTA:

La Superintendencia del Subsidio Familiar, se permite dar respuesta indicando que los tipos de alarma que se deben enviar automáticamente podrían ser, pero no limitarse a las mencionadas en la observación, alertas críticas, advertencias, incidentes de seguridad, en lo referente a la necesidad de conocer si los correos de alarma han sido recibidos y leídos, no es estrictamente necesario, sin embargo, si se debe contar con una bitácora de las notificaciones enviadas.

OBSERVACIÓN No.7

Observación No. 7 Documento: “10 PROYECTO DE PLIEGO DE CONDICIONES SOC” Tema: “1.3. Especificaciones Técnicas Generales del SOC” Página(s): 28 Texto: “El servicio SOC debe ser compatible con los métodos de recopilación de logs de la industria (Syslog, WMI, JDBC y SNMPv3”.

Por lo anterior solicitamos a la Superintendencia indicar si hay consideraciones especiales para la integración de sistemas en la nube frente a sistemas on-premises.

RESPUESTA:

La Superintendencia del Subsidio Familiar, se permite dar respuesta indicando que los aspectos de consideración podrían ser, pero no limitarse a los métodos de recopilación de logs, los aspectos de rendimiento y latencia, aquellos relacionados a las buenas prácticas de seguridad, se debe tener en cuenta la escalabilidad y de igual manera la interoperabilidad de las soluciones en la recopilación de logs para su integración en nube y on-premises.

OBSERVACIÓN No.8

Documento: “10 PROYECTO DE PLIEGO DE CONDICIONES SOC” Tema: “1.3. Especificaciones Técnicas Generales del SOC” Página(s): 31 Texto: “Los canales de comunicación (red de datos) se centralizan en la ciudad de Bogotá y el contratista será encargado de dimensionar, diseñar, adquirir, instalar, configurar, operar y administrar la arquitectura tecnológica del servicio de monitoreo.”.

Por lo anterior solicitamos a la Superintendencia indicar qué protocolos de configuración y seguridad se aplicarán para garantizar la integridad de la red y los datos transmitidos.

RESPUESTA:

La Superintendencia del Subsidio Familiar, en respuesta a su observación, se permite aclarar que los canales de comunicación seguros a utilizar podrán ser, VPN Site to Site (IPSec), comunicación cifrada entre origen y destino el cual maneje el proveedor en su arquitectura tecnológica con la cual prestará el servicio.

OBSERVACIÓN No.9

Documento: “10 PROYECTO DE PLIEGO DE CONDICIONES SOC” Tema: “1.4. Requerimientos Específicos - Correlación y Alertamiento de Eventos de Seguridad” Página(s): 31 Texto: “El contratista deberá asegurar el almacenamiento, disponibilidad y recuperación de los LOGs y la información generada en la ejecución del servicio contratado.”. Por lo anterior solicitamos a la Superintendencia aclarar:

- ¿Cuál es el volumen estimado de datos y logs que se generarán durante la ejecución del servicio? (en GB o TB)?
- ¿Cuál será la estrategia de backup para asegurar la integridad y disponibilidad de los logs y la información?
- ¿Qué procedimientos se seguirán para la recuperación de datos?

RESPUESTA:

La Superintendencia del Subsidio Familiar, en respuesta a sus observaciones, se permite indicar que el volumen estimado de datos en este momento no se tiene contemplado, las estrategias de backup para asegurar la integridad y disponibilidad de los logs y la información deben ser definidas por el contratista y estas deben estar alineadas a las buenas prácticas de la industria, de igual manera se informa que al igual que para las estrategias de backup, el contratista será quien defina los procedimientos que se seguirán para la recuperación de datos, siempre que estos garanticen la integridad de los datos y esten alineados con las buenas prácticas.

OBSERVACIÓN No.10

Documento: “10 PROYECTO DE PLIEGO DE CONDICIONES SOC” Tema: “1.4. Requerimientos Específicos - Correlación y Alertamiento de Eventos de Seguridad” Página(s): 32 Texto: “Es importante que el contratista defina un plan de respaldo en caso de borrados accidentales provocados y presentarlo, una vez se firme el acta de inicio.”. Por lo anterior solicitamos a la Superintendencia aclarar:

- ¿Qué tipos de datos y logs deben incluirse en el plan de respaldo?
- ¿Con qué frecuencia se debe realizar el respaldo de los datos?

RESPUESTA:

La Superintendencia del Subsidio Familiar, se permite dar respuesta indicando que los aspectos de consideración podrían ser, pero no limitarse a Logs de eventos de seguridad de los diferentes registros generados por los sistemas, datos de alta relevancia, logs de acceso y todos los datos de auditoría, en referencia al respaldo, se recomienda que se realicen según su criticidad en respaldos diarios, semanales y mensuales, se recalca que la podrían presentarse diferentes frecuencias en los respaldos según su criticidad y significancia.

OBSERVACIÓN No.11

Documento: “10 PROYECTO DE PLIEGO DE CONDICIONES SOC” Tema: “1.4. Requerimientos Específicos - Correlación y Alertamiento de Eventos de Seguridad” Página(s): 34 Texto: “El contratista deberá generar reportes de eventos y de análisis de tendencias, para tomar las acciones preventivas y/o correctivas, tales como: instalación de parches, actualización de versiones, modificación de políticas y configuraciones. Además, debe quedar registros de cuándo, dónde y cómo se presentan los incidentes, así como definir nuevos reportes acorde a las necesidades de la SSF. ” Por lo anterior solicitamos a la Superintendencia aclarar:

- ¿Qué información detallada debe incluirse en los registros de incidentes?
- ¿Qué información específica debe incluirse en los reportes sobre la instalación de parches, actualizaciones de versiones y cambios en configuraciones?

RESPUESTA:

La Superintendencia del Subsidio Familiar, en respuesta a la observación del interesado, se permite informar que la información a incluir en los registros podría ser, pero no limitarse a: Identificación única del incidente, descripción, seguimientos, impacto, respuesta y solución.

Para lo referente a la información específica en los reportes, podría incluir, pero no limitarse a: Descripción del cambio, justificación del cambio, comparativo entre las versiones, impacto y aprobación.

OBSERVACIÓN No.12

Documento: “10 PROYECTO DE PLIEGO DE CONDICIONES SOC” Tema: “1.3. Especificaciones Técnicas Generales del SOC” Página(s): 27 Texto: “El servicio de SOC debe tener la capacidad en tiempo real para detectar, recolectar, cruzar y consolidar patrones sobre la información recolectada, para poder alertar tempranamente los problemas, priorizando los activos más importantes”

Por lo anterior solicitamos a la Superintendencia indicar si se espera que el SOC utilice tecnologías avanzadas como inteligencia artificial o análisis predictivo para detectar patrones de amenaza.

RESPUESTA:

La Superintendencia del Subsidio Familiar, en respuesta a la observación del interesado, se permite citar lo que se encuentra descrito en el numeral “1.3. Especificaciones Técnicas Generales del SOC” Página: 28 donde se indica que “El Servicio SOC deberá contar con tecnologías cognitivas para acelerar el proceso de investigación de potenciales incidentes de seguridad, dicha inteligencia artificial deberá analizar fuentes como: mensajes de X, información de foros, boletines de seguridad, artículos, Wikis, presentaciones de conferencias, reportes de analistas y bases de conocimiento.” Por lo anterior nos permitimos informar que la entidad si solicita la aplicación de inteligencias avanzadas como inteligencia artificial.

OBSERVACIÓN No.13

Documento: “10 PROYECTO DE PLIEGO DE CONDICIONES SOC” Tema: “1.8. Requerimientos Específicos – Categorías de Eventos de Seguridad a Monitorear” Página(s): 36 Texto: “El contratista debe contar con un portal de informes, métricas e indicadores que usará la SSF para seguimiento, en el cual se deben entregar perfiles de usuarios al supervisor y los que autorice el mismo”. Por lo anterior solicitamos a la Superintendencia aclarar:

- ¿Qué tipo de informes, métricas e indicadores deben estar disponibles en el portal?
- ¿Se espera que el portal acepte la personalización de los informes o dashboards según las necesidades del supervisor o usuarios autorizados?
- ¿El portal deberá incluir registros de auditoría para controlar quién accede a los informes y métricas?

RESPUESTA:

La Superintendecia del Subsidio Familiar, en respuesta a la observación del interesado se permite informar, que las métricas e indicadores que se dispondrán en el dashboard serán aquellos definidos conjuntamente, donde la información presentada genere valor, por tal motivo se espera que el portal acepte la personalización de los informes o dashboards según la necesidad, igualmente el portal si pudiese contar con registros de auditoría.

OBSERVCION No.14

Documento: “ANEXO 09 anexo técnico soc” Tema: “ESPECIFICACIONES TÉCNICAS GENERALES” Página(s): 3 Texto: “El SOC debe poder utilizar herramientas de su propiedad para colectar, procesar, monitorear y correlacionar como mínimo 4500 EPS (Eventos por segundo) sin costos adicionales para la entidad. Se deberá adjuntar los documentos vigentes necesarios que demuestren que el proveedor del servicio SOC está autorizado y cuenta con el entrenamiento de utilizar dichas herramientas.”

Por lo anterior solicitamos a la Superintendencia indicar la documentación específica que debe ser acreditada por los proveedores del servicio SOC para demostrar su autorización y capacidad de utilizar estas herramientas.

RESPUESTA:

La Superintendencia del Subsidio Familiar, en respuesta a su observación se permite informar que los documentos solicitados, son aquellos brindados por el fabricante donde se indique la idoneidad del uso de las herramientas a utilizar.

OBSERVACIÓN No.15

Documento: “10 PROYECTO DE PLIEGO DE CONDICIONES SOC” Tema: “6.3.2 CERTIFICACIÓN EQUIPO DE TRABAJO” Página(s): 96 - 99 Texto: “El proponente deberá aportar una certificación suscrita por el representante legal en donde garantiza que para la cobertura del servicio cuenta con el personal idóneo deberá presentar Hojas de vida con la oferta de todo el personal requerido con soportes de formación académica y de experiencia ANEXO 10. ” Solicitamos a la Entidad aclarar si con la oferta presentada se debe adjuntar documentación soporte del personal requerido dentro del presente proceso, lo anterior en atención a que en el anexo 10 “Personal Mínimo Requerido” solo se indica el compromiso de cumplimiento del suministro en la etapa contractual de los perfiles del Gerente de proyecto, Consultor Senior despliegue y Líder SOC, mismo compromiso que se indica en el numeral 1.1 Especificaciones Técnicas Generales del Servicio SOC “Para la ejecución del contrato y el cumplimiento de los niveles de servicio solicitados, el contratista dispondrá del talento humano que él considere necesario...”, sin embargo en el numeral 6.3.2 se indican más perfiles. De otro lado, y en caso de que la aclaración anterior sea afirmativa, solicitamos aclarar e indicar de manera detallada cuáles perfiles deben ser acreditados junto con la oferta.

RESPUESTA:

Frente a la inquietud en la cual se solicita la no exigencia de las hojas de vida para determinar si el proponente cumple o no cumple, ver respuesta a la observación No. 2 del interesado OPEN GROUP

OBSERVACIÓN No.16

Documento: “10 PROYECTO DE PLIEGO DE CONDICIONES SOC” Tema: “6.3.2 CERTIFICACIÓN EQUIPO DE TRABAJO” Página(s): 96 - 99 Texto: “Gerente de proyecto: Profesión: Título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines. Posgrado: posgrado en Gerencia de Proyectos o Gerencia de Proyectos en Ingeniería de Telecomunicaciones o Administración de Empresas con Especialidad en Dirección de Proyectos. Certificaciones: PMP - Project Management Professional o Prince”.

Solicitamos a la Entidad en aras de tener igualdad de condiciones y por ende mayor posibilidad de búsqueda y cumplimiento del perfil del Gerente de Proyecto, que la certificación PMP-Project Management Professional o Prince sea opcional, así mismo que se amplíe el campo de la especialidad incluyendo un especialista en seguridad de la información o seguridad informática especializaciones que cumplen el perfil requerido pues guarda concordancia con los requisitos de las carreras afines según SNIES.

RESPUESTA:

Ver respuesta a la observación No. 1 del interesado OPEN GROUP

OBSERVACIÓN No.17

Documento: “10 PROYECTO DE PLIEGO DE CONDICIONES SOC” Tema: “6.3.2 CERTIFICACIÓN EQUIPO DE TRABAJO” Página(s): 96 - 99 Texto: “Consultor Senior despliegue:...Certificaciones: Certificación dada por el fabricante de la herramienta SIEM propuesta. Auditor Líder ISO 27001:2013 Auditor Lider ISO 27001:2022, CEH - Certified Ethical Hacker o CISM - Certified Information Security Manager o CISSP - Certified Information Systems Segurity Professional, Lead Cybersegurity Manager ISO/IEC 27032:2012 o Lead Cybersegurity Professional Certificate (LCSPC), Introductorio de Seguridad en Redes LACNIC o Seguridad en BGP con RPKI e IRR LACNIC Experiencia mínima: 5 años como profesional ejecutando proyectos y/o labores consultor especialista

en seguridad de la información o Ciberseguridad Experiencia específica: 4 proyectos en Despliegue de la herramienta propuesta para SIEM y uno de estos contratos que contenga despliegue de mínimo 2 de las siguientes herramientas SOAR, HONEYPOT, PROTECCIÓN DE MARCA, GESTIÓN DE VULNERABILIDADES para el sector gobierno”

Para efectos de tener una mayor pluralidad y transparencia en el requerimiento de los perfiles exigidos, teniendo en cuenta que la solicitud de la Entidad para este perfil está enfocada en un profesional con experticia en solo el sector público quitando la posibilidad de ofrecer profesionales en cuya experiencia laboral han ejecutado labores en sectores de la economía privados y que cumple con el conocimiento necesario para respaldar el proyecto, solicitamos a la entidad que para acreditar para la experiencia específica se modifique el requisito estableciendo que sea un máximo de 4 proyectos, así mismo incluir que también se pueda aportar proyectos en el sector privado. En cuanto a las certificaciones exigidas solicitamos colocar un tope mínimo de 2 de las certificaciones requeridas en este perfíl.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA

OBSERVACIÓN No.18

Documento: “10 PROYECTO DE PLIEGO DE CONDICIONES SOC” Tema: “6.3.2 CERTIFICACIÓN EQUIPO DE TRABAJO” Página(s): 96 - 99 Texto: “Líder SO: Profesión: título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines Posgrado: Posgrado en seguridad de la información o Seguridad de Redes Telemáticas o Seguridad Física y de la informática o Seguridad informática Certificaciones: CHFI - Computer Hacking Forensic Investigator, Auditor Interno ISO 27001:2013 o Auditor Líder ISO 27001:2013, Auditor Líder ISO 27001:2022, CEH - Certified Ethical Hacker, ITIL v3 o superior, Introductorio de Seguridad en Redes LACNIC o Seguridad en BGP con RPKI e IRR LACNIC Experiencia mínima: 7 años como profesional ejecutando proyectos y/o labores consultor especialista en seguridad de la información o Ciberseguridad Experiencia específica: 3 años como Líder SOC”

Solicitamos a la Entidad reducir la cantidad de certificaciones solicitadas y modificar este requerimiento permitiendo que se acredite mínimo 2 certificaciones de las relacionadas en el perfil, por otra parte que la experiencia mínima requerida sea de mínimo 3 años de los

cuales se certifique 1 año como Líder SOC. Lo anterior, permitiría una mayor posibilidad de búsqueda de profesionales que en el mercado cuentan con experiencia pero que para el tipo de perfil requerido se torna muy exigente los tiempos y documentación solicitada generando que se reduzca la posibilidad de la demanda de estos profesionales.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA

OBSERVACIÓN No.19

Documento: “10 PROYECTO DE PLIEGO DE CONDICIONES SOC” Tema: “6.3.2 CERTIFICACIÓN EQUIPO DE TRABAJO” Página(s): 96 - 99 Texto: “Consultor Técnico SOC: ...Certificaciones: Auditor Líder ISO 27001:2022, Seguridad en BGP con RPKI e IRR LACNIC. Curso o Certificación dada por el fabricante de la herramienta SIEM propuesta, Auditor Líder ISO 27001:2013, Cybersecurity Manager ISO/IEC 27032:2012 o Cyber Security Foundation Professional Certificate (CSFPC)

Solicitamos a la Entidad reducir la cantidad de certificaciones solicitadas modificando el requerimiento a mínimo 2 certificaciones de las relacionadas para el perfil, ampliando el rango de búsqueda de profesionales que cuenten con la experiencia y conocimiento para poner al servicio de la Entidad. En los anteriores términos se dejan planteadas las observaciones frente a la Convocatoria Pública y documentos anexos.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA

PRESENTADA POR: E&C INGENIEROS

OBSERVACIÓN No.1

Para los siguientes perfiles, solicitamos muy respetuosamente tomar en consideración las siguientes sugerencias:

PERFIL GERENTE DE PROYECTO

Profesión: Título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines. Posgrado: posgrado en Gerencia de Proyectos o Gerencia de Proyectos en Ingeniería de Telecomunicaciones o Administración de Empresas con Especialidad en Dirección de Proyectos. Certificaciones: PMP - Project Management Professional o Prince. Experiencia mínima: 10 años como profesional ejecutando proyectos y/o labores como director o gerente de proyectos en el sector de tecnología Experiencia especifica: 5 años en Ciberseguridad, Seguridad informática, Seguridad de la Información y, Certificaciones: Auditor Lider ISO 27001:2022, Cobit 5 o ITIL v4, CISM Certified Information Security Manager o CISSP Certified Information Systems Segurity Professional, Scrum Master.

Propuesta de modificación:

Profesión: Título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines. Posgrado: Especialización y/o maestría en gerencia de proyectos en ingeniería de telecomunicaciones y/o Gestión de proyectos tecnológicos Experiencia mínima: 10 años como profesional ejecutando proyectos y/o labores como director o gerente de proyectos en el sector de tecnología Experiencia especifica: 5 años en Ciberseguridad, Seguridad informática, Seguridad de la Información y, Certificaciones: Se permita acreditar con al menos 3 de las siguientes certificaciones ITIL 4 Managing Professional Certificate SCRUM MASTER PV6 LACNIC BASICO ISO 27001:2022 AUDITOR INTERNO Y/O LIDER.

PERFIL CONSULTOR SENIOR DESPLIEGUE

Profesión: Título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines. Posgrado: Posgrado en Seguridad de la información o Seguridad informática o Seguridad de Redes Telemáticas o Seguridad Física y de la informática, Certificaciones: Certificación dada por el fabricante de la herramienta SIEM propuesta. Auditor Líder ISO 27001:2013 Auditor Lider ISO 27001:2022, CEH - Certified Ethical Hacker o CISM - Certified Information Security Manager o CISSP - Certified Information Systems Segurity Professional, Lead Cybersegurity Manager ISO/IEC 27032:2012 o Lead Cybersegurity Professional Certificate (LCSPC), Introductorio de Seguridad en Redes LACNIC o Seguridad en BGP con RPKI e IRR LACNIC Experiencia mínima: 5 años como

profesional ejecutando proyectos y/o labores consultor especialista en seguridad de la información o Ciberseguridad Experiencia especifica: 4 proyectos en Despliegue de la herramienta propuesta para SIEM y uno de estos contratos que contenga despliegue de mínimo 2 de las siguientes herramientas SOAR, HONEYPOT, PROTECCION DE MARCA, GESTION DE VULNERABILIDADES para el sector gobierno.

Agradecemos de antemano se tengan en cuenta nuestras OBSERVACIÓNes con el fin de permitir que la empresa pueda participar en este proceso garantizando total pluralidad, transparencia, eficiencia operacional y competitividad en esta clase de procesos.

Propuesta de modificación:

Se solicita respetuosamente eliminar certificación del SIEM de la herramienta propuesta, pues esto sesgaría la participación del personal que cuenta con la Experiencia, pero no está certificado por alguna marca en específico.

En cuanto a la Certificación ISO 27001 auditor líder: solicitamos respetuosamente se pueda acreditar Auditor Líder ISO 27001:2013 o Auditor Lider ISO 27001:2022.

PERFIL LIDER SOC

Profesión: título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines Posgrado: Posgrado en seguridad de la información o Seguridad de Redes Telemáticas o Seguridad Física y de la informática o Seguridad informática Certificaciones: CHFI - Computer Hacking Forensic Investigator, Auditor Interno ISO 27001:2013 o Auditor Líder ISO 27001:2013, Auditor Lider ISO 27001:2022, CEH - Certified Ethical Hacker, ITIL v3 o superior, Introductorio de Seguridad en Redes LACNIC o Seguridad en BGP con RPKI e IRR LACNIC Experiencia mínima: 7 años como profesional ejecutando proyectos y/o labores consultor especialista en seguridad de la información o Ciberseguridad Experiencia especifica: 3 años como Líder SOC.

Propuesta de modificación:

Profesión: título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines Posgrado: Posgrado en seguridad de la información o Seguridad de Redes Telemáticas o Seguridad Física y de la informática o Seguridad informática Certificaciones: Se permita acreditar con al menos 5 de las siguientes certificaciones: CHFI - Computer Hacking Forensic Investigator, Auditor Interno ISO 27001:2013 o Auditor Líder ISO 27001:2013 o Auditor Lider ISO 27001:2022, CEH - Certified Ethical Hacker, ITIL v3 o superior, Introductorio de Seguridad en Redes LACNIC o Seguridad en BGP con RPKI e IRR LACNIC, Cobit 5 Fundations,PECB ISO 31000 Lead Risk Manage. Experiencia mínima:

7 años como profesional ejecutando proyectos y/o labores consultor especialista en seguridad de la información o Ciberseguridad Experiencia especifica: 3 años como Líder SOC.

PERFIL CONSULTOR TÉCNICO SOC

Profesión: Título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines Certificaciones: Auditor Lider ISO 27001:2022, Seguridad en BGP con RPKI e IRR LACNIC. Curso o Certificación dada por el fabricante de la herramienta SIEM propuesta, Auditor Lider ISO 27001:2013, Cybersecurity Manager ISO/IEC 27032:2012 o Cyber Security Foundation Professional Certificate (CSFPC) Experiencia mínima: 4 años como profesional ejecutando proyectos y/o labores como consultor en Seguridad o Ciberseguridad Experiencia especifica: 3 proyectos en Ciberseguridad, Seguridad informática, Seguridad de la Información o SOC.

Propuesta de modificación:

Se solicita respetuosamente eliminar certificación del SIEM de la herramienta propuesta, pues esto sesgaría la participación del personal que cuenta con la Experiencia, pero no está certificado por alguna marca en específico. Formación: Ingeniería Electrónica, de Sistemas o Telecomunicaciones. Especialización en Seguridad Informática. Experiencia mínima: 4 años como profesional ejecutando proyectos y/o labores como consultor en Seguridad o Ciberseguridad Experiencia especifica: 3 proyectos en Ciberseguridad, Seguridad informática, Seguridad de la Información o SOC Certificaciones: Se permita acreditar con al menos 5 de las siguientes certificaciones: ITIL v4 Foundation, Auditor Interno ISO 27001:2013 o superior, IPV6 LACNIC Avanzado, Seguridad en BGP con RPKI e IRR LACNIC. Curso o Certificación dada por el fabricante de la herramienta SIEM propuesta, Auditor Lider ISO 27001:2013, Cybersecurity Manager ISO/IEC 27032:2012 o Cyber Security Foundation Professional Certificate (CSFPC)

PERFIL ANALISTA NIVEL 2 DE SOC

Profesión: Título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines Certificaciones: Certificación vigente como profesional, analista, especialista y arquitecto de seguridad de redes o su equivalente en la solución ofertada. Emitida por el fabricante. Experiencia mínima: 5 años como profesional ejecutando proyectos y/o labores como consultor en Seguridad o Ciberseguridad Experiencia especifica: 5 años en implementación y/o administración de soluciones de seguridad.

Propuesta de modificación:

Certificaciones: Certificación vigente como profesional, analista, especialista y arquitecto de seguridad de redes o su equivalente. Se solicita respetuosamente eliminar la frase “de la solución ofertada emitida por el fabricante”, esto sesgaría la participación de personal idóneo que cuenta con la Experiencia, pero no está certificado por alguna marca en específico.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA

OBSERVACIÓN No.2

Se Solicita respetuosamente eliminar el numeral b del requerimiento basándose en los siguientes argumentos:

Principio de Proporcionalidad: La solicitud de requisitos excesivos puede ser considerada desproporcionada en relación con el objetivo del contrato o servicio. El principio de proporcionalidad en el derecho administrativo establece que las exigencias deben ser adecuadas, necesarias y proporcionadas al fin que se busca. Requerir licenciamiento y transferencias de propiedad para herramientas específicas puede limitar innecesariamente la participación de proveedores que, aunque no cumplan con esos requisitos, podrían ofrecer servicios de calidad.

Acceso a la Competencia La exigencia de certificaciones específicas puede restringir la competencia. Limitar el acceso a licitaciones o contratos a solo aquellos proveedores que han cumplido con condiciones muy específicas (como haber entregado licencias con transferencia de propiedad) podría crear un monopolio o un oligopolio en el mercado de servicios. Esto puede ir en contra de los principios de libre competencia y puede dar lugar a prácticas de mercado desleales.

Falta de Relación Directa con la Capacidad Técnica La experiencia en la entrega de licenciamiento y herramientas específicas no necesariamente refleja la capacidad técnica y profesional del proveedor para realizar el servicio en cuestión. Otros factores, como la experiencia general en el sector, la calidad del servicio y la reputación del proveedor, son igualmente relevantes y no deberían ser menospreciados. Se podría argumentar que la capacidad técnica se puede demostrar de otras formas que no impliquen requisitos tan restrictivos. Inclusión de Nuevos Proveedores Al establecer criterios tan rígidos, se puede

excluir a proveedores nuevos o más pequeños que, aunque carezcan de la experiencia específica solicitada, pueden ofrecer servicios innovadores y eficaces.

Esto podría ser contradictorio con las políticas de fomento al emprendimiento y a la inclusión de pequeñas y medianas empresas en el mercado. Normativa y Legalidad Es importante revisar si la normativa que regula los procedimientos de contratación pública o el contexto específico de la entidad permite la inclusión de requisitos tan específicos. Si la normativa establece un marco más flexible para la evaluación de la capacidad técnica, la solicitud de estos requisitos podría ser considerada ilegal o abusiva. Posibilidad de Demostrar Experiencia Alternativa Se puede argumentar que la experiencia en el campo de la ciberseguridad, la protección de datos y otros servicios relacionados puede ser demostrada a través de proyectos anteriores, referencias de clientes, o certificaciones de calidad que no estén estrictamente vinculadas a la entrega de herramientas específicas. La inclusión de experiencias alternativas podría enriquecer el proceso de selección.

RESPUESTA:

No es clara la observación del interesado toda vez que menciona el numeral b del requerimiento, pero no específica el requerimiento en sí.

OBSERVACIÓN No.3

Solicitamos la eliminación del requerimiento de presentar el valor de los bienes o servicios en contratos que no se relacionen con la interventoría de proyectos TIC o sistemas de videovigilancia.

Con el fin de facilitar la participación de proveedores en el proceso de subsidio familiar, solicito la eliminación del requerimiento de presentar el valor de los bienes suministrados o de los servicios prestados, específicamente en aquellos contratos que incluyan la prestación de servicios diferentes a la interventoría de proyectos TIC o sistemas de videovigilancia.

1. Relevancia del Objeto del Contrato: El objeto principal de nuestro contrato es la prestación de servicios de monitoreo y atención de incidentes de seguridad de la información. Este servicio se centra en garantizar la integridad, confidencialidad y disponibilidad de la información, lo que no implica la necesidad de valorar bienes o servicios adicionales que no se relacionan directamente con el núcleo del servicio a prestar.

2. Focalización de Recursos: La exigencia de presentar el valor de bienes y servicios ajenos a la atención de incidentes de seguridad de la información puede resultar en una carga administrativa innecesaria y desviar la atención y los recursos de los proveedores, que deben concentrarse en cumplir con los estándares de calidad y eficiencia requeridos en la seguridad de la información.

3. Impacto en la Competitividad: Al eliminar este requerimiento, se promoverá una mayor competitividad entre los proveedores de servicios de seguridad de la información, facilitando su participación en el proceso de subsidio familiar. Esto puede resultar en mejores ofertas y en un servicio más eficaz y adaptado a las necesidades del contrato.

4. Alineación con Normativas: Este enfoque es consistente con la normativa vigente que busca simplificar los procesos administrativos y fomentar la transparencia y eficiencia en la contratación pública.

RESPUESTA:

No se acepta la solicitud del interesado ya que las certificaciones requeridas son esenciales para garantizar la idoneidad del oferente y su experiencia para la ejecución de actividades asociadas al objeto establecido. Para el caso específico del presente proceso, el requisito del que trata la solicitud de certificaciones representa un indicador clave de la capacidad del proveedor para cumplir con los requisitos del servicio, por tal motivo se mantiene el requisito con el fin de asegurar que los oferentes cumplan con los estándares necesarios para la correcta ejecución del contrato.

OBSERVACIÓN No.4

Solicitamos que se incluya las siguientes actividades y/u obligaciones dentro de la acreditación de la experiencia:
• Centro de Operaciones de Seguridad (SOC), que se encarga de la gestión de la seguridad de la información a través de un monitoreo constante de la infraestructura tecnológica

• identificación proactiva de vulnerabilidades, la detección de amenazas, y la mitigación de incidentes de seguridad informática

• soporte técnico especializado mediante el monitoreo permanente de la plataforma base de tecnologías de la información (TI). Nuestro servicio permite la detección proactiva de eventos e incidentes de seguridad, asegurando la protección continua de la infraestructura IT.

RESPUESTA:

Ver respuesta a la observación No. 7 del interesado COINSA

OBSERVACIÓN No.5

SOLICITUD DE INCLUSIÓN DE CERTIFICACIONES ISO

1. Con el fin de garantizar que el proponente esté alineado y comprometido con el cuidado del medio ambiente y la reducción de la huella de carbono, el oferente deberá contar con una certificación vigente en Sistemas de Gestión Ambiental. Esta certificación acreditará que las operaciones del oferente, incluyendo la implementación y administración de licencias de software, están alineadas con prácticas sostenibles y responsables desde un punto de vista ambiental. La certificación deberá ser emitida directamente por el ente certificador y deberá presentarse junto con la oferta económica al cierre del proceso de licitación actual.

2. El oferente deberá alinearse a las políticas de seguridad de la entidad, así como el modelo MSPI del Ministerio de las Telecomunicaciones de Colombia – Mintic, así mismo el oferente deberá certificar que sus servicios de seguridad y mesa de servicios se encuentran certificados en estado vigente con la norma de estándares internacionales de Sistemas de Gestión de Seguridad de la Información(sgs), certificación que debe ser entregada junto con la oferta económica al cierre del proceso de licitación actual, (dicha certificación debe ser expedida directamente a el oferente por el ente certificador)

3. El prestador de servicio debe contar con certificación vigente en la norma de estándares internacionales del Sistema de Gestión de Servicios para los procesos relacionados con seguridad, a fin de garantizar la calidad, gestión y mejora de los servicios de TI. Se deberá adjuntar a la oferta una copia de la certificación emitida por el ente certificador directamente al oferente.

RESPUESTA:

La Superintendencia del subsidio familiar, no acoge la observación presentada, ya que las certificaciones de que trata la presente recomendación, la legislación colombiana no exige que los oferentes cuenten con las mismas para participar en procesos contractuales, por lo que exigir estás podría limitar la participación de oferentes que, aunque no cuenten con las certificaciones citadas, tienen la capacidad técnica y experiencia para cumplir con los requisitos de la entidad.

Así las cosas, aunque las certificaciones mencionadas son valiosas y demuestran un compromiso con la calidad, la seguridad y la sostenibilidad, no pueden ser exigidas como requisitos obligatorios en un proceso contractual, si no están respaldadas por la legislación vigente en Colombia. Imponer estos requisitos podría restringir la competencia, incrementar los costos y limitar la participación de oferentes calificados

OBSERVACIÓN No. 6

OBSERVACIÓNES NIVEL TECNICO

(VER TABLA)

ÍTEM	CITA	OBSERVACIÓN

1	6.3.2 CERTIFICACIÓN EQUIPO DE TRABAJO/Consultor Senior despliegue/Certificaciones: Certificación dada por el fabricante de la herramienta SIEM propuesta.	Según lo verificado en el ANEXO 09. Anexo Técnico_SOC.docx, en el numeral 1.3. "Especificaciones Técnicas Generales del SOC", ítem 1, se establece que "El SOC deberá tener la capacidad de integrarse con el SIEM de propiedad de la Superintendencia del Subsidio Familiar, el cual es ArcSight (logger y ArcMC) del fabricante MicroFocus. Asimismo, deberá contar con la capacidad de configurar, parametrizar y gestionar dicho SIEM." Esto indica que el SIEM a soportar ya es propiedad de la entidad, siendo ArcSight la herramienta implementada. Por lo tanto, no es necesario que los oferentes propongan un nuevo SIEM. En este contexto, solicitamos a la entidad que elimine el requisito establecido en el perfil 6.3.2 "Certificación Equipo de Trabajo/Consultor Senior despliegue/Certificaciones: Certificación dada por el fabricante de la herramienta SIEM propuesta". Consideramos que, dado que la herramienta SIEM ya está implementada, la certificación en cuestión no es aplicable. Proponemos que este requisito sea sustituido por la opción de que el oferente demuestre, a través de contratos ejecutados, experiencia en la administración de herramientas de correlación de eventos de seguridad. Es importante resaltar que un equipo SOC generalmente se compone de especialistas en la correlación de eventos de seguridad, independientemente de las tecnologías o herramientas utilizadas. Limitar el proceso a una certificación específica o a una marca restringe injustamente la pluralidad de oferentes. Por ello, solicitamos que se considere nuestra solicitud de modificación para garantizar un proceso más inclusivo.

2	El servicio SOC deberá contar con una capacidad de retención de información mínima de seis (6) meses, para extracción de información de forma segura y generación de reportes.	De acuerdo con lo revisado en el ANEXO 09. Anexo Técnico_SOC.docx, en el numeral 1.3. "Especificaciones Técnicas Generales del SOC", ítem 1, se especifica que "El SOC deberá tener la capacidad de integrarse con el SIEM de propiedad de la Superintendencia del Subsidio Familiar, el cual es ArcSight (logger y ArcMC) del fabricante MicroFocus." Esto indica que la infraestructura del SIEM ya forma parte de la entidad. En este sentido, solicitamos confirmar si el requisito de "El servicio SOC deberá contar con una capacidad de retención de información mínima de seis (6) meses, para extracción de información de forma segura y generación de reportes" implica que los oferentes deben considerar la provisión de un sitio de
2	El servicio SOC deberá contar con una capacidad de retención de información mínima de seis (6) meses, para extracción de información de forma segura y generación de reportes.	De acuerdo con lo revisado en el ANEXO 09. Anexo Técnico_SOC.docx, en el numeral 1.3. "Especificaciones Técnicas Generales del SOC", ítem 1, se especifica que "El SOC deberá tener la capacidad de integrarse con el SIEM de propiedad de la Superintendencia del Subsidio Familiar, el cual es ArcSight (logger y ArcMC) del fabricante MicroFocus." Esto indica que la infraestructura del SIEM ya forma parte de la entidad. En este sentido, solicitamos confirmar si el requisito de "El servicio SOC deberá contar con una capacidad de retención de información mínima de seis (6) meses, para extracción de información de forma segura y generación de reportes" implica que los oferentes deben considerar la provisión de un sitio de almacenamiento adicional para los logs generados por el SIEM actual de la entidad, o si esta capacidad de retención ya está cubierta por la infraestructura existente. Agradecemos la aclaración para poder ajustar adecuadamente nuestra propuesta.

3	6.3.2 CERTIFICACIÓN EQUIPO DE TRABAJO/Consultor Tecnico SOC/Certificaciones: Curso o Certificación dada por el fabricante de la herramienta SIEM propuesta.	Según lo verificado en el ANEXO 09. Anexo Técnico_SOC.docx, en el numeral 1.3. "Especificaciones Técnicas Generales del SOC", ítem 1, se establece que "El SOC deberá tener la capacidad de integrarse con el SIEM de propiedad de la Superintendencia del Subsidio Familiar, el cual es ArcSight (logger y ArcMC) del fabricante MicroFocus. Asimismo, deberá contar con la capacidad de configurar, parametrizar y gestionar dicho SIEM." Esto indica que el SIEM a soportar ya es propiedad de la entidad, siendo ArcSight la herramienta implementada. Por lo tanto, no es necesario que los oferentes propongan un nuevo SIEM. En este contexto, solicitamos a la entidad que elimine el requisito establecido en el perfil6.3.2 CERTIFICACIÓN EQUIPO DE TRABAJO/Consultor Tecnico SOC/Certificaciones: Curso o Certificación dada por el fabricante de la herramienta SIEM propuesta.: Curso o certificación dada por el fabricante de la herramienta SIEM propuesta". Consideramos que, dado que la herramienta SIEM ya está implementada, la certificación en cuestión no es aplicable. Proponemos que este requisito sea sustituido por la opción de que el oferente demuestre, a través de contratos ejecutados, experiencia en la administración de herramientas de correlación de eventos de seguridad. Es importante resaltar que un equipo SOC generalmente se compone de especialistas en la correlación de eventos de seguridad, independientemente de las tecnologías o herramientas utilizadas. Limitar el proceso a una certificación específica o a una marca restringe injustamente la pluralidad de oferentes. Por ello, solicitamos que se considere nuestra solicitud de modificación para garantizar un proceso más inclusivo.

4	1.5. Requerimientos Específicos – Almacenamiento de Logs El contratista deberá asegurar el almacenamiento, disponibilidad y recuperación de los LOGs y la información generada en la ejecución del servicio contratado. El tiempo de custodia de la información técnica de LOGs será de seis (6) meses. El tiempo de custodia de los reportes, estadísticas, análisis de Tendencia, métricas e indicadores será por la duración del contrato. Es importante que el contratista defina un plan de respaldo en caso de borrados accidentales o provocados y presentarlo, una vez se firme el acta de inicio.	De acuerdo con lo revisado en el ANEXO 09. Anexo Técnico_SOC.docx, en el numeral 1.3. "Especificaciones Técnicas Generales del SOC", ítem 1, se establece que "El SOC deberá tener la capacidad de integrarse con el SIEM de propiedad de la Superintendencia del Subsidio Familiar, el cual es ArcSight (logger y ArcMC) del fabricante MicroFocus." Esto indica que la infraestructura del SIEM ya forma parte de la entidad. Adicionalmente, en el numeral 1.5. "Requerimientos Específicos – Almacenamiento de Logs", se menciona lo siguiente: El contratista deberá asegurar el almacenamiento, disponibilidad y recuperación de los LOGs y la información generada en la ejecución del servicio contratado. El tiempo de custodia de la información técnica de LOGs será de seis (6) meses. El tiempo de custodia de los reportes, estadísticas, análisis de tendencia, métricas e indicadores será por la duración del contrato. Es importante que el contratista defina un plan de respaldo en caso de borrados accidentales o provocados, y lo presente una vez se firme el acta de inicio. Dado que la infraestructura del SIEM ya pertenece a la entidad, solicitamos confirmar si estos requerimientos implican que los oferentes deben considerar la provisión de un sitio de almacenamiento adicional para los logs generados por el SIEM actual de la entidad. De ser así, solicitamos detalles adicionales sobre las expectativas en cuanto a la infraestructura requerida para cumplir con la retención de seis (6) meses y la custodia de reportes por la duración del contrato. Esto nos permitirá ajustar nuestra propuesta para cumplir con los requerimientos de manera precisa.

5	ANEXO 10 OFERTA ECONÓMICA	Solicitamos a la entidad de la manera más atenta aclarar lo siguiente: En el ANEXO 10 "OFERTA ECONÓMICA", se indican dos servicios adicionales: Servicio de gestión de vulnerabilidades Servicio de ethical hacking Sin embargo, no se encuentran especificadas ni en el pliego de condiciones ni en el ANEXO TÉCNICO NÚMERO 9 las especificaciones técnicas o cantidades a las que se les aplicarán dichos servicios. Agradecemos indicar en qué anexo técnico o en qué parte del pliego se encuentran dichas solicitudes, o agregar el archivo en el que se detallen estas especificaciones, incluyendo la cantidad de equipos, sistemas operativos y tipo de análisis requerido. Esto es fundamental para poder presentar una oferta precisa y ajustada a los requerimientos de la entidad.

RESPUESTA:

Frente a la cita 1, ver respuesta a la observación No. 2 del interesado OPEN GROUP, Ver respuesta a la observación No. 1 y No. 2 del interesado PASSWORD CONSULTING SERVICES SAS

Frente a la cita 2, 3 y 4 Ver respuesta a la observación No. 1 y No. 2 del interesado PASSWORD CONSULTING SERVICES SAS, Ver respuesta a la observación No. 7 del interesado COINSA

Frente a la cita 5: Nos permitimos informar que en el Anexo 09 se anexó la información correspondiente a lo solicitado en la observación referente al servicio de gestión de vulnerabilidades y al servicio de ethical hacking, y nos permitimos informar que los activos de información a los que se aplicarán los servicios son aproximadamente 300.

OBSERVACIONES INTERESADO CONWARE S.A.S

OBSERVACIÓN No.1

Condiciones de la experiencia específica relacionada:

b) Haber entregado licenciamiento con transferencia de propiedad a cliente final de las herramientas de amenazas de la red, y herramienta de suplantación de marca, dichas entregas deben estar certificadas por los respectivos fabricantes.

Las certificaciones de experiencia deben contener los servicios de configuración y parametrización o implementación de dichas herramientas

Condiciones de la experiencia específica relacionada:

d) Haber sido iniciada y terminada en los últimos dos (2) años.

Solicitamos amablemente a la entidad eliminar este requerimiento de certificaciones y experiencia específica, ya que los clientes no certifican este tipo de información y las políticas de seguridad establecen que es confidencial. Este requisito no garantiza la pluralidad de oferentes y está orientado a organizaciones específicas.

RESPUESTA:

Ver respuesta a la observación No. 7 del interesado COINSA

OBSERVACIÓN No.2

Solicitamos respetuosamente a la entidad no requerir la presentación de hojas de vida y soportes académicos con la oferta, ya que la Ley 1150 de 2007, artículo 5, prohíbe exigirlas como condición habilitante en el pliego de condiciones. Sugerimos una carta de compromiso firmada por el representante legal, comprometiéndose a entregar la información completa si resulta adjudicado.

RESPUESTA:

Ver respuesta a la observación No. 2 del interesado OPEN GROUP

OBSERVACIÓN No.3

Para el Gerente de Proyecto, solicitamos permitir la formación con posgrados en Gerencia de Proyectos o áreas afines, junto con certificaciones como ISO 27001, Cobit, ITIL, CISM o PMP.

RESPUESTA:

Ver respuesta a la observación No. 1 del interesado OPEN GROUP

OBSERVACIÓN No.4

Solicitamos extender el posgrado requerido para el Gerente de Proyecto a programas en Seguridad Informática, Seguridad de la Información o áreas relacionadas.

RESPUESTA:

Ver respuesta a la observación No. 1 del interesado OPEN GROUP

OBSERVACIÓN No.5

Para el Consultor Senior, solicitamos aceptar títulos en Ingeniería de Sistemas o afines, junto con un posgrado en Seguridad de la Información.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA

OBSERVACIÓN No.6

Que la experiencia para el Consultor Senior sea acreditable con un proyecto en implementación de SIEM o herramientas complementarias.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA

OBSERVACIÓN No.7

Para el Líder SOC, solicitamos aceptar certificaciones en CHFI, Auditoría ISO o CEH, considerando la relevancia para las funciones del cargo.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA

OBSERVACIÓN No.8

Para el Consultor Técnico SOC, solicitamos incluir certificaciones en ISO 27001 o formación en seguridad específica según los requerimientos.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA

OBSERVACIÓN No.9

Solicitamos que la experiencia del Consultor Técnico SOC incluya un mínimo de un proyecto en ciberseguridad o SOC.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA

OBSERVACIÓN No.10

Para el Analista de SOC, se solicita que la experiencia se acredite con cinco años en seguridad o ciberseguridad.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA

OBSERVACIÓN No.11

El SOC deberá contar con la capacidad de integrarse y gestionar el SIEM propiedad de la Superintendencia del Subsidio Familiar, que corresponde a ArcSight (Logger y ArcMC) del fabricante MicroFocus. Además, el SOC debe utilizar herramientas propias para la recolección, procesamiento, monitoreo y correlación de al menos 4,500 EPS (Eventos por segundo), sin generar costos adicionales para la entidad. Para cumplir con estos requisitos, se deberá adjuntar la documentación vigente que demuestre que el proveedor del servicio SOC está autorizado y cuenta con el entrenamiento necesario para utilizar dichas herramientas.

Solicitamos que el anexo económico sea clarificado, especialmente en la columna de valor total ofertado.

RESPUESTA:

Ver respuesta a la observación No. 1 y No. 2 del interesado PASSWORD CONSULTING SERVICES SAS

Ver respuesta a la observación No. 4 del interesado ITELCA

OBSERVACION No.12

Consultor Senior despliegue

Profesión: Título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines. Posgrado: Posgrado en Seguridad de la información o Seguridad informática o Seguridad de Redes Telemáticas o Seguridad Física y de la informática.

Certificaciones: Certificación dada por el fabricante de la herramienta SIEM propuesta. Auditor Líder ISO 27001:2013 Auditor Lider ISO 27001:2022, CEH - Certified Ethical Hacker

o CISM - Certified Information Security Manager o CISSP - Certified Information Systems Segurity Professional, Lead Cybersegurity Manager ISO/IEC 27032:2012 o Lead Cybersegurity Professional Certificate (LCSPC), Introductorio de Seguridad en Redes LACNIC o Seguridad en BGP con RPKI e IRR LACNIC.

Experiencia mínima: 5 años como profesional ejecutando proyectos y/o labores consultor especialista en seguridad de la información o Ciberseguridad

Experiencia especifica: 4 proyectos en Despliegue de la herramienta propuesta para SIEM y uno de estos contratos que contenga despliegue de mínimo 2 de las siguientes herramientas SOAR, HONEYPOT, PROTECCION DE MARCA, GESTION DE VULNERABILIDADES para el sector gobierno.

Agradecemos confirmar la funcionalidad que cumplirá el SIEM ArcSight.

RESPUESTA:

Ver respuesta a la observación No. 7 del interesado ITELCA

Ver respuesta a la observación No. 1 y No. 2 del interesado PASSWORD CONSULTING SERVICES SAS

OBSERVACIÓN No.13

Líder SOC

Profesión: título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines

Posgrado: Posgrado en seguridad de la información o Seguridad de Redes Telemáticas o Seguridad Física y de la informática o Seguridad informática

Certificaciones: CHFI - Computer Hacking Forensic Investigator, Auditor Interno ISO 27001:2013 o Auditor Líder ISO 27001:2013, Auditor Lider ISO 27001:2022, CEH - Certified Ethical Hacker, ITIL v3 o superior, Introductorio de Seguridad en Redes LACNIC o Seguridad en BGP con RPKI e IRR LACNIC.

Solicitamos confirmar si habrá dos SIEM en operación y si se requerirá conectar con el SIEM de la entidad.

RESPUESTA:

Ver respuesta a la observación No. 7 del interesado ITELCA

Ver respuesta a la observación No. 1 y No. 2 del interesado PASSWORD CONSULTING SERVICES SAS

OBSERVACIÓN No.14

Solicitamos aclarar si los 4,500 EPS son mensuales o para el periodo completo.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado OPEN GROUP

OBSERVACIÓN No.15

Proponemos que se incluya un conjunto de certificaciones para validar la operatividad del SOC: ISO 27001, 27032, 22301 y SOC 2 Tipo II, para asegurar la pluralidad.

RESPUESTA:

La Superintendencia del Subsidio Familiar no acoge la observación realizada, puesto que como lo indica Colombia Compra, las certificaciones de gestión de calidad no se pueden exigir como requisitos habilitantes o puntuables, esto según el artículo 5, parágrafo 2, de la Ley 1150 de 2007 normativa que establece que las «certificaciones de sistemas de gestión de calidad no serán objetos de calificación ni establecerse como documento habilitante para participar en licitaciones o concursos»

Ver respuesta a la observación No. 5 del interesado ITELCA.

OBSERVACIÓN No.16

Analista Nivel 2 de SOC- Sugerimos ajustar los requisitos del personal para reflejar las certificaciones exigidas en otras categorías.

RESPUESTA:

Ver respuesta a la observación No. 7 del interesado ITELCA

OBSERVACIÓN No.17

La cobertura del servicio deberá estar enmarcado en el cumplimiento de las normas ISO 20000-1 e ISO 27001.

Solicitamos reducir la experiencia requerida a dos años para favorecer la pluralidad.

RESPUESTA:

Ver respuesta a la Observación No. 4 interesado COINSA SAS.

OBSERVACIÓN No.18

El lugar de domicilio del contrato será la ciudad de Bogotá D.C., el lugar de ejecución del contrato será en la sede de la Superintendencia del Subsidio Familiar ubicada en la carrera 69 No. 25 B-44 en la ciudad de Bogotá D.C.

Se sugiere ajustar el requerimiento para que el servicio cumpla con ISO 20000 o 27001.

RESPUESTA:

Ver respuesta a la Observación No. 4 interesado COINSA SAS.

De igual manera con base en la observación del interesado, se realiza la modificación en los documentos definitivos del proceso de la siguiente manera:

El lugar de domicilio del contrato será la ciudad de Bogotá D.C., el lugar de ejecución del contrato será en la ciudad de Bogotá D.C. y el DataCenter Ubicado en el municipio de Tocancipa en las Instalaciones de HostDime ubicada en Zona Franca de Tocacancipa.

OBSERVACIÓN No.19

El CONTRATISTA deberá entregar dentro de los siguientes diez (10) días hábiles siguientes a la firma del acta de inicio el procedimiento integral para la gestión de incidentes de seguridad y evaluación de vulnerabilidades, incluyendo técnicas de Ethical Hacking, en el cual se establezca la periodicidad de los informes y reportes que soporten la gestión y operación del SOC y de los servicios contratados, los cuales deberán contener como mínimo la siguiente información.

Solicitamos confirmar si el personal debe trabajar en sitio o es posible de manera remota.

RESPUESTA:

El personal mínimo requerido deberá adelantar sus funciones de acuerdo con su rol y en la ubicación en la cual el proponente tenga su SOC, de igual manera se podrá requerir presencialidad ya sea en las instalaciones de la entidad o en donde se ubique su datacenter en caso de requerirse adelantar actividades en la infraestructura tecnológica física de la entidad

OBSERVACIÓN No.20

Proponemos que se aclaren los detalles de ethical hacking y su frecuencia estimada.

RESPUESTA:

La Superintendencia del Subsidio Familiar, en respuesta a su observación, se permite informar que la información requerida se encuentra en el anexo No 09 en el numeral 1.5.

OBSERVACIONES INTERESADO OLIMPIA

OBSERVACIÓN No.1

De acuerdo con las especificaciones técnicas generales dispuesto en el pliego de condiciones, la entidad solicita: “El contratista deberá contar con personal certificado en las herramientas con la que el SOC presta el servicio de monitoreo, correlación y demás.”

Solicitamos amablemente que, de forma alternativa, se permita acreditar experiencia en el manejo de dichas herramientas, teniendo en cuenta que la experiencia práctica es un indicados sólido de competencia técnica y se fomenta la participación de proveedores con equipos competentes que puedan garantizar la calidad del servicio.

RESPUESTA:

Ver respuesta a la Observación No. 4 interesado COINSA SAS.

OBSERVACIÓN No.2

En el literal 1.1 especificaciones técnicas generales del SOC dispuesto en el pliego de condiciones, la Entidad señala los profesionales mínimos requeridos para la ejecución del contrato. Al respecto, nos permitimos sugerir:

Para el rol GERENTE DE PROYECTO, solicitamos respetuosamente se requiera únicamente una de las certificaciones requeridas, sea Certificación vigente como Auditor Lider ISO 27001:2022 y/o Cobit 5 y/o ITIL v4 y/o CISM Certified Information Security Manager y/o CISSP Certified Information Systems Segurity Professional y/o Scrum Master y/o PMP y/o Prince. Todas las certificaciones son reconocidas a nivel internacional y garantizan un alto nivel de competencia y capacidad en la gestión de proyecto. Al permitir al menos una de las certificaciones, se podrá ampliar el número de candidatos potenciales sin comprometer la calidad y competencia necesaria para el éxito del proyecto.

Para el rol CONSULTOR SENIO DESPLIEGUE solicitamos respetuosamente se requiera al menos dos de las certificaciones requeridas, sea Certificación vigente dada por el fabricante de la herramienta SIEM propuesta y/o Auditor Líder ISO 27001:2013 y/o Auditor Lider ISO 27001:2022 y/o CEH - Certified Ethical Hacker y/o CISM - Certified Information Security Manager y/o CISSP - Certified Information Systems Segurity Professional y/o Lead Cybersegurity Manager ISO/IEC 27032:2012 y/o Lead Cybersegurity Professional Certificate (LCSPC) y/o Introductorio de Seguridad en Redes LACNIC y/o Seguridad en BGP con RPKI y/o IRR LACNIC. Todas las certificaciones son reconocidas a nivel internacional y garantizan un alto nivel de competencia y capacidad en la gestión de proyecto. Al permitir al menos dos de las certificaciones, se podrá ampliar el número de candidatos potenciales sin comprometer la calidad y competencia necesaria para el éxito del proyecto.

Adicionalmente, respecto a la experiencia especifica, solicitamos respetuosamente que se requiera como mínimo la presentación de un proyecto en el que se haya desplegado la herramienta propuesta para SIEM y uno de estos contratos que contenga despliegue de mínimo 1 de las herramientas mencionadas (SOAR, HONEYPOT, PROTECCION DE MARCA, GESTION DE VULNERABILIDADES) tanto en el sector gobierno como privado. Lo anterior, garantiza que los postulantes cuenten con la experiencia necesaria para implementar soluciones efectivas y seguras, asegurando que tienen un conocimiento práctico y profundo de las herramientas en un contexto similar al del cliente; además, incentiva la participación de proveedores capacitados que puedan demostrar su competencia técnica, promoviendo así un proceso de selección más inclusivo y competitivo, sin comprometer la calidad de las soluciones ofrecidas.

Para el rol LIDER SOC solicitamos respetuosamente se requiera al menos una de las certificaciones requeridas, sea certificación CHFI - Computer Hacking Forensic Investigator y/o Auditor Interno ISO 27001:2013 y/o Auditor Líder ISO 27001:2013 y/o Auditor Lider ISO 27001:2022 y/o CEH - Certified Ethical Hacker y/o ITIL v3 o superior y/oIntroductorio de Seguridad en Redes LACNIC y/o Seguridad en BGP con RPKI y/o IRR LACNIC. Todas las certificaciones son reconocidas a nivel internacional y garantizan un alto nivel de competencia y capacidad en la gestión de proyecto. Al permitir al menos una de las certificaciones, se podrá ampliar el número de candidatos potenciales sin comprometer la calidad y competencia necesaria para el éxito del proyecto.

Para el rol CONSULTOR TÉCNICO SOC solicitamos respetuosamente se requiera al menos una de las certificaciones requeridas, sea certificación Auditor Lider ISO 27001:2022 y/o Seguridad en BGP con RPKI y/o IRR LACNIC y/o Curso o Certificación dada por el fabricante de la herramienta SIEM propuesta y/o Auditor Lider ISO 27001:2013 y/o Cybersecurity Manager ISO/IEC 27032:2012 y/o Cyber Security Foundation Professional Certificate (CSFPC). Todas las certificaciones son reconocidas a nivel internacional y garantizan un alto nivel de competencia y capacidad en la gestión de proyecto. Al permitir al menos una de las certificaciones, se podrá ampliar el número de candidatos potenciales sin comprometer la calidad y competencia necesaria para el éxito del proyecto.

Respecto al rol ANALISTA NIVEL 2 DE SOC no es clara la redacción de las certificaciones solicitadas, requerimos amablemente aclarar que certificaciones se necesitan para este perfil, toda vez que su redacción se presta para ambigüedad dentro de la interpretación.

RESPUESTA:

Ver respuesta a la observación No. 7 del interesado ITELCA

OBSERVACIÓN No.4

De conformidad con el literal 1.3 especificaciones técnicas generales del SOC, la entidad señala: “El SOC debe poder utilizar herramientas de su propiedad para colectar, procesar, monitorear y correlacionar como mínimo 4500 EPS (Eventos por segundo) sin costos adicionales para la entidad. Se deberá adjuntar los documentos vigentes necesarios que demuestren que el proveedor del servicio SOC está autorizado y cuenta con el entrenamiento de utilizar dichas herramientas.” (Subrayado por fuera del texto original) Solicitamos amablemente aclarar el soporte esperado por la entidad. En este caso ¿Podría ser una carta firmada por el representante legal del contratista? ¿Estos soportes deberán entregarse durante la ejecución del contrato?

RESPUESTA:

La Superintendencia del Subsidio Familiar, en respuesta a su observación indica que los soportes deben ser dados por el proveedor directamente, y deben ser entregados en la etapa de la presentación de la oferta.

OBSERVACIÓN No.5

Respecto al literal 1.3 especificaciones técnicas generales del SOC, la entidad solicita: “El servicio SOC, debe estar en capacidad de integrarse con otras herramientas relacionadas a este tipo de servicio, además el proponente debe estar en la capacidad de desarrollar las integraciones o los conectores y/o API necesarios para las distintas fuentes de datos, sin generar costos adicionales para la SuperSubsidio” (Subrayado por fuera del texto original).

Solicitamos amablemente aclarar cuáles serán las otras herramientas a las que deberá integrarse el contratista, con la finalidad de realizar una evaluación más precisa de los costos, evitando que el valor del servicio se incremente de manera desproporcionada y genere un posible desequilibrio económico en el contrato.

RESPUESTA:

La Superintendencia del Subsidio Familiar, en respuesta a su observación, aclaramos que, para las herramientas adicionales, la entidad cuenta con un SIEM (ArcSight), el cual tiene

vigencia hasta el 31 de diciembre de 2024, y Tenable IO, el cual tiene vigencia hasta el 06 de diciembre de 2024.

OBSERVACIÓN No.6

Con relación al numeral 3.3 disponibilidad del servicio SOC, se solicita a la entidad permita que la disponibilidad mencionada en los SLA IMPLEMENTACIÓN DEL SERVICIO, se requiera en un porcentaje de disponibilidad desde el 99,6%. Lo anterior, teniendo en cuenta que las solicitudes actuales de disponibilidad del servicio son 99,96% y 99,7% respectivamente, van encaminadas a un esquema “activo” – “activo” encareciendo los costos de la solución y por ende el presupuesto estimado por la entidad no sería suficiente para apalancar dicha solicitud.

RESPUESTA:

La Superintendencia del Subsidio Familiar, en respuesta a su observación, informa que se tendrá en cuenta la variación del componente de disponibilidad.

OBSERVACIÓN No.7

En el numeral 3.4 – descuentos por menores niveles de servicio SOC dispuesto en la ficha técnica, se describen los descuentos desde el 10% hasta un 100% sobre el servicio afectado. Consideramos que una sanción máxima del 100% es excesiva y podría generar eventualmente un desequilibrio contractual, por esto, solicitamos respetuosamente se modifiquen los descuentos y se establezca un límite máximo del 5% para cada uno de los indicadores señalados. Asimismo, solicitamos respetuosamente que el valor del descuento se aplique únicamente al servicio afectado y no al valor total de la factura, garantizando que las sanciones sean justas y proporcionales, reflejando con precisión el impacto del incumplimiento sin penalizar otros servicios que se encuentren funcionando correctamente.

RESPUESTA:

No se acoge la solicitud del interesado. Los descuentos que fueron establecidas durante el periodo de estructuración del proceso obedecen a un ejercicio de análisis de las necesidades de la entidad y resultan proporcionales a la misma, por ende, no es posible acoger la solicitud del interesado. De igual manera es necesario para fines de estructuración de la propuesta económica, tener en cuenta el plazo de ejecución del contrato.

OBSERVACIÓN No.8

Se aclara al interesado que de acuerdo con lo descrito en el acápite 1.7 del pliego de condiciones se describen claramente las condiciones del plazo de ejecución del contrato.

RESPUESTA:

Ver respuesta a la observación No. 1 y No. 2 del interesado PASSWORD CONSULTING SERVICES SAS

OBSERVACIÓN No.9

Respecto con el numeral 1.8 lugar de ejecución dispuesto en el pliego de condiciones, la entidad señala: “El lugar de domicilio del contrato será la ciudad de Bogotá D.C., el lugar de ejecución del contrato será en la sede de la Superintendencia del Subsidio Familiar ubicada en la carrera 69 No. 25 B-44 en la ciudad de Bogotá D.C.” De acuerdo con el objeto del presente proceso, los servicios pueden prestarse de forma virtual en su totalidad, por lo cual solicitamos amablemente que los servicios se ejecuten en modalidad remota, y excepcionalmente, con justificación previa acordada entre las partes, se presten presencialmente.

RESPUESTA:

Ver respuesta a la observación No. 18 y observación No. 19 del interesado COMWARE

OBSERVACIÓN No.10

Con relación al numeral 6 del literal 1.8.1 obligaciones generales dispuesto en el pliego de condiciones: “Reportar al supervisor, de manera inmediata, cualquier novedad o anomalía que pueda afectar la ejecución del contrato.” El término “inmediato” resulta ambiguo y puede generar expectativas poco realistas respecto al tiempo de respuesta, además esta depende del nivel impacto e incidencia. En todo caso, solicitamos amablemente modificar la redacción de obligación de la siguiente manera: “Reportar al supervisor cualquier novedad o anomalía que pueda afectar la ejecución del contrato.”

RESPUESTA:

No se acoge la solicitud del interesado, toda vez que la misión en si de un SOC es poder realizar el monitoreo en tiempo real de las acciones que representen un riesgo a nivel de seguridad informática para la entidad y su funcionamiento así lo debe garantizar.

OBSERVACIÓN No.11

Respecto al numeral 2 del literal 1 obligaciones específicas del contratista dispuesto en el pliego de condiciones, la entidad solicita que “Allegar dentro de los cinco (5) días hábiles siguientes a la firma del acta de inicio las hojas de vida del equipo de trabajo para validación y aprobación del Supervisor del contrato, así como el cronograma de trabajo que se desarrollara durante la ejecución del contrato.” Solicitamos amablemente extender el plazo a diez (10) días hábiles a partir de la suscripción del acta de inicio. Esto permitirá al contratista recopilar y verificar adecuadamente la documentación necesaria, al igual que coordinar internamente el equipo de recursos humanos y gestión de proyectos para la debida ejecución del contrato, asegurando una transición fluida entre la etapa de adjudicación y la implementación del SOC.

RESPUESTA:

No se acoge la solicitud del interesado toda vez que 5 días hábiles posteriores a la suscripción del acta de inicio representa un periodo suficiente para la recolección de información, más aún teniendo en cuenta que los perfiles deben presentarse en conjunto con la propuesta durante la etapa precontractual.

OBSERVACIÓN No.12

Amablemente le solicitamos remitirse al numeral 1.11 del pliego de condiciones

RESPUESTA:

Ver respuesta observación No. 1 interesado ITELCA

OBSERVACIÓNES No.13

Con relación al literal 4.3.1 experiencia del proponente y del equipo de trabajo dispuesto en el pliego de condiciones, con la finalidad de garantizar una mayor participación de proponentes calificados, solicitamos que se amplíe el periodo de evaluación de la experiencia a contratos finalizados en los últimos cinco (5) años, en lugar de los últimos dos (2) años. Esta solicitud está alineada con los lineamientos de la Guía para Determinar y Verificar los Requisitos Habilitantes en los Procesos de Contratación de Colombia Compra Eficiente, que reconoce que la experiencia no pierde relevancia con el paso del tiempo; por el contrario, dicho documento sugiere que los proponentes que continúan desarrollando sus actividades en el sector adquieren mayor capacidad y experticia a lo largo del tiempo.

RESPUESTA:

Ver respuesta a la Observación No. 7 interesado COINSA SAS.

OBSERVACIÓN No.14

Respecto al literal b) de las condiciones de la experiencia específica relacionada, la entidad solicita: “Haber entregado licenciamiento con transferencia de propiedad a cliente final de las herramientas de amenazas de la red, y herramienta de suplantación de marca, dichas entregas deben estar certificadas por los respectivos fabricantes. Las certificaciones de experiencia deben contener los servicios de configuración y parametrización o implementación de dichas herramientas.” Solicitamos amablemente eliminar el presente literal, teniendo en cuenta que el objeto del presente proceso de contratación es el de prestar un servicio de monitoreo y atención de incidentes.

RESPUESTA:

Ver respuesta a la Observación No. 7 interesado COINSA SAS.

OBSERVACIÓN No.15

Con relación al literal d) de las condiciones de la experiencia específica relacionada en el pliego de condiciones, la entidad solicita demostrar experiencia “iniciada y terminada en los últimos dos (2) años” Solicitamos que se acepte la acreditación de experiencia mediante contratos finalizados en los últimos dos (2) años, lo cual permitirá a los proponentes

demostrar su capacidad con proyectos de mayor duración, que pudieron haberse iniciado antes pero que finalizaron recientemente, manteniendo la validez y relevancia de su experiencia. Esto está en línea con los principios de contratación que buscan asegurar la calidad y ejecución efectiva del servicio, sin limitar injustificadamente la participación de proponentes con experiencia sólida en ciberseguridad.

RESPUESTA:

Ver respuesta a la Observación No. 7 interesado COINSA SAS.

OBSERVACIÓN No.16

Respecto a las multas dispuestas en la minuta del contrato, solicitamos amablemente se modifique su redacción, toda vez que se debe considerar que las multas deben ser un mecanismo razonable y no punitivo, cuyo propósito sea incentivar el cumplimiento sin afectar de manera desmedida la estabilidad financiera del contratista. Las sanciones por incumplimiento ya están contempladas en otros apartados, por lo que esta penalidad adicional genera un desequilibrio contractual y duplica el castigo por el mismo incumplimiento.

RESPUESTA:

No se acoge la solicitud del interesado. Las multas que fueron establecidas durante el periodo de estructuración del proceso obedecen a un ejercicio de análisis de las necesidades de la entidad y resultan proporcionales a la misma, por ende, no es posible acoger la solicitud del interesado.

OBSERVACIÓN No.17

Con relación al riesgo No. 5 dispuesto en la matriz (en Word) de riesgos relacionado a “deficiencias en la planificación y ejecución del contrato”. Consideramos que dicho riesgo sea compartido, toda vez que la entidad debe garantizar la disponibilidad y colaboración de su equipo para poder cumplir con la ejecución del contrato.

RESPUESTA:

La Superintendencia del Subsidio familiar, en respuesta a su observación se permite indicar que la matriz de riesgo final es aquella que se encuentra publicada en su versión PDF, se aclara que se suprimirá su versión en WORD.

OBSERVACIÓN No.18

Solicitamos amablemente ajustar el anexo 11 – oferta económica, toda vez que la modalidad de selección será por subasta inversa.

RESPUESTA:

Ver respuesta a la observación No. 4 del interesado ITELCA

OBSERVACIÓN No.19

Solicitamos amablemente confirmar cuál de los documentos corresponde a la matriz de riesgos final, dado que se encuentran dos versiones publicadas, una en formato pdf y otra en Word, con información distinta entre ellas.

RESPUESTA:

La Superintendencia del Subsidio familiar, en respuesta a su observación se permite indicar que la matriz de riesgo final es aquella que se encuentra publicada en su versión PDF, se aclara que se suprimirá su versión en WORD.

OBSERVACIÓN No.20

En el ítem 1.1 – Especificaciones Técnicas Generales del Servicio SOC dispuesto en la ficha técnica 10 proyecto de pliego de condiciones, se describen los perfiles mínimos que se deben tener en la ejecución, se solicita a la entidad nos confirme si la disponibilidad de dichos perfiles es del 100% o se pueden tener de forma parcial, adicional si los perfiles ejecutaran sus labores de forma presencial o virtual.

RESPUESTA:

Ver respuesta a la observación No. 19 del interesado COMWARE

OBSERVACIÓN No.21

Se solicita a la entidad aclarar, si se recibirán las configuraciones actuales del servicio debemos montar la configuración de cero.

RESPUESTA:

Ver respuesta a la observación No. 1 y No. 2 del interesado PASSWORD CONSULTING SERVICES SAS

PRESENTADA POR: BPO HAPPIFY

OBSERVACIÓN No. 3

Solicitamos a la entidad aclarar la forma de pago, en particular el segundo pago, ya que se establece que se realizará tras la recepción satisfactoria del Plan de Gestión de Seguridad del SOC por un período de un año. Esto contrasta con el plazo de ejecución del contrato, que es de tres meses, hasta el 31 de diciembre de 2024, según lo indicado en el numeral 1.7 del plazo de ejecución.

RESPUESTA:

Se aclara al interesado que de acuerdo con lo descrito en el acápite 1.7 Y 11 del pliego de condiciones se describen claramente las condiciones del plazo de ejecución del contrato y su forma de pago

OBSERVACIÓN No. 4

Respetuosamente, solicitamos a la entidad eliminar el requisito de certificaciones y experiencia específica, ya que estas no son certificadas por los clientes y la información relacionada con las herramientas es confidencial debido a políticas de seguridad

RESPUESTA:

Ver respuesta a la observación No. 2 del interesado ITELCA

OBSERVACIÓN No. 5

Para garantizar la pluralidad de oferentes, solicitamos a la entidad que se consideren contratos finalizados y ejecutados en los últimos dos años.

RESPUESTA:

La Superintendencia del Subsidio Familiar, no acepta la observación, puesto que los contratos deben estar en estado finalizados, puesto que de esta manera se garantiza la correcta finalización de este.

OBSERVACIÓN No. 6

Solicitamos a la entidad no exigir la presentación de hojas de vida y soportes académicos y de experiencia del equipo mínimo requerido junto con la oferta, ya que esto limita la participación de oferentes. En su lugar, proponemos permitir la entrega de una carta de compromiso firmada por el representante legal, en la cual se comprometa a presentar la información requerida para cada perfil mencionado en el documento en caso de resultar adjudicado.

RESPUESTA:

Ver respuesta a la observación No. 2 del interesado OPEN GROUP

OBSERVACIÓN No. 7

Para el cargo de Gerente de Proyecto, solicitamos permitir acreditar la formación de la siguiente manera: Posgrado en Gerencia de Proyectos, Gerencia de Proyectos en Ingeniería de Telecomunicaciones o Administración de Empresas con Especialidad en Dirección de Proyectos. Además, debe contar con al menos dos de las siguientes certificaciones: Auditor Líder ISO 27001:2022, Cobit 5, ITIL v4, CISM, CISSP, Scrum Máster, PMP, Prince, CSFPC o CC

RESPUESTA:

La Superintendencia del Subsidio Familiar, en respuesta de su observación acoge parcialmente la solicitud del interesado, en la inclusión de la certificación Project Management Professional (PMP). De esta manera en los documentos definitivos se establecerá lo siguiente:

Rol	Profesión en Colombia (Carreras Afines según SNIES)
Gerente de proyecto	Profesión: Título profesional en ingeniería de sistemas o telecomunicaciones o electrónica o informática o afines. Posgrado: posgrado en Gerencia de Proyectos o Gerencia de Proyectos en Ingeniería de Telecomunicaciones o Administración de Empresas con Especialidad en Dirección de Proyectos. Certificaciones: PMP - Project Management Professional o Prince. Experiencia mínima: 10 años como profesional ejecutando proyectos y/o labores como director o gerente de proyectos en el sector de tecnología Experiencia especifica: 5 años en Ciberseguridad, Seguridad informática, Seguridad de la Informacióny. Certificaciones: Auditor Lider ISO 27001:2022, Cobit 5 o ITIL v4, CISM Certified Information Security Manager o CISSP Certified Information Systems Segurity Professional, Scrum Master, Project Management Professional (PMP)

OBSERVACIÓN No. 8

Solicitamos ampliar el requisito de posgrado para el cargo de Gerente de Proyecto a programas en Seguridad Informática, Seguridad de la Información o áreas afines.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA en referencia al perfil de gerente de proyecto.

OBSERVACIÓN No. 9

Para el Consultor Senior en despliegue, solicitamos permitir acreditar la formación con un título profesional en Ingeniería de Sistemas, Telecomunicaciones, Electrónica, Informática o afines, y un posgrado en Seguridad de la Información, Seguridad Informática, Seguridad de Redes Telemáticas o Seguridad Física y de la Informática. Además, debe contar con al menos dos de las siguientes certificaciones: Certificación del fabricante de la herramienta SIEM propuesta, Auditor Líder ISO 27001:2013 o 2022, CEH, CISM, CISSP, Lead Cybersecurity Manager o Lead Cybersecurity Professional Certificate, entre otros.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA en referencia al perfil de consultor senior.

OBSERVACIÓN No. 10

Solicitamos que la experiencia específica para el Consultor Senior en despliegue se pueda acreditar con al menos un proyecto en la implementación de la herramienta SIEM propuesta, o un contrato que incluya el despliegue de al menos dos de las siguientes herramientas: SOAR, Honeypot, Protección de Marca o Gestión de Vulnerabilidades, para el sector gubernamental o privado.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA en referencia al perfil de consultor senior.

OBSERVACIÓN No. 11

Para el perfil de Líder SOC, solicitamos que se permita acreditar la formación con al menos dos de las siguientes certificaciones: CHFI, Auditor Interno o Líder ISO 27001, CEH, ITIL v3 o superior, o certificaciones de seguridad en redes de LACNIC.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA en referencia al perfil de Líder SOC

OBSERVACIÓN No. 12

Para el Consultor Técnico SOC, solicitamos permitir que la formación sea acreditada con al menos dos de las siguientes certificaciones: Auditor Líder ISO 27001:2022 o 2013, Seguridad en BGP con RPKI e IRR LACNIC, certificación del fabricante de la herramienta SIEM propuesta, Cybersecurity Manager ISO/IEC 27032:2012 o CSFPC.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA en referencia al perfil de Consultor Técnico SOC

OBSERVACIÓN No. 13

Solicitamos que la experiencia específica del Consultor Técnico SOC pueda acreditarse con al menos un proyecto en Ciberseguridad, Seguridad Informática, Seguridad de la Información o SOC.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA en referencia al perfil de Consultor Técnico SOC

OBSERVACIÓN No. 14

Para el Analista Nivel 2 de SOC, solicitamos permitir que la experiencia pueda acreditarse con cinco años en proyectos o funciones de consultoría en Seguridad o Ciberseguridad, o en la implementación y administración de soluciones de seguridad.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA en referencia al perfil de Analista 2 de SOC

OBSERVACIÓN No. 15

Solicitamos a la entidad aclarar el anexo económico, ya que la columna "Valor Total Ofertado Incluido IVA" podría interpretarse como el resultado de multiplicar el "Valor Unitario de Referencia Incluido IVA" por el "Tiempo (meses)", lo cual superaría el presupuesto. Esto podría inducir a error al diligenciar la oferta económica.

RESPUESTA:

Ver respuesta a la observación No. 4 del interesado ITELCA.

OBSERVACIÓN No. 16

Solicitamos amablemente a la entidad confirmar cuál será la funcionalidad específica del SIEM ArcSight en el proyecto.

RESPUESTA:

La funcionalidad del SIEM ArcSight, de la entidad no tiene una funcionalidad específica más allá de otro SIEM, sin embargo, nos permitimos aclarar que su vigencia es hasta el 31 de diciembre de 2024

OBSERVACIÓN No. 17

Solicitamos que la entidad confirme si nuestro entendimiento es correcto al asumir que estarán operativos dos SIEM. Agradecemos también confirmar si se requerirá la conexión de nuestro SIEM con el de la entidad o si únicamente se trabajará con el SIEM ya existente.

RESPUESTA:

Ver respuesta a la observación No. 1 del interesado PASSWORD CONSULTING SERVICES SAS.

OBSERVACIÓN No. 18

Solicitamos a la entidad aclarar la cantidad de EPS relacionados, especificando si los 4,500 EPS corresponden al total del periodo del contrato o si se refieren a un volumen mensual.

RESPUESTA:

La Superintendencia del Subsidio Familiar, se permite aclarar que con relación a los 4500 EPS, hacen referencia a que en un segundo existan al menos 4500 EPS Eventos.

OBSERVACIÓN No. 19

Agradecemos que la entidad precise la cantidad de fuentes para cada uno de los dispositivos mencionados, tales como servidores, equipos de cómputo, bases de datos, equipos de seguridad y cuentas de correo electrónico.

RESPUESTA:

La Superintendencia del Subsidio Familiar, en respuesta a su observación, se permite aclarar que la entidad cuenta con aproximadamente 300 activos de información.

OBSERVACIÓN No. 20

Solicitamos respetuosamente a la entidad eliminar los siguientes requisitos de certificación: la certificación del fabricante de la herramienta SIEM propuesta, ya que el rol es más estratégico que técnico; y la certificación en Seguridad en BGP con RPKI e IRR de LACNIC, pues se enfoca en un área muy específica de la seguridad de redes, cuya aplicabilidad directa en el día a día de un Líder SOC puede ser limitada, además de afectar la pluralidad de oferentes.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA

OBSERVACIÓN No. 21

Respetuosamente, solicitamos a la entidad suprimir la exigencia de la certificación en Seguridad en BGP con RPKI e IRR de LACNIC, ya que esta se especializa en un ámbito muy específico de la seguridad de redes. Si bien es relevante para la infraestructura de red, su aplicabilidad directa al trabajo diario de un Líder SOC es limitada y no garantiza la pluralidad de oferentes.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA

OBSERVACIÓN No. 21

Agradecemos a la entidad considerar la inclusión de los siguientes requisitos de certificación y experiencia: Posgrado obligatorio a nivel de maestría en temas de tecnología, ya que una formación avanzada refleja un mayor nivel de competencia en áreas técnicas y de gestión, fundamentales para un Líder SOC. Asimismo, se sugiere añadir certificaciones como C)DFE, C)IHE, C)PTE, que demuestran conocimientos en investigación forense digital, manejo de incidentes de seguridad y pruebas de penetración, capacidades esenciales para liderar la respuesta a incidentes y evaluar la seguridad organizacional. Proponemos también ampliar la experiencia requerida a cinco años como Líder SOC, para garantizar un conocimiento sólido en la gestión del área.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA

OBSERVACIÓN No. 23

Solicitamos eliminar los siguientes requisitos de certificación: Seguridad en BGP con RPKI e IRR LACNIC, dada su naturaleza específica en la seguridad de redes, lo cual limita la pluralidad de oferentes; Cybersecurity Manager ISO/IEC 27032:2012 o CSFPC, orientadas a la gestión organizacional de la seguridad de la información, lo que no es estrictamente necesario para un rol técnico SOC; y Auditor Líder ISO 27001:2013 o 2022, más apropiadas para funciones de consultoría o auditoría en lugar de un perfil técnico SOC.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA

OBSERVACIÓN No. 24

Sugerimos añadir al perfil de Consultor Técnico SOC las siguientes certificaciones: CEH (Certified Ethical Hacker), para identificar vulnerabilidades en sistemas; D)DFE (Digital

Forensic Examiner) y CHFI V9 (Computer Hacking Forensic Investigator), orientadas a la investigación forense digital; Certified in Cybersecurity, para conocimientos amplios en seguridad de la información; y SCRUM Fundamentos, para demostrar habilidades en gestión de proyectos y trabajo en equipo.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA

OBSERVACIÓN No. 25

Respetuosamente solicitamos a la entidad reducir la experiencia específica requerida a dos años.

RESPUESTA:

Ver respuesta a la observación No. 3 del interesado ITELCA

OBSERVACIÓN No. 26

Solicitamos ajustar el requerimiento para que la cobertura del servicio cumpla con las normas ISO 20000-1 o ISO 27001.

RESPUESTA:

Ver respuesta a la Observación No. 4 interesado COINSA SAS.

OBSERVACIÓN No. 27

Agradecemos a la entidad aclarar si el personal requerido para la operación del SOC deberá estar en sitio o si es posible trabajar de manera remota.

RESPUESTA:

Ver respuesta a la Observación No. 4 del interesado COMWARE S.A.S

OBSERVACIÓN No. 27

Solicitamos amablemente a la entidad confirmar si se requerirán ejercicios de ethical hacking, y en caso afirmativo, indicar la cantidad de objetivos y la frecuencia estimada para la realización de estos ejercicios.

RESPUESTA:

Ver respuesta a la Observación No. 4 del interesado E&C INGENIEROS

OBSERVACIÓN No. 29

En cuanto a la referencia "El contratista deberá tener un SOC propio", proponemos que se incluya un listado de certificaciones y auditorías específicas que aseguren la calidad y capacidad operativa del SOC, tales como ISO/IEC 27001, ISO/IEC 27032, ISO/IEC 22301 y SOC 2 Tipo II. Estas certificaciones garantizarían de manera objetiva que el SOC cumple con los estándares de seguridad exigidos y posee la capacidad necesaria para operar efectivamente en territorio nacional.

RESPUESTA:

La Superintendencia del Subsidio Familiar no acoge la observación realizada, puesto que como lo indica Colombia Compra, las certificaciones de gestión de calidad no se pueden exigir como requisitos habilitantes o puntuables, esto según el artículo 5, parágrafo 2, de la Ley 1150 de 2007 normativa que establece que las «certificaciones de sistemas de gestión de calidad no serán objetos de calificación ni establecerse como documento habilitante para participar en licitaciones o concursos»

Ver respuesta a la Observación No. 5 del interesado ITELCA.

Cordial saludo,

LUISA FERNANDA PARDO SÁNCHEZ
Jefe Oficina TIC

Proyectó:
Juan Pablo López – Aspectos Jurídicos Oficina TIC
Juan Diego Trujillo – Aspectos Financieros Oficina TIC
David Quintero Rodríguez – Aspectos Técnicos Oficina TIC
Juan José Olivella– Aspectos Técnicos Oficina TIC