CONSOLIDADO DE RESPUESTAS A LAS OBSERVACIONES
PROCESO SSF SASI 003 DE 2024 SOC

Bogotá D.C., 22 de octubre de 2024

Señores:
EMPRESA E&C INGENIEROS
EMPRESA COMWARE S.A.
EMPRESA ITELCA
EMPRESA COINSA S.A.S.
EMPRESA OPEN GROUP
EMPRESA OLIMPIA IT SAS
EMPRESA PASSWORD CONSULTING SERVICES SAS
EMPRESA YALK TIL SAS
EMPRESA INNOVATECH

ASUNTO: Consolidado de respuestas a las observaciones al proyecto de pliego de condiciones del proceso de Selección Abreviada Por Subasta Inversa 003 de 2024 SOC

Por medio de la presente, se procede a consolidar las respuestas a las observaciones allegadas dentro del proceso de Selección Abreviada Por Subasta Inversa No. 003 de 2024, SOC cuyo objeto es: *"PRESTAR SERVICIOS DE MONITOREO Y ATENCIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (ID: OTIC-756)"* de la siguiente manera:

Numero total observa - ciones	No.	Tipo	Observación	Documento respuesta
		EMPRESA: E&C INGENIEROS		
1	1	Observación carácter Tecnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

			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.	
2	2	Observación carácter financiero	Índice de liquidez: Mayor o igual a 1.10 Solicitamos respetuosamente modificar el índice de liquidez de tal manera que el requerimiento sea mayor o igual a 1.7., de esta manera la Entidad garantizará que el proponente adjudicatario cuenta con la suficiente solvencia para ejecutar el futuro contrato, así mismo este indicador se ajusta al presente sector .	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS FINANCIERAS
3	3	Observación carácter técnico	Experiencia del Proponente Condiciones de la experiencia específica relacionada: 1. 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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

			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. 2. 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. Actividades y Obligaciones en la Acreditación de Experiencia: Solicitamos que se incluya las siguientes actividades y/u obligaciones dentro de la acreditacion 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. 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.	
4	4	Observación carácter técnico	OBSERVACIONES DE NIVEL TÉCNICO item cita observacion 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 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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

			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	

		EMPRESA: COMWARE S.A. :		
5	1	Observación carácter jurídico	Solicitaremos a la entidad disminuir el porcentaje (%) asignado a las multas al 0,5%, considerando que los cumplimientos ya están cubiertos por el amparo correspondiente.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS JURIDICAS
6	2	Observación carácter FINANCIERO	Solicitamos amablemente a la entidad modificar el indicador de 'Razón Cobertura de Intereses' a un valor mayor o igual a 1.1, dado que el requisito de 1.25 supera los estándares habituales en la industria y afecta la capacidad de reinversión, fundamental para la competitividad en un mercado dinámico. Además, no refleja la realidad económica actual, caracterizada por altas tasas de interés y desaceleración económica. Reducirlo no compromete la ejecución del proyecto.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS FINANCIERAS
	3	Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Solicitamos extender el posgrado requerido para el Gerente de Proyecto a programas en Seguridad Informática, Seguridad de la Información o áreas relacionadas.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Para el Consultor Senior, solicitamos aceptar títulos en Ingeniería de Sistemas o afines, junto con un posgrado en Seguridad de la Información.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Solicitamos que la experiencia para el Consultor Senior sea acreditable con un proyecto en implementación de SIEM o herramientas complementarias.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

		Observación carácter técnico	Para el Líder SOC, solicitamos aceptar certificaciones en CHFI, Auditoría ISO o CEH, considerando la relevancia para las funciones del cargo.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Para el Consultor Técnico SOC, solicitamos incluir certificaciones en ISO 27001 o formación en seguridad específica según los requerimientos.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Solicitamos que la experiencia del Consultor Técnico SOC incluya un mínimo de un proyecto en ciberseguridad o SOC.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Para el Analista de SOC, se solicita que la experiencia se acredite con cinco años en seguridad o ciberseguridad.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Solicitamos que el anexo económico sea clarificado, especialmente en la columna de valor total ofertado.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Solicitamos que el anexo económico sea clarificado, especialmente en la columna de valor total ofertado.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Agradecemos confirmar la funcionalidad que cumplirá el SIEM ArcSight.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Solicitamos confirmar si habrá dos SIEM en operación y si se requerirá conectar con el SIEM de la entidad.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Solicitamos aclarar si los 4,500 EPS son mensuales o para el periodo completo.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Solicitamos confirmar la cantidad de fuentes para servidores y dispositivos relevantes.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Sugerimos ajustar los requisitos del personal para reflejar las certificaciones exigidas en otras categorías.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Solicitamos reducir la experiencia requerida a dos años para favorecer la pluralidad.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Se sugiere ajustar el requerimiento para que el servicio cumpla con ISO 20000 o 27001.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

		Observación carácter técnico	Solicitamos confirmar si el personal debe trabajar en sitio o es posible de manera remota.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Proponemos que se aclaren los detalles de ethical hacking y su frecuencia estimada.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

		EMPRESA: ITELCA		
15	1	Observación carácter jurídico	Capítulo VIII - Minuta del Contrato (página 113): Solicitamos que la entidad considere reducir el porcentaje asignado a las multas al 0,5%, ya que los cumplimientos también están cubiertos por el amparo de cumplimiento.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS JURIDICAS
16	2	Observación carácter FINANCIERO	Indicadores Financieros - Razón de Cobertura de Intereses (página 89): Solicitamos modificar el indicador a un valor igual o mayor a 1.1, debido a que el índice de 1.25 exigido supera los estándares del sector de TI y limita la capacidad de reinversión en un contexto económico con altas tasas de interés y desaceleración. Reducirlo a 1.1 facilitaría una mejor gestión de recursos y no comprometería la ejecución del proyecto	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS FINANCIERAS
17	3	Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
18	4	Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

19	5	Observación carácter técnico	• 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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
20	6	Observación carácter técnico	• 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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

		EMPRESA: COINSA S.A.S.	

22	1	Observación carácter técnico	**Observacion 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 Informaciónу. 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. **Justificación:** Solicitamos amablemente a la entidad retirar de los requerimientos solicitados la siguientes certificaciones: **CISM (Certified Information Security Management) , CISSP Certified Infprmation Systems Security .** Estas certificaciones avalan las competencias de profesional en seguridad de la información donde su labor va ser más relevante y de valor, en la implementación de los procesos que tienen que ver con las buenas prácticas en la identificación y clasificación de los activos informáticos la identificación de riesgos y categorización de los mismos. El perfil especifico solicitado es de un gerente de proyectos el cual dentro de sus competencias permitirá que el proyecto se ejecute de principio a fin dentro del cronograma y el alcance especificado en los anexos técnicos entre el contratista y la entidad, además de coordinar las actividades en su ejecución y que se implementen las buenas prácticas bajos los marcos de referencia como PMP, ITIL V4 entre otros. En cuanto a la experiencia solicitada permitir que sean cinco (5) años ya sea en proyectos de TI o en proyectos de seguridad dado que de la manera como la están solicitando el profesional para da cumplimiento debería tener 15 años de experiencia, diez (10) años de TI y cinco (5) en seguridad.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

Observación 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

1.1 ESPECIFICACIONES TÉCNICAS GENERALES DEL SERVICIO DE SOC

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.

Observación 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

1.1 ESPECIFICACIONES TÉCNICAS GENERALES DEL SERVICIO DE SOC

Solicitamos amablemente a la entidad que para el profesional solicitado, Líder de SOC se modifiqu dicho requerimiento de la siguiente manera:

Mínimo Un (1) Ingeniero de Sistemas, Informática, Telemática, Electrónico o carreras afines, co especialización en seguridad informática y/o en seguridad de la información y/o ciberseguridad y Redes Telemáticas y/o Seguridad Física y de la Informática y/o maestría en seguridad informática y maestría en seguridad de la información y/o ciberseguridad. **Con experiencia mínima de tres (3) año 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 solicita **CHFI - Computer Hacking Forensic Investigator , CEH - Certified Ethical Hacke Introductorio de Seguridad en Redes LACNIC o Seguridad en BGP con RPKI e IR LACNIC ,** estas certificaciónes estan mas relacionas con el perfil de un arquitecto especialista de seguridad y ciberseguridad de nivel 3. Requerir estas certificaciones para líder de SOC que dentro de sus actividades más relevantes están encaminadas a la operació las buenas prácticas en los procesos implementados para el servicio, la auditoria de lo informes, la verificación de las actividades y el seguimiento entre otras, podemos evidenci que sesga el proceso y no esta dando la oportunidad a que los demás oferentes pueda cumplir con estos requerimientos solicitados para el perfil.

Mencionado lo anterior solicitamos amabelemente a la entidad retirar del requerimiento esta certifiaciones para el perfil solicitado Líder de SOC: **CHFI - Computer Hacking Forensic Investigato , CEH - Certified Ethical Hacker, Introductorio de Seguridad en Redes LACNIC o Seguridad e BGP con RPKI e IRR LACNIC** Y QUE la experiencia especifica mínima requerida para el profesion sea de tres (3) años en proyectos de TI y Mínimo dos (2) años como coordinador líder de SOC.

Observación 4:

Se solicita amablemente a la entidad que de acuerdo con el requerimiento **Especificacione Técnicas Generales Herramienta SIEM, incluir el siguiente requerimiento:**

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

Justificación:

Es importante iniciar a definir que la CMDB (Configuration Management DataBase) es un concep introducido por ITIL - ISO 20000 para la gestión de servicios de TI. Esta base de datos permi administrar y gestionar todos los activos necesarios para la prestación del servicio en el SOC de entidad, así como la correlación e interrelación de los elementos o activos; por ejemplo, cuando se ca un servidor de aplicaciones podemos controlar a través de estas relaciones, e identificar a qu elementos están comprometiendo e incluso llegar a ver qué servicios se están afectando.
La integración con la CMDB es necesaria para identificar los servicios a monitorear, realizar análisis d riesgos y dotar de controles a los elementos más sensibles a posibles amenazas. Por lo tanto, se solici

a la entidad incluir este requerimiento dentro de las especificaciones técnicas de la herramienta d SIEM.

Observación 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

1.1 ESPECIFICACIONES TÉCNICAS GENERALES DEL SERVICIO DE 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.

Observación 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 Even 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 l membresía del fabricante de la herramienta SIEM propuesta. Ademas que en la carta s evidencie que cuenta con una especialización de SOC para la operación del servicio.

Justificación:

Los niveles de membresía de los oferentes de las herramientas tipo SIEM requieren d conocimientos y experiencia para la implementacion, administración, soporte, monitoreo correlación y alertamiento para la prestación del servicio solicitado en el objeto del presente proceso. Dicho esto, los oferentes que cuentan con estas competencias certificadas por los fabricantes son evaluados tanto en certificaciones de su equipo de especialistas de ingeniería y en la experiencia en la ejecución de este tipo de proyectos.

Observación 7:

Según el numeral 4.3.1 EXPERIENCIA DEL PROPONENTE, se requiere que los propon 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 l experiencia debe ser exigida en términos proporcionales y razonables, teniendo en cuenta l naturaleza y complejidad del objeto contractual. Esta modificación permitirá ampliar la concurrencia de oferentes sin comprometer la calida de los servicios a contratar, en conformidad con los principios de selección objetiva y d transparencia consagrados en la Ley 80 de 1993 y la Ley 1150 de 2007.	

		EMPRESA: OPEN GROUP		
23	1	Observación carácter financiero	OBSERVACIONES FINANCIERAS: Solicitamos amablemente modificar la fórmula para evaluar los indicadores financieros en los casos de formula oferente plural de la siguiente manera: • Form ula solicitada en el proyecto de pliego de condiciones : 4. Ponderación de los componentes de los indicadores n esta opción cada uno de los integrantes del oferente aporta al valor total del omponente del indicador proporcionalmente con su participación en la figura, sto es, unión temporal o consorcio. a siguiente es la fórmula aplicable: $$Indicador = \frac{Numerador_1 * Participación_1 + \cdots + Numerador_n * Participación_n}{Denominador_1 * Participación_1 + \cdots + Denominador_n * Participación_n} = \frac{\sum_{i=1}^{n} Numerador_i * Participación_i}{\sum_{i=1}^{n} Denominador_i * Participación_i}$$ onde i representa a una empresa que conforma el oferente plural y n es el úmero total de empresas integrantes del oferente plural (unión temporal o onsorcio). • Solicitud del futuro proponente. solicita respetuosamente a la entidad aceptar la sumatoria ponderada de los indicadores según centaje de participación, evaluando la unión temporal en su totalidad, entendiendo que la uraleza de las anteriores es complementarse entre sus integrantes según la siguiente formula. 1. Sumatoria Ponderada $$\text{ndicador en valor monetario} = Indicador_1 * Participación_1 + \cdots + Indicador_i * Participación_i + \cdots + Indicador_n * Participación_n$$ $$= \sum_{i=1}^{n} Indicador_i * Participación_i$$ nde i representa a una empresa que conforma el oferente plural y n es el mero total de empresas integrantes del oferente plural (unión temporal o nsorcio). a opción incentiva a que el integrante del proponente plural con los mejores licadores tenga una mayor participación en dicho proponente plural.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS FINANCIERAS

			"Los consorcios y las uniones temporales son mecanismos de asociación fundamentados en la colaboración empresarial, mediante los cuales sus integrantes se unen y organizan en forma conjunta para lograr con mayor eficacia la obtención del derecho a ser adjudicatarios de un contrato estatal, compartiendo recursos de toda índole para su ejecución, así como las utilidades y los riesgos." Concepto Colombia Compra Eficiente máximo rector en contratación estatal, MANUAL PARA DETERMINAR Y VERIFICAR LOS REQUISITOS HABILITANTES EN LOS PROCESOS DE CONTRATACIÓN.	
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Se le solicita a la entidad aclarar el tamaño de los LOGS según su capacidad de tiempo de almacenamiento del Firewall y del WAF	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

		EMPRESA: OLIMPIA IT SAS		
		Observación carácter JURIDICO	De acuerdo con el literal i) del numeral 1.17 procedimiento dispuesto en el pliego de condiciones, la entidad solicita: "En consecuencia, la subasta culminará una vez se cumpla el tiempo establecido para la realización de esta, y no se realicen más lances válidos." Solicitamos amablemente aclarar si en los últimos segundos de la subasta, se presenta un lance valido ¿El tiempo de la subasta se amplía? De ser así ¿Cuántos minutos adicionales se extiende?	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS JURIDICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

			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 ivel 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.	

		Observación carácter técnico	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?	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	¿Qué tipos de fuentes de datos utiliza actualmente la Superintendencia del Subsidio Familiar? ¿Son estructuradas, no estructuradas o semiestructuradas?	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	¿Cuáles son las expectativas sobre la frecuencia de recolección de metadatos de estas fuentes (en tiempo real, lotes, etc.)?	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
43	19	Observación carácter técnico	¿Existe un listado inicial de sinónimos y acrónimos que ya está en uso, o se espera que construyamos ese listado desde cero?	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
44	20	Observación carácter técnico	¿Con qué frecuencia se actualizan los sinónimos y acrónimos, y qué procesos de gobernanza se deben implementar para asegurar su consistencia?	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		EMPRESA: INGENIUM COLOMBIA SAS		
130	1	Observación carácter técnico	Solicitamos a la entidad incluir como experiencia habilitante la que incluya proyectos de Gobierno de datos e integridad de datos, ya que estos proyectos demuestran la experiencia de los profesionales en establecer políticas, procesos y tecnologías que aseguren la correcta administración de los datos. La experiencia en integridad de datos es vital para proyectos donde se necesita garantizar que los datos almacenados, transmitidos y procesados cumplan con estándares de calidad, sean confiables y estén protegidos de alteraciones no autorizadas. Los proyectos previos en los que los candidatos hayan trabajado con la integridad de datos son una base sólida para garantizar que pueden cumplir con las exigencias de Microsoft Purview, que tiene funcionalidades específicas para mantener la calidad e integridad de los datos	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		EMPRESA: MANAGEMENT AND QUALITY SAS		
131	1	Observación carácter técnico	En cuanto al numeral PERSONAL MÍNIMO REQUERIDO para todos los perfiles Entendemos que para la ejecución del contrato este puede darse de manera remota, asegurando el usode herramientas y mecanismos que garanticen la calidad del servicio y productos requeridos; por favor ratificar si nuestro entendimiento es correcto.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
132	2	Observación carácter técnico	En cuanto al numeral PERSONAL MÍNIMO REQUERIDO para todos los perfiles Entendemos que, para calcular la experiencia requerida de cada uno de los perfiles, se tomará la desde la fecha de inicio y fecha de terminación de la certificación laboral, más no por la fecha de proyectos si llegase a tener la certificación. Por favor ratificar si nuestro entendimiento es correcto	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

133	3	Observación carácter técnico	En cuanto al numeral PERSONAL MÍNIMO REQUERIDO para todos los perfiles Entendemos que, para calcular los años de experiencia de los profesionales, se tomará en cuenta la fecha de inicio y la fecha de terminación de la certificación laboral, y no las fechas específicas de los proyectos. Esto es debido a que la mayoría de los profesionales han tenido una trayectoria laboral continua con los futuros proponentes y han ejecutado una gran variedad de proyectos dentro de la misma compañía. Dividir los tiempos en los que han laborado los profesionales por proyecto resulta complicado, ya que estos proyectos a menudo se traslapan. Esto implicaría criterios inalcanzables o no viables para determinar la experiencia. Por favor, ratifiquen si nuestro entendimiento es correcto	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
134	4	Observación carácter técnico	En cuanto al numeral PERSONAL MÍNIMO REQUERIDO para todos los perfiles Entendemos que cuando la entidad “afines” hace referencia a que la formación académica se encuentren en el mismo Núcleo Básico del Conocimiento – NBC de los requeridos; por favor ratificar si nuestro entendimiento es correcto	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
135	5	Observación carácter técnico	Entendemos que si el proponente certifica al profesional se debe adjuntar la certificación laboral y el contrato para evidenciar el vínculo laboral; pero teniendo presente que el CONTRATO entre el profesional y el proponente se rige por el derecho privado no está obligado a tener un nombramiento o cargo específico; por lo tanto, solicitamos de manera atenta y respetuosa a la entidad permitir a los proponentes que se evidencien los requerimientos de roles o funciones u obligaciones dentro de la certificación laboral. Con el fin de demostrar que el profesional cuenta con la experiencia requerida por la entidad	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
136	6	Observación carácter técnico	Por favor proveer la siguiente información para cada uno de los sistemas de SIMON y SIGER: a. Motor de base de datos y versión b. Número de tablas del modelo, que potencialmente se deben utilizar c. Número de registros estimados que se deben trabajar d. ¿Las bases de datos se encuentran On-Premise o Cloud?	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
137	7	Observación carácter técnico	7. Entendemos que la entidad al inicio del proyecto tendrá habilitados los servicios de Azure Purview, Databricks y otros servicios requeridos para la ejecución del proyecto, y que los entregará a la firma consultora para la ejecución de las actividades del contrato. Por favor confirmar.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
138	8	Observación carácter técnico	8.Para los entregables descritos en la sección “4. Entregables y/o productos”, particularmente para “Evaluación de la Situación Actual: Realizar un análisis detallado de la situación actual de los datos en la Superintendencia, identificando problemas, oportunidades y desafíos a abordar” Entendemos que el alcance de esta actividad está acotado a las bases de datos que soportan los sistemas de información SIMON y SIGER. Por favor confirmar	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

139	9	Observación carácter técnico	9. Para la “Fase 2. Diseño y Configuración” piden “Migración de Datos: Migrar los datos existentes hacia la nueva solución de gobierno de datos, asegurando la integridad y consistencia de estos.” Entendemos que cuando se refieren a “migrar los datos” hacen referencia a extraer la información necesaria para la Gestión de metadatos, la Gestión de glosario empresarial, la Gestión de catálogos de datos, y la Gestión de linaje de datos, y no corresponde a migrar información de estos sistemas de información hacia los servicio de Azure. Por favor confirmar.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
140	10	Observación carácter técnico	Respecto del entregable “Glosario de términos completo que define los conceptos clave utilizados en la entidad” entendemos que corresponde al Glosario de datos asociado a los términos de negocio más relevantes de los sistemas de información SIMON y SIGER. Por favor confirmar.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
141	11	Observación carácter técnico	11. Entendemos que los entregables esperados para la Gestión de Catálogo de Datos se encuentra acotada a los sistemas de información SIMON y SIGER. Por favor confirmar.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
142	12	Observación carácter técnico	12. En los entregables de “Gestión de Catálogo de Datos” piden “Perfiles de datos que proporcionen información detallada sobre la estructura, calidad y contenido de cada conjunto de datos”. e. Cuando indican “perfiles de datos” entendemos que se refieren a informes estadísticos del estado de los datos en los sistemas de información SIMON y SIGER. Por favor confirmar.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
143	13	Observación carácter técnico	13. Respecto del tiempo de ejecución, en el documento de Estudio de Mercado VF mencionan que el presupuesto del proyecto es por cuatro (4) meses, como se ve en la siguiente imagen: y en el documento de “Estudio Previo” mencionan que son dos (2) meses, como se ve en la siguiente imagen: ¿Por favor pueden confirmar cuál es el plazo de ejecución del proyecto?	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		EMPRESA: ITPERFORMA SAS		

144	1	Observación carácter técnico	Solicitamos respetuosamente a la entidad para el numeral “EXPERIENCIA DEL PROPONENTE NACIONAL”, se ajuste 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, los proponentes deberán acreditar experiencia mediante la presentación de máximo dos (2) certificaciones y/o copias de minutas y/o actas de liquidación de contratos ejecutados en los **últimos cuatro (4) años** y hasta la fecha de la presentación de la oferta, registrados en el Registro Único de Proponentes RUP en las, las cuales deberán contar con las siguientes clasificaciones, dicho lo anterior deberá diligenciarse en su totalidad el ANEXO 8 – ACREDITACIÓN EXPERIENCIA MÍNIMA HABILITANTE DEL PROPONENTE. • 80101500 Servicios de consultoría de negocios y administración corporativa • 81112000 Servicios de datos • 80101600 Gerencia de proyectos El objeto y/o actividades principales de los contratos relacionados para acreditar la experiencia del proponente deben consistir en características iguales o similares al objeto del presente proceso: **• Analizar, diseñar, definir y/o estructurar el Modelo de Gobierno de Datos usando metodologías como el DAMA -DMBOK (Data Management Body of Knowledge).** **• Adquisición y/o implementación de plataformas de soporte para el modelo de gobierno de datos.** CARACTERÍSTICAS GENERALES DE LOS CONTRATOS PRESENTADOS PARA ACREDITAR LA EXPERIENCIA EXIGIDA. a. Haber sido la experiencia ejecutada para entidades públicas, mixtas, organismos multilaterales, o privados. b. Haber sido iniciada y terminada en los últimos **cuatro (4) años.** c. La sumatoria de la cuantía de las certificaciones deberá ser mayor o igual al 100% del presupuesto oficial asignado para el presente proceso. d. 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: ✓ Entidad Contratante ✓ Contratista ✓ Objeto del contrato ✓ Número de contrato (si registra) ✓ Valor del Contrato ✓ Fecha de inicio (día, mes y año) ✓ Fecha de terminación del contrato (día, mes y año) - Nombre, firma y cargo de la persona que expide la certificación (representante legal o persona autorizada de la empresa que expide la certificación) ✓ Si en los documentos válidos aportados para la acreditación de experiencia solo se evidencia fecha (mes, año) de terminación del Contrato: se tendrá en cuenta como fecha de terminación de la ejecución	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
145	2	Observación carácter técnico	En primer lugar, respetuosamente solicitamos a la entidad eliminar el puntaje adicional asignado en el proceso para el factor “Emprendimientos y empresas de mujeres”	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

			En segundo lugar, solicitamos a la entidad en el factor 2 ASPECTOS TÉCNICOS, EXPERIENCIA ADICIONAL DEL PROPONENTE se ajuste de la siguiente forma: El proponente que aporte una (1) certificación adicional que involucre la ejecución de las siguientes actividades: Estructuración de modelo de datos, implementar un modelo operativo para el levantamiento de requerimientos, definir y coordinar los roles y responsabilidades del servicio, entrega de un esquema de visualización y auto servicio de datos, arquitectura de datos y apalancamiento de tecnologías que soporte la estrategia de datos. Haber sido ejecutada para entidades públicas, mixtas, organismos multilaterales, o privados en los últimos 3 años por el valor total del proceso o superior. Dicha solicitud, busca garantizar que la evaluación de la experiencia adicional refleje lacomplejidad y especialización requeridas en la ejecución de proyectos de datos en el contexto actual. Las actividades mencionadas, como la estructuración de un modelo de datos, la implementación de un modelo operativo para el levantamiento de requerimientos, y la definición de roles y responsabilidades del servicio, son clave para garantizar una gestión integral de la información. Estas actividades no solo son relevantes para asegurar una correcta implementación técnica, sino también para garantizar la continuidad y eficiencia en la toma de decisiones basada en datos. Además, incluir entidades públicas, mixtas, organismos multilaterales o privadas en los últimos tres años como referencia asegura que los proponentes cuenten con experiencia actualizada en proyectos de alta relevancia y puedan ofrecer soluciones robustas y alineadas a las necesidades tanto del sector público como privado. Este ajuste proporcionará a la entidad un criterio más preciso para evaluar propuestas con un enfoque especializado en gestión y estrategia de datos, apalancado en tecnologías innovadoras.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
			En tercer lugar, solicitamos a la entidad en el factor 2 ASPECTOS TÉCNICOS, FORMACIÓN ACADÉMICA ADICIONAL DE UN INTEGRANTE DEL PERSONAL BASE, se ajuste de la siguiente forma: El proponente que oferte un Arquitecto de Datos que sea profesional como (Carreras Afines según SNIES), Ingeniero de Sistemas, Ingeniero de Software, Ingeniero de Computación, Ingeniero Electrónico, con (1) un posgrado en: ✓ Arquitectura de software, ✓ Gestión de proyectos, Ingeniería de software ✓ Sistemas informáticos ✓ Analítica de datos ✓ Ciencia de datos ✓ Ciencias de la computación, Gestión de información) ✓ Gerencia de proyectos en inteligencia de negocios. Adicionalmente que cuente con certificaciones en Microsoft Certified Professional, Microsoft Azure Developer Associate y que cuente con una experiencia de más de 2 años de implementación en arquitectura de soluciones en herramientas Microsoft.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

146	3	Observación carácter financiero	Solicitamos el ajuste de los indicadores financieros de conformidad con las normativas que rigen los procesos de contratación pública en Colombia, con el fin de garantizar que la evaluación de los proponentes sea equitativa y alineada con los principios de eficiencia, eficacia y transparencia estipulados en la Ley 80 de 1993, Estatuto General de Contratación de la Administración Pública, y en la Ley 1150 de 2007, que modificó algunos aspectos del Estatuto de Contratación. 1. Índice de liquidez: Este indicador se ajusta para garantizar que el proponente cuente con la capacidad de cubrir sus pasivos corrientes con activos corrientes, asegurando liquidez suficiente para responder ante eventuales obligaciones contractuales. Un índice igual o mayor a 1.5 asegura una adecuada solvencia y capacidad de gestión operativa. 2. Índice de endeudamiento: La solicitud de un índice de endeudamiento menor o igual al 55% refleja la búsqueda de proponentes que no estén excesivamente apalancados y que, por lo tanto, presenten menores riesgos financieros, en línea con los principios de transparencia y solvencia en la contratación pública. 3. Rentabilidad del Patrimonio y del Activo: Estos indicadores de capacidad organizacional se ajustan para garantizar que las empresas no solo sean solventes, sino también rentables, y que cuenten con una estructura patrimonial y operativa que permita afrontar los compromisos contractuales de manera eficiente. Un patrimonio con rentabilidad mayor o igual al 15% y una rentabilidad del activo igual o superior al 6% aseguran la capacidad de generar valor a partir de sus operaciones, contribuyendo a la sostenibilidad y cumplimiento del contrato.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS FINANCIERAS
		EMPRESA: BICODE SAS		
147	1	Observación carácter técnico	Le solicitamos a la entidad aclarar si la ejecución del presente contrato, se podrá hacer de manera virtual	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
148	2	Observación carácter técnico	En caso de que la experiencia requerida se encuentre englobada en un contrato general con un objeto más amplio, se deberá allegar la certificación con la discriminación del objeto específico de la experiencia acreditada y los servicios objeto de la presente contratación. Se aceptará que se allegue de manera adicional, la certificación de este contrato, siempre y cuando en ella se discriminen los servicios por parte de la entidad o persona que contrató los contrató y el monto que corresponde al servicio objeto del presente proceso.” Solicitamos respetuosamente que se revise el requerimiento relacionado con la discriminación específica de servicios en las certificaciones de experiencia. Es importante señalar que en la mayoría de los casos, las entidades públicas no emiten certificaciones discriminadas de servicios dentro de contratos de naturaleza general o multiobjeto, ya que su práctica habitual es certificar únicamente el cumplimiento del objeto global del contrato. En ese sentido, solicitamos que se acepte la experiencia en contratos con múltiples objetos, sin exigir la discriminación detallada de cada servicio. Esta flexibilización permitirá una participación más amplia y justa, considerando la realidad de cómo las entidades públicas manejan este tipo de certificaciones.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
			Solicitamos a la entidad aclarar si las certificaciones deben cumplir en su totalidad o con alguno de los códigos UNSPSC. En caso de que se deban cumplir en su totalidad, la solicitamos a la entidad modificar la experiencia general, a que los contratos deben encontrarse clasificados en ALGUNOS de los siguientes códigos:	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

		Observación carácter técnico	En “EXPERIENCIA ADICIONAL DEL PROPONENTE: “El proponente que aporte una (1) certificación adicional que involucre la ejecución de al menos una de las siguientes actividades: Estructuración de modelo de datos, implementar un modelo operativo para el levantamiento de requerimientos, definir y coordinar los roles y responsabilidades del servicio, entrega de un esquema de visualización y auto servicio de datos, arquitectura de datos y apalancamiento de :tecnologías que soporte la estrategia de datos. Haber sido ejecutada para entidades públicas, mixtas, organismos multilaterales, o privados en los últimos 3 años por el valor total del proceso o superior” Le solicitamos a la entidad aclararnos si proyectos con las siguientes actividades cumpliría con lo requerido para la obtención de puntos: 1. Gobierno de datos 2. Analítica de datos, generación de modelos analíticos 3. Desarrollo de software	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Solicitamos a la entidad de manera respetuosa, tener en cuenta la experiencia de los perfiles requeridos a partir de finalización y aprobación del pensum académico y no de la obtención de la tarjeta profesional, lo anterior se fundamenta en el decreto de Ley 19 de 2012 (Ley Anti Trámites), artículo 229 que establece: “Para el ejercicio de las diferentes profesiones acreditadas por el Ministerio de Educación Nacional, la experiencia profesional se computará a partir de la terminación y aprobación del pensum académico de educación superior. Se exceptúan de esta condición las profesiones relacionadas con el sistema de seguridad social en salud las cuales la experiencia profesional se computará a partir de la inscripción o registro profesional”. Así mismo la Sala de Consulta y Servicio Civil del Consejo de Estado – M.P: Gustavo Aponte Santos, del 17 de Julio de 2008, establece también que la experiencia debe contarse a partir de la terminación del pensum académico, pues no puede darse aplicación a la Ley 842 pues por regla general las normas no tienen efecto retroactivo sino rigen a futuro, por lo anterior la Ley 842 no puede afectar situaciones jurídicas consolidadas antes de la fecha de su promulgación. Por lo tanto, solicitamos de manera muy respetuosa sea tenida en cuenta dicha observación	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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 cuales 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. De esta manera, aseguraremos una planificación adecuada, tanto en la gestión de los recursos como en la sostenibilidad financiera del proyecto.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

			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.	
		Observación carácter técnico	De acuerdo con el literal 1.7 plazo de ejecución dispuesto por el pliego de condiciones, la entidad señala: “El plazo de ejecución del contrato será hasta el 31 de diciembre de 2024, contado a partir del cumplimiento de los requisitos de perfeccionamiento (suscripción), ejecución (registro presupuestal y aprobación de la garantía única) del contrato y suscripción de Acta de Inicio”. Solicitamos amablemente aclarar si este corresponde únicamente a la fase de implementación de la solución; o en su defecto, aclarar que tipo de actividades se deberán ejecutar en este intervalo.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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.”	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Respecto al segundo pago establecido en el literal 1.11 forma de pago dispuesto en el pliego de condiciones, solicitamos amablemente aclarar qué debe incluir el "conjunto de informes" requerido para el pago	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

			tiempo.	
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Solicitamos amablemente ajustar el anexo 11 – oferta económica, toda vez que la modalidad de selección será por subasta inversa.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter JURIDICO	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS JURIDICAS
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Se solicita a la entidad aclarar, si se recibirán las configuraciones actuales del servicio o debemos montar la configuración de cero.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

		EMPRESA: PASSWORD CONSULTING SERVICES SAS		
		Observación carácter técnico	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 es ta 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?	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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?	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	En el caso que se deba contemplar un SIEM adicional, cual es el propósito de tener 2 SIEM ?	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	¿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?	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

		EMPRESA: YALK TIL SAS		
		Observación carácter técnico	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?	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

			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)?	
		Observación carácter técnico	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?	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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?	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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? .	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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?	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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?	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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,	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

			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?	
192	12	Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS 2
		Observación carácter técnico	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?	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

			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.	
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

			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	
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		EMPRESA: INNOVATECH		
		Observación carácter juridico	Solicitamos a la entidad reducir el porcentaje (%) asignado a las multas al 0,5%, considerando que los cumplimientos ya están cubiertos por el amparo correspondiente.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS juridicas
		Observación carácter financiera	Respetuosamente, solicitamos a la entidad ajustar el indicador de "Razón Cobertura de Intereses" a un valor mayor o igual a 1.1. El requisito de un índice de 1.25 es elevado, superando los estándares habituales en la industria de TI y afectando la capacidad de reinversión, crucial para mantener la innovación y competitividad en un mercado dinámico. Además, el índice de 1.25 no refleja la realidad económica actual del país, marcada por altas tasas de interés y una desaceleración económica, lo que dificulta mantener dicho nivel de cobertura sin comprometer los recursos para el desarrollo de proyectos. Reducir el indicador a 1.1 no pondría en riesgo la ejecución del proyecto, ya que la empresa cuenta con una sólida estructura financiera que garantiza el cumplimiento de sus obligaciones. Esta modificación permitiría gestionar mejor los recursos y enfocar esfuerzos en el crecimiento sostenido.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS FINANCIERAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Para garantizar la pluralidad de oferentes, solicitamos a la entidad que se consideren contratos finalizados y ejecutados en los últimos dos años.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

			cual se comprometa a presentar la información requerida para cada perfil mencionado en el documento en caso de resultar adjudicado.	
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Solicitamos amablemente a la entidad confirmar cuál será la funcionalidad específica del SIEM ArcSight en el proyecto.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Respetuosamente solicitamos a la entidad reducir la experiencia específica requerida a dos años.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	Solicitamos ajustar el requerimiento para que la cobertura del servicio cumpla con las normas ISO 20000-1 o ISO 27001.	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS
		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS

		Observación carácter técnico	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	DOCUMENTO ADJUNTO DENOMINADO: RESPUESTAS TECNICAS