RESPUESTAS A OBSERVACIONES AL PLIEGO DE CONDICIONES DEFINITIVO

Por medio del presente se da respuesta a las observaciones presentadas al pliego de condiciones definitivo, dentro del proceso SAMC-01-FCM-2024, cuyo objeto es: *Prestar por sus propios medios, con plena autonomía técnica, administrativa y operacional los servicios profesionales especialistas en seguridad de la información, ciberseguridad, riesgos digitales, Gobierno digital de la Federación Colombiana de Municipios, en cumplimiento de la función pública asignada.*

El oferente **ZAPHIRECORP**, presentó las siguientes observaciones al informe de verificación así:

Observación 1:

> *"Buenas Tardes*
>
> *respetados señores Federacion de municipios, muy humilde y respetuosamente presentamos las siguientes observaciones al pliego de condiciones.*
>
> *1) solicitamos mantener el perfil inicialmente concebido para el proyecto .. con lo cual se garantize la idoneidad y robustez al proyecto," (SIC)*

Respuesta observación 1:

NO SE ACPETA LA OBSERVACIÓN toda vez que se realizaron modificaciones solicitadas por los interesados, lo que permite entonces una mayor pluralidad de ofertes.

Observación 2:

> *"2) solicitamos tener en cuenta las certificaciones, y experiencia del profesional propuesto para el proceso, de modo que se otorguen puntos ponderables por la capacitacion tecnica y experiencia que tenga el recurso propuesto. esto con el fin de darle mayor robustez y confianza a la emtidad de que el profesional propuesto cuente con toda la experiencia necesaria y mas, para realizar este proceso de vital importancia para la federacion."*

Respuesta observación 2:

NO SE ACPETA LA OBSERVACIÓN toda vez que este proceso NO es un concurso de méritos y no estamos buscando una mayor calificación sino un perfil que cumpla con los requisitos mínimos habilitantes para satisfacer la necesidad de la entidad con este contrato.

El oferente **SECURITY SOLUTIONS & EDUCATION SAS.**, presentó las siguientes observaciones al informe de verificación así:

Observación 1:

"Se observa que en el documento "Pliego de condiciones definitivo - SAMC-01-FCM-2024", en el perfil solicitado para el CISO, requieren como títulos de posgrado, únicamente Especialización o Maestría en Seguridad de la Información; sin embargo, observando el objeto de esta contratación, no simplemente solicitan servicios especializados en seguridad de la información, sino también en ciberseguridad, riesgos y Gobierno digitales. Razón por la cual sugerimos importante incluir:

- *Especializaciones o Maestrías en Seguridad Informática,*
- *Especializaciones o Maestrías en ciberseguridad y/o*
- *Especializaciones o Maestrías en Administración de Riesgos Informáticos."*

Respuesta observación 1:

SE ACEPTA LA OBSERVACIÓN y en aras de propender por la pluralidad de oferentes, la ficha técnica quedará así, tal como constará en la adenda:

CISO (Chief Information Security Officer)	
Formación Académica	**Experiencia Mínima**
<u>Título de Pregrado</u> ❖ Ingeniero de Sistemas, de Telecomunicaciones, Electrónico o Ingenierías afines <u>Título de Postgrado</u> ❖ Especialización o Maestría en Seguridad de la Información, en ciberseguridad, en Administración de Riesgos Informáticos, en seguridad de la información o seguridad informática. <u>Certificación obligatoria (una de las dos).</u> ❖ Auditor Lider ISO 27001 V.2013 o ❖ Auditor Lider ISO 27001 V.2022 (Preferiblemente).	❖ Experiencia específica de al menos ocho (8) años en proyectos relacionados con seguridad de la información, en roles de Líder, Consultor, Asesor u Oficial en Seguridad de la Información.

CISO (Chief Information Security Officer)	
Formación Académica	**Experiencia Mínima**
Debe contar con al menos 4 de las siguientes certificaciones vigentes: ❖ CISM - Certified Information Security Management ❖ CERTIFIED ETHICAL HACKER (CEH). ❖ ECIH EC-COUNCIL CERTIFIED INCIDENT HANDLER ❖ CISSP - Certified Information Systems Security Professional ❖ CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER ❖ MANAGER CYBERSECURITY ISO/IEC 27032 ❖ LEAD INCIDENT MANAGER ISO 27035	

NOTA: *Todas las certificaciones deben estar vigentes al cierre del presente proceso, todas las certificaciones serán validadas atreves de las respectivas plataformas del ente certificador, de tal manera poder validar la vigencia de las mismas.*

Observación 2:

"En cuanto a las certificaciones adicionales exigidas, por la misma razón expuesta en la observación 1, vemos importante incluir otras certificaciones igualmente significativas para el objeto de este proyecto, como:

• Auditor Líder en Gestión de Riesgos: ISO 31000:2018,

• CRISC (Certified in Risk and Information System Control) y/o

• CISA (Certified Information Systems Auditor)"

Respuesta observación 2:

NO SE ACEPTA LA OBSERVACIÓN ya que el profesional solicitado es para suplir las funciones de un Oficial de seguridad de la información (CISO), que apoye y mejore la madurez del MSPI de la Organización, cabe aclarar que las normas ISO normalmente en el capítulo de planificación tratan del manejo y acciones de los riesgos, por esto es obligatorio para el perfil solicitado la certificación en Auditor Lider ISO 27001 V.2013 o V.2022.

Así las cosas, la entidad solicita en los requisitos mínimos habilitantes la certificación anteriormente señalada, toda vez que en los conocimientos que esta refleja se encuentra inmerso el manejo de los riesgos. De esta manera, solicitar más certificaciones restringiría la pluralidad de oferentes y no estarían directamente relacionadas con el objeto a contratar.

Observación 3:

"Por otro lado, teniendo en cuenta que la norma ISO 27001:2022 fue publicada en octubre de 2022, y la ISO/IEC mantiene la vigencia de la norma anterior por los tres años siguientes, es decir, hasta octubre de 2025, dando la oportunidad a que las personas que están certificadas en la norma anterior tengan tiempo para actualizar su certificación. Es así como, amablemente solicitamos sea tenida en cuenta también la certificación de Auditor Líder ISO/IEC 27001:2013 en la sección de Certificación obligtoria, ya que aún nos encontramos en el período de transición indicado por la ISO/IEC."

Respuesta observación 3:

SE ACEPTA LA OBSERVACIÓN y en aras de propender por la pluralidad de oferentes, la ficha técnica quedará así, tal como constará en la adenda:

CISO (Chief Information Security Officer)	
Formación Académica	**Experiencia Mínima**
Título de Pregrado ❖ Ingeniero de Sistemas, de Telecomunicaciones, Electrónico o Ingenierías afines Título de Postgrado ❖ Especialización o Maestría en Seguridad de la Información, en ciberseguridad, en Administración de Riesgos Informáticos, en seguridad de la información o seguridad informática. Certificación obligatoria (una de las dos). ❖ Auditor Lider ISO 27001 V.2013 o ❖ Auditor Lider ISO 27001 V.2022 (Preferiblemente). Debe contar con al menos 4 de las siguientes certificaciones vigentes: ❖ CISM - Certified Information Security Management ❖ CERTIFIED ETHICAL HACKER (CEH). ❖ ECIH EC-COUNCIL CERTIFIED INCIDENT HANDLER ❖ CISSP - Certified Information Systems Security Professional ❖ CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER ❖ MANAGER CYBERSECURITY ISO/IEC 27032 ❖ LEAD INCIDENT MANAGER ISO 27035	❖ Experiencia específica de al menos ocho (8) años en proyectos relacionados con seguridad de la información, en roles de Líder, Consultor, Asesor u Oficial en Seguridad de la Información.

NOTA: *Todas las certificaciones deben estar vigentes al cierre del presente proceso, todas las certificaciones serán validadas atreves de las respectivas plataformas del ente certificador, de tal manera poder validar la vigencia de las mismas*.

Observación 4:

"En el documento de respuesta a observaciones, indican que solamente exigirán dos certificaciones; sin embargo, en el pliego de condiciones definitivo, volvieron a aparecer las cuatro:

CISO (Chief Information Security Officer)	
Formación Académica	**Experiencia Mínima**
❖ Ingeniero de Sistemas, de Telecomunicaciones, Electrónico o Ingenierías afines Título de Postgrado ❖ Especialización o Maestría en Seguridad de la Información. Certificación obligatoria ❖ Auditor Líder ISO 27001 V.2022 Debe contar con al menos 4 de las siguientes certificaciones vigentes: ❖ CISM - Certified Information Security Management ❖ CERTIFIED ETHICAL HACKER (C|EH). ❖ ECIH EC-COUNCIL CERTIFIED INCIDENT HANDLER ❖ CISSP - Certified Information Systems Security Professional ❖ CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER ❖ MANAGER CYBERSECURITY ISO/IEC 27032 ❖ LEAD INCIDENT MANAGER ISO 27035	menos ocho (8) años en proyectos relacionados con seguridad de la información, en roles de Líder, Consultor, Asesor u Oficial en Seguridad de la Información.

En la respuesta a observaciones, páginas 3, 4, 6, 8, 12, 13:"

CISO (Chief Information Security Officer)	
Formación Académica	**Experiencia Mínima**
Título de Pregrado ❖ Ingeniero de Sistemas, de Telecomunicaciones, Electrónico o Ingenierías afines Título de Postgrado ❖ Especialización o Maestría en Seguridad de la Información. Certificación obligatoria ❖ Auditor Líder ISO 27001 V.2022 Debe contar con al menos 2 de las siguientes certificaciones vigentes: ❖ CISM - Certified Information Security Management ❖ CERTIFIED ETHICAL HACKER (C|EH). ❖ ECIH EC-COUNCIL CERTIFIED INCIDENT HANDLER ❖ CISSP - Certified Information Systems Security Professional ❖ CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER ❖ MANAGER CYBERSECURITY ISO/IEC 27032 ❖ LEAD INCIDENT MANAGER ISO 27035	❖ Experiencia específica de al menos siete (7) años en proyectos relacionados con seguridad de la información, en roles de Líder, Consultor, Asesor u Oficial en Seguridad de la Información.

Respuesta observación 4:

SE ACLARA al observante que, tal como está establecido en el pliego de condiciones definitivo, se requerirán mínimo cuatro (4) certificaciones de las que se enumeran en la lista de la ficha técnica. Para mayor precisión, se adjunta nuevamente la ficha:

CISO (Chief Information Security Officer)	
Formación Académica	**Experiencia Mínima**
Título de Pregrado ❖ Ingeniero de Sistemas, de Telecomunicaciones, Electrónico o Ingenierías afines Título de Postgrado ❖ Especialización o Maestría en Seguridad de la Información, en ciberseguridad, en Administración de Riesgos Informáticos, en seguridad de la información o seguridad informática. Certificación obligatoria (una de las dos). ❖ Auditor Lider ISO 27001 V.2013 o ❖ Auditor Lider ISO 27001 V.2022 (Preferiblemente). Debe contar con al menos 4 de las siguientes certificaciones vigentes: ❖ CISM - Certified Information Security Management ❖ CERTIFIED ETHICAL HACKER (CEH). ❖ ECIH EC-COUNCIL CERTIFIED INCIDENT HANDLER ❖ CISSP - Certified Information Systems Security Professional ❖ CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER ❖ MANAGER CYBERSECURITY ISO/IEC 27032 ❖ LEAD INCIDENT MANAGER ISO 27035	❖ Experiencia específica de al menos ocho (8) años en proyectos relacionados con seguridad de la información, en roles de Líder, Consultor, Asesor u Oficial en Seguridad de la Información.

NOTA: *Todas las certificaciones deben estar vigentes al cierre del presente proceso, todas las certificaciones serán validadas atreves de las respectivas plataformas del ente certificador, de tal manera poder validar la vigencia de las mismas.*

El oferente **DIGITAL TRANSFORMATION LAB S.A.S**, presentó las siguientes observaciones al informe de verificación así:

Observación 1:

ID	Documento	Ubicación	Observación
1	PLIEGO DE CONDICIONES DEFINITIVO	Capítulo "II. CONDICIONES DE EXPERIENCIA / CAPACIDAD TÉCNICA" Literal "b) DOCUMENTOS TÉCNICOS ADICIONALES" Perfil: "CISO (Chief Information Security Officer)" Página: 46	El texto dice: "Debe contar con al menos 4 de las siguientes certificaciones vigentes: ❖ CISM - Certified Information Security Management ❖ CERTIFIED ETHICAL HACKER (C|EH). ❖ ECIH EC-COUNCIL CERTIFIED INCIDENT HANDLER ❖ CISSP - Certified Information Systems Security Professional ❖ CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER ❖ MANAGER CYBERSECURITY ISO/IEC 27032 ❖ LEAD INCIDENT MANAGER ISO 27035" De manera respetuosa solicitamos, mantener la robustez del perfil solicitado, se deben dar puntos adicionales dentro ítem "2. EVALUACIÓN TÉCNICA - ítem de "calidad"" para quien acredite al menos 2 certificaciones adicionales a las 4 solicitas y que estén dentro de las listadas anteriormente.

Respuesta observación 1:

NO SE ACEPTA LA OBSERVACIÓN toda vez que este proceso NO es un concurso de méritos y no estamos buscando una mayor calificación sino un perfil que cumpla con los requisitos mínimos habilitantes para satisfacer la necesidad de la entidad con este contrato.

Observación 2:

ID	Documento	Ubicación	Observación
2	PLIEGO DE CONDICIONES DEFINITIVO	Capítulo "IV. FACTORES DE EVALUACIÓN" Numeral "2. EVALUACIÓN TÉCNICA - ítem de "calidad"" Página: 52	Respetuosamente solicitamos modificar el siguiente texto que aparece en los numerales 2.1, 2.2 y 2.3: "El profesional que realizará la trasferencia de conocimiento debe tener al menos 2 de las siguientes certificaciones (CEH, CPTE, CHFI o CHFE)." Y reemplazarlo por el siguiente: "El profesional que realizará la trasferencia, de conocimiento, que en su caso puede ser el CISO propuesto, debe tener al menos 1 (una) de las siguientes certificaciones (CEH,

			CPTE, CHFI o CHFE). Esta certificación debe ser presentada con la propuesta" Esto puesto que más de una certificación resultan redundantes por la naturaleza de la transferencia de conocimiento y el alcance de dichas certificaciones.

Respuesta observación 2:

NO SE ACEPTA LA OBSERVACIÓN, y en aras de procurar por la pluralidad de oferentes, la entidad no solicitará acreditaciones o certificaciones diferentes a las que se enumeran en los requisitos mínimos habilitantes. En este sentido, se otorgarán los puntos simplemente con el compromiso de realizar la transferencia de conocimiento, según el cuadro de la evaluación técnica contemplado en el pliego de condiciones definitivo.

Para estos efectos, el cuadro de evaluación técnica quedará así, tal como constará en la adenda:

CONCEPTO	PUNTAJE MÁXIMO
2. EVALUACIÓN TÉCNICA - ítem de "calidad"	**20,00**
2.1 El oferente que ofrezca trasferencia de conocimiento en análisis forense y hacking ético a cuatro (4) funcionarios de la Dirección de Tecnologías de la Información, de la Federación Colombiana de Municipios, como base de conocimiento y mejora continua al MSPI	**20,00**
2.2 El oferente que ofrezca trasferencia de conocimiento en análisis forense y hacking ético a tres (3) funcionarios de la Dirección de Tecnologías de la Información, de la Federación Colombiana de Municipios, como base de conocimiento y mejora continua al MSPI	**10,00**
2.3 El oferente que ofrezca trasferencia de conocimiento en análisis forense y hacking ético a dos (2) funcionarios de la Dirección de Tecnologías de la Información, de la Federación Colombiana de Municipios, como base de conocimiento y mejora continua al MSPI	**5,00**

Observación 3:

ID	Documento	Ubicación	Observación
3	PLIEGO DE CONDICIONES DEFINITIVO	Capítulo "IV. FACTORES DE EVALUACIÓN" Numeral "2. EVALUACIÓN TÉCNICA - ítem de "calidad""	A fin de propender por el mejor perfil posible para la entidad, respetuosamente solicitamos que se le entreguen al menos 10 puntos de este ítem de "calidad" para aquellos que en el profesional propuesto como "CISO (Chief Information Security Officer)" acrediten al menos 2 certificaciones

		Página: 52	adicionales diferentes a las 4 mínimas solicitadas para este perfil, y que estén dentro de las siguientes: ❖ CISM - Certified Information Security Management ❖ CERTIFIED ETHICAL HACKER (CEH). ❖ ECIH EC-COUNCIL CERTIFIED INCIDENT HANDLER ❖ CISSP - Certified Information Systems Security Professional ❖ CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER ❖ MANAGER CYBERSECURITY ISO/IEC 27032 ❖ LEAD INCIDENT MANAGER ISO 27035” En este sentido de manera respetuosa solicitamos que el máximo puntaje otorgado producto de los numerales 2.1, 2.2 y 2.3 sea de 10 puntos.

Respuesta observación 3:

NO SE ACPETA LA OBSERVACIÓN toda vez que este proceso NO es un concurso de méritos y no estamos buscando una mayor calificación sino un perfil que cumpla con los requisitos mínimos habilitantes para satisfacer la necesidad de la entidad con este contrato.

El oferente **INFRAESTRUCTURAS SEGURAS SAS**, presentó las siguientes observaciones al informe de verificación así:

Observación 1:

“ Por medio de la presente, solicitamos la limitación de INFRAESTRUCTURAS SEGURAS S.A.S., identificada con NIT No. 901.188.624-1, como MIPYME para participar en la oportunidad relacionada con el proceso SAMC-01-FCM-2024 (Presentación de oferta), el cual consiste en la contratación del servicio de "Prestar por sus propios medios, con plena autonomía técnica, administrativa y operacional los servicios profesionales especialistas en seguridad de la información, ciberseguridad, riesgos digitales, G."

Adjuntamos la documentación que certifica nuestra clasificación como MIPYME, conforme a las normativas vigentes, y quedamos atentos a cualquier requerimiento adicional”

Respuesta observación 1:

NO SE ACEPTA LA OBSERVACIÓN, y se reitera lo enunciado en la **RESOLUCIÓN N° 57 DE 2024** *"Por medio de la cual se da apertura y se conforma el comité evaluador del proceso* SAMC-01-FCM-2024", que dice:

> *"Que, antes de la apertura del presente proceso de selección, y de conformidad con las fechas establecidas en el cronograma del proceso, se recibió una solicitud de limitación a Mipymes, por parte de SECUTIRY SOLUTIONS & EDUCATION S.A.S con Nit. 900.310.978-2. Sin embargo, al allegarse solo una solicitud, el proceso no se limitará, de conformidad con lo establecido en los artículos 2.2.1.2.4.2.2 y 2.2.1.2.4.2.4 del Decreto 1082 de 2015."*

Observación 2:

> *"Buenas tardes*
>
> *Con el fin de tener mayor pluralidad de oferentes sometemos a consideración de la entidad la siguiente observación:*
>
> *Para el CISO (perfil minino a presentar) solicitamos se admita la especialización en seguridad informática*
>
> *Para el CISO (perfil minino a presentar) solicitamos se admitan 2 o más de las siguienes certificaciones: CISM, CEH, CISSP, ECIH, CDPSE, MANAGER CIBERSECURITY ISO 2 7032, LEAD INCIDENT MANAGER ISO 27035*
>
> *Tal como estan los pliegos el CISO exigido requiere obligatoriamente ostentar 5 certificaciones lo cual limita en extrema la participación plural de oferentes."*

Respuesta observación 2:

SE ACEPTA PARCIALMENTE la observación, en la medida en que se acepta la inclusión de la especialización solicitada, tal como constará en la adenda.

Ahora bien, en lo que respecta a requerir menos certificaciones de las solicitadas, la entidad **NO ACEPTA**, pues esto afectaría los requisitos mínimos solicitados y, por lo tanto, la correcta ejecución del objeto contractual.

CISO (Chief Information Security Officer)	
Formación Académica	**Experiencia Mínima**
<u>Título de Pregrado</u> ❖ Ingeniero de Sistemas, de Telecomunicaciones, Electrónico o Ingenierías afines <u>Título de Postgrado</u>	❖ Experiencia específica de al menos ocho (8) años en proyectos relacionados con seguridad de la información, en roles de Líder, Consultor, Asesor u Oficial en

CISO (Chief Information Security Officer)	
Formación Académica	**Experiencia Mínima**
❖ Especialización o Maestría en Seguridad de la Información, en ciberseguridad, en Administración de Riesgos Informáticos, en seguridad de la información o seguridad informática. <u>Certificación obligatoria (una de las dos).</u> ❖ Auditor Lider ISO 27001 V.2013 o ❖ Auditor Lider ISO 27001 V.2022 (Preferiblemente). <u>Debe contar con al menos 4 de las siguientes certificaciones vigentes:</u> ❖ CISM - Certified Information Security Management ❖ CERTIFIED ETHICAL HACKER (CEH). ❖ ECIH EC-COUNCIL CERTIFIED INCIDENT HANDLER ❖ CISSP - Certified Information Systems Security Professional ❖ CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER ❖ MANAGER CYBERSECURITY ISO/IEC 27032 ❖ LEAD INCIDENT MANAGER ISO 27035	Seguridad de la Información.

<u>NOTA:</u> *<u>Todas las certificaciones deben estar vigentes al cierre del presente proceso, todas las certificaciones serán validadas atreves de las respectivas plataformas del ente certificador, de tal manera poder validar la vigencia de las mismas</u>.*

El oferente **SOFTGIC SAS**, presentó las siguientes observaciones al informe de verificación así:

Observación 1:

> *"Solicitamos amablemente a la entidad, aclarar si para el perfil CISO, se requieren al menos 2 certificaciones o 4, ya que en el pliego definitivo indican que deben ser al menos 4 y*
>
> *en las respuestas de observaciones se indica que al menos 2"*

Respuesta observación 1:

SE ACLARA al observante que, tal como está establecido en el pliego de condiciones definitivo, se requerirán mínimo cuatro (4) certificaciones de las que se enumeran en la lista de la ficha técnica. Para mayor precisión, se adjunta nuevamente la ficha:

CISO (Chief Information Security Officer)	
Formación Académica	**Experiencia Mínima**
<u>Título de Pregrado</u> ❖ Ingeniero de Sistemas, de	❖ Experiencia específica de al menos ocho (8) años en

CISO (Chief Information Security Officer)	
Formación Académica	**Experiencia Mínima**
Telecomunicaciones, Electrónico o Ingenierías afines Título de Postgrado ❖ Especialización o Maestría en Seguridad de la Información, en ciberseguridad, en Administración de Riesgos Informáticos, en seguridad de la información o seguridad informática. Certificación obligatoria (una de las dos). ❖ Auditor Lider ISO 27001 V.2013 o ❖ Auditor Lider ISO 27001 V.2022 (Preferiblemente). Debe contar con al menos 4 de las siguientes certificaciones vigentes: ❖ CISM - Certified Information Security Management ❖ CERTIFIED ETHICAL HACKER (CEH). ❖ ECIH EC-COUNCIL CERTIFIED INCIDENT HANDLER ❖ CISSP - Certified Information Systems Security Professional ❖ CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER ❖ MANAGER CYBERSECURITY ISO/IEC 27032 ❖ LEAD INCIDENT MANAGER ISO 27035	proyectos relacionados con seguridad de la información, en roles de Líder, Consultor, Asesor u Oficial en Seguridad de la Información.

NOTA: *Todas las certificaciones deben estar vigentes al cierre del presente proceso, todas las certificaciones serán validadas atreves de las respectivas plataformas del ente certificador, de tal manera poder validar la vigencia de las mismas*.

El oferente **NEVITECH S.A.S**, presentó las siguientes observaciones al informe de verificación así:

Observación 1:

"Mediante la presente y comedidamente nos permitimos presentar las siguientes

observaciones definitivas al proceso de selección así:

1. PROFESIONAL REQUERIDO CON LA PRESENTACIÓN DE LA OFERTA

CISO (Chief Information Security Officer)	
Formación Académica	**Experiencia Mínima**
Título de Pregrado ❖ Ingeniero de Sistemas, de Telecomunicaciones, Electrónico o Ingenierías	❖ Experiencia específica de al menos siete (7) años en proyectos relacionados

CISO (Chief Information Security Officer)	
Formación Académica	**Experiencia Mínima**
afines Título de Postgrado ❖ Especialización o Maestría en Seguridad de la Información. Certificación obligatoria ❖ Auditor Lider ISO 27001 V.2022 Debe contar con al menos 2 de las siguientes certificaciones vigentes: ❖ CISM - Certified Information Security Management ❖ CERTIFIED ETHICAL HACKER (C|EH). ❖ ECIH EC-COUNCIL CERTIFIED INCIDENT HANDLER ❖ CISSP - Certified Information Systems Security Professional ❖ CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER ❖ MANAGER CYBERSECURITY ISO/IEC 27032 ❖ LEAD INCIDENT MANAGER ISO 27035	con seguridad de la información, en roles de Lider, Consultor, Asesor u Oficial en Seguridad de la Información.

De acuerdo con el perfil definido por la entidad, solicitamos a la misma la extensión de los posgrados solicitados así:

- ***Especialización o maestría en Seguridad de la Información o Seguridad Informática o Riesgos Informáticos o Ciberseguridad.***

  Dichos posgrados en concreto de acuerdo con el Sistema Nacional de Información de la Educación Superior son afines entre si desde sus núcleos básicos de conocimiento.

  De esta manera al igual que para el caso de los pregrados solicitados, instamos a tener en cuenta a la entidad los posgrados afines a la Seguridad de la Información los cuales no comportan un riesgo en la idoneidad del futuro perfil en la ejecución del proyecto."

Respuesta observación 1:

SE ACEPTA LA OBSERVACIÓN, en la medida en que se incluirán los posgrados solicitados, para procurar la pluralidad de oferentes, tal como constará en la adenda. Por otro lado, la entidad aclara que la ficha técnica referida no es la que está establecida en el pliego de condiciones definitivo.

CISO (Chief Information Security Officer)	
Formación Académica	**Experiencia Mínima**
Título de Pregrado ❖ Ingeniero de Sistemas, de Telecomunicaciones, Electrónico o Ingenierías afines Título de Postgrado	❖ Experiencia específica de al menos ocho (8) años en proyectos relacionados con seguridad de la información, en roles de Líder, Consultor, Asesor u Oficial en

CISO (Chief Information Security Officer)	
Formación Académica	**Experiencia Mínima**
❖ Especialización o Maestría en Seguridad de la Información, en ciberseguridad, en Administración de Riesgos Informáticos, en seguridad de la información o seguridad informática. <u>Certificación obligatoria (una de las dos).</u> ❖ Auditor Lider ISO 27001 V.2013 o ❖ Auditor Lider ISO 27001 V.2022 (Preferiblemente). <u>Debe contar con al menos 4 de las siguientes certificaciones vigentes:</u> ❖ CISM - Certified Information Security Management ❖ CERTIFIED ETHICAL HACKER (CEH). ❖ ECIH EC-COUNCIL CERTIFIED INCIDENT HANDLER ❖ CISSP - Certified Information Systems Security Professional ❖ CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER ❖ MANAGER CYBERSECURITY ISO/IEC 27032 ❖ LEAD INCIDENT MANAGER ISO 27035	Seguridad de la Información.

NOTA: *Todas las certificaciones deben estar vigentes al cierre del presente proceso, todas las certificaciones serán validadas atreves de las respectivas plataformas del ente certificador, de tal manera poder validar la vigencia de las mismas.*

Observación 2.1:

2. EVALUACIÓN TÉCNICA - ítem de "calidad" (Máximo 20 puntos)

Se asignará el puntaje relacionado con el componente técnico de calidad de conformidad con el cuadro que se describe a continuación:

2.1 2. EVALUACIÓN TÉCNICA - ítem de "calidad" El puntaje máximo será de veinte (20) puntos.	PUNTAJE
2.1 El oferente que ofrezca trasferencia de conocimiento en análisis forense y hacking ético a cuatro (4) funcionarios de la Dirección de Tecnologías de la Información, de la Federación Colombiana de Municipios, como base de conocimiento y mejora continua al MSPI; El profesional que realizará la trasferencia de conocimiento debe tener al menos 2 de las siguientes certificaciones (CEH, CPTE, CHFI o CHFE).	**20,00**

"1. Solicitamos a la entidad en primera oportunidad la disminución de las certificaciones requeridas a solo (1) de las enlistadas, es decir (CEH o CPTE o CHFI o CHFE).

Consideramos que la exigencia de dos certificaciones del instituto EC-Council resultan redundantes a la hora del profesional elegido realizar la transferencia

de conocimiento pertinente, máxime que dichas certificaciones oscilan sobre tópicos similares y su enfoque diferencial se encuentra es aspectos técnicos a detalles que no son necesarios para la labor en cuestión."

Respuesta observación 2.1:

NO SE ACEPTA LA OBSERVACIÓN, y en aras de procurar por la pluralidad de oferentes, la entidad no solicitará acreditaciones o certificaciones diferentes a las que se enumeran en los requisitos mínimos habilitantes. En este sentido, se otorgarán los puntos simplemente con el compromiso de realizar la transferencia de conocimiento, según el cuadro de la evaluación técnica contemplado en el pliego de condiciones definitivo.

Para estos efectos, el cuadro de evaluación técnica quedará así, tal como constará en la adenda:

CONCEPTO	PUNTAJE MÁXIMO
3. EVALUACIÓN TÉCNICA - ítem de "calidad"	**20,00**
2.4 El oferente que ofrezca trasferencia de conocimiento en análisis forense y hacking ético a cuatro (4) funcionarios de la Dirección de Tecnologías de la Información, de la Federación Colombiana de Municipios, como base de conocimiento y mejora continua al MSPI	**20,00**
2.5 El oferente que ofrezca trasferencia de conocimiento en análisis forense y hacking ético a tres (3) funcionarios de la Dirección de Tecnologías de la Información, de la Federación Colombiana de Municipios, como base de conocimiento y mejora continua al MSPI	**10,00**
2.6 El oferente que ofrezca trasferencia de conocimiento en análisis forense y hacking ético a dos (2) funcionarios de la Dirección de Tecnologías de la Información, de la Federación Colombiana de Municipios, como base de conocimiento y mejora continua al MSPI	**5,00**

Observación 2.2:

"2. Para la acreditación y obtención del puntaje máximo descrito por la entidad, es necesario el llenado de un formato especifico fijado? ¿O se puede realizar en formato libre que designe cada oferente?"

Respuesta observación 2.2:

SE ACLARA que la entidad no dispuso ningún formato específico para estos fines, simplemente debe acreditarse el compromiso de cumplimiento de la transferencia de conocimiento, según el cuadro de la evaluación técnica contemplado en el pliego de condiciones definitivo.

Observación 2.3:

> *"3. Solicitamos a la entidad, se aclare si es necesario el aporte de la certificación respectiva que escoja el oferente o se debe anexar hoja de vida completa del profesional que realizará la transferencia de conocimiento."*

Respuesta observación 2.3:

SE ACLARA que la persona que se ofrezca para la transferencia de conocimiento debe ser la misma que va a ejecutar el contrato. En este sentido, su perfil se validará en los requisitos mínimos habilitantes.

El oferente **ITPERFORMA SAS**, presentó las siguientes observaciones al informe de verificación así:

Observación 1:

> *"De manera respetuosa, se solicita la modificación del requisito que permita a los interesados acreditar contratos con al menos dos (2) códigos UNSPSC de la lista total, con el fin de garantizar la pluralidad de oferentes y la libre concurrencia. Aunque se establecen diez (10) códigos UNSPSC en total, varios de ellos pueden considerarse accesorios o secundarios en relación con el objeto contractual, siendo al menos cuatro (4) los directamente relacionados con los servicios a contratar: 801015, 801016, 81112000 y 43233200. Cabe destacar que el alcance de las actividades a ejecutar no incluye la provisión de infraestructura o bienes, sino la operación de servicios especializados de seguridad informática.*
>
> *Por lo anterior, solicitamos comedidamente que solo se exijan dos (2) de los cuatro (4) códigos principales relacionados directamente con el proyecto, con el fin de fomentar una mayor participación de interesados."*

Respuesta observación 1:

NO SE ACEPTA LA OBSERVACIÓN y la entidad continuará con el requisito establecido en el pliego de condiciones definitivo, toda vez que así asegura la pluralidad de oferentes y la satisfacción de su necesidad, cuandoquiera que los códigos indicados guardan relación con el objeto o las actividades que de él se derivan.

El oferente **INGENIUM COLOMBIA SAS**, presentó las siguientes observaciones al informe de verificación así:

Observación 1:

> *"EXPERIENCIA MINIMA DEL PROPONENTE*

El pliego establece:

De manera respetuosa se solicita que, con el fin de garantizar la pluralidad de los oferentes y la libre concurrencia, se modifique el requisito que permita a los interesados aportar contratos que acrediten mínimo (2) códigos UNSPSC del total de la lista. Esto teniendo en cuenta que, si bien se establece una codificación de un total de 10 códigos UNSPSC, varios de ellos se pueden considerar como accesorios o secundarios frente al objeto contractual, siendo al menos 4 los directamente relacionados con los servicios a contratar, a saber: 801015, 801016, y 8111200 y 43233200. Esto teniendo en cuenta que dentro del alcance de las actividades a ejecutar no se comprende la disposición de infraestructura o entrega de bienes, sino la operación de los servicios de seguridad informática a nivel especializado.

Con base a lo anterior, comedidamente a se solicita que sean exigibles únicamente dos (2) de los (4) códigos principales relacionados directamente con el proyecto con fin de permitir la amplia participación de interesados."

Respuesta observación 1:

NO SE ACPETA LA OBSERVACIÓN y la entidad continuará con el requisito establecido en el pliego de condiciones definitivo, toda vez que así asegura la pluralidad de oferentes y la satisfacción de su necesidad, cuandoquiera que los códigos indicados guardan relación con el objeto o las actividades que de él se derivan.

El oferente **PRICEWATERHOUSECOOPERS ASESORES GERENCIALES S.A.S.**, presentó las siguientes observaciones al informe de verificación así:

Observación 1:

"Se solicita respetuosamente se aclare si el objeto del proceso es la contratación de servicios profesionales especialistas en seguridad de la información, ciberseguridad, riesgos digitales, Gobierno digital."

Respuesta observación 1:

SE ACLARA que el objeto del proceso es "Prestar por sus propios medios, con plena autonomía técnica, administrativa y operacional los servicios profesionales especialistas en seguridad de la información, ciberseguridad, riesgos digitales, Gobierno digital de la Federación Colombiana de Municipios, en cumplimiento de la función pública asignada."

Observación 2:

"Para el perfil del CISO solicitamos amablemente incluir como opcional la siguiente certificación: Auditor Interno ISO 27001 V.2022"

Respuesta observación 2:

NO SE ACEPTA LA OBSERVACIÓN ya que el profesional solicitado es para suplir las funciones de un Oficial de seguridad de la información (CISO), que apoye y mejore la madurez del MSPI de la Organización, cabe aclarar que las normas ISO normalmente en el capítulo de planificación tratan del manejo y acciones de los riesgos, por esto es obligatorio para el perfil solicitado la certificación en Auditor Lider ISO 27001 V.2013 o V.2022.

Así las cosas, la entidad solicita en los requisitos mínimos habilitantes la certificación anteriormente señalada, toda vez que en los conocimientos que esta refleja se encuentra inmerso el manejo de los riesgos. De esta manera, solicitar más certificaciones restringiría la pluralidad de oferentes y no estarían directamente relacionadas con el objeto a contratar.

Observación 3:

> *"Para el perfil del CISO solicitamos amablemente incluir como opcional la siguiente certificación: ITIL versión 3 o superior."*

Observación 4:

> *"Para el perfil del CISO solicitamos amablemente incluir como opcional la siguiente certificación: Auditor Interno ISO 22301"*

Observación 5:

> *"Para el perfil del CISO solicitamos amablemente incluir como opcional la siguiente certificación: CPTE"*

Observación 6:

> *"Para el perfil del CISO solicitamos amablemente incluir como opcional la siguiente certificación: SCRUM"*

Respuesta las observaciones 3, 4, 5 y 6: NO SE ACEPTA LA OBSERVACIÓN ya que el profesional solicitado se requiere para suplir las funciones de un Oficial de seguridad de la información (CISO), que apoye y mejore la madurez del MSPI de la Organización.

Así las cosas, la entidad solicita en los requisitos mínimos habilitantes la certificación anteriormente señalada, toda vez que en los conocimientos que esta refleja se encuentra inmerso el manejo de los riesgos. De esta manera, solicitar más certificaciones restringiría la pluralidad de oferentes y no estarían directamente relacionadas con el objeto a contratar.

Dicho lo anterior, la entidad está llamada a validar aquella información contenida en el Registro Único de Proponentes, de manera privativa.

Se firma en Bogotá el tres (3) de octubre de 2024.

Original Firmado

Germán Alberto Duque Beltrán
Miembro Comité Evaluador – Componente Técnico