Bogotá D.C., 16 de septiembre de 2026

Señores

CROSSBORDER, GRIN, Limitación a Mipymes, DATASECURITY, DINATEL GROUP, FUNDACIÓN PARQUE TECNOLÓGICO DE SOFTWARE DE TULUÁ, IN TECH SAS, Multisoftware Transaccional S.A.S, SOFTESTING, SSE S.A.S, Stratech, STS S.A.S, 2SECURE, INDTECH FCM & NEVITECH.

Referencia: Proceso No. SAMC-001-FCM-2026

Asunto: Respuestas a Observaciones

Federación Colombiana de Municipios

A las observaciones:

<table>
<tr><th>Proponente</th><th>Observación</th><th>Respuesta</th></tr>
<tr>
<td>CROSSBORDER</td>
<td>
<table>
<tr><td>Observación</td><td>Solicitamos amablemente a la entidad incluir como otra de las alternativas la certificación Certified Ethical Hacker (CEH) del EC-Council y/o Computer Hacking Forensic Investigator del EC-Council, quedando el requisito de la siguiente manera:

Los ingenieros con título profesional en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería de Software, Ingeniería de telecomunicaciones o profesiones afines. Deberá contar con al menos 2 de las siguientes certificaciones:

- Certificación a nivel profesional en seguridad de sistemas de información (CISSP)
- Certificación en control de riesgos y sistemas de información (CRISC)</td></tr>
</table>
</td>
<td>
Al validar la observación, se ACEPTA, y esta serán tenidas en cuenta en el pliego de condiciones definitivo, por lo tanto, el requisito quedará así:
Para el desarrollo del contrato, se requiere que el contratista cuente como mínimo con el siguiente personal:
<table>
<tr><th>CANTIDAD PERSONAS</th><th>FORMACIÓN ACADÉMICA</th></tr>
<tr><td>1</td><td>Ingeniero con título profesional en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería de Software, Ingeniería de telecomunicaciones</td></tr>
</table>
</td>
</tr>
</table>

			o profesiones afines.

Los ingenieros con título profesional en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería de Software, Ingeniería de telecomunicaciones o profesiones afines.
Deberá contar con al menos 2 de las siguientes certificaciones:

- Quedando así:
-
- -
  Certificación a nivel profesional en seguridad de sistemas de información (CISSP)
- -
  Certificación en control de riesgos y sistemas de información (CRISC)
- -
  Certificación en Web Application Scanner
- -
  Certificación en Vulnerability Management Detección and Response
- - Certified Ethical Hacker (CEH) (Obligatoria)
- - Computer Hacking Forensic Investigator
- -
  Certificación OSCP Offensive Security Certified Professional

<table>
<tr>
<td>CROSSBORDER</td>
<td>
<table>
<tr><th colspan="2">Observación No. 2</th></tr>
<tr><td>Documento</td><td>Pliego de condiciones definitivo</td></tr>
<tr><td>Página / Hoja</td><td>54</td></tr>
<tr><td>Numeral</td><td>2.2. Evaluación técnica – ítem de “Pruebas de ataque de dirigidos de phishing”</td></tr>
<tr><td>Texto del requisito</td><td>
<table>
<tr><th>2.2 EVALUACIÓN TÉCNICA - ítem de “Pruebas de ataque de dirigidos de Phishing” El puntaje máximo será de diez (10) puntos.</th><th>PUNTAJE</th></tr>
<tr><td>2.2.1 El oferente que ofrezca, cincuenta (50) pruebas adicionales de ataques dirigidos de phishing a funcionarios específicos de la Entidad, adicionales a las cantidades mínimas solicitadas en el presente proceso.</td><td>10</td></tr>
<tr><td>2.2.2 El oferente que ofrezca, treinta (30) pruebas adicionales de ataques dirigidos de phishing a funcionarios específicos de la Entidad, adicionales a las cantidades mínimas solicitadas en el presente proceso.</td><td>8</td></tr>
<tr><td>2.2.3 El oferente que ofrezca, veinte (20) pruebas adicionales de ataques dirigidos de phishing a funcionarios específicos de la Entidad, adicionales a las cantidades mínimas solicitadas en el presente proceso.</td><td>5</td></tr>
</table>
</td></tr>
<tr><td>Observación</td><td>Solicitamos respetuosamente a la entidad aclarar si cuando se refieren a la cantidad de pruebas quieren decir que es la cantidad de funcionarios objetivo de las pruebas o la cantidad de veces que hay que realizar pruebas.</td></tr>
</table>
</td>
<td>Al validar la observación, se ACLARA, que, los 50 corresponden cantidad de funcionarios adicionales a los solicitados en las pruebas iniciales, que según la ficha corresponden a los 200 usuarios descritos en la justificación de la necesidad. ítem 1 Pruebas de Ingeniería Social externas dirigidas al personal de la Federación Colombiana de Municipios en cumplimiento de la función pública asignada.</td>
</tr>
<tr>
<td>DATASECURITY</td>
<td>
I. Observaciones al Aviso de Convocatoria

1. Discrepancia en la modalidad del proceso

Lo publicado. El Aviso de Convocatoria identifica el proceso como “Selección Abreviada por Subasta Inversa”, mientras que en la plataforma SECOP II el proceso se encuentra publicado bajo la modalidad de Selección Abreviada de Menor Cuantía (SAMC-001-FCM-2026).

Observación: Solicitamos a la entidad aclarar y, de ser el caso, corregir el Aviso de Convocatoria para que la modalidad allí consignada coincida con la registrada en SECOP II, con el fin de evitar interpretaciones que puedan inducir a error a los interesados sobre las reglas aplicables al proceso.
</td>
<td>Remitirse al documento de respuestas jurídicas.</td>
</tr>
<tr>
<td></td>
<td>
2. Discrepancia en el objeto del proceso

Lo publicado en el Aviso de Convocatoria. El objeto descrito corresponde a la adquisición de una plataforma tecnológica bajo modelo SaaS para la gestión de riesgos y el fortalecimiento de la postura de seguridad, la detección temprana de exposiciones de información en entornos digitales, incluida Deep y Dark Web, y la prevención de suplantación de marca y phishing.

Lo publicado en SECOP II. El objeto registrado corresponde a la prestación de servicios especializados para la ejecución de pruebas de hacking ético y análisis de vulnerabilidades en servicios internos y servicios publicados en Internet.

Observación: Es de nuestro entendimiento que la entidad requiere una plataforma tipo Saas especializado de etical hacking automatizado, que esta permita integrarse con las herramientas que la entidad ya cuenta actualmente. solicitamos aclarar si nuestro requerimiento es correcto.
</td>
<td>Remitirse al documento de respuestas jurídica.</td>
</tr>
<tr>
<td></td>
<td>
3. Certificado de homologación CVE

Lo exigido por la ficha técnica. Se solicita adjuntar en los informes presentados un certificado de homologación de CVE (Common Vulnerabilities and Exposures) expedido por MITRE, o la ruta de la página de CVE donde se evidencie que la herramienta ofrecida está homologada por dicha entidad.

Observación: Los identificadores CVE son asignados a vulnerabilidades específicas y no constituyen una homologación o certificación de herramientas; en consecuencia, no existe una entidad que expida el certificado exigido. Con el fin de garantizar la pluralidad de oferentes y la neutralidad tecnológica, solicitamos precisar que lo verificable es la referenciación de los hallazgos mediante identificadores CVE vigentes, y no una certificación de homologación de la herramienta.
</td>
<td>Al validar la observación, se ACEPTA, y esta serán tenidas en cuenta y se verán reflejadas en la ficha técnica y en los documentos definitivos, así:

Para la realización de esta prueba, se deben usar las herramientas pertinentes y usadas para el desarrollo de las pruebas de penetración, que referencien los hallazgos mediante identificadores CVE (Common Vulnerabilities and Exposures), conforme a www.mitre.org, y deben estar actualizadas a la fecha de su utilización. Para lo anterior, se deberá adjuntar en los informes presentados la referenciación CVE de cada hallazgo, o la ruta de la</td>
</tr>
</table>

		página de CVE donde se pueda evidenciar el identificador reportado por la herramienta ofrecida.
	4. Certificación o documento de propiedad de las herramientas **Lo exigido por la ficha técnica.** El proponente debe demostrar la propiedad o autorización de uso explícita del fabricante de las herramientas utilizadas, para lo cual deberá allegar certificación o documento que soporte el requisito. **Observación:** Solicitamos a la entidad modificar esta exigencia, dado que un requisito de certificación de propiedad expedida por el fabricante restringe la pluralidad de oferentes y puede favorecer a marcas puntuales sobre otras igualmente idóneas, sin que ello se traduzca en una mejor prestación del servicio. **Texto propuesto:** "La herramienta deberá permitir la generación de los informes y entregables solicitados de manera automática, sin límite en el número de generaciones ni costo adicional durante el plazo de ejecución del contrato."	Al validar la observación, se **ACEPTA**, en la medida en que el futuro contratista podrá utilizar plataformas o herramienta licenciadas u *Open source.* Por lo tanto, esta modificación se verá reflejada en la ficha técnica y en los documentos definitivos, quedando de la siguiente manera: *La herramienta deberá permitir la generación de los informes y entregables solicitados de manera automática, sin límite en el número de generaciones ni costo adicional durante el plazo de ejecución del contrato. Sin importar si es una plataforma licenciada o de uso libre.*
	Lo exigido por la ficha técnica. Se ejecutarán dos (2) ciclos completos de análisis de vulnerabilidades (test y retest) sobre un alcance de 100 direcciones IP, con el fin de validar la identificación inicial de hallazgos y la efectividad de las acciones de remediación implementadas. **Observación:** Se sugiere a la entidad contemplar que la remediación sea únicamente acompañada por parte del oferente, dado que este proceso requiere acceso a la infraestructura, redes y ciberseguridad de la entidad para ejecutarse directamente, lo cual puede afectar la línea de producción. **Texto propuesto:** "Con el fin de validar la identificación inicial de hallazgos y realizar el proceso de remediación únicamente acompañado por el oferente, para evitar posibles afectaciones a la línea de producción."	**SE ACLARA** al observante que el documento técnico es claro y más adelante se refiere, dentro de las condiciones técnicas para su realización, que esto está a cargo del contratista. Motivo por el cual, no procedería ninguna precisión mayor en el texto. En otras palabras, todo lo establecido en los documentos técnicos, recae exclusivamente entre el futuro contratista y la Federación Colombiana de Municipios. Por otro lado, es enfática la entidad al insistir en que ningún proceso del futuro contrato podrá ser ejecutado por una persona diferente al contratista.

	III. Recomendaciones técnicas a la Ficha Técnica **6. Documentación centralizada** Se recomienda a la entidad que el numeral de entregables y documentación del ethical hacking solicitado para la duración del contrato, se realice durante una plataforma que permita realizar de forma automática esta capacidad por lo tanto recomendamos incluir el siguiente numeral, **Numeral:** Incluir plataforma Saas de ethical hacking automatizado en la que pueda tener acceso a el proceso y hoja de ruta de pasa procedimiento de ethical hacking, resultados, entregables y actualizaciones del servicio contratado en tiempo real, así como contar con una cantidad ilimitada de usuarios dentro de dicha plataforma.	Al validar la observación presentada **NO SE ACEPTA**, toda vez que la consideración de esta plataforma no tiene incidencia directa en la ejecución del objeto contractual. Entonces, requerirla sería afecta la pluralidad de oferentes. No obstante, se aclara que, si el proponente cuenta con una plataforma centralizada que permita consultar y visualizar los entregables requeridos, se podrá aceptar dicho mecanismo **como medio de entrega**, siempre que garantice su disponibilidad, integridad y trazabilidad. En este sentido, se precisa que la disposición de este mecanismo de entrega no constituye una condición habilitante ni un requisito que determine la participación o no de un proponente en el proceso. **PERO POR NINGÚN MOTIVO LA PLATAFORMA, HERRAMIENTA O SOLUCIÓN, REEMPLAZARÁ LOS SERVICIOS REQUERIDOS EN LA NECESIDAD DE LA ENTIDAD. ES DECIR, EL FUTURO CONTRATO SERÁ DE UNA PRESTACIÓN DE SERVICIOS, Y NO LA COMPRAVENTA DE UN LICENCIAMIENTO PARA EL USO DE ESTAS SOLUCIONES.**

	7. Priorización de hallazgos por severidad y explotabilidad Se recomienda contemplar una plataforma que priorice los hallazgos identificados considerando la severidad CVSS y la existencia de explotación conocida (EPSS), contrastando con catálogos públicos de vulnerabilidades, con el fin de orientar el plan de mitigación hacia las vulnerabilidades de mayor riesgo real para la entidad.	Al validar la observación presentada **NO SE ACEPTA**, toda vez que la consideración de esta plataforma no tiene incidencia directa en la ejecución del objeto contractual. Entonces, requerirla sería afecta la pluralidad de oferentes. Sobre todo, teniendo en cuenta que lo que se busca es la prestación de un servicio y no el licenciamiento de uso de una herramienta.
	8. Consolidación de hallazgos automáticos y manuales Se recomienda que la herramienta designada permita la ejecución de análisis autónomos sobre el alcance autorizado, así como el registro y la gestión de las pruebas ejecutadas manualmente por los consultores, de manera que los hallazgos de ambos orígenes queden consolidados en un único repositorio, bajo el mismo esquema de clasificación, severidad y estados.	Al validar la observación presentada **NO SE ACEPTA**, toda vez que la consideración de esta plataforma no tiene incidencia directa en la ejecución del objeto contractual. Entonces, requerirla sería afecta la pluralidad de oferentes. Adicionalmente, se está pretendiendo con el proceso de contratación la prestación de un servicio y no el licenciamiento de uso de una plataforma o solución. No obstante, se aclara que, si el proponente cuenta con una plataforma centralizada que permita hacer las pruebas y consultar y visualizar los entregables requeridos, se podrá aceptar dicho mecanismo **como medio de entrega**, siempre que garantice su disponibilidad, integridad y trazabilidad. **PERO POR NINGÚN MOTIVO LA PLATAFORMA, HERRAMIENTA O SOLUCIÓN, REEMPLAZARÁ LOS SERVICIOS REQUERIDOS EN LA NECESIDAD DE LA ENTIDAD. ES DECIR, EL FUTURO CONTRATO SERÁ DE UNA PRESTACIÓN DE SERVICIOS, Y NO LA COMPRAVENTA DE UN**

		LICENCIAMIENTO PARA EL USO DE ESTAS SOLUCIONES.
	9. Plataforma SaaS para las pruebas de Ingeniería Social Se recomienda a la entidad que las pruebas de Ingeniería Social se ejecuten y gestionen desde una plataforma SaaS dispuesta para el servicio, que permita la construcción y programación de las campañas y el registro del resultado por usuario evaluado —incluyendo entrega efectiva, apertura, interacción con el vector y entrega de credenciales—, así como la comparación entre las pruebas ejecutadas durante el plazo del contrato, con el fin de identificar la reincidencia de los usuarios evaluados.	Al validar la observación presentada **NO SE ACEPTA**, toda vez que la consideración de esta plataforma no tiene incidencia directa en la ejecución del objeto contractual. Entonces, requerirla sería afecta la pluralidad de oferentes No obstante, se aclara que, si el proponente cuenta con una plataforma centralizada que permita hacer las pruebas y consultar y visualizar los entregables requeridos, se podrá aceptar dicho mecanismo **como medio de entrega**, siempre que garantice su disponibilidad, integridad y trazabilidad. **PERO POR NINGÚN MOTIVO LA PLATAFORMA, HERRAMIENTA O SOLUCIÓN, REEMPLAZARÁ LOS SERVICIOS REQUERIDOS EN LA NECESIDAD DE LA ENTIDAD. ES DECIR, EL FUTURO CONTRATO SERÁ DE UNA PRESTACIÓN DE SERVICIOS, Y NO LA COMPRAVENTA DE UN LICENCIAMIENTO PARA EL USO DE ESTAS SOLUCIONES.** En este sentido, se precisa que la disposición de este mecanismo de entrega no constituye una condición habilitante ni un requisito que determine la participación o no de un proponente en el proceso.
	IV. Solicitudes de aclaración sobre el Pliego de Condiciones **10. Documentos técnicos adicionales – personal mínimo requerido** El pliego señala que, para el desarrollo del contrato, se requiere que el contratista cuente como mínimo con determinado personal. Solicitamos aclarar si los perfiles de dicho personal deben adjuntarse con la oferta como documento técnico habilitante, o si basta con el compromiso del contratista de disponerlo durante la ejecución contractual.	Al validar la observación presentada, SE ACLARA, que los perfiles de dicho personal deben adjuntarse con la oferta.
	- Certificación a nivel profesional en seguridad de sistemas de información (CISSP)	La entidad ACLARA que en el Pliego de Condiciones se expresa textualmente cómo debe acreditarse cada uno de los

	- Certificación en control de riesgos y sistemas de información (CRISC) - Certificación en Web Application Scanner - Certificación en Vulnerability Management Detección and Response - Certified Ethical Hacker (CEH) (Obligatoria) - Computer Hacking Forensic Investigator - Certificación OSCP Offensive Security Certified Professional	requisitos de puntaje, es decir, a través de una carta en que certifique la cantidad de pruebas adicionales que realizará, de acuerdo con las especificaciones previamente detalladas, junto con los documentos de la ofertas. Por favor remitirse directamente a los factores de evaluación determinados en el pliego.
	12. Pruebas adicionales ofertables El pliego contempla la posibilidad de ofrecer cincuenta (50) pruebas adicionales a las cantidades mínimas solicitadas, sin especificar cuáles son esas cantidades mínimas de referencia por cada tipo de prueba. Solicitamos que se precisen dichas cantidades mínimas, de manera que los oferentes puedan estructurar ofrecimientos adicionales comparables entre sí y bajo los mismos parámetros establecidos en el anexo técnico.	Al validar la observación presentada, SE ACLARA que las pruebas corresponden a las actividades descritas en la "Descripción y Justificación de la Necesidad" de la Ficha técnica, ítem 1, relacionadas con la ejecución de pruebas de Ingeniería Social externas dirigidas al personal de la Federación Colombiana de Municipios, en el marco de la función pública asignada, detallándose que deben ser correspondientes a 200 usuarios. Así las cosas, el criterio puntuable se refiere a 50 pruebas adicionales de *Phishing*.
	13. Forma de pago y tipo de remuneración Solicitamos aclarar contra cuáles entregables específicos se facturará cada pago, teniendo en cuenta que el anexo técnico contempla múltiples productos por fase y por tipo de prueba (informes ejecutivos, informes técnicos, planes de mitigación y actas de socialización, entre otros).	Al validar la observación presentada, SE ACLARA que el valor del contrato será pagado, de acuerdo como se establece en el estudio previo y en el pliego de condiciones: el primer pago, contra el recibido del plan de trabajo en su totalidad de las pruebas de hacking ético y; el segundo una vez se hagan las entregas de los análisis de vulnerabilidades sobre los servicios internos y servicios publicados en Internet definidos en el alcance contractual.

	Con fundamento en lo expuesto, solicitamos respetuosamente al Comité Asesor y Evaluador: • Aclarar y, de ser procedente, corregir el objeto y la modalidad del proceso consignados en el Aviso de Convocatoria, de forma que coincidan con lo publicado en SECOP II. • Modificar los apartes de la Ficha Técnica señalados en el numeral II, conforme a los textos propuestos, con el fin de garantizar la pluralidad de oferentes y la neutralidad tecnológica del proceso. • Evaluar la incorporación de las recomendaciones técnicas descritas en el numeral III. • Dar respuesta a las solicitudes de aclaración del numeral IV, con la precisión suficiente para que los interesados puedan estructurar su oferta sobre reglas ciertas. Agradecemos la atención prestada a la presente observación y quedamos atentos a la respuesta de la entidad a través de la plataforma SECOP II.	Al validar sus peticiones se indica que estas serán tenidas en cuenta conforme a las respuestas dadas en cada observación.
DINATEL GROUP	**Observación 1:** Se solicita aclarar la forma de pago y establecer de manera expresa la correspondencia entre cada pago previsto en el contrato y los entregables que deberán ser presentados y recibidos a satisfacción para habilitar su respectiva facturación.	Al validar la observación presentada, SE ACLARA, que El valor del contrato será pagado en dos pagos iguales, él primero una vez se haya recibido el plan de trabajo en su totalidad de las pruebas de hacking ético y el segundo una vez se hagan las entregas de los análisis de vulnerabilidades sobre los servicios internos y servicios publicados en Internet definidos en el alcance contractual.
	Observación 2: solicitamos a la entidad aclarar si la acreditación de los perfiles correspondientes al personal mínimo requerido constituye un requisito habilitante que deba ser demostrado con la presentación de la oferta, o si el requisito es únicamente para el futuro contratista.	La entidad ACLARA que sí es un requisito habilitante, por tanto, deberá acreditarse al momento de presentación de la oferta.
	Observación 3: se solicita a la entidad indicar cuales son las cantidades mínimas previstas para cada modalidad de prueba requerida, ya que para la asignación de puntaje podrán ser ofrecidas por los proponentes, hasta un máximo de cincuenta (50) pruebas adicionales. Lo anterior con el propósito de garantizar que los ofrecimientos sean presentados y evaluados bajo condiciones uniformes.	Al validar la observación presentada, SE ACLARA que las pruebas corresponden a las actividades descritas en la "Descripción y Justificación de la Necesidad" de la Ficha técnica, ítem 1, relacionadas con la ejecución de pruebas de Ingeniería Social externas dirigidas al personal de la Federación Colombiana de Municipios, en el marco de la función pública asignada, detallándose que deben ser correspondientes a 200 usuarios. Así las cosas, el criterio puntuable se refiere a 50 pruebas adicionales de *Phishing*.

	Observación 4: Frente al requisito que establece la presentación de un certificado de homologación CVE emitido por MITRE, consideramos necesario revisar la forma en que se encuentra planteada esta exigencia. El estándar CVE tiene como finalidad proporcionar identificadores únicos para vulnerabilidades de seguridad conocidas, por lo que su función está asociada a la identificación y consulta de vulnerabilidades, y no a la certificación o acreditación de las herramientas empleadas para efectuar pruebas de seguridad. exigir un supuesto certificado de homologación de la herramienta podría generar una condición de difícil cumplimiento y limitar innecesariamente la participación de tecnologías que, aun siendo técnicamente idóneas, utilizan y reportan identificadores CVE de manera válida. solicitamos que el requisito sea ajustado para que la validación se concentre en los resultados obtenidos durante las pruebas y en la posibilidad de comprobar los identificadores CVE asociados a los hallazgos, garantizando así que la condición sea objetiva, verificable y aplicable independientemente del fabricante de la herramienta.	Al validar la observación, se ACEPTA, y esta serán tenidas en cuenta y se verán reflejadas en la ficha técnica y en los documentos definitivo. Así: Para la realización de esta prueba, se deben usar las herramientas pertinentes y usadas para el desarrollo de las pruebas de penetración, que referencien los hallazgos mediante identificadores CVE (Common Vulnerabilities and Exposures), conforme a www.mitre.org, y deben estar actualizadas a la fecha de su utilización. Para lo anterior, se deberá adjuntar en los informes presentados la referenciación CVE de cada hallazgo, o la ruta de la página de CVE donde se pueda evidenciar el identificador reportado por la herramienta ofrecida. La herramienta deberá permitir la generación de los informes y entregables solicitados de manera automática, sin límite en el número de generaciones ni costo adicional durante el plazo de ejecución del contrato.
	Retest atado a la remediación de la Entidad. El 2° ciclo (retest) y por ende el 2° pago dependen de que la FCM remedie entre test y retest. Si la Entidad se demora en corregir, nos cuelgan la entrega y hay multas hasta el 10%. Observación: que el plazo de retest y su pago se cuenten a partir de que la Entidad confirme por escrito la remediación, para que no nos sancionen por demoras que no controlamos.	Al validar la observación presentada, SE ACLARA, que El valor del contrato será pagado en dos pagos: 1. Él primero una vez se hayan recibido el plan de trabajo en su totalidad de las pruebas de hacking ético. 2. El segundo una vez se hagan las entregas de los análisis de vulnerabilidades sobre los servicios internos y servicios publicados en Internet definidos en el alcance contractual.
	Coherencia de modalidad. El pliego arrastra encabezados de "subasta inversa" y referencias a "SaaS" que no corresponden a este objeto (menor cuantía, ponderado). Observación de forma para que el pliego definitivo quede coherente y el fallo no sea impugnable después. Nos conviene un proceso legalmente sólido si ganamos.	Remitirse al documento de respuestas jurídicas.

	Infraestructura autorizada (cláusula 7). Prohíbe almacenar, procesar o analizar la información "fuera de la infraestructura autorizada" salvo autorización escrita. Nuestro modelo analiza y hashea evidencia en laboratorio controlado propio. Observación puntual: que se reconozca expresamente que el análisis en un entorno controlado y autorizado del contratista cumple la cláusula, para no quedar obligados a trabajar solo en sitio.	Al validar la observación presentada, SE ACLARA, que a lo expuesto: en la Obligaciones Especificas # 7 Mantener absoluta reserva, confidencialidad y custodia de toda la información conocida durante la ejecución del contrato, absteniéndose de almacenar, procesar, divulgar, copiar o analizar información de la Federación Colombiana de Municipios fuera de la infraestructura autorizada, salvo autorización expresa y escrita de la Entidad. En otras palabras, la obligación se refiere a que la infraestructura autorizada será la propia del contratista. El caso contrario sería, disponer de ella, en una infraestructura ajena a la suya.
4. FUNDACIÓN PARQUE TECNOLÓGICO DE SOFTWARE DE TULUÁ	**OBSERVACIÓN No. 2 — ACLARACIÓN SOBRE ACREDITACIÓN DE EXPERIENCIA ESPECÍFICA Y CÓDIGOS UNSPSC** **Asunto:** Aclaración sobre el alcance de la afinidad del objeto en la acreditación de la experiencia mínima requerida. El numeral II del pliego de condiciones señala que el proponente debe acreditar su experiencia con contratos identificados con por lo menos uno de los códigos UNSPSC clasificados (81111800, 81111801, 81112208, 81141801), pero reglón seguido indica que: *"deberá acreditarse que el contrato versa sobre procesos de ética hacking y análisis de vulnerabilidades"*. Teniendo en cuenta que en la contratación estatal colombiana la clasificación RUP mediante códigos UNSPSC constituye plena prueba de la experiencia según el artículo 6 de la Ley 1150 de 2007, y que la gestión de vulnerabilidades y seguridad lógica se encuentra incorporada intrínsecamente en servicios integrales de administración de componentes de sistemas (811118), soporte de seguridad (811122) y análisis de riesgos (811418): **Solicitud:** Aclarar expresamente si son válidos para la habilitación de la experiencia aquellos contratos registrados en el RUP que contengan al menos uno de los códigos UNSPSC señalados, y en cuyas obligaciones o actividades se hayan contemplado componentes de administración de seguridad informática, aseguramiento de servidores, análisis de riesgo o soporte de plataformas, sin exigir que la denominación textual del objeto del contrato deba rezar de manera idéntica y restrictiva "ethical hacking".	Al validar la observación presentada, NO SE ACEPTA. Se aclara que el código UNSPSC 81111801 – Servicios de administración y seguridad de sistemas de información (incluye pruebas de vulnerabilidad y hacking ético) guarda relación directa con las actividades y el objeto del proceso a contratar, particularmente en lo referente a servicios especializados de seguridad de la información y pruebas de seguridad. No obstante, con el propósito de garantizar la pluralidad y participación de oferentes, la Entidad ha contemplado códigos adicionales que permiten ampliar el universo de posibles proponentes que puedan acreditar su experiencia relacionada con el objeto contractual. La inclusión de estos códigos no implica que se prescinda de la verificación de la experiencia requerida. Por el contrario, los proponentes deberán acreditar mediante los contratos aportados

		la experiencia específica y relacionada con las actividades objeto del proceso, de manera que la Entidad pueda verificar que cuentan con la capacidad técnica y experiencia necesaria para ejecutar las obligaciones contractuales. Es importante tener en cuenta que basta la coincidencia a nivel de clase (tercer nivel, es decir, 811118, 811122 o 811418) respecto de los cuatro códigos de la tabla. Como un contrato puede registrarse con diferentes códigos en el RUP, independente de su objeto, la entidad amplía la cantidad de los mismos, así como que estos apunten a diferentes denominaciones que pueden estar relacionadas con el ramo de la Cyberseguridad. No obstante, sí se precisa que, como se menciona en el pliego, los contratos aportados prueben, en su objeto, obligaciones o anexos técnicos, que en su ejecución se realizaron actividades de hacking ético o análisis de vulnerabilidades. Toda vez que esto es lo propio del objeto a contratar.
5. GRUPO INTALEN	**OBSERVACIÓN 1 — Extender el criterio diferencial de número de contratos a las Mipyme en general** Numeral observado: Capítulo "Criterios Diferenciales de Experiencia del Proponente Relacionada en el RUP", en el cual se establece que los emprendimientos y empresas de mujeres, y las empresas de personas con discapacidad, "podrán cumplir con la experiencia habilitante a través de la acreditación de máximo cuatro (4) [o cinco (5), según el numeral] contratos... cuya sumatoria sea igual o superior a 72 SMMLV", mientras que el literal "B. MIPYMES domiciliadas en Colombia" únicamente regula la forma de acreditar la condición de Mipyme, sin extender este mismo número diferencial de contratos a este grupo. Fundamento: el artículo 31 de la Ley 2069 de 2020 y el Decreto 1860 de 2021 facultan a las entidades estatales para fijar requisitos habilitantes diferenciales a favor de las Mipyme, entre ellos un mayor número de contratos permitidos para acreditar experiencia, sin que la norma reserve este beneficio exclusivamente a los subgrupos de empresas de mujeres o de personas con discapacidad. Excluir de este beneficio a las Mipyme en general restringe injustificadamente la pluralidad de oferentes. Petición concreta: modificar el pliego de condiciones para que el criterio diferencial de número de contratos (hasta cuatro o cinco, en lugar de tres) se extienda también a los proponentes que acrediten únicamente la condición de Mipyme domiciliada en Colombia, en las mismas condiciones de valor (72 SMMLV).	Remitirse al documento de respuestas jurídicas.

57(1) 5934020 - Fax: 57 (1) 5934027
fcm@fcm.org.co - contacto@fcm.org.co www.fcm.org.co
Cra7. N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica
Federación Colombiana de Municipios @Fedemunicipios Federación Colombiana de Municipios

	OBSERVACIÓN 2 — Aclarar la referencia a "212 SMMLV" y la variable sin diligenciar en los criterios diferenciales Numeral observado: en el capítulo "I. CAPACIDAD JURÍDICA – DOCUMENTOS JURÍDICOS HABILITANTES", numeral "Criterios Diferenciales de Experiencia del Proponente Relacionada en el RUP", se lee textualmente: "...estos actores podrán cumplir con la experiencia habilitante a través de la acreditación de máximo (X) contratos que cumplan con las condiciones antes señaladas, cuya sumatoria sea igual o superior al cien por ciento (100%) del presupuesto oficial, expresado en salarios mínimos legales mensuales vigentes, es decir, 212 S.M.M.L.V." Fundamento: esta cifra de 212 SMMLV no corresponde al presupuesto oficial del presente proceso ($124.846.243, equivalente a aproximadamente 71,3 SMMLV 2026), y la variable "(X)" del número de contratos quedó sin diligenciar. Esta imprecisión genera incertidumbre sobre cuál es la regla realmente aplicable —si esta, o la de 72 SMMLV establecida más adelante en el capítulo de "Condiciones de Experiencia / Capacidad Técnica"—, en detrimento de la transparencia y la selección objetiva. Petición concreta: aclarar o corregir esta sección, confirmando expresamente que la sumatoria mínima exigible para los criterios diferenciales es de 72 SMMLV, y precisar el número máximo de contratos aplicable a cada categoría diferencial, eliminando la referencia a "212 SMMLV" en caso de tratarse de un remanente de otro proceso.	Remitirse al documento de respuestas jurídicas.
	OBSERVACIÓN 3 — Aclarar el nivel de exigencia de los códigos UNSPSC (tercer nivel vs. nivel de producto) Numeral observado: la tabla de "Condiciones de Experiencia / Capacidad Técnica" está encabezada como "N° del código hasta el 3 nivel", pero incluye los códigos 81111801 y 81141801, que corresponden en realidad al cuarto nivel (producto) de la clasificación UNSPSC, y no al tercer nivel (clase), como sí ocurre con los códigos 81111800 y 81112208 de la misma tabla. Fundamento: el Registro Único de Proponentes (RUP) certifica la experiencia únicamente a nivel de clase (tercer nivel). Exigir de facto un nivel de producto en dos de los cuatro códigos habilitantes puede generar el rechazo indebido de proponentes cuyo RUP no desagregue la información hasta ese nivel, en contravía de la verificación objetiva de requisitos habilitantes prevista en el artículo 6 de la Ley 1150 de 2007. Petición concreta: confirmar que, para efectos de este proceso, basta la coincidencia a nivel de clase (tercer nivel, es decir, 811118, 811122 o 811418) respecto de los cuatro códigos de la tabla, ajustando la redacción de los códigos 81111801 y 81141801 a su nivel de clase correspondiente (811118 y 811418). Agradecemos su atención y quedamos pendientes de la respuesta a estas observaciones dentro del término dispuesto en el cronograma del proceso.	Al validar la observación presentada, NO SE ACEPTA. Se aclara que el código UNSPSC 81111801 – Servicios de administración y seguridad de sistemas de información (incluye pruebas de vulnerabilidad y hacking ético) guarda relación directa con las actividades y el objeto del proceso a contratar, particularmente en lo referente a servicios especializados de seguridad de la información y pruebas de seguridad. No obstante, con el propósito de garantizar la pluralidad y participación de oferentes, la Entidad ha contemplado códigos adicionales que permiten ampliar el universo de posibles proponentes que puedan acreditar su experiencia relacionada con el objeto contractual. La inclusión de estos códigos no implica que se prescinda de la verificación de la experiencia requerida. Por el contrario, los proponentes deberán acreditar mediante los contratos aportados la experiencia específica y relacionada con las actividades objeto del proceso, de manera que la Entidad pueda verificar que cuentan con la capacidad técnica y experiencia necesaria para

		ejecutar las obligaciones contractuales. Es importante tener en cuenta que basta la coincidencia a nivel de clase (tercer nivel, es decir, 811118, 811122 o 811418) respecto de los cuatro códigos de la tabla. Como un contrato puede registrarse con diferentes códigos en el RUP, independente de su objeto, la entidad amplía la cantidad de los mismos, así como que estos apunten a diferentes denominaciones que pueden estar relacionadas con el ramo de la Ciberseguridad. No obstante, sí se precisa que, como se menciona en el pliego, los contratos aportados prueben, en su objeto, obligaciones o anexos técnicos, que en su ejecución se realizaron actividades de hacking ético o análisis de vulnerabilidades. Toda vez que esto es lo propio del objeto a contratar.
IN TECH SAS	**Observación 1:** Se solicita aclarar la forma de pago y establecer de manera expresa la correspondencia entre cada pago previsto en el contrato y los entregables que deberán ser presentados y recibidos a satisfacción para habilitar su respectiva facturación.	Al validar la observación presentada, SE ACLARA, que El valor del contrato será pagado en dos pagos iguales, él primero una vez se haya recibido el plan de trabajo en su totalidad de las pruebas de hacking ético y el segundo una vez se hagan las entregas de los análisis de vulnerabilidades sobre los servicios internos y servicios publicados en Internet definidos en el alcance contractual.
	Observación 2: solicitamos a la entidad aclarar si la acreditación de los perfiles correspondientes al personal mínimo requerido constituye un requisito habilitante que deba ser demostrado con la presentación de la oferta, o si el requisito es únicamente para el futuro contratista.	La entidad ACLARA que sí es un requisito habilitante, por tanto, deberá acreditarse al momento de presentación de la oferta.
	Observación 3: se solicita a la entidad indicar cuales son las cantidades mínimas previstas para cada modalidad de prueba requerida, ya que para la asignación de puntaje podrán ser ofrecidas por los proponentes, hasta un máximo de cincuenta (50) pruebas adicionales. Lo anterior con el propósito de garantizar que los ofrecimientos sean presentados y evaluados bajo condiciones uniformes.	Al validar la observación presentada, SE ACLARA que las pruebas corresponden a las actividades descritas en la "Descripción y Justificación de la

		Necesidad" de la Ficha técnica, ítem 1, relacionadas con la ejecución de pruebas de Ingeniería Social externas dirigidas al personal de la Federación Colombiana de Municipios, en el marco de la función pública asignada, detallándose que deben ser correspondientes a 200 usuarios. Así las cosas, el criterio puntuable se refiere a 50 pruebas adicionales de *Phishing*.
	Observación 4: Frente al requisito que establece la presentación de un certificado de homologación CVE emitido por MITRE, consideramos necesario revisar la forma en que se encuentra planteada esta exigencia. El estándar CVE tiene como finalidad proporcionar identificadores únicos para vulnerabilidades de seguridad conocidas, por lo que su función está asociada a la identificación y consulta de vulnerabilidades, y no a la certificación o acreditación de las herramientas empleadas para efectuar pruebas de seguridad. exigir un supuesto certificado de homologación de la herramienta podría generar una condición de difícil cumplimiento y limitar innecesariamente la participación de tecnologías que, aun siendo técnicamente idóneas, utilizan y reportan identificadores CVE de manera válida. solicitamos que el requisito sea ajustado para que la validación se concentre en los resultados obtenidos durante las pruebas y en la posibilidad de comprobar los identificadores CVE asociados a los hallazgos, garantizando así que la condición sea objetiva, verificable y aplicable independientemente del fabricante de la herramienta.	Al validar la observación, se ACEPTA, y esta serán tenidas en cuenta y se verán reflejadas en la ficha técnica y en los documentos definitivo. Así: Para la realización de esta prueba, se deben usar las herramientas pertinentes y usadas para el desarrollo de las pruebas de penetración, que referencien los hallazgos mediante identificadores CVE (Common Vulnerabilities and Exposures), conforme a www.mitre.org, y deben estar actualizadas a la fecha de su utilización. Para lo anterior, se deberá adjuntar en los informes presentados la referenciación CVE de cada hallazgo, o la ruta de la página de CVE donde se pueda evidenciar el identificador reportado por la herramienta ofrecida. La herramienta deberá permitir la generación de los informes y entregables solicitados de manera automática, sin límite en el número de generaciones ni costo adicional durante el plazo de ejecución del contrato.

	Observación 5: las actividades de remediación pueden involucrar modificaciones sobre servidores, aplicaciones, dispositivos de red, configuraciones de seguridad y demás componentes de la infraestructura tecnológica. La intervención directa de terceros sobre estos elementos podría generar impactos no previstos sobre la disponibilidad o continuidad de los servicios que se encuentren en operación es por esto que solicitamos que las actividades de remediación sean ejecutadas por el personal autorizado de la Entidad, contando con el acompañamiento y la orientación técnica del contratista. solicitamos que se ajuste el alcance previsto para los ciclos de *test* y *retest*, y lego de los hallazgos identificados durante el análisis de vulnerabilidades, el proponente realice el acompañamiento y asesoría técnica a personal designado por la Entidad para la implementación de las acciones de remediación. Las modificaciones sobre la infraestructura tecnológica serán efectuadas por la Entidad, de acuerdo con sus procedimientos internos de gestión de cambios y control de ambientes productivos. Posteriormente, el proponente realizará el respectivo retest sobre las cien (100) direcciones IP objeto del alcance, con el propósito de verificar la efectividad de las medidas implementadas	Al validar la observación, NO SE ACEPTA, toda vez que el presente proceso y el futuro contrato corresponden a la prestación de un servicio, y no a un servicio de consultoría. La Entidad agradece la recomendación orientada al fortalecimiento y seguimiento de las actividades previstas en la ficha técnica; sin embargo, dicha actividad no se encuentra contemplada dentro del alcance del presente requerimiento, por lo cual no resulta procedente su incorporación al objeto y alcance contractual. En consecuencia, se mantienen las condiciones y actividades establecidas en los documentos del proceso.
	Observación 6: Respecto de la exigencia mediante la cual se solicita acreditar, a través de certificación o documento expedido por el fabricante, la propiedad o autorización expresa para utilizar las herramientas destinadas a la ejecución de las actividades, pedimos que sea exigible únicamente, que las herramientas dispuestas por el proponente para la ejecución de las actividades se encuentren disponibles durante el plazo de ejecución del contrato y cuenten con las funcionalidades necesarias para realizar las pruebas requeridas, así como para generar de manera automática los informes y entregables establecidos por la Entidad, sin restricciones respecto del número de generaciones y sin que se genere un costo adicional para el contrato.	Al validar la observación, se **ACEPTA**, en la medida en que el futuro contratista podrá utilizar plataformas o herramienta licenciadas u *Open source.* Por lo tanto, esta modificación se verá reflejada en la ficha técnica y en los documentos definitivos, quedando de la siguiente manera: *La herramienta deberá permitir la generación de los informes y entregables solicitados de manera automática, sin límite en el número de generaciones ni costo adicional durante el plazo de ejecución del contrato. Sin importar si es una plataforma licenciada o de uso libre.*
	Observación 7: Respecto de la exigencia mediante la cual se solicita acreditar, a través de certificación o documento expedido por el fabricante, la propiedad o autorización expresa para utilizar las herramientas destinadas a la ejecución de las actividades, pedimos que sea exigible únicamente, que las herramientas dispuestas por el proponente para la ejecución de las actividades se encuentren disponibles durante el plazo de ejecución del contrato y cuenten con las funcionalidades necesarias para realizar las pruebas requeridas, así como para generar de manera automática los informes y entregables establecidos por la Entidad, sin restricciones respecto del número de generaciones y sin que se genere un costo adicional para el contrato.	Al validar la observación, se **ACEPTA**, en la medida en que el futuro contratista podrá utilizar plataformas o herramienta licenciadas u *Open source.* Por lo tanto, esta modificación se verá reflejada en la ficha técnica y en

		los documentos definitivos, quedando de la siguiente manera: *La herramienta deberá permitir la generación de los informes y entregables solicitados de manera automática, sin límite en el número de generaciones ni costo adicional durante el plazo de ejecución del contrato. Sin importar si es una plataforma licenciada o de uso libre.*
	Observación 8: Considerando que las actividades de *ethical hacking* generarán información durante las diferentes etapas de ejecución del contrato, se considera conveniente que la Entidad cuente con un mecanismo que permita consolidar y consultar esta información de manera organizada y permanente. Por lo que se sugiere a la entidad solicitar a los oferentes que el servicio deba: disponer de una plataforma SaaS especializada en Ethical hacking que permita centralizar y consultar la información asociada a las actividades ejecutadas, metodología, hoja de ruta del servicio, avance de los procedimientos, resultados, vulnerabilidades identificadas, informes, entregables y actualizaciones. La información deberá encontrarse disponible para consulta en línea durante la ejecución del contrato y la plataforma deberá permitir el acceso de un número ilimitado de usuarios autorizados por la Entidad."	Al validar la observación presentada **NO SE ACEPTA**, toda vez que la consideración de esta plataforma no tiene incidencia directa en la ejecución del objeto contractual. Entonces, requerirla sería afecta la pluralidad de oferentes. No obstante, se aclara que, si el proponente cuenta con una plataforma centralizada que permita consultar y visualizar los entregables requeridos, se podrá aceptar dicho mecanismo **como medio de entrega**, siempre que garantice su disponibilidad, integridad y trazabilidad. En este sentido, se precisa que la disposición de este mecanismo de entrega no constituye una condición habilitante ni un requisito que determine la participación o no de un proponente en el proceso. **PERO POR NINGÚN MOTIVO LA PLATAFORMA, HERRAMIENTA O SOLUCIÓN, REEMPLAZARÁ LOS SERVICIOS REQUERIDOS EN LA NECESIDAD DE LA ENTIDAD. ES DECIR, EL FUTURO CONTRATO SERÁ DE UNA PRESTACIÓN DE SERVICIOS, Y NO LA COMPRAVENTA DE UN LICENCIAMIENTO PARA EL USO DE ESTAS SOLUCIONES.**

57(1) 5934020 - Fax: 57 (1) 5934027
fcm@fcm.org.co - contacto@fcm.org.co www.fcm.org.co
Cra7. N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica
Federación Colombiana de Municipios @Fedemunicipios Federación Colombiana de Municipios

	Observación 9: Respecto del factor de evaluación mediante el cual se asignan diez (10) puntos por las recomendaciones adicionales de hardening, solicitamos a la Entidad precisar cuál será el mecanismo utilizado para verificar el cumplimiento de este criterio y determinar la asignación del puntaje. Esto es crítico ya que solo existe la posibilidad de obtener el puntaje cumpliendo desde la presentación de la oferta ya que no es subsanable.	Al validar la observación, se ACLARA, que, los 50 corresponden cantidad de funcionarios adicionales a los solicitados en las pruebas iniciales, que según la ficha corresponden a los 200 usuarios descritos en la justificación de la necesidad. ítem 1 Pruebas de Ingeniería Social externas dirigidas al personal de la Federación Colombiana de Municipios en cumplimiento de la función pública asignada.
	Observación 10: se recomienda a la entidad incorporar el requisito para que las pruebas de Ingeniería Social no se gestionen únicamente mediante informes aislados si no que se pida a los oferentes que el servicio cuente con una plataforma SaaS especializada para la ejecución y administración de campañas de Ingeniería Social, que permita configurar, programar y realizar seguimiento de las pruebas efectuadas. La solución deberá registrar, como mínimo, los eventos asociados a la entrega del ejercicio, apertura, interacción con el contenido o vector utilizado y eventual suministro de credenciales, cuando corresponda. Asimismo, deberá conservar el histórico de las campañas realizadas y permitir comparar los resultados obtenidos por los usuarios en las diferentes pruebas, con el propósito de identificar comportamientos recurrentes o reincidencias durante la ejecución del contrato.	Al validar la observación presentada **NO SE ACEPTA**, toda vez que la consideración de esta plataforma no tiene incidencia directa en la ejecución del objeto contractual. Entonces, requerirla sería afecta la pluralidad de oferentes. No obstante, se aclara que, si el proponente cuenta con una plataforma centralizada que permita consultar y visualizar los entregables requeridos, se podrá aceptar dicho mecanismo **como medio de entrega**, siempre que garantice su disponibilidad, integridad y trazabilidad. En este sentido, se precisa que la disposición de este mecanismo de entrega no constituye una condición habilitante ni un requisito que determine la participación o no de un proponente en el proceso. **PERO POR NINGÚN MOTIVO LA PLATAFORMA, HERRAMIENTA O SOLUCIÓN, REEMPLAZARÁ LOS SERVICIOS REQUERIDOS EN LA NECESIDAD DE LA ENTIDAD. ES DECIR, EL FUTURO CONTRATO SERÁ DE UNA PRESTACIÓN DE SERVICIOS, Y NO LA COMPRAVENTA DE UN LICENCIAMIENTO PARA EL USO DE ESTAS SOLUCIONES.**

	Observación 11: Respecto del factor de evaluación mediante el cual se asignan diez (10) puntos por las recomendaciones adicionales de hardening, solicitamos a la Entidad precisar cuál será el mecanismo utilizado para verificar el cumplimiento de este criterio y determinar la asignación del puntaje. Esto es crítico ya que solo existe la posibilidad de obtener el puntaje cumpliendo desde la presentación de la oferta ya que no es subsanable. con el objetivo de evitar que la información quede separada y permitir una gestión uniforme de severidad, clasificación y estado. Solicitamos a la entidad considerar incorporar el requisito que la solución deberá permitir integrar en un repositorio centralizado los hallazgos obtenidos mediante análisis automatizados y aquellos identificados como resultado de pruebas manuales realizadas por los consultores. Para ambos tipos de hallazgos deberá ser posible utilizar criterios comunes de clasificación, valoración de severidad, documentación y gestión de estados, permitiendo realizar su consulta y seguimiento desde un mismo entorno.	La entidad ACLARA que en el Pliego de Condiciones se expresa textualmente cómo debe acreditarse cada uno de los requisitos de puntaje, es decir, a través de una carta en que certifique la cantidad de pruebas adicionales que realizará, de acuerdo con las especificaciones previamente detalladas, junto con los documentos de la ofertas. Por favor remitirse directamente a los factores de evaluación determinados en el pliego. Sin embargo, la entidad ENFATIZA en que el presente proceso NO busca el licenciamiento de uso de una plataforma sino una prestación de servicios, de manera que no es aceptable la presentación de una herramienta para satisfacer la necesidad acá presentada.
	Observación 12: Con el propósito de que los resultados obtenidos durante las actividades de seguridad sean útiles para la toma de decisiones y la definición de las acciones correctivas, solicitamos se exija a los oferentes contar con funcionalidades que permitan clasificar y priorizar las vulnerabilidades identificadas a partir de criterios de riesgo, incluyendo como mínimo la valoración de severidad mediante CVSS y la consideración de indicadores de probabilidad de explotación, tales como EPSS. La plataforma deberá permitir complementar o contrastar dicha información con catálogos y fuentes públicas de vulnerabilidades, con el propósito de facilitar la identificación de aquellos hallazgos que requieran atención prioritaria por parte de la Entidad.	NO SE ACEPTA la observación y la entidad ENFATIZA en que el presente proceso NO busca el licenciamiento de uso de una plataforma sino una prestación de servicios, de manera que no es aceptable la presentación de una herramienta para satisfacer la necesidad acá presentada. Por ello, no puede exigirse ningún tipo de funcionalidad ya que no se está solicitando una plataforma o herramienta.
Multisoftware Transaccional S.A.S	**Observación No. 1:** Respetuosamente solicitamos a la entidad requerir los documentos para la acreditación de experiencia de los perfiles solicitados, únicamente al proponente adjudicatorio. Lo anterior, teniendo en cuenta que dicha documentación contiene información de carácter confidencial y datos personales del talento humano propuesto, cuya divulgación masiva no resulta necesaria para la evaluación inicial de las ofertas. Esta medida permite salvaguardar el derecho a la protección de datos personales, evitar la circulación innecesaria de información sensible y mantener la reserva de la información laboral de los profesionales. Adicionalmente, la verificación detallada de los perfiles puede realizarse de manera efectiva en la etapa previa a la suscripción del contrato, sin afectar la idoneidad del contratista seleccionado ni los principios de transparencia, selección objetiva y pluralidad de oferentes que rigen la contratación pública.	Al validar la observación presentada, NO SE ACEPTA. La Entidad considera necesario que los documentos requeridos para acreditar la formación académica, experiencia y demás requisitos establecidos para los perfiles profesionales sean presentados junto con la propuesta, toda vez que estos constituyen elementos necesarios para verificar desde la etapa de evaluación el cumplimiento de las condiciones técnicas exigidas en el proceso.

		La presentación de dicha documentación permite a la Entidad verificar oportunamente la idoneidad, formación, experiencia y cumplimiento de los requisitos mínimos del equipo de trabajo propuesto, garantizando que la oferta evaluada cuente con el recurso humano requerido para la adecuada ejecución del objeto contractual.
	Observación No. 3: Se solicita amablemente a la entidad ampliar el criterio de acreditación de la formación del personal requerido, permitiendo que los requisitos establecidos puedan ser acreditados mediante certificaciones y/o cursos relacionados con las áreas de conocimiento indicadas en el pliego.	Al validar la observación presentada, NO SE ACEPTA. La Entidad mantiene los requisitos de formación establecidos para los perfiles profesionales, teniendo en cuenta que estos fueron definidos de acuerdo con la naturaleza, complejidad y especialidad de las actividades que serán desarrolladas en el marco del objeto contractual. La exigencia de formación académica busca garantizar que los profesionales asignados al contrato cuenten con una base de conocimientos integral y suficiente para desarrollar las actividades objeto del proceso, particularmente aquellas relacionadas con seguridad de la información, evaluación de vulnerabilidades, pruebas de penetración y demás actividades especializadas contempladas. Adicionalmente, no se están pidiendo requisitos de formación desproporcionados y se está presentando un amplio espectro académico y de formación para su cumplimiento.
	Observación No. 4: Se solicita amablemente a la entidad permitir que las certificaciones exigidas puedan ser acreditadas por diferentes integrantes del equipo de trabajo, sin que necesariamente recaigan en una sola persona, siempre que el equipo propuesto, en su conjunto, demuestre contar con las certificaciones, conocimientos y experiencia requeridos para la correcta ejecución del contrato.	Al validar la observación NO SE ACEPTA, puesto que no se están pidiendo requisitos de formación desproporcionados y se está presentando un amplio espectro académico y de formación para su cumplimiento.

	Observación No. 5: Solicitamos amablemente a la entidad aclarar si los tres (3) ejercicios de Ingeniería Social contemplados para doscientos (200) usuarios corresponden a tres (3) lanzamientos, cada uno dirigido a los 200 usuarios, o si los tres (3) lanzamientos en conjunto deberán cubrir una población total de 200 usuarios, distribuidos entre los diferentes ejercicios.	Al validar la observación, se ACLARA que, los tres (3) ejercicios de Ingeniería Social contemplados para doscientos (200) usuarios corresponden a tres (3) lanzamientos, cada uno dirigido a los 200 usuarios, los tres (3) lanzamientos en conjunto deberán cubrir una población total de 200 usuarios, distribuidos entre los diferentes ejercicios. Entendiendo que Los ejercicios de Ingeniería Social son pruebas controladas que simulan técnicas de manipulación o engaño dirigidas a las personas, con el fin de evaluar su nivel de concienciación y capacidad para identificar y responder ante posibles amenazas de seguridad, como phishing, smishing, vishing o suplantación de identidad, es necesarios hacer como mínimo dos de los 4 que entre en el concepto.
	Observación No. 6: Establecer el valor o porcentaje de cada pago: Solicitamos indicar el porcentaje o valor correspondiente a cada uno de los dos pagos, junto con sus entregables y criterios de aprobación. La redacción actual no permite establecer cuánto se pagará por el plan de trabajo y cuánto quedará condicionado a la entrega final.	Al validar la observación presentada, SE ACLARA, que El valor del contrato será pagado en dos pagos iguales, él primero una vez se haya recibido el plan de trabajo en su totalidad de las pruebas de hacking ético y el segundo una vez se hagan las entregas de los análisis de vulnerabilidades sobre los servicios internos y servicios publicados en Internet definidos en el alcance contractual.
	Observación No. 7: Garantizar dos meses efectivos de ejecución: Solicitamos confirmar que el contratista dispondrá de dos meses completos desde el cumplimiento de los requisitos de ejecución. La fecha límite del 27 de diciembre de 2026 podría reducir el plazo si existen demoras en la firma, aprobación de garantías, entrega de accesos o autorización de las pruebas.	Remitirse al documento de respuestas jurídicas.
	Observación No. 8: Definir el plazo para aprobar los entregables: Solicitamos establecer un plazo máximo para que el supervisor revise y apruebe cada entregable. Las demoras de la Entidad en emitir observaciones o aprobaciones deberían ampliar proporcionalmente el cronograma de ejecución y pago.	Al validar la observación, se ACLARA que, plazo máximo para que el supervisor revise y apruebe cada entregable no debe será superior a 5 días hábiles.

	Observación No. 9: Aclarar la base de comparación económica: Solicitamos confirmar si las ofertas se compararán sobre el valor total incluido IVA o sobre el valor antes de IVA. Esta precisión es necesaria para asegurar un tratamiento comparable entre oferentes con diferentes responsabilidades tributarias.	SE ACLARA que, como dice claramente el Pliego de Condiciones, las ofertas deberán ser presentadas incluyendo todos los impuestos a que haya lugar y será sobre ese valor que se comparen las ofertas económicas. En otras palabras, se entenderá que el valor presentado por el proponente INCLUYE todos los impuestos.
SOFTESTING	**OBSERVACIÓN No. 1 – Listado de precios de herramientas para análisis de vulnerabilidades e Ethical Hacking** De acuerdo con el alcance técnico establecido en el Proyecto de Pliego, el contratista deberá ejecutar actividades de análisis de vulnerabilidades, Ethical Hacking, Pen Testing e Ingeniería Social, sobre los activos, aplicaciones, direcciones IP y usuarios definidos por la Entidad. Adicionalmente, dentro del Plan de Trabajo y Plan de Pruebas se exige especificar, entre otros aspectos, las herramientas a utilizar. Así mismo, la Entidad establece la ejecución de dos (2) ciclos completos de pruebas (test y retest) para los análisis de vulnerabilidades y Ethical Hacking, sobre un alcance de 100 direcciones IP, correspondientes a 50 IP privadas y 50 IP públicas. En consideración a que la ejecución de estas actividades requiere herramientas y licenciamientos especializados, resulta indispensable que los proponentes cuenten con información suficiente para dimensionar objetivamente los costos asociados a dichas soluciones dentro de la oferta económica. Por lo anterior, solicitamos a la Entidad suministrar el listado detallado de las herramientas, soluciones y/o licenciamientos contemplados para la ejecución de las actividades de análisis de vulnerabilidades y Ethical Hacking, incluyendo, de ser aplicable, las soluciones comercializadas por WhIP Solutions, junto con sus respectivos precios o valores de referencia. La información deberá permitir identificar, como mínimo, el nombre de la herramienta o solución, alcance, modalidad de licenciamiento, cantidad requerida, vigencia y valor o presupuesto estimado, así como indicar expresamente si estos costos deben ser asumidos por el contratista e incluidos dentro de su oferta económica. Esta información es necesaria para garantizar que todos los proponentes puedan estructurar sus ofertas bajo condiciones económicas comparables, objetivas y técnicamente dimensionadas, evitando que la ausencia de información sobre los costos de herramientas y licenciamientos genere diferencias significativas en la estructuración de las propuestas o afecte la adecuada ejecución del objeto contractual. **Solicitud a la Entidad:** Solicitamos a la Entidad suministrar el listado y valores de referencia de las herramientas y licenciamientos requeridos para la ejecución de las pruebas objeto del proceso, indicando expresamente cuáles de estos costos deberán ser incluidos por los proponentes dentro de sus ofertas económicas.	Al validar la observación, se **ACEPTA**, en la medida en que el futuro contratista podrá utilizar plataformas o herramienta licenciadas u *Open source.* Por lo tanto, esta modificación se verá reflejada en la ficha técnica y en los documentos definitivos, quedando de la siguiente manera: *La herramienta deberá permitir la generación de los informes y entregables solicitados de manera automática, sin límite en el número de generaciones ni costo adicional durante el plazo de ejecución del contrato. Sin importar si es una plataforma licenciada o de uso libre.*

	OBSERVACIÓN No. 2 - Inclusión de la Certificación CEH – Certified Ethical Hacker En el apartado correspondiente a Documentos Técnicos Adicionales, la Entidad establece que el contratista deberá contar con al menos una persona con formación profesional en áreas relacionadas con ingeniería y que deberá acreditar como mínimo dos (2) certificaciones de un listado determinado. Dentro de las certificaciones contempladas se encuentran CISSP, CRISC, CCNP, Web Application Scanner, Vulnerability Management Detection and Response, Cloud Security Specialist y Auditor ISO 27001:2022, entre otras. No obstante, el objeto contractual está orientado específicamente a la ejecución de pruebas de hacking ético y análisis de vulnerabilidades, y dentro de las obligaciones específicas del contratista se establece expresamente la ejecución de actividades de Ethical Hacking y Pen Testing. Adicionalmente, la Entidad exige que la experiencia del proponente se encuentre relacionada directamente con procesos de Ethical Hacking y análisis de vulnerabilidades, lo que evidencia que estas competencias constituyen el núcleo técnico del objeto contractual. En este sentido, resulta necesario que el requisito de certificaciones del personal mantenga una relación directa con las actividades técnicas que efectivamente serán ejecutadas durante el contrato. Por lo anterior, solicitamos a la Entidad incluir expresamente la certificación CEH – Certified Ethical Hacker dentro del listado de certificaciones válidas para acreditar la idoneidad del profesional requerido. La inclusión de esta certificación resulta técnicamente pertinente frente al objeto del proceso, toda vez que permite acreditar conocimientos especializados directamente relacionados con actividades de Ethical Hacking, identificación y evaluación de vulnerabilidades y pruebas de seguridad, que hacen parte integral del alcance contractual. Asimismo, su inclusión permitiría que el requisito de capacidad técnica se encuentre debidamente alineado con el objeto, las obligaciones y las actividades que deberá desarrollar el contratista, garantizando a su vez una mayor concurrencia de profesionales que cuentan con certificaciones especializadas en seguridad ofensiva. **Solicitud a la Entidad:** La Entidad deberá modificar el apartado correspondiente a los Documentos Técnicos Adicionales e incluir expresamente la certificación CEH – Certified Ethical Hacker como certificación válida para acreditar la idoneidad del profesional requerido.	Al validar la observación presentada, SE ACEPTA. En consecuencia, el ajuste correspondiente será incorporado en los documentos definitivos del proceso. Se precisa que esta observación fue presentada por el proponente CROSSBORDER observación #1. Para mayor claridad sobre el alcance de la modificación y su aplicación, se recomienda remitirse a la respuesta emitida a dicha observación.
SSE S.A.S	**1. Observación sobre el perfil del personal requerido (Página 46 del Proyecto de Pliego)** En el documento se establece como requisito que el profesional responsable cuente con al menos dos (2) certificaciones entre las siguientes: CISSP, CRISC, CCNP, certificaciones en Web Application Scanner, Vulnerability Management Detection and Response, administración de firewall, Cloud Security y Auditor ISO/IEC 27001:2022. Tratándose de un contrato cuyo objeto es la ejecución de pruebas de hacking ético y análisis de vulnerabilidades, respetuosamente solicito considerar la inclusión de la certificación: **CEH – Certified Ethical Hacker (EC-Council):** Esta certificación es reconocida internacionalmente como estándar para profesionales en pruebas de penetración, y es requerida en múltiples marcos de referencia globales, incluyendo EC-Council, DoD 8570, y el NICE Cybersecurity Workforce Framework. Su incorporación resulta plenamente coherente con el alcance	Al validar la observación presentada, SE ACEPTA PARCIALMNETE. En consecuencia, el ajuste correspondiente será incorporado en los documentos definitivos del proceso. Se precisa que esta observación respecto a la solicitud de las certificaciones remítase a las respuesta CROSSBORDER observación #1 y SOFTESTING

57(1) 5934020 - Fax: 57 (1) 5934027
fcm@fcm.org.co - contacto@fcm.org.co www.fcm.org.co
Cra7. N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica
Federación Colombiana de Municipios @Fedemunicipios Federación Colombiana de Municipios

	técnico del proceso y con las actividades de intrusión controlada previstas en el pliego. Adicionalmente, sugiero considerar como válidos posgrados directamente relacionados con el objeto contractual, tales como: 1. Especialización en Seguridad de la Información 2. Especialización en Seguridad Informática 3. Especialización o Maestría en Ciberseguridad Estos programas académicos aportan competencias avanzadas en gestión y ejecución de pruebas de seguridad, fortaleciendo la idoneidad del personal técnico que participará en el proyecto.	observación 2. Para mayor claridad sobre el alcance de la modificación y su aplicación, se recomienda remitirse a la respuesta emitida a dichas observaciones. con respecto a la solicitud de considerar los títulos de posgrado como equivalentes a las certificaciones requeridas, NO SE ACEPTA. lo anterior, teniendo en cuenta que un posgrado corresponde a una formación académica formal y de profundización, mientras que las certificaciones relacionadas con estándares, metodologías o competencias específicas acreditan conocimientos y habilidades particulares en un ámbito determinado requerido para la ejecución de este contrato. en consecuencia, los requisitos de formación académica y las certificaciones profesionales se consideran de naturaleza diferente y, por tanto, no son equivalentes ni sustituibles entre sí, de acuerdo con las necesidades técnicas y el objeto del proceso.
	2. Observación sobre la formulación de la propuesta económica El pliego indica: *"Al formular la oferta económica el proponente deberá tener en cuenta las condiciones y especificaciones de los elementos vender y las propias del sitio y la región donde el mismo se desarrollará."* Respetuosamente solicito aclarar el alcance de esta instrucción, en razón a que el objeto del contrato corresponde a la ejecución de pruebas de seguridad sobre infraestructura tecnológica, actividades que —según el mismo pliego— se desarrollan de manera remota, sin requerir desplazamientos físicos, logística regional o costos asociados a condiciones del sitio. La aclaración permitirá garantizar uniformidad en la elaboración de las propuestas económicas y evitar interpretaciones divergentes entre los oferentes. Agradezco la atención prestada y quedo atenta a las aclaraciones que la Entidad considere pertinentes.	Remitirse al documento de respuestas jurídicas.

57(1) 5934020 - Fax: 57 (1) 5934027
fcm@fcm.org.co - contacto@fcm.org.co www.fcm.org.co
Cra7. N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica
Federación Colombiana de Municipios @Fedemunicipios Federación Colombiana de Municipios

STRATECH	**1. Consideración técnica** Desde el punto de vista técnico, consideramos adecuado que los resultados del análisis de vulnerabilidades tengan como referencia el estándar CVE (Common Vulnerabilities and Exposures) administrado dentro del programa CVE, permitiendo una identificación, clasificación y trazabilidad homogénea de las vulnerabilidades encontradas. No obstante, consideramos que exigir que el proponente demuestre necesariamente la propiedad o una autorización de uso explícita emitida por el fabricante de cada herramienta utilizada puede resultar técnicamente restrictivo y no constituye, por sí mismo, un elemento determinante para demostrar la capacidad técnica del proponente para ejecutar correctamente un análisis de vulnerabilidades. El resultado de un ejercicio de análisis de vulnerabilidades depende principalmente de factores como: 1. La experiencia y competencias del equipo profesional que ejecutará las pruebas. 2. La metodología utilizada para la identificación, validación, clasificación y reporte de vulnerabilidades. 3. La capacidad técnica para realizar análisis automatizados y manuales. 4. La utilización de herramientas especializadas, comerciales, libres, de código abierto o desarrolladas internamente, siempre que su uso sea legítimo. 5. La capacidad de correlacionar los hallazgos con identificadores CVE cuando estos existan. 6. La validación técnica de falsos positivos y falsos negativos. 7. La capacidad para generar informes técnicos y ejecutivos trazables, reproducibles y técnicamente sustentados. En consecuencia, la herramienta constituye un medio para ejecutar el servicio, mientras que la competencia técnica, metodología, experiencia y capacidad del equipo constituyen elementos esenciales para acreditar la idoneidad del proponente. Adicionalmente, existen múltiples herramientas de seguridad informática que permiten realizar análisis de vulnerabilidades en modalidad caja blanca y caja negra y cuya información puede ser correlacionada con CVE, incluyendo soluciones comerciales, herramientas de código abierto y herramientas desarrolladas o integradas por los propios proveedores de servicios de ciberseguridad. Por lo anterior, condicionar la participación a que el fabricante de la herramienta expida una certificación o autorización expresa puede generar una situación en la cual el cumplimiento de un requisito del proceso dependa de la decisión comercial o administrativa de un tercero ajeno al proponente.	Al validar la observación, se ACEPTA, y esta serán tenidas en cuenta y se verán reflejadas en la ficha técnica y en los documentos definitivo. Así: Para la realización de esta prueba, se deben usar las herramientas pertinentes y usadas para el desarrollo de las pruebas de penetración, que referencien los hallazgos mediante identificadores CVE (Common Vulnerabilities and Exposures), conforme a www.mitre.org, y deben estar actualizadas a la fecha de su utilización. Para lo anterior, se deberá adjuntar en los informes presentados la referenciación CVE de cada hallazgo, o la ruta de la página de CVE donde se pueda evidenciar el identificador reportado por la herramienta ofrecida. La herramienta deberá permitir la generación de los informes y entregables solicitados de manera automática, sin límite en el número de generaciones ni costo adicional durante el plazo de ejecución del contrato.
	2. Consideración jurídica Desde la perspectiva de la contratación estatal, consideramos importante que las condiciones técnicas del proceso se encuentren orientadas a garantizar la pluralidad de oferentes, la libre concurrencia, la selección objetiva, la igualdad de oportunidades y la participación de empresas de diferentes tamaños, evitando requisitos que puedan constituir barreras de acceso que no resulten indispensables para satisfacer la necesidad que pretende contratar la entidad. La exigencia de una autorización expresa del fabricante podría generar una restricción indirecta de la competencia, particularmente para pequeñas y medianas empresas especializadas en ciberseguridad que cuentan con personal certificado, experiencia comprobable, metodologías propias y capacidad técnica suficiente para ejecutar el servicio, pero que utilizan diferentes herramientas tecnológicas dependiendo de la naturaleza del activo, alcance y metodología de evaluación. En este sentido, consideramos que la capacidad del proponente debería poder acreditarse mediante mecanismos objetivos y verificables, tales como: 1. Certificaciones y hojas de vida del personal especializado. 2. Experiencia específica en análisis de vulnerabilidades, ethical hacking o pruebas de seguridad. 3. Certificaciones profesionales en ciberseguridad. 4. Metodología de análisis y evaluación de vulnerabilidades. 5. Evidencia de la capacidad técnica y operativa. 6. Descripción de las herramientas que serán utilizadas. 7. Licenciamiento legítimo cuando la herramienta comercial así lo requiera. 8. Informes o entregables de ejercicios anteriores, cuando jurídicamente sea posible aportarlos. 9. Procedimientos para identificación, validación, clasificación y tratamiento de vulnerabilidades. 10. Capacidad para identificar y reportar vulnerabilidades mediante identificadores CVE cuando corresponda.	Al validar la observación presentada, SE ACEPTA PARCIALMENTE, en la medida en que el futuro contratista podrá utilizar plataformas o herramienta licenciadas u *Open source.* Por lo tanto, esta modificación se verá reflejada en la ficha técnica y en los documentos definitivos, quedando de la siguiente manera: *La herramienta deberá permitir la generación de los informes y entregables solicitados de manera automática, sin límite en el número de generaciones ni costo adicional durante el plazo de ejecución del contrato. Sin importar si es una plataforma licenciada o de uso libre.*

	De esta manera, se garantizaría que la entidad pueda verificar efectivamente la idoneidad, capacidad y legalidad del servicio, sin hacer depender la participación de una certificación expedida por un fabricante específico.	Por otra parte, los documentos y requisitos relacionados con el profesional que hará parte del equipo de trabajo deberán ser presentados y acreditados junto con la propuesta, de acuerdo con las condiciones establecidas en los documentos del proceso. Esto significa que, la entidad NO ACEPTARÁ, homologaciones o propuestas alternativas en este o en ningún otro ítem.
	OBSERVACIÓN No. 2 AL ANEXO TÉCNICO – IDONEIDAD DEL PERSONAL TÉCNICO MÍNIMO REQUERIDO **Web Site: www.stratech.com.co E-Mail: ventas@stratech.com.co** **Visítenos: Carrera 100 # 23 H 22 Oficina 401 – Bogotá Colombia** **NIT 901.117.326-8** **Régimen común.** STRATECH **Asunto:** Solicitud de inclusión de la certificación Certified Ethical Hacker (CEH) dentro de las opciones válidas para el equipo de trabajo. **Consideración técnica y solicitud:** En el apartado correspondiente a Documentos Técnicos Adicionales, la Entidad enlista una serie de certificaciones admitidas para acreditar la idoneidad del ingeniero propuesto (tales como CISSP, CRISC, CCNP, entre otras). Teniendo en cuenta que el objeto principal del presente proceso de selección es la *"ejecución de pruebas de hacking ético y análisis de vulnerabilidades"*, solicitamos a la Entidad modificar el pliego de condiciones e incluir expresamente la certificación **CEH – Certified Ethical Hacker** como certificación válida para acreditar la idoneidad del profesional requerido. Esta credencial representa un estándar global de la industria, diseñado específica y exclusivamente para validar las competencias prácticas y teóricas en la ejecución de pruebas de intrusión y auditorías de seguridad ofensiva, por lo cual guarda absoluta pertinencia y estricta proporcionalidad con las actividades que el profesional deberá desarrollar durante la ejecución del contrato. Su inclusión garantizará una mayor pluralidad de oferentes altamente calificados en la materia.	Al validar la observación, se ACEPTA, y esta serán tenidas en cuenta y se verán reflejadas en la ficha técnica y en los documentos definitivo.

57(1) 5934020 - Fax: 57 (1) 5934027
fcm@fcm.org.co - contacto@fcm.org.co www.fcm.org.co
Cra7. N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica
Federación Colombiana de Municipios @Fedemunicipios Federación Colombiana de Municipios

STS S.A.S	**OBSERVACIÓN 1** El pliego de condiciones solicita el siguiente perfil, Respetados señores: Estructurar un equipo de trabajo idóneo y perfectamente alineado con el objeto del contrato resulta determinante para contar con profesionales en ingeniería con la experiencia y especialización técnica requeridas para garantizar el éxito del proyecto. En las especificaciones del personal mínimo requerido se solicitan certificaciones de carácter general o administrativo (como administración de equipos de red, firewalls o auditoría de cumplimiento), las cuales no se corresponden de forma directa con la naturaleza operativa y especializada de la pruebas de *Ethical Hacking*, análisis de vulnerabilidades e ingeniería social requeridas por la Federación. Contar con personal con perfiles más idóneos e idénticos al alcance real de las actividades evitará deficiencias en la profundidad técnica de las evaluaciones y asegurará la entrega de hallazgos y remediaciones de alto valor para la seguridad de la Entidad. Por lo anterior, **solicitamos respetuosamente reestructurar y ajustar las exigencias de perfil y certificaciones del personal mínimo**, orientándolas hacia certificaciones y competencias focalizadas estrictamente en ciberseguridad ofensiva, pruebas de penetración y evaluación de vulnerabilidades. Esto permitirá a la Entidad contar con el equipo verdaderamente capacitado y adecuado para cumplir a cabalidad con los objetivos del contrato.	Al validar la observación, se ACEPTA, y esta serán tenidas en cuenta y se verán reflejadas en la ficha técnica y en los documentos definitivo. Donde se ajustará orientándolas hacia certificaciones y competencias focalizadas estrictamente en ciberseguridad ofensiva, eliminado: 1. Certificación en ejecución y/o administración de firewall en fábricas de ciberseguridad. 2. Certificación CCNP (Cisco Certified Network Professional). Quedando así: - Certificación a nivel profesional en seguridad de sistemas de información (CISSP) - Certificación en control de riesgos y sistemas de información (CRISC) - Certificación en Web Application Scanner - Certificación en Vulnerability Management Detección and Response - Certified Ethical Hacker (CEH) (Obligatoria) - Computer Hacking Forensic Investigator - Certificación OSCP Offensive Security Certified Professional
	OBSERVACIÓN 2 Requerimiento de certificación solicitado por la entidad. • Certificación CCNP (Cisco Certified Network Professional) Solicitamos muy respetuosamente a la entidad eliminar las certificaciones de Certificación CCNP (Cisco Certified Network Professional) teniendo en cuenta que esta certificación valida destrezas para diseñar, implementar, auditar rutas BGP/OSPF, conmutación (Switches), arquitectura de datos, SD-WAN y resolver problemas de conectividad/operatividad de redes corporativas. El contrato exige evaluar la seguridad lógica, vulnerabilidades e intrusión en sistemas, aplicaciones y activos. Saber configurar enrutamiento dinámico o administradores de red no prueba de ninguna manera que el profesional sepa ejecutar ataques de intrusión, evadir controles de ciberseguridad, analizar código o auditar vulnerabilidades lógicas, esta no es una certificación que apoye el objeto y las condiciones de la ficha técnica publicada.	Al validar la observación, se ACEPTA, y esta serán tenidas en cuenta y se verán reflejadas en la ficha técnica y en los documentos definitivo. Donde se ajustará orientándolas hacia certificaciones y competencias focalizadas estrictamente en ciberseguridad ofensiva, eliminado: 1. Certificación CCNP (Cisco Certified Network Professional). Quedando así:

57(1) 5934020 - Fax: 57 (1) 5934027
fcm@fcm.org.co - contacto@fcm.org.co www.fcm.org.co
Cra7. N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica
Federación Colombiana de Municipios @Fedemunicipios Federación Colombiana de Municipios

		- Quedando así: - Certificación a nivel profesional en seguridad de sistemas de información (CISSP) - Certificación en control de riesgos y sistemas de información (CRISC) - Certificación en Web Application Scanner - Certificación en Vulnerability Management Detección and Response - Certified Ethical Hacker (CEH) (Obligatoria) - Computer Hacking Forensic Investigator - Certificación OSCP Offensive Security Certified Professional
	OBSERVACIÓN 3 Requerimiento de certificación solicitado por la entidad. • Certificación en ejecución y/o administración de firewall en fábricas de ciberseguridad Solicitamos muy respetuosamente a la entidad eliminar las certificaciones de Certificación en ejecución y/o administración de firewall en fábricas de ciberseguridad, teniendo en cuenta que esta no guarda relación directa con la ejecución del objeto contractual, por las siguientes razones técnicas, administrar o configurar un firewall es una labor de seguridad defensiva orientada a la operación de la infraestructura tecnológica. Por el contrario, el objeto del presente proceso exige la ejecución de *Ethical Hacking*, análisis de vulnerabilidades y pruebas de penetración (*Red Team*). Saber operar la consola de un firewall de un fabricante no acredita de ninguna manera que el profesional posea las destrezas de hacking ético para identificar o explotar vulnerabilidades, evadir controles o auditar aplicaciones web. En este sentido el contratista adjudicatario tendrá la función de auditar y evaluar la seguridad de la Entidad, más no de administrar, configurar o mantener sus dispositivos de red o firewalls. Por ende, exigir competencias de administración de equipos resulta inocuo para el desarrollo operativo del proyecto	Al validar la observación, se ACEPTA, y esta serán tenidas en cuenta y se verán reflejadas en la ficha técnica y en los documentos definitivo. Quedando así: - Certificación a nivel profesional en seguridad de sistemas de información (CISSP) - Certificación en control de riesgos y sistemas de información (CRISC) - Certificación en Web Application Scanner - Certificación en Vulnerability Management Detección and Response - Certified Ethical Hacker (CEH) (Obligatoria) - Computer Hacking Forensic Investigator - Certificación OSCP Offensive Security Certified Professional

	OBSERVACIÓN 4 Requerimiento de certificación solicitado por la entidad. • Certificación como especialista de Cloud Security Solicitamos muy respetuosamente a la entidad eliminar las certificaciones de Certificación como especialista de Cloud Security teniendo en cuenta que la especialización en *Cloud Security* valida competencias en el diseño de arquitectura, gobernanza y configuración de controles de seguridad en plataformas de nube. No obstante, el objeto de esta selección es la *ejecución de pruebas de hacking ético, análisis de vulnerabilidades e ingeniería social* sobre 100 direcciones IP (públicas y privadas), dominios y aplicaciones web. Las metodologías de prueba de penetración (como OWASP u OSSTMM) evalúan la seguridad lógica del servicio independientemente de su lugar de alojamiento. Contar con una certificación de arquitectura de nube no acredita la habilidad técnica ofensiva para descubrir fallas de seguridad o realizar auditorías de intrusión en la plataforma de la Entidad.	Al validar la observación, se ACEPTA, y esta serán tenidas en cuenta y se verán reflejadas en la ficha técnica y en los documentos definitivo. Quedando así: - Certificación a nivel profesional en seguridad de sistemas de información (CISSP) - Certificación en control de riesgos y sistemas de información (CRISC) - Certificación en Web Application Scanner - Certificación en Vulnerability Management Detección and Response - Certified Ethical Hacker (CEH) (Obligatoria) - Computer Hacking Forensic Investigator - Certificación OSCP Offensive Security Certified Professional
	OBSERVACIÓN 5 Requerimiento de certificación solicitado por la entidad. • **Formación como Auditor ISO 27001:2022** Solicitamos respetuosamente a la Entidad ajustar el requisito técnico del perfil solicitando que la **Certificación como Auditor Lider ISO/IEC 27001:2022** emitida por un organismo de certificación acreditado (ej. PECB, IRCA, BSI), teniendo en cuenta que un certificado de *formación* (como lo solicita el pliego) o *asistencia* únicamente acredita que la persona presenció una cantidad de horas lectivas, sin certificar el dominio ni la habilidad práctica. Por el contrario, la certificación de **Auditor Lider** exige la evaluación rigurosa de competencias bajo el estándar ISO/IEC 17024, validando no solo la absorción de conocimientos, sino la capacidad de planear, ejecutar, liderar y emitir dictámenes de auditoría alineados con los controles de la versión 2022 del estándar. De esta manera se eleva el estándar de aseguramiento para la Entidad, garantizando un profesional capacitado para evaluar la eficacia de los Controles de Seguridad de la Información frente al estado del arte actual.	Al validar la observación, se ACEPTA, y esta serán tenidas en cuenta y se verán reflejadas en la ficha técnica y en los documentos definitivo. Quedando así: - Certificación a nivel profesional en seguridad de sistemas de información (CISSP) - Certificación en control de riesgos y sistemas de información (CRISC) - Certificación en Web Application Scanner - Certificación en Vulnerability Management Detección and Response - Certified Ethical Hacker (CEH) (Obligatoria) - Computer Hacking Forensic Investigator - Certificación OSCP Offensive Security Certified Professional

57(1) 5934020 - Fax: 57 (1) 5934027
fcm@fcm.org.co - contacto@fcm.org.co www.fcm.org.co
Cra7. N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica
Federación Colombiana de Municipios @Fedemunicipios Federación Colombiana de Municipios

	OBSERVACIÓN 6 Se solicita a la entidad de manera muy respetuosa, tener en cuenta y requerir la certificación **CEH v12 (Certified Ethical Hacker)**, expedida por EC-Council, ya que es el estándar internacional para profesionales en seguridad ofensiva y pruebas de intrusión lo que garantiza: 1. Alineación 100% con el Alcance: Evalúa y capacita en los dominios de la seguridad ofensiva, incluyendo hacking de aplicaciones web, análisis de vulnerabilidades, prueba de redes inalámbricas, evasión de firewalls y campañas de Ingeniería Social (Phishing), requeridas expresamente por la Federación. 2. Adherencia a Metodologías Exigidas: La certificación se fundamenta en marcos como OWASP Top 10, OSSTMM y NIST 800-115, metodologías expresamente solicitadas en el pliego de condiciones del proceso. 3. La certificación CEH v12 garantiza que el personal asignado cuente con la idoneidad técnica real para cumplir el contrato, protegiendo el principio de libre concurrencia al no restringir el proceso por marcas de hardware de red específicas.	Al validar la observación, se ACEPTA, y esta serán tenidas en cuenta y se verán reflejadas en la ficha técnica y en los documentos definitivo. Quedando así: - Certificación a nivel profesional en seguridad de sistemas de información (CISSP) - Certificación en control de riesgos y sistemas de información (CRISC) - Certificación en Web Application Scanner - Certificación en Vulnerability Management Detección and Response - Certified Ethical Hacker (CEH) (Obligatoria) - Computer Hacking Forensic Investigator - Certificación OSCP Offensive Security Certified Professional
	OBSERVACIÓN 7 Así las cosas, solicitamos respetuosamente a la Entidad fortalecer los requisitos de idoneidad técnica del personal mínimo requerido en el numeral **II. CONDICIONES DE EXPERIENCIA / CAPACIDAD TÉCNICA - b) DOCUMENTOS TÉCNICOS ADICIONALES**, garantizando que la ingeniería asignada cuente con la especialización real que demanda el proyecto. El objeto del presente proceso es la *ejecución práctica de pruebas de hacking ético, análisis de vulnerabilidades e ingeniería social*. Por ende, resulta indispensable que el profesional propuesto cuente, como requisito habilitante obligatorio, con una acreditación internacional en ciberseguridad ofensiva. Las certificaciones exclusivamente orientadas a la administración de infraestructura de red o productos comerciales no prueban las destrezas operativas de intrusión y auditoría requeridas por la Federación. En consecuencia, proponemos que se exija que el profesional de ingeniería cuente de forma **OBLIGATORIA con la Certificación CEH v12 (Certified Ethical Hacker)** —por guardar relación directa e inequívoca con el alcance contractual— y que, adicionalmente, acredite **al menos dos (2) de las siguientes certificaciones complementarias**: • **Certificación CEH v12 (Certified Ethical Hacker) *(Obligatoria)*** • Certificación a nivel profesional en seguridad de sistemas de información (CISSP) • Formación o Certificación como Auditor Líder ISO/IEC 27001:2022 • Certificación en Vulnerability Management Detection and Response • Certificación en Web Application Scanner	Al validar la observación, se ACEPTA, y esta serán tenidas en cuenta y se verán reflejadas en la ficha técnica y en los documentos definitivo. Quedando así: - Certificación a nivel profesional en seguridad de sistemas de información (CISSP) - Certificación en control de riesgos y sistemas de información (CRISC) - Certificación en Web Application Scanner - Certificación en Vulnerability Management Detección and Response - Certified Ethical Hacker (CEH) (Obligatoria) - Computer Hacking Forensic Investigator

		- Certificación OSCP Offensive Security Certified Professional
	OBSERVACIÓN 8 – EXPERIENCIA DEL PROPONENTE Respetados señores, De manera atenta solicitamos a la entidad aclarar y/o ajustar el requisito establecido para la acreditación de experiencia, específicamente en lo relacionado con la exigencia de que los contratos aportados versen simultáneamente sobre procesos de **Ethical Hacking y Análisis de Vulnerabilidades**. Actualmente se establece que: "(...) deberá acreditarse que el contrato versa sobre procesos de ética hacking y análisis de vulnerabilidades." Frente a lo anterior, solicitamos respetuosamente que la Entidad permita acreditar la experiencia requerida mediante contratos cuyo objeto, obligaciones o anexos técnicos contemplen **Ethical Hacking y/o Análisis de Vulnerabilidades**, siempre que, en conjunto, los contratos aportados acrediten experiencia directamente relacionada con el objeto del proceso y cumplan con el valor mínimo establecido de 72 SMMLV. Lo anterior, teniendo en cuenta que la misma condición establece la posibilidad de presentar entre **una (1) y máximo tres (3) certificaciones o actas de liquidación**, por lo cual consideramos que la experiencia puede ser acreditada mediante diferentes contratos que, de manera individual o conjunta, demuestren la experiencia específica requerida por la Entidad. En este sentido, por ejemplo, un proponente podría acreditar experiencia mediante un contrato cuyo alcance corresponda a **Ethical Hacking** y otro contrato cuyo alcance corresponda a **Análisis de Vulnerabilidades**, siempre que la sumatoria de los contratos cumpla con el valor mínimo requerido y que las actividades ejecutadas guarden relación directa con el objeto del proceso. Esta aclaración permitiría garantizar una mayor **pluralidad de oferentes**, evitando restringir la participación exclusivamente a aquellos proponentes que hayan ejecutado ambos servicios dentro de un mismo contrato, aun cuando cuenten con experiencia comprobable y específica en cada una de las actividades objeto del proceso. Por lo anterior, solicitamos a la Entidad modificar la redacción del requisito para que se establezca que la experiencia podrá acreditarse mediante contratos cuyo objeto, obligaciones o anexos técnicos contemplen **Ethical Hacking y/o Análisis de Vulnerabilidades**, pudiendo acreditarse ambas experiencias mediante uno o varios de los contratos permitidos, cuya sumatoria sea igual o superior a 72 SMMLV. Agradecemos a la Entidad aclarar este aspecto con el fin de garantizar una interpretación objetiva del requisito y promover la participación plural de oferentes con experiencia real y verificable en las actividades requeridas.	Al validar la observación, se ACEPTA que, y se corregirá en el Pliego, incluyendo "y/o". Así, la experiencia puede ser acreditada de manera individual un proponente podría acreditar experiencia mediante un contrato cuyo alcance corresponda a Ethical Hacking y otro contrato cuyo alcance corresponda a Análisis de Vulnerabilidades, siempre que la sumatoria de los contratos cumpla con el valor mínimo requerido y que las actividades ejecutadas guarden relación directa con el objeto del proceso.
OBSERVACIONES EXTEMPORÁNEAS		
2SECURE	**1. Presupuesto oficial y disponibilidad presupuestal** 1. El Certificado de Disponibilidad Presupuestal CDP-2026-00147 del 10 de julio de 2026 ampara la suma de $127.840.000, mientras que el presupuesto oficial estimado del proceso, determinado a partir del estudio de mercado, es de $124.846.243. Solicitamos confirmar si la diferencia entre ambos valores ($2.993.757) corresponde a un margen de contingencia presupuestal de la Entidad y precisar si dicho excedente podrá destinarse a cubrir eventuales adiciones, imprevistos o ajustes en la ejecución del contrato, o si por el contrario no tiene relación con el presente proceso.	Al validar la observación, SE ACLARA que, el valor correspondiente al Certificado de Disponibilidad Presupuestal (CDP) No. CDP-2026-00147 no corresponde al valor estimado del proceso. El valor estimado del proceso es de $124.846.243, determinado con base en los resultados obtenidos en el estudio de mercado realizado para establecer el valor de los servicios requeridos, que se encuentra detallado dentro de los estudios previos, publicados den la plataforma SECOP II. En este sentido, dicho valor corresponde al precio de referencia identificado a partir del comportamiento y las condiciones actuales del mercado para la prestación del servicio objeto del proceso.

		Por lo anterior, el valor del CDP constituye la disponibilidad presupuestal destinada a respaldar el proceso, pero no determina por sí mismo el valor estimado de la contratación, toda vez que este último se establece a partir del análisis y estudio de mercado efectuado por la Entidad.
	2. Plazo de ejecución del contrato 2. El pliego de condiciones y los estudios previos señalan que "el plazo de ejecución del contrato será de dos (2) meses contado a partir del cumplimiento de los requisitos de ejecución y hasta el 27 de diciembre de 2026". De acuerdo con el cronograma, la adjudicación se realizaría el 5 de octubre de 2026, la suscripción del contrato dentro de los dos (2) días siguientes y el cumplimiento de los requisitos de ejecución dentro de los dos (2) días siguientes a la suscripción, es decir, hacia el 9 de octubre de 2026. Un plazo de dos (2) meses contado desde esa fecha vencería aproximadamente el 9 de diciembre de 2026, fecha anterior al 9 de diciembre de 2026, es decir, con antelación al 27 de diciembre de 2026 mencionado en el mismo numeral. Solicitamos aclarar si el plazo de ejecución es efectivamente de dos (2) meses calendario, o si la fecha del 27 de diciembre de 2026 constituye el plazo real de ejecución (superior a dos meses), con el fin de dimensionar adecuadamente el cronograma de actividades, el plan de pruebas y el equipo de trabajo a ofertar.	Remitir al documento de respuestas jurídico.
	3. Alcance técnico – Ficha Técnica (Formato 2) 3. La tabla resumen de cantidades de la Ficha Técnica (Formato 2) señala "100 activos críticos" tanto para el ítem de Análisis de Vulnerabilidades como para el de Ethical Hacking (este último descrito como "100 activos críticos y dos dominios"), mientras que en el desarrollo del alcance técnico (Fase 1) se hace referencia reiterada a "100 direcciones IP, distribuidas en 50 IP privadas y 50 IP públicas". Solicitamos confirmar si "activos críticos" y "direcciones IP" corresponden al mismo universo de 100 elementos, o si se trata de universos distintos y, en consecuencia, el alcance real de las pruebas supera las 100 IP inicialmente descritas.	Al validar la observación, SE ACLARA que, los "activos críticos" y "direcciones IP" corresponden al mismo universo de 100 elemento.
	4. Se solicita precisar el alcance y contenido del concepto "dos (2) dominios" incluido en el ítem de Ethical Hacking de la tabla resumen de la Ficha Técnica, dado que dicho concepto no vuelve a desarrollarse en el resto de la ficha técnica ni en los estudios previos (por ejemplo, si se trata de dominios de Directorio Activo, dominios de correo/DNS, o dominios web).	Al validar la observación, SE ACLARA que, el alcance y contenido del concepto DNS y dominios web, (fcm.org.co y simit.org.co).
	5. Para las pruebas de intrusión a aplicaciones web bajo metodología OWASP, el pliego indica que "la Federación Colombiana de Municipios proveerá el entorno desde el cual se realizarán las pruebas". Se solicita precisar el número de aplicaciones web objeto de esta prueba, su criticidad y tecnología base, y confirmar si dichas aplicaciones están incluidas dentro del universo de 100 IP/activos críticos del alcance general o si constituyen un ítem adicional e independiente para efectos de dimensionamiento del esfuerzo y del equipo de trabajo.	*Al validar la observación, **SE ACLARA** que el alcance corresponde directamente a las aplicaciones expuestas a Internet, considerando su huella digital y superficie de exposición externa. En total, se contemplan diez (10) aplicaciones, las cuales se encuentran comprendidas dentro del alcance definido en las cien (100) direcciones IP. Por lo anterior, el alcance establecido permite realizar la evaluación de seguridad sobre las aplicaciones y los activos asociados que se encuentran expuestos desde Internet.*
	6. Se solicita indicar el número exacto de servicios o aplicaciones publicados en Internet a evaluar, así como su criticidad, con el fin de dimensionar adecuadamente el esfuerzo de las pruebas de intrusión externas.	*Al validar la observación, **SE ACLARA** que el alcance corresponde directamente a las aplicaciones expuestas a Internet, considerando su huella digital y superficie de exposición externa.*

		En total, se contemplan diez (10) aplicaciones, las cuales se encuentran comprendidas dentro del alcance definido en las cien (100) direcciones IP. Por lo anterior, el alcance establecido permite realizar la evaluación de seguridad sobre las aplicaciones y los activos asociados que se encuentran expuestos desde Internet.
	7. El pliego establece “3 pruebas de Ingeniería Social durante el plazo del contrato” dirigidas a una muestra representativa de “máximo 200 usuarios”. No es claro si las tres (3) pruebas deben aplicarse, cada una, sobre la totalidad de los 200 usuarios (lo que implicaría hasta 600 interacciones individuales), o si la muestra de 200 usuarios se distribuye entre las tres (3) pruebas programadas durante la ejecución del contrato. Se solicita aclarar este punto para efectos de dimensionar adecuadamente el servicio y su oferta económica.	Al validar la observación**, SE ACLARA** que el alcance establece la realización de tres (3) pruebas de Ingeniería Social durante el plazo de ejecución del contrato, orientadas a evaluar el comportamiento y nivel de respuesta del personal frente a ataques específicamente diseñados bajo técnicas de ingeniería social. Cada una de las tres (3) pruebas deberá aplicarse sobre la totalidad de los doscientos (200) usuarios definidos en el alcance, de manera que cada ejercicio permita evaluar el comportamiento de la población objetivo y obtener resultados comparables para identificar oportunidades de mejora en materia de concientización y prevención.
	8. El pliego exige que las herramientas utilizadas para las pruebas de penetración se encuentren “homologadas por el CVE (Common Vulnerabilities and Exposures) y www.mitre.org” y sean “licenciadas o de propiedad del oferente”, permitiendo complementarlas con “herramientas de uso libre o gratuito”. Solicitamos aclarar si el requisito de homologación CVE/MITRE aplica únicamente a las herramientas principales licenciadas, o si también resulta exigible para las herramientas de código abierto o gratuitas de uso complementario (p. ej. Nmap, OWASP ZAP, Metasploit Community), y precisar el mecanismo mediante el cual se acreditará dicha homologación para herramientas de este tipo.	Al validar la observación, se ACEPTA, y esta serán tenidas en cuenta y se verán reflejadas en la ficha técnica y en los documentos definitivos, así: Para la realización de esta prueba, se deben usar las herramientas pertinentes y usadas para el desarrollo de las pruebas de penetración, que referencien los hallazgos mediante identificadores CVE (Common Vulnerabilities and Exposures), conforme a www.mitre.org, y deben estar actualizadas a la fecha de su utilización. Para lo anterior, se deberá adjuntar en los informes presentados la referenciación CVE de cada hallazgo, o la ruta de la

		página de CVE donde se pueda evidenciar el identificador reportado por la herramienta ofrecida. En la medida en que el futuro contratista podrá utilizar plataformas o herramienta licenciadas u *Open source.* Por lo tanto, esta modificación se verá reflejada en la ficha técnica y en los documentos definitivos, quedando de la siguiente manera: *La herramienta deberá permitir la generación de los informes y entregables solicitados de manera automática, sin límite en el número de generaciones ni costo adicional durante el plazo de ejecución del contrato. Sin importar si es una plataforma licenciada o de uso libre.*
	9. El numeral de Experiencia Mínima del Proponente exige acreditar, mediante mínimo una (1) y máximo tres (3) certificaciones o actas de liquidación, una sumatoria igual o superior a 72 SMMLV. Tomando el salario mínimo mensual legal vigente para 2026 ($1.750.905), dicho umbral equivale a $126.065.160, cifra que supera el presupuesto oficial del propio proceso ($124.846.243). Se solicita confirmar si este es el umbral pretendido por la Entidad, dado que resulta superior al valor total del contrato a suscribir, lo cual podría limitar innecesariamente la pluralidad de oferentes.	La entidad ACLARA que el presupuesto oficial, es decir, el valor máximo del contrato es de $124.846.243. No obstante, el valor de los contratos para acreditar la experiencia, deberá sumar mínimo 72 salarios mínimos. Esto, sin limitar la pluralidad de oferentes, pues es un valor acorde con el presupuesto oficial.
	10. Se solicita aclarar si el único perfil de personal técnico mínimo exigido (un ingeniero con al menos dos (2) de las ocho (8) certificaciones enunciadas) resulta suficiente, a juicio de la Entidad, para ejecutar la totalidad del alcance contratado (análisis de vulnerabilidades sobre 100 IP, ethical hacking interno, externo y de aplicaciones web, e ingeniería social sobre hasta 200 usuarios) dentro del plazo de ejecución, o si la Entidad prevé o admite la vinculación de personal adicional por parte del contratista sin que ello sea objeto de puntaje adicional, conforme lo señala el propio pliego al indicar que “el contratista cuenta con plena independencia y autonomía” para definir el personal adicional que considere necesario.	Al validar la observación, SE ACLARA que el presente proceso está orientado a la contratación de una empresa especializada que cuente con la capacidad técnica y operativa necesaria para ejecutar la totalidad de las actividades previstas en el alcance contractual. En este sentido, el requisito establecido en los documentos definitivos respecto del personal técnico mínimo corresponde a la exigencia mínima que deberá acreditar el proponente para efectos de participar en el proceso, esto es, un (1) profesional que

57(1) 5934020 - Fax: 57 (1) 5934027
fcm@fcm.org.co - contacto@fcm.org.co www.fcm.org.co
Cra7. N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica
Federación Colombiana de Municipios @Fedemunicipios Federación Colombiana de Municipios

		cumpla con las condiciones de formación, experiencia y certificaciones establecidas por la Entidad. Lo anterior no limita ni restringe la conformación del equipo de trabajo que el futuro contratista considere necesario para garantizar la adecuada, oportuna y efectiva ejecución de las actividades contratadas, incluyendo el análisis de vulnerabilidades, ethical hacking interno, externo y de aplicaciones web, así como las pruebas de ingeniería social. Por tanto, el proponente podrá disponer de personal adicional, de acuerdo con su capacidad técnica, metodología y estrategia de ejecución, sin que la vinculación de dicho personal adicional sea objeto de puntaje adicional, en concordancia con lo establecido en los documentos del proceso respecto de la autonomía e independencia del contratista para definir los recursos requeridos para la ejecución del contrato.
	11. Se solicita confirmar si certificaciones vigentes equivalentes en la industria (p. ej. OSCP, CEH, eJPT, CPTE) para el perfil técnico, distintas a las ocho (8) enunciadas en el pliego, serán aceptadas como equivalentes para acreditar la idoneidad del personal mínimo, o si el listado contenido en el pliego es taxativo y excluyente.	Al validar la observación, se ACEPTA PARCIALMENTE la observación, y esta serán tenidas en cuenta en el pliego de condiciones definitivo, por lo tanto, el requisito quedará así: Para el desarrollo del contrato, se requiere que el contratista cuente como mínimo con el siguiente personal:

CANTIDAD PERSONAS	FORMACIÓN ACADÉMICA
1	Ingeniero con título profesional en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería de Software, Ingeniería de

57(1) 5934020 - Fax: 57 (1) 5934027
fcm@fcm.org.co - contacto@fcm.org.co www.fcm.org.co
Cra7. N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica
Federación Colombiana de Municipios @Fedemunicipios Federación Colombiana de Municipios

		telecomunicaciones o profesiones afines. Los ingenieros con título profesional en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería de Software, Ingeniería de telecomunicaciones o profesiones afines. Deberá contar con al menos 2 de las siguientes certificaciones: - Quedando así: - - - Certificación a nivel profesional en seguridad de sistemas de información (CISSP) - - Certificación en control de riesgos y sistemas de información (CRISC) - - Certificación en Web Application Scanner - - Certificación en Vulnerability Management Detección and Response - - Certified Ethical Hacker (CEH) (Obligatoria) - - Computer Hacking Forensic Investigator - - Certificación OSCP Offensive Security Certified Professional
	12. Se solicita confirmar que la vigencia de noventa (90) días calendario exigida para la garantía de seriedad de la oferta, contada desde la fecha de cierre del proceso (22 de septiembre de 2026), resulta suficiente frente a la fecha de adjudicación prevista (5 de octubre de 2026), y que no se requerirá	Remitirse al documento de respuestas jurídicas.

	ampliación adicional de dicha garantía salvo que se presenten prórrogas al cronograma del proceso.	
	13. Frente al ítem 2.1 de la evaluación técnica (10 recomendaciones adicionales de hardening, hasta 10 puntos), se solicita precisar si dichas recomendaciones deben referirse necesariamente a hallazgos identificados durante la ejecución del propio contrato —lo cual solo podría verificarse en la etapa de ejecución— o si, conforme lo señala el numeral "Forma de acreditar", basta con la carta de compromiso suscrita por el representante legal en la que se comprometa a entregarlas como parte de los productos del contrato. Por favor aclarar a que hace referencia el alcance solicitado.	Al validar la observación, se ACLARA que, recomendaciones deben referirse a hallazgos identificados durante la ejecución del propio contrato y como se expres de manera clara en la Forma de acreditar en el pliego una carta que debe venir suscrita por el representante legal y esta convertirá automáticamente en una obligación especifica del contrato.
	14. Frente al ítem 2.2 de la evaluación técnica (pruebas adicionales de ataques dirigidos de phishing, hasta 10 puntos), se solicita aclarar si las pruebas adicionales ofertadas (20, 30 o 50, según el tramo) se suman a la muestra máxima de 200 usuarios definida en el alcance de ingeniería social, o si corresponden a un universo de usuarios o interacciones adicional e independiente de dicha muestra.	Al validar la observación presentada, SE ACLARA que las pruebas corresponden a las actividades descritas en la "Descripción y Justificación de la Necesidad" de la Ficha técnica, ítem 1, relacionadas con la ejecución de pruebas de Ingeniería Social externas dirigidas al personal de la Federación Colombiana de Municipios, en el marco de la función pública asignada, detallándose que deben ser correspondientes a 200 usuarios. Así las cosas, el criterio puntuable se refiere a 50 pruebas **adicionales** de *Phishing*. Es decir, que se suman a las 200 mínimas requeridas en el contrato.
INDTECH FCM	**OBSERVACIÓN No. 1** **Solicitud de flexibilización de los requisitos financieros habilitantes** Respetados señores, analizado el numeral correspondiente a la **Capacidad Financiera y Organizacional**, respetuosamente solicitamos a la Entidad revisar y flexibilizar algunos de los requisitos financieros establecidos, considerando la naturaleza del objeto contractual, correspondiente a un servicio especializado de ciberseguridad y pruebas de seguridad ofensiva, el cual depende principalmente del conocimiento especializado, certificaciones del personal y metodologías técnicas, más que de inversiones significativas en infraestructura física o activos de capital. Si bien observamos que el pliego permite acreditar los indicadores con el **mejor año fiscal disponible en el RUP de los últimos tres (3) años**, lo cual resulta positivo para la pluralidad de oferentes, consideramos que algunos indicadores continúan siendo restrictivos para empresas especializadas del sector de ciberseguridad y servicios profesionales.	Remitirse al documento de respuestas financieras.

	Solicitamos evaluar la posibilidad de ajustar los siguientes indicadores, y proponemos considerar: • Liquidez ≥ 1,10. • Endeudamiento ≤ 75%. • Patrimonio ≥ 50% del presupuesto oficial. • Capital de Trabajo ≥ 50% del presupuesto oficial. Lo anterior teniendo en cuenta que el objeto contractual corresponde a servicios profesionales especializados de seguridad informática y no implica suministro de bienes, adquisición de infraestructura o ejecución de obras que demanden elevados requerimientos financieros. Adicionalmente, esta modificación favorecería los principios de pluralidad de oferentes, libre concurrencia y selección objetiva sin comprometer la capacidad financiera de los futuros contratistas.	
	OBSERVACIÓN No. 2 **Ampliación de certificaciones aceptadas para el perfil técnico mínimo requerido** Respetados señores, solicitamos respetuosamente ampliar el conjunto de certificaciones aceptadas para acreditar el perfil técnico mínimo exigido para el profesional requerido. El objeto del proceso contempla actividades de: • Análisis de Vulnerabilidades. • Ethical Hacking. • Pen Testing. • Ingeniería Social. Sin embargo, las certificaciones actualmente exigidas incluyen: • CISSP. • CRISC. • CCNP. • Vulnerability Management. • Web Application Scanner. • Cloud Security. • Firewall Security. • ISO 27001 Auditor. Observamos que algunas de estas certificaciones se encuentran orientadas a: • Gobierno de TI. • Gestión de riesgos. • Auditoría. • Redes. • Infraestructura. y no necesariamente acreditan competencias específicas en actividades de Pentesting, Ethical Hacking o Seguridad Ofensiva, que constituyen el núcleo del objeto contractual. Por lo anterior solicitamos permitir certificaciones equivalentes o superiores relacionadas con: • Ethical Hacking. • Penetration Testing. • Vulnerability Assessment. • Application Security. • Offensive Security. • Red Team.	Al validar la observación, se ACEPTA PARCIALMENTE la observación, y esta serán tenidas en cuenta en el pliego de condiciones definitivo, por lo tanto, el requisito quedará así: Para el desarrollo del contrato, se requiere que el contratista cuente como mínimo con el siguiente personal: **CANTIDAD PERSONAS** | **FORMACIÓN ACADÉMICA** 1 | Ingeniero con título profesional en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería de Software, Ingeniería de telecomunicaciones o profesiones afines. Los ingenieros con título profesional en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería de Software, Ingeniería de telecomunicaciones o profesiones afines. Deberá contar con al menos 2 de las siguientes certificaciones:

57(1) 5934020 - Fax: 57 (1) 5934027
fcm@fcm.org.co - contacto@fcm.org.co www.fcm.org.co
Cra7. N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica
Federación Colombiana de Municipios @Fedemunicipios Federación Colombiana de Municipios

	• Blue Team. • Purple Team. • Web Application Security. • Threat Intelligence. Incluyendo entre otras: • CEH. • CPENT. • Pentest+. • Security+. • OSCP. • OSEP. • GPEN. • GXPN. • GCIH. • eWPT. • Burp Suite Certified Practitioner. • Certificaciones equivalentes emitidas por fabricantes u organizaciones internacionalmente reconocidas. Consideramos que estas certificaciones guardan una relación más directa con el objeto contractual y permiten acreditar capacidades técnicas especializadas para la ejecución de las actividades requeridas.	- Quedando así: - - - Certificación a nivel profesional en seguridad de sistemas de información (CISSP) - - Certificación en control de riesgos y sistemas de información (CRISC) - - Certificación en Web Application Scanner - - Certificación en Vulnerability Management Detección and Response - - Certified Ethical Hacker (CEH) (Obligatoria) - - Computer Hacking Forensic Investigator - - Certificación OSCP Offensive Security Certified Professional Se incorporan dos (2) de las certificaciones propuestas, para un total de siete (7) certificaciones entre las cuales el proponente podrá acreditar el requisito habilitante. Esta modificación se realiza teniendo en cuenta la pertinencia de las certificaciones frente al objeto y alcance del proceso, así como los diferentes niveles de profundización y especialización, incluyendo certificaciones de nivel avanzado, intermedio y complementario, que en conjunto permiten acreditar las competencias requeridas para la

		adecuada ejecución de las actividades previstas en el contrato. En consecuencia, el requisito habilitante queda establecido con un universo de siete (7) certificaciones posibles, de las cuales deberán acreditarse dos (2).
	OBSERVACIÓN No. 3 **Reconocimiento de certificaciones de fabricantes especializados en ciberseguridad** Respetados señores, solicitamos que la Entidad permita acreditar el perfil técnico con certificaciones emitidas por fabricantes líderes en ciberseguridad cuando estas demuestren competencias directamente relacionadas con: • Threat Intelligence. • EDR/XDR. • Seguridad ofensiva. • Detección y respuesta. • Seguridad de aplicaciones. • Protección avanzada contra amenazas. A manera de ejemplo, podrían ser admitidas certificaciones como: • Kaspersky Anti Targeted Attack Administration. • Kaspersky Threat Intelligence. • Kaspersky Next EDR. • Kaspersky Industrial Cybersecurity. • Microsoft Defender XDR. • CrowdStrike Falcon. • SentinelOne. • Fortinet Security Operations. • Palo Alto Cortex. Estas certificaciones acreditan conocimientos directamente asociados a la identificación, evaluación y mitigación de vulnerabilidades, así como a la investigación y respuesta frente a amenazas avanzadas, aspectos alineados con los objetivos del presente proceso.	Al validar la observación, **NO SE ACEPTA,** toda vez que las certificaciones propuestas corresponden, en su mayoría, a conocimientos y competencias asociados a la administración, configuración, operación o uso de plataformas y soluciones específicas de determinados fabricantes. Si bien dichas competencias son relevantes dentro del ámbito general de la ciberseguridad, no son equivalentes a las competencias específicas requeridas para la ejecución de las actividades objeto del presente proceso y teniendo en cuenta las observaciones realizados por los proponentes de manera global se ajustaron estás, particularmente las relacionadas con análisis de vulnerabilidades, ethical hacking interno y externo, pruebas de seguridad sobre aplicaciones web y demás actividades de evaluación ofensiva contempladas en el alcance contractual. En este sentido, la Entidad estableció certificaciones que guardan una relación directa con las actividades objeto del contrato, entre ellas Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP), certificaciones relacionadas con Web Application Security y Vulnerability Management, entre otras previstas en los documentos del proceso. Por lo anterior, la Entidad considera que las certificaciones actualmente establecidas permiten acreditar conocimientos y competencias directamente relacionados con el alcance técnico requerido,

<table>
<tr>
<td></td>
<td></td>
<td>manteniendo la correspondencia entre los requisitos de formación y certificación exigidos y las actividades que deberá ejecutar el futuro contratista.
Adicionalmente, se precisa que la Entidad no desconoce la experiencia, conocimientos o certificaciones adicionales que pueda acreditar el proponente o el personal que disponga para la ejecución del contrato; sin embargo, para efectos de acreditar el requisito mínimo establecido en el proceso, deberán cumplirse las condiciones expresamente definidas en los documentos definitivos.</td>
</tr>
<tr>
<td></td>
<td>OBSERVACIÓN No. 4
Definición de certificaciones válidas para la competencia en Firewalls
Respetados señores, el pliego establece como requisito: "Certificación en ejecución y/o administración de firewall en fábricas de ciberseguridad".
No obstante, el requisito no establece:
• Fabricantes válidos.
• Nivel de certificación requerido.
• Alcance técnico mínimo.
• Equivalencias aceptadas.

Lo anterior puede generar interpretaciones subjetivas durante la evaluación de las ofertas.
Por tal motivo solicitamos respetuosamente definir expresamente cuáles certificaciones serán consideradas válidas para acreditar esta competencia, incluyendo fabricantes líderes del mercado tales como:
• Fortinet.
• Palo Alto Networks.
• Check Point.
• Kaspersky.
• Sophos.
• Cisco.
• WatchGuard.
• SonicWall.
• Stormshield.
• Forcepoint.
• Otros fabricantes equivalentes.
Igualmente solicitamos que se permita acreditar esta competencia mediante certificaciones oficiales del fabricante, programas de entrenamiento especializado o certificaciones equivalentes emitidas por entidades reconocidas. Esta precisión permitirá garantizar objetividad, transparencia y pluralidad de oferentes durante la etapa de evaluación.</td>
<td>Al validar la observación, se ACEPTA PARCIALMENTE la observación, y esta serán tenidas en cuenta en el pliego de condiciones definitivo, por lo tanto, el requisito quedará así:
Para el desarrollo del contrato, se requiere que el contratista cuente como mínimo con el siguiente personal:

Se aclara que, teniendo en cuenta las observaciones recibidas y el alcance técnico del presente proceso, no se considera necesario exigir certificaciones específicas emitidas por fabricantes, toda vez que estas no corresponden directamente a las competencias técnicas que la Entidad requiere acreditar para la ejecución de las actividades objeto del contrato.
En consecuencia, el requisito se mantiene y queda establecido de la siguiente manera:

<table>
<tr><th>CANTIDAD PERSONAS</th><th>FORMACIÓN ACADÉMICA</th></tr>
<tr><td>1</td><td>Ingeniero con título profesional en</td></tr>
</table>
</td>
</tr>
</table>

57(1) 5934020 - Fax: 57 (1) 5934027
fcm@fcm.org.co - contacto@fcm.org.co www.fcm.org.co
Cra7. N° 74B-56 - Piso 18 Bogotá D.C. Colombia - Suramérica
Federación Colombiana de Municipios @Fedemunicipios Federación Colombiana de Municipios

		<table><tr><td></td><td>Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería de Software, Ingeniería de telecomunicaciones o profesiones afines.</td></tr></table> Los ingenieros con título profesional en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería de Software, Ingeniería de telecomunicaciones o profesiones afines. Deberá contar con al menos 2 de las siguientes certificaciones: - Certificación a nivel profesional en seguridad de sistemas de información (CISSP) - Certificación en control de riesgos y sistemas de información (CRISC) - Certificación en Web Application Scanner - Certificación en Vulnerability Management Detección and Response - Certified Ethical Hacker (CEH) (Obligatoria) - Computer Hacking Forensic Investigator - Certificación OSCP Offensive Security Certified Professional
NEVITECH	Respetuosamente solicitamos a la Entidad incluir dentro de las certificaciones válidas para acreditar el perfil profesional requerido la certificación CISM – Certified Information Security Manager, expedida por ISACA. La solicitud resulta técnica y directamente relacionada con el objeto contractual, orientado a la ejecución de pruebas de hacking ético y análisis	Respuesta a la observación Al validar la observación, NO SE ACEPTA, toda vez que el alcance del presente proceso requiere acreditar competencias técnicas directamente relacionadas con la ejecución de actividades de análisis

	de vulnerabilidades, cuyo propósito final es fortalecer la postura de seguridad institucional. La certificación CISM acredita conocimientos y competencias en gobierno de seguridad de la información, gestión de riesgos de seguridad, desarrollo y gestión de programas de seguridad y gestión de incidentes, incluyendo dentro de sus contenidos aspectos asociados al análisis de vulnerabilidades y deficiencias de controles, así como a la evaluación y prueba de controles de seguridad. Adicionalmente, se observa que la Entidad actualmente admite CRISC, también expedida por ISACA, por lo cual resulta razonable permitir CISM como una alternativa adicional, considerando que ambas certificaciones desarrollan competencias asociadas a la gestión de riesgos y controles de seguridad, aunque desde enfoques distintos. ISACA describe CRISC como una certificación orientada al riesgo y controles de TI, mientras que CISM se concentra específicamente en la gestión de la seguridad de la información. En consecuencia, ampliar el requisito no disminuye la idoneidad técnica del perfil ni modifica la necesidad de acreditar al menos dos (2) certificaciones; por el contrario, permite reconocer una credencial internacional directamente relacionada con la seguridad de la información y favorece una mayor pluralidad de profesionales idóneos. Solicitud: modificar el listado incluyendo: – Certificación CISM (Certified Information Security Manager) expedida por ISACA. De esta manera se conserva íntegramente la exigencia de acreditar mínimo dos (2) certificaciones, ampliando únicamente las alternativas técnicamente válidas.	de vulnerabilidades, ethical hacking interno y externo, pruebas de seguridad sobre aplicaciones web e ingeniería social. La certificación CISM tiene un enfoque principalmente orientado a la gestión, gobierno, administración de riesgos y dirección de programas de seguridad de la información, por lo cual, si bien sus conocimientos son pertinentes para la gestión integral de la seguridad, no permite acreditar de manera directa las competencias técnicas específicas requeridas para la ejecución de pruebas de penetración y evaluación ofensiva de seguridad contempladas en el objeto contractual. En consecuencia, la Entidad considera que las certificaciones definidas en los documentos del proceso presentan una relación más directa con las actividades técnicas que serán desarrolladas durante la ejecución contractual, particularmente aquellas relacionadas con ethical hacking, penetration testing, análisis de vulnerabilidades y seguridad de aplicaciones web. Por lo anterior, no se acepta la inclusión de la certificación CISM como equivalente para acreditar el requisito de certificación del personal técnico mínimo, y se mantiene lo establecido en los documentos definitivos del proceso. Esta medida se adopta, en parte, como resultado de las observaciones presentadas por los proponentes, las cuales fueron analizadas y tenidas en cuenta por la Entidad.
	2) PRUEBAS DE ANÁLISIS DE VULNERABILIDADES: Requerimiento Técnico	Al validar la observación, se ACEPTA, y esta serán tenidas en cuenta y se verán reflejadas en la ficha técnica y en los documentos definitivo.

	Para la generación de los informes solicitados se deberá tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre (www.mitre.org). El proponente, debe demostrar la propiedad o autorización de uso explícita del fabricante, de las herramientas utilizadas en el desarrollo de este proyecto. Para lo cual deberá allegar certificación o documento que soporte el requisito. Observación: Solicitamos a la entidad que dicha exigencia sea requerida únicamente al proponente adjudicatario, previo al inicio de la ejecución de las pruebas que requieran dichas herramientas, y no como requisito que deba acreditarse con la presentación de la oferta. Lo anterior teniendo en cuenta que la propiedad, licenciamiento o autorización de uso de las herramientas constituye una condición propia de la ejecución contractual y no una condición necesaria para determinar la capacidad técnica del oferente al momento de presentar su propuesta, es decir, la actual condición limita la pluralidad e igualdad de oferentes ya que implica contar con herramientas costosas para presentar a un proceso público donde concurren diversas empresas y el resultado es variable. Esta conclusión se refuerza con la propia estructuración del Anexo Técnico, en el cual se establece que el contratista deberá elaborar y presentar a la Federación Colombiana de Municipios un plan de pruebas y actividades, así como las herramientas a utilizar, las cuales deberán ser aprobadas. En consecuencia, es precisamente en dicha etapa cuando se concretarán las herramientas que efectivamente serán empleadas durante la ejecución contractual. Adicionalmente, el mismo requerimiento permite que las herramientas sean licenciadas, de propiedad del oferente o complementadas con herramientas de uso libre o gratuito, por lo cual exigir desde la presentación de la oferta una autorización explícita de fabricante puede resultar innecesariamente restrictivo frente a herramientas que eventualmente ni siquiera serán utilizadas por un oferente que no resulte adjudicatario. La modificación solicitada no disminuye las condiciones técnicas ni de seguridad exigidas por la Entidad, pues el adjudicatario deberá demostrar, antes de utilizar cada herramienta que así lo requiera, que cuenta con las correspondientes licencias, derechos de uso o autorizaciones, garantizando la legalidad de los componentes empleados durante las pruebas de hacking ético y análisis de vulnerabilidades.	Así: Para la realización de esta prueba, se deben usar las herramientas pertinentes y usadas para el desarrollo de las pruebas de penetración, que referencien los hallazgos mediante identificadores CVE (Common Vulnerabilities and Exposures), conforme a www.mitre.org, y deben estar actualizadas a la fecha de su utilización. Para lo anterior, se deberá adjuntar en los informes presentados la referenciación CVE de cada hallazgo, o la ruta de la página de CVE donde se pueda evidenciar el identificador reportado por la herramienta ofrecida. La herramienta deberá permitir la generación de los informes y entregables solicitados de manera automática, sin límite en el número de generaciones ni costo adicional durante el plazo de ejecución del contrato.

Proyecto: Ing Juan Carlos Gamarra Anaya

Original Firmado

JUAN CARLOS GAMARRA ANAYA

Profesional Dirección Tecnologías de la Información
Miembro del Comité Evaluador