



RESPUESTA A OBSERVACIONES PRESENTADAS AL PROYECTO DE PLIEGO DE CONDICIONES DEL PROCESO FGN-NC-LP-0003-2025

1. NEXURA INTERNACIONAL SAS

OBSERVACIÓN 1

En relación con el factor técnico de **Especialista en Seguridad de la Información** (criterio ponderable), el pliego establece que el profesional propuesto debe acreditar al menos cuatro (4) de las certificaciones allí relacionadas. Al respecto, solicitamos que también se considere válida la formación académica a nivel de especialización o maestría en programas afines a lo requerido.

RESPUESTA 1

La Fiscalía General de Nación No acepta la observación, la maestría solicitada garantiza un nivel específico de conocimiento práctico y actualizado en áreas críticas de la seguridad de la información, lo anterior, permitirá identificar y mitigar riesgos de seguridad en cada etapa del desarrollo, aplicar principios de seguridad desde la fase de análisis y arquitectura, realizar revisiones de código seguras, entre otras actividades de seguridad informática.

OBSERVACIÓN 2

De igual manera, solicitamos que, para el mismo factor técnico de **Especialista en Seguridad de la Información** (criterio ponderable), se permita acreditar formación académica a nivel de maestría en áreas como seguridad de la información, seguridad informática, ciberseguridad o ingeniería de software.

RESPUESTA 2

La Fiscalía General de Nación , Aclara que el requisito solicitado incluye maestría en seguridad de la información, requerimiento que será ampliado a maestrías afines según el SNIES

2. AUTENTIC SOLUCIONES TECNOLÓGICAS

OBSERVACIÓN 1

En atención al principio de pluralidad de oferentes y libre concurrencia que rige la contratación estatal en Colombia, respetuosamente presentamos las siguientes observaciones: El pliego de condiciones en sus factores ponderables exige la presentación de un perfil de Especialista de seguridad de la información:

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                            |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Especialista de Seguridad de la Información | Ingeniero de Sistemas, de Telecomunicaciones, Electrónico o ingenierías afines con Maestría en Seguridad de la Información<br><br>Deberá contar con por lo menos cuatro (4) de las siguientes certificaciones vigentes: <ul style="list-style-type: none"><li>• LEAD IMPLEMENTER ISO 27001 v 2022</li><li>• CISM - CERTIFIED INFORMATION SECURITY MANAGEMENT</li><li>• CERTIFIED ETHICAL HACKER (CEH)</li><li>• ECIH EC-COUNCIL CERTIFIED INCIDENT HANDLER</li><li>• CISSP - CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL</li><li>• CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER</li><li>• MANAGER CYBERSECURITY ISO/IEC 27032</li></ul> | Experiencia específica de al menos diez (10) años en proyectos relacionados con seguridad de la información, en roles de Líder, Consultor, Asesor u Oficial en Seguridad de la Información |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Que debe contar con cuatro certificaciones en materia de seguridad informática como requisito para otorgar puntaje dentro del proceso. Si bien reconocemos la importancia de garantizar altos estándares de seguridad en la prestación de los servicios, consideramos que la cantidad y especificidad de certificaciones solicitadas resultan excesivas y pueden generar una restricción injustificada en la participación de oferentes, limitando la competencia y reduciendo las posibilidades de obtener la mejor oferta para la entidad. Teniendo en cuenta que todas las certificaciones se refieren a la seguridad informática y de la información, solicitar 4

82





resulta redundante porque una o dos son necesarias para demostrar la idoneidad del profesional. Cabe recordar que el artículo 5 de la Ley 1150 de 2007 establece que las condiciones de participación deben diseñarse de manera que no constituyan barreras de acceso injustificadas para los interesados. Así mismo, la Corte Constitucional y el Consejo de Estado han señalado en reiterada jurisprudencia que los pliegos no pueden incluir exigencias desproporcionadas que restrinjan la pluralidad de oferentes. En particular, la Sección Tercera del Consejo de Estado ha sostenido que: "a Administración no se encuentra autorizada para restringir la participación de los interesados, estableciendo, a su discrecionalidad, reglas que desconozcan la igualdad de condiciones, como cuando sin fundamento alguno determina un mejor derecho para algunos de los participantes, mediante el sistema de la precalificación o caprichosamente fija condicionamientos para direccionar la participación de unos pocos oferentes, práctica que no se encuentra autorizada en la legislación colombiana y que indudablemente vicia de nulidad el contrato" (Consejo de Estado, Sentencia del 29 de agosto de 2007, Radicación No. 15324).

En este sentido, solicitamos respetuosamente a la entidad que se revisen y ajusten los requisitos relacionados con certificaciones de seguridad informática, de manera que se exija únicamente lo estrictamente necesario y proporcional al objeto contractual, permitiendo una mayor participación de proponentes y garantizando los principios de igualdad, transparencia, libre concurrencia y selección objetiva consagrados en la Ley 80 de 1993 y la Ley 1150 de 2007.

#### **RESPUESTA 1**

La Fiscalía General de Nación No acepta su observación, si bien se reconoce la importancia de garantizar la pluralidad de oferentes y la libre concurrencia en los procesos de contratación estatal, conforme a lo dispuesto en el artículo 5 de la Ley 1150 de 2007 y la jurisprudencia del Consejo de Estado, también es deber de la entidad garantizar la selección objetiva del contratista más idóneo, en función de la naturaleza especializada del objeto contractual.

La exigencia de estas cuatro certificaciones no constituye una barrera injustificada, sino una medida proporcional y técnica que responde al análisis de riesgo del proceso, la criticidad de los servicios contratados y la necesidad de contar con personal altamente calificado en un campo que exige estándares internacionales de seguridad. Tal como lo establece el Concepto C-456 de 2025 de la Agencia Nacional de Contratación Pública, los requisitos técnicos pueden ser ponderables siempre que estén debidamente justificados y alineados con el objeto contractual.

Adicionalmente, la jurisprudencia del Consejo de Estado ha señalado que la autonomía de la entidad para definir los requisitos técnicos está limitada por los principios de proporcionalidad, transparencia y selección objetiva.

El pliego de condiciones está definido como el reglamento que disciplina el procedimiento licitatorio de selección del contratista y delimita el contenido y alcance del contrato. Es un documento que establece una preceptiva jurídica de obligatorio cumplimiento para la administración y el contratista, no sólo en la etapa precontractual sino también en la de ejecución y en la fase final del contrato. Si el proceso licitatorio resulta fundamental para la efectividad del principio de transparencia y del deber de selección objetiva del contratista, el pliego determina, desde el comienzo, las condiciones claras, expresas y concretas que revelan las especificaciones jurídicas, técnicas y económicas, a que se someterá el correspondiente Contrato. (Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Tercera, Consejero Ponente: Alier Eduardo Hernández Enríquez, 19 de julio de 2001, radicación número: 11001-03-26-000-1996-3771-01(12037))

En este caso, la exigencia de cuatro certificaciones responde a la necesidad de asegurar un nivel mínimo de especialización en áreas complementarias de la seguridad informática (gestión, respuesta a incidentes, hacking ético, privacidad, etc.), sin que ello implique una restricción arbitraria o discriminatoria.

#### **3. TODOSISTEMNS STI**

**Perfil Especialista en Seguridad de la Información**





|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                             |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Especialista de Seguridad de la Información | Ingeniero de Sistemas, de Telecomunicaciones, Electrónico o ingenierías afines con Maestría en Seguridad de la Información.<br><br>Deberá contar con por lo menos cuatro (4) de las siguientes certificaciones vigentes:                                                                                                                                                                                              | Experiencia específica de al menos diez (10) años en proyectos relacionados con seguridad de la información, en roles de Líder, Consultor, Asesor u Oficial en Seguridad de la Información. |
|                                             | <ul style="list-style-type: none"><li>• LEAD IMPLEMENTER ISO 27001 v.2022</li><li>• CISM - CERTIFIED INFORMATION SECURITY MANAGEMENT</li><li>• CERTIFIED ETHICAL HACKER (CEH).</li><li>• ECIH EC-COUNCIL CERTIFIED INCIDENT HANDLER</li><li>• CISSP - CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL</li><li>• CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER</li><li>• MANAGER CYBERSECURITY ISO/IEC 27032</li></ul> |                                                                                                                                                                                             |

#### OBSERVACIÓN 1

Formación académica demasiado restringida

**Exigido:** Maestría en Seguridad de la Información.

Solicitamos que se acepte título de pregrado en áreas afines con especialización en Seguridad de la Información (ISO, CISSP, CISM, etc.), dado que estas acreditaciones son equivalentes en conocimiento y práctica.

#### RESPUESTA 1

La Fiscalía General de Nación No acepta su observación y se permite aclarar que, para el título de pregrado se está solicitando: *Ingeniero de Sistemas, de Telecomunicaciones, Electrónico o ingenierías Afines*. Respecto del posgrado, este se amplió a posgrados afines según el SNIES

#### OBSERVACIÓN 2

Cuatro certificaciones simultáneamente

**Exigido:** Mínimo 4 certificaciones vigentes entre: ISO 27001 Lead Implementer, CISM, CEH, ECIH, CISSP, CDPSE, Manager Cybersecurity ISO/IEC 27032.

Solicitamos que se reduzca a mínimo dos (2) **certificaciones vigentes**, considerando la profundidad de cada una (ej. CISSP o CISM ya abarcan un amplio espectro).

#### RESPUESTA 2

La Fiscalía General de Nación No acepta su observación, la exigencia de estas cuatro certificaciones responde al análisis de riesgo del proceso, la criticidad de los servicios contratados y la necesidad de contar con personal altamente calificado en un campo que exige estándares internacionales de seguridad. Tal como lo establece el Concepto C-456 de 2025 de la Agencia Nacional de Contratación Pública, los requisitos técnicos pueden ser ponderables siempre que estén debidamente justificados y alineados con el objeto contractual.

Adicionalmente, la jurisprudencia del Consejo de Estado ha señalado que la autonomía de la entidad para definir los requisitos técnicos está limitada por los principios de proporcionalidad, transparencia y selección objetiva.





El pliego de condiciones está definido como el reglamento que disciplina el procedimiento licitatorio de selección del contratista y delimita el contenido y alcance del contrato. Es un documento que establece una preceptiva jurídica de obligatorio cumplimiento para la administración y el contratista, no sólo en la etapa precontractual sino también en la de ejecución y en la fase final del contrato. Si el proceso licitatorio resulta fundamental para la efectividad del principio de transparencia y del deber de selección objetiva del contratista, el pliego determina, desde el comienzo, las condiciones claras, expresas y concretas que revelan las especificaciones jurídicas, técnicas y económicas, a que se someterá el correspondiente Contrato. (Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Tercera, Consejero Ponente: Alíer Eduardo Hernández Enríquez, 19 de julio de 2001, radicación número: 11001-03-26-000-1996-3771-01(12037))

En este caso, la exigencia de cuatro certificaciones responde a la necesidad de asegurar un nivel mínimo de especialización en áreas complementarias de la seguridad informática (gestión, respuesta a incidentes, hacking ético, privacidad, etc.), sin que ello implique una restricción arbitraria o discriminatoria.

### **OBSERVACIÓN 3**

#### **Experiencia específica de 10 años mínimo**

**Exigido:** Al menos 10 años en proyectos de Seguridad de la Información en roles de Líder/Consultor/Oficial.

Solicitamos que se reduzca a **5 años de experiencia comprobable**, suficiente para garantizar idoneidad técnica.

Adicionalmente, solicitamos se informe cuáles serían las funciones del especialista de seguridad de la información y el % de disponibilidad para el proyecto.

### **RESPUESTA 3**

La Fiscalía General de Nación No acepta su observación, La exigencia de experiencia específica responde a la complejidad técnica y el nivel de criticidad del objeto contractual, el cual involucra la protección de activos de información, la gestión de riesgos cibernéticos, la implementación de controles normativos (como ISO 27001, ISO 27032, entre otros) y la ejecución de auditorías en procesos críticos de TI.

En este caso, la experiencia mínima de 10 años se considera necesaria para garantizar la idoneidad técnica del profesional, dado que, la seguridad de la información requiere conocimientos avanzados y experiencia acumulada en múltiples dominios técnicos y normativos, la gestión de incidentes, auditorías, y diseño de políticas de seguridad exige madurez profesional y criterio experto, que se desarrolla con años de práctica, la experiencia en roles de liderazgo y consultoría implica responsabilidad estratégica, no solo operativa, lo cual justifica un umbral superior.

Frente al porcentaje de disponibilidad se indica que no se requiere presencialidad, sin embargo, deberá estar disponible cuando el supervisor del contrato lo requiera.

## **4. ENTELGY**

### **OBSERVACIÓN 1**

#### **Anexo Técnico 3**

Se solicita amablemente aclarar si las licencias y accesos a estas plataformas serán provistos por la FGN, para que el contratista solo desarrolle sobre ellas.

### **RESPUESTA 1**

La Fiscalía General de Nación, Aclara que Si, las licencias y accesos a las plataformas requeridas para el desarrollo de los productos de software serán provistas por la Fiscalía General de la Nación (FGN).

La entidad garantizará que el contratista cuente con los accesos correspondientes a los entornos y herramientas necesarias para el cumplimiento de las obligaciones contractuales, incluyendo los sistemas institucionales, herramientas de control de versiones, integración continua, servidores de despliegue, plataformas de autenticación, entre otras, de acuerdo con lo establecido en el Anexo Técnico No. 3 – Herramientas Tecnológicas.

En dicho documento se detalla que la FGN cuenta con un conjunto de herramientas tecnológicas y de infraestructura sobre las cuales el contratista deberá trabajar. El contratista no deberá adquirir licencias por su cuenta, ya que estas serán proporcionadas y administradas por la entidad.





#### **OBSERVACIÓN 2**

##### **Anexo Técnico 3**

Se solicita amablemente aclarar si el alcance incluye también soporte y mantenimiento de aplicaciones en versiones anteriores a Java 17 (por ejemplo, Java 8 o 11), dado que estas aún son comunes en ambientes legados de la FGN.

#### **RESPUESTA 2**

La Fiscalía General de Nación, Aclara que Sí, el alcance del contrato incluye el soporte y mantenimiento de aplicaciones desarrolladas en versiones anteriores a Java 17, tales como Java 8 o Java 11, siempre que estas tecnologías estén actualmente en uso en los sistemas de información de la Fiscalía General de la Nación (FGN).

Tal como se establece en el **Anexo Técnico 3 – Herramientas Tecnológicas**, la entidad dispone de un ecosistema tecnológico heterogéneo, en el cual coexisten diversas versiones de lenguajes de programación, herramientas y frameworks. En este contexto, el contratista deberá atender requerimientos técnicos sobre soluciones existentes que aún se encuentran operativas y que fueron desarrolladas con tecnologías consideradas como "legadas", incluyendo versiones previas de Java.

La obligación de soporte comprende ajustes correctivos, evolutivos o adaptativos sobre estas aplicaciones, hasta tanto la FGN implemente su renovación tecnológica o migración a versiones más recientes. Lo anterior incluye también la compatibilidad con entornos de ejecución actuales, interoperabilidad con otros sistemas institucionales y atención de vulnerabilidades de seguridad.

#### **OBSERVACIÓN 3**

##### **Anexo Técnico 4**

Se solicita amablemente corregir la denominación a Python para evitar ambigüedad en la validación de experiencia. Actualmente aparece así: "Desarrollador Phytton"

#### **RESPUESTA 3**

La Fiscalía General de Nación No acepta la observación. Tal como se encuentra descrito en el Anexo Técnico 4 – Equipo de Trabajo, la denominación actual corresponde a "Desarrollador Phytton". No obstante, se aclara que dicha denominación hace referencia al lenguaje de programación Python, lenguaje interpretado, de alto nivel y tipado dinámico, ampliamente utilizado en el desarrollo de software.

Esta precisión terminológica no representa un cambio en el alcance técnico ni en los perfiles requeridos, sino una aclaración conceptual para efectos de interpretación unificada en la evaluación de la experiencia de los proponentes. Por lo tanto, se mantendrá la redacción actual en los documentos del proceso.

#### **OBSERVACIÓN 4**

##### **Anexo Técnico 4**

Al validar el proceso exigen certificaciones muy específicas (ej. IASA, SOA, WSO2; CMMI Professional; TOGAF; Scrum; ITIL; DevOps; Lean Six Sigma; Design Thinking). Se propone flexibilizar aceptando certificaciones equivalentes en arquitectura de software, soluciones e integración (ej. AWS, Azure, Google Cloud Architect, o certificaciones oficiales de Oracle, Red Hat, IBM en integración y arquitectura).

#### **RESPUESTA 4**

La Fiscalía General de Nación No acepta la observación. Las certificaciones solicitadas en el Anexo Técnico 4 – Equipo de Trabajo corresponden a estándares internacionalmente reconocidos en metodologías, marcos de trabajo y buenas prácticas para el desarrollo, integración, gestión de servicios y arquitectura de software. Estas fueron definidas con el fin de asegurar un alto nivel de idoneidad técnica y metodológica del equipo de trabajo requerido para la ejecución del contrato. La aclaración anterior no implica modificación del alcance técnico ni del listado de certificaciones previstas, sino que permite un margen razonable de validación para certificaciones que cumplan equivalencia técnica y profesional con las previstas.

#### **OBSERVACIÓN 5**

##### **Anexo Técnico 4**





Se solicita a la entidad amablemente que por favor se identifique el ecosistema de seguridad actual de la FGN, de manera que el oferente pueda plantear integración y pruebas alineadas a lo existente, en lugar de asumir nuevas plataformas.

#### **RESPUESTA 5**

La Fiscalía General de Nación No acepta la observación. El alcance del presente proceso no contempla la revelación detallada del ecosistema de seguridad actual de la Fiscalía General de la Nación, en atención a las políticas institucionales de seguridad de la información, confidencialidad y protección de infraestructuras críticas.

No obstante, se aclara que, durante la fase de ejecución del contrato, el contratista contará con acceso a los lineamientos técnicos, plataformas autorizadas y requerimientos específicos de seguridad de la información definidos por el grupo de Seguridad y la Subdirección de Tecnologías de la Información y las comunicaciones. Esto garantizará que la integración y las pruebas se realicen de manera alineada al ecosistema vigente, con acompañamiento técnico de la Entidad.

En ese sentido, los oferentes deberán asumir dentro de su propuesta técnica la capacidad de realizar integraciones y adaptaciones de acuerdo con los entornos tecnológicos existentes, los cuales serán formalmente comunicados durante la etapa de alistamiento y ejecución del contrato, bajo acuerdos de confidencialidad y protocolos de acceso establecidos.

#### **OBSERVACIÓN 6**

##### **Anexo Técnico 4**

Se solicita amablemente ampliar el plazo a 10 o 15 días hábiles, o permitir la presentación inicial de perfiles equivalentes mientras se gestionan los reemplazos definitivos, asegurando continuidad del servicio.

#### **RESPUESTA 6**

La Fiscalía General de Nación No acepta la observación. De acuerdo con lo estipulado en el Anexo Técnico 4 – Equipo de Trabajo, y en concordancia con los principios de planeación y ejecución eficiente del contrato, los perfiles propuestos deben cumplir con las condiciones mínimas requeridas desde la presentación de la oferta, garantizando la disponibilidad inmediata del recurso humano a la firma del contrato.

Esto se debe a que el modelo de fábrica de software requiere un alistamiento operativo ágil, donde la fase de inicio y transición se encuentra condicionada al despliegue efectivo de los equipos técnicos definidos, sin afectar los cronogramas establecidos ni la atención a las solicitudes de desarrollo priorizadas por la Entidad.

No obstante, conforme a la normativa vigente, en caso de presentarse eventualidades durante la ejecución del contrato, el contratista podrá solicitar reemplazos de personal debidamente justificados, los cuales serán evaluados por la Entidad conforme a los requisitos del proceso, sin que ello implique modificación de las condiciones iniciales de selección ni del objeto contractual.

#### **5. IT MANAGERS SAS**

#### **OBSERVACIÓN 1**

| DOCUMENTO      | NUMERAL  | LO SOLICITADO - CITA TEXTUAL                                                                                                           | OBSERVACIÓN                                                                                                                                          |
|----------------|----------|----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| ESTUDIO PREVIO | 2.6 (37) | Entregar garantía sobre los desarrollos realizados durante la ejecución del contrato y 12 meses posteriores a la finalización de este. | Solicitamos a la entidad aclarar: ¿Si los 12 meses se establecen cuando se realice el paso a producción de cada Historia de usuario o requerimiento? |

#### **RESPUESTA 1**



La garantía a la que hace referencia el numeral 2.6 (37) del Estudio Previo aplica a la totalidad de los desarrollos entregados en el marco del contrato, y su término de 12 meses se computa a partir de la **finalización del contrato**, no desde el paso a producción de cada historia de usuario o requerimiento individual.

Esto se fundamenta en la naturaleza integral del contrato de fábrica de software, en donde los entregables se consolidan como parte de un proceso continuo de desarrollo, prueba, validación y despliegue. Por lo tanto, la garantía se activa una vez se ha cumplido la totalidad de las obligaciones contractuales y se haya formalizado el acta de terminación o liquidación correspondiente.

Durante el periodo de garantía (12 meses), el contratista deberá responder por los defectos o fallas atribuibles a los desarrollos ejecutados, realizando sin costo adicional los ajustes, correcciones o mantenimientos necesarios para mantener el adecuado funcionamiento de las funcionalidades entregadas, conforme a los estándares técnicos y funcionales acordados.

#### OBSERVACIÓN 2

| DOCUMENTO      | NUMERAL   | LO SOLICITADO - CITA TEXTUAL                                                                                                         | OBSERVACIÓN                                                                                                                                  |
|----------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| ESTUDIO PREVIO | Página 21 | Se dimensiona la necesidad en función de la capacidad operativa de recurso humano: * 3 analistas y 27 desarrolladores especializados | Solicitamos a la entidad aclarar: ¿Los 27 desarrolladores son solo desarrolladores o acá se está incluyendo Tester QA, DEVOPS y demás roles? |

#### RESPUESTA 2

La Fiscalía General de Nación, Aclara que la estimación mencionada en la página 21 del Estudio Previo corresponde exclusivamente a desarrolladores especializados, enmarcados en los diferentes lenguajes, arquitecturas y tecnologías requeridas por la entidad, de acuerdo con lo señalado en los Anexos Técnicos del proceso. Es decir, los 27 recursos no incluyen perfiles adicionales como QA Tester, DevOps, Arquitectos, Líderes Técnicos, ni otros roles complementarios.

Estos perfiles adicionales como profesionales QA, especialistas en aseguramiento de la calidad, automatización de pruebas, especialistas en DevOps, analistas de seguridad, entre otros, se encuentran descritos y dimensionados de manera independiente en el Anexo Técnico 4 – Equipo de Trabajo, el cual establece con precisión el número mínimo y el perfil requerido para cada uno de estos roles.

Por tanto, la mención en el Estudio Previo debe ser entendida como una estimación de la demanda total de desarrolladores a nivel técnico-operativo, sin que esto sustituya ni modifique la estructura de perfiles y cantidad mínima exigida en los documentos técnicos del proceso.

#### OBSERVACIÓN 3

| DOCUMENTO      | NUMERAL   | LO SOLICITADO - CITA TEXTUAL                                                        | OBSERVACIÓN                                                                                                                                                                                            |
|----------------|-----------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ESTUDIO PREVIO | Página 21 | Aproximadamente 4.800 horas mensuales para un total de 38.400 horas durante 8 meses | Solicitamos a la entidad aclarar: ¿Qué pasa si las 38400 horas ósea los 8 meses no son suficientes para abarcar los requerimientos existentes ya que el desarrollo de las aplicaciones es a la medida? |

#### RESPUESTA 3

La Fiscalía General de Nación, Aclara que la proyección de 38.400 horas durante 8 meses corresponde a una estimación inicial de carga de trabajo con base en el análisis histórico de requerimientos, la capacidad instalada y la proyección de necesidades de intervención técnica priorizada en los sistemas de información.

No obstante, se aclara que:





- El modelo contractual planteado es bajo demanda (fábrica de software), lo que implica que la ejecución se encuentra sujeta a la gestión de requerimientos priorizados, dentro del marco de horas contratadas.
- En caso de que la demanda de atención supere las horas inicialmente estimadas y contratadas, la entidad evaluará la ejecución presupuestal y el avance del contrato, y podrá adoptar mecanismos administrativos y contractuales que permitan garantizar la continuidad del servicio, conforme a la normatividad vigente.
- La FGN cuenta con procesos internos de planeación y priorización técnica de historias de usuario y requerimientos funcionales, a través de mecanismos definidos en los equipos de producto, los cuales permiten hacer una asignación eficiente de los recursos del contrato.
- Adicionalmente, los entregables bajo el modelo fábrica deben ser definidos y aprobados en ciclos iterativos (sprints), donde se validan el avance, las cargas y los entregables, asegurando trazabilidad sobre el uso de horas y permitiendo ajustes y gestión oportuna ante eventuales desviaciones de alcance.

Por tanto, el alcance del contrato está vinculado a la capacidad contratada (38.400 horas), y cualquier necesidad adicional deberá gestionarse a través de los procedimientos administrativos y legales, según las disposiciones contractuales y presupuestales de la entidad.

#### OBSERVACIÓN 4

| DOCUMENTO                                                                    | NUMERAL                    | LO SOLICITADO - CITA TEXTUAL                                                                                                                         | OBSERVACIÓN                                                                                                                                                                     |
|------------------------------------------------------------------------------|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ANEXO TECNICO1_<br>CONDICIONES<br>_MINIMAS_DEL_PRODUCT<br>O<br>_DEL_SOFTWARE | MANTENIMIENTO Y<br>SOPORTE | Soporte Técnico: Se establecerán acuerdos de soporte técnico para garantizar la disponibilidad y el correcto funcionamiento de los sistemas de la FG | Solicitamos a la entidad aclarar: ¿Se brindará soporte única y exclusivamente a las nuevas funcionalidades o también se deberá dar soporte a sistemas existentes de la entidad? |

#### RESPUESTA 4

La Fiscalía General de Nación, Aclara que la obligación de brindar soporte técnico en el marco del contrato **se limita exclusivamente a las funcionalidades desarrolladas por el contratista** durante la vigencia del contrato y que hayan sido puestas en producción como resultado de los requerimientos aprobados por la FGN.

El contratista **no será responsable del soporte técnico general ni correctivo** de sistemas o componentes no intervenidos directamente en el marco del contrato. Tampoco se exigirá soporte sobre funcionalidades previas o legadas que no hayan sido objeto de modificación, desarrollo o mantenimiento por parte del contratista. Sin embargo, las actividades que realice la fábrica y que tengan como resultado incidentes o problemas técnicos colaterales, se deben analizar dentro de las mesas de concertación y definir si estas actividades realizadas por el contratista comprometieron algún riesgo o la materialización del mismo.

El propósito del alcance de soporte es **garantizar la estabilidad, funcionamiento y continuidad** de las soluciones entregadas bajo el modelo de fábrica de software, durante su ciclo de vida y periodo de garantía establecido. Cualquier requerimiento de soporte sobre sistemas existentes por fuera del alcance contractual será tramitado directamente por la FGN o mediante otros mecanismos definidos por la entidad.



#### OBSERVACIÓN 5

| DOCUMENTO                                                                   | NUMERAL                                                      | LO SOLICITADO - CITA TEXTUAL                                                                                                                                                                                                                                                                                                                                                                                                                            | OBSERVACIÓN                                                                                                                                                                                       |
|-----------------------------------------------------------------------------|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ANEXO<br>TECNICO1_CONDICIONES<br>_MINIMAS_DEL_<br>PRODUCTO_DEL_<br>SOFTWARE | 6.<br>Transferencia<br>de<br>Conocimiento y<br>Documentación | Capacitación y Transferencia de Conocimiento: El proveedor se compromete a realizar una transferencia de conocimiento efectiva al equipo de la Fiscalía, garantizando que los desarrollos y nuevas funcionalidades sean comprendidos y puedan ser gestionados por el equipo técnico de la entidad. Como mínimo a los veintiocho (28) funcionarios y contratistas de la Subdirección con una intensidad horaria mínima de 4 horas por sesión programada. | Solicitamos a la entidad aclarar: ¿Las sesiones se realizarán presenciales y virtuales, después de cada paso a producción o al finalizar la ejecución del proyecto se darán estas capacitaciones? |

#### RESPUESTA 5

La Fiscalía General de Nación, Aclara que la transferencia de conocimiento es un componente esencial del contrato y debe garantizarse conforme a las condiciones mínimas

establecidas por la FGN. En ese sentido, la entidad aclara lo siguiente:

- Modalidad de las sesiones: Las sesiones de transferencia de conocimiento podrán ser realizadas en modalidad presencial, virtual o mixta, dependiendo de la disponibilidad del equipo de la Subdirección de Sistemas de Información y de las condiciones logísticas de cada entrega. Esta flexibilidad garantiza la cobertura y participación efectiva de los 28 funcionarios y contratistas designados.
- Momento de ejecución: Las jornadas de transferencia de conocimiento deberán realizarse después de cada paso a producción o entrega parcial significativa, especialmente cuando se trate de desarrollos que introduzcan nuevas funcionalidades o afecten componentes críticos del sistema. De esta forma se asegura una comprensión oportuna del producto entregado y su correcta gestión por parte del equipo técnico institucional.
- Sesiones complementarias: Adicionalmente, la FGN podrá programar una sesión global de cierre al finalizar el contrato, con el fin de consolidar el conocimiento transferido y reforzar aspectos transversales en cuanto a arquitectura, documentación técnica, lineamientos de mantenimiento y buenas prácticas aplicadas durante la ejecución.

Lo anterior, responde a la necesidad de garantizar una adopción efectiva, sostenible y progresiva del conocimiento generado en el marco del contrato.

#### OBSERVACIÓN 6

| DOCUMENTO                                                                   | NUMERAL                                  | LO SOLICITADO - CITA TEXTUAL                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | OBSERVACIÓN                                                                                                              |
|-----------------------------------------------------------------------------|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| ANEXO<br>TECNICO1_CONDICIONES<br>_MINIMAS_DEL_<br>PRODUCTO_DEL_<br>SOFTWARE | Entorno de<br>Desarrollo y<br>Despliegue | <ul style="list-style-type: none"> <li>• Ambientes de Desarrollo y Preproducción: El contratista deberá proporcionar un ambiente de desarrollo y pruebas seguro para los aplicativos encargados por la FGN, asegurando que estos ambientes estén aislados del entorno de producción y cumplan con las políticas de seguridad.</li> </ul> <p>Los despliegues en entornos de preproducción deberán estar debidamente planificados y documentados, asegurando que se realicen todas las pruebas de</p> | Por favor aclarar si los ambientes donde estarán desplegados serán en la entidad o en la infraestructura del contratista |





|  |  |                                                     |  |
|--|--|-----------------------------------------------------|--|
|  |  | seguridad antes del despliegue final en producción. |  |
|--|--|-----------------------------------------------------|--|

#### RESPUESTA 6

La Fiscalía General de Nación, Aclara que con base en la política institucional y en las condiciones definidas en el proceso contractual, los ambientes de desarrollo, pruebas, preproducción y producción serán provistos por la Fiscalía General de la Nación (FGN). Esto incluye:

- La entidad dispondrá de la infraestructura tecnológica necesaria (física o en la nube) para alojar los entornos requeridos durante la ejecución del contrato.
- Las licencias, accesos, herramientas de despliegue y demás componentes de plataforma también serán suministrados por la FGN para asegurar una integración adecuada con los sistemas existentes.
- El contratista deberá realizar la configuración técnica, instalación, pruebas, despliegue y adecuación funcional de los aplicativos dentro de los ambientes proporcionados por la entidad y alineados con los procesos y procedimientos que la subdirección de tecnologías, estos serán de obligatorio cumplimiento y el contratista debe adherirse a la metodología actual y la evolución tecnológica que este enmarcada en el plan de transformación digital de la Entidad.
- Asimismo, deberá coordinar con el equipo técnico de la FGN para la correcta utilización de estos entornos, respetando los lineamientos de seguridad, control de acceso, auditoría y uso de recursos definidos por la Subdirección de Sistemas de Información.

Si bien el Anexo Técnico 1 menciona que el contratista "deberá proporcionar un ambiente de desarrollo y pruebas seguro", se aclara que esta responsabilidad se limita a la gestión y configuración técnica de dichos ambientes, más no a la provisión de infraestructura ni licencias, las cuales serán suministradas directamente por la FGN. Todos los despliegues deberán estar debidamente documentados, coordinados con la entidad y planificados conforme a las políticas vigentes, garantizando la trazabilidad, reversibilidad y control de cambios en cada fase del ciclo de vida del software.

#### OBSERVACIÓN 7

| DOCUMENTO                             | NUMERAL                                                  | LO SOLICITADO - CITA TEXTUAL                                                                                                                                                                                                                                                                                                                                                                                             | OBSERVACIÓN                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ANEXO_TECNICO_4<br>_EQUIPO_DE_TRABAJO | CONFORMACIÓN DE EQUIPOS DE TRABAJO Y PERFILES REQUERIDOS | Para la correcta ejecución del proyecto y la atención de los requerimientos de la entidad, se conformarán equipos de trabajo con perfiles específicos, asignados según las fases o etapas del proyecto.<br>El contratista se compromete a presentar a la FGN, en un plazo máximo de cinco (5) días hábiles posteriores a la firma del acta de inicio, al menos una hoja de vida por cada uno de los siguientes perfiles: | Solicitamos a la entidad aclarar: ¿Es necesario que los roles tengan las certificaciones mencionadas?<br>¿Todos los perfiles son necesarios Desarrollador PHP y Python, Desarrollador PHP WordPress, Líder de Desarrollo BPM, Desarrollador BPM, Implementador ECM, Administrador ECM Y BAW, ya que no es claro para estos especialistas cuanto puedan estar en el proyecto? |

#### RESPUESTA 7





La exigencia de certificaciones específicas mencionadas en los perfiles descritos en el **Anexo Técnico 4** tiene como objetivo asegurar que el personal asignado cuente con conocimientos técnicos actualizados y alineados con estándares internacionales. Sin embargo:

- **No todas las certificaciones son obligatorias para todos los perfiles.**
- La obligatoriedad o deseabilidad de una certificación dependerá del perfil específico.

El oferente debe revisar el detalle del perfil en el Anexo Técnico 4 para identificar en qué casos una certificación es requerida o valorada como parte del criterio de experiencia o formación.

Sobre la necesidad de presentar todos los perfiles desde el inicio: **Sí, se deben presentar las hojas de vida correspondientes a todos los perfiles requeridos en el Anexo Técnico 4**, en el plazo establecido (cinco días hábiles tras la firma del acta de inicio), tal como se solicita en el proceso.

Sin embargo, esto **no implica que todos los perfiles deban estar en dedicación plena desde el inicio del contrato**. La necesidad operativa de algunos especialistas (por ejemplo, *Implementador ECM, Administrador BAW*) puede activarse según la naturaleza y programación de los desarrollos priorizados. Por lo tanto, la FGN **requiere garantizar la disponibilidad del recurso**, aun si su intervención específica se da en etapas posteriores y el contratista **puede gestionar las asignaciones de carga horaria y activación gradual** de estos roles conforme a la planificación aprobada por la entidad y según la metodología de trabajo establecida

#### OBSERVACIÓN 8

| DOCUMENTO                                        | NUMERAL                                                    | LO SOLICITADO - CITA TEXTUAL                                                                                                                                                                                        | OBSERVACIÓN                                                                                                                             |
|--------------------------------------------------|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 7.<br>Complemento al<br>Pliego de<br>Condiciones | 5.3.2<br>REQUISITO<br>TÉCNICO<br>HABILITANTE<br>ADICIONAL: | El proponente (Si es proponente plural lo podrá acreditar uno de sus integrantes) deberá acreditar que cuenta con la Certificación CMMI NIVEL 3 la que debe estar vigente mínimo durante la ejecución del contrato. | Solicitamos a la entidad ajustar los pliegos a CMMI <u>DEV</u> nivel 3. Con el fin de dar claridad el tipo de CMMI que se debe aportar. |

#### RESPUESTA 8

La Fiscalía General de Nación No acepta la observación. Con el propósito de ofrecer mayor precisión terminológica y técnica a los interesados, a entidad aclara que la certificación exigida como requisito técnico habilitante corresponde a:

**CMMI para Desarrollo (CMMI-DEV) en su Nivel 3 o superior**, vigente durante la ejecución del contrato.

Esta precisión se realiza en atención a la necesidad de **alinear el modelo de madurez requerido con el objeto contractual**, el cual está centrado en el desarrollo de software a la medida, donde el modelo CMMI-DEV (y no CMMI-SVC u otros) resulta ser el aplicable conforme a las buenas prácticas reconocidas internacionalmente.

Por lo anterior, se aclara que:

- Se exige **Certificación CMMI para Desarrollo (CMMI-DEV) Nivel 3 (o superior)**.
- Esta certificación debe estar **vigente durante toda la ejecución del contrato**.

#### OBSERVACIÓN 9

ER





| DOCUMENTO                               | NUMERAL            | LO SOLICITADO - CITA TEXTUAL                                                                                                                                                                         | OBSERVACIÓN                                                                                                                                                                                                                                                       |
|-----------------------------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7. Complemento al Pliego de Condiciones | 6.2 FACTOR TÉCNICO | Para el ítem No. 1. Se otorgarán 23 puntos, al proponente (Si es proponente plural lo podrá acreditar uno de sus integrantes) que acredite la Certificación CMMI DATA y/o DEV NIVEL 3 o CMMI NIVEL 5 | Solicitamos a la entidad ajustar el requerimiento de la siguiente manera: acredite la Certificación CMMI DATA NIVEL 3 y / o CMMI DEV NIVEL 5, de esta forma se diferencia de la certificación CMMI habilitante y da claridad del tipo de certificación a aportar. |

#### RESPUESTA 9

La Fiscalía General de Nación acepta parcialmente, los proponentes para la acreditación del factor técnico ponderable podrán acreditar cualquiera de las siguientes certificaciones:

- CMMI DATA Nivel 3 o superior
- CMMI (cualquier representación) Nivel 5

Se reitera que el criterio técnico no interfiere con el requisito habilitante, sino que complementa la evaluación con puntaje adicional. La actual formulación permite que los proponentes acrediten diferentes tipos de certificaciones según su especialización y madurez, sin generar ambigüedad, ya que las categorías "DATA", "DEV" o "nivel 5" son reconocidas en el marco del modelo CMMI.

#### OBSERVACIÓN 10

| DOCUMENTO                               | NUMERAL            | LO SOLICITADO - CITA TEXTUAL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | OBSERVACIÓN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7. Complemento al Pliego de Condiciones | 6.2 FACTOR TÉCNICO | <p>Para el ítem No. 2. Se otorgarán 20,25 puntos, a la oferta que incluya un especialista en seguridad y vulnerabilidades que garantice que los desarrollos cumplan con las mejores prácticas en materia de seguridad de la información, de acuerdo con el siguiente perfil:</p> <p style="text-align: center;">Perfil<br/>Especialista de Seguridad de la Información</p> <p style="text-align: center;">Formación Académica<br/>Ingeniero de Sistemas, de Telecomunicaciones, Electrónico o ingenierías afines con Maestría en Seguridad de la Información.</p> <p>Deberá contar con por lo menos cuatro (4) de las siguientes certificaciones vigentes:</p> <ul style="list-style-type: none"> <li>• LEAD IMPLEMENTER ISO 27001 v.2022</li> <li>• CISM - CERTIFIED INFORMATION SECURITY MANAGEMENT <ul style="list-style-type: none"> <li>• CERTIFIED ETHICAL HACKER (C EH).</li> <li>• ECIH EC-COUNCIL CERTIFIED INCIDENT HANDLER</li> </ul> </li> <li>• CISSP - CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL <ul style="list-style-type: none"> <li>• CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER</li> </ul> </li> <li>• MANAGER CYBERSECURITY ISO/IEC 27032</li> </ul> | <p>Solicitamos a la entidad ajustar el perfil solicitado, teniendo en cuenta que en el desarrollo del objeto contractual del presente proceso se deben considerar otros factores a la hora de asegurar la información, considerando el tipo de información y de datos que resguarda y maneja la FGN en el desarrollo de sus funciones. Por lo anterior sugerimos a la entidad ajustar las certificaciones así:</p> <p>Debe contar con por lo menos ocho (8) las siguientes certificaciones activas y vigentes:</p> <ol style="list-style-type: none"> <li>1. MICROSOFT CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE</li> <li>2. MICROSOFT CERTIFIED CYBERSECURITY ARCHITECT EXPERT</li> <li>3. MICROSOFT CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT</li> <li>4. MICROSOFT CERTIFIED DEVOPS ENGINEER EXPERT</li> <li>5. CISM - CERTIFIED INFORMATION SECURITY MANAGEMENT de ISACA</li> <li>6. CRISC - CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL DE ISACA</li> </ol> |





|  |  |                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                          |
|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  | <p>Experiencia Mínima</p> <p>Experiencia específica de al menos diez (10) años en proyectos relacionados con seguridad de la información, en roles de Líder, Consultor, Asesor u Oficial en Seguridad de la Información.</p> | <p>7. CEH - CERTIFIED ETHICAL HACKER de EC-COUNCIL</p> <p>8. ECIH - CERTIFIED INCIDENT HANDLER de EC-COUNCIL</p> <p>9. CISSP - CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL de ISC2</p> <p>10. CDPSE - CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER de ISACA</p> <p>11. CERTIFIED SECURITY+ DE COMPTIA</p> <p>12. CERTIFIED SECURITY ENGINEER GOLD DE IPV6 FORUM</p> |
|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### RESPUESTA 10

La Fiscalía General de Nación acepta parcialmente la observación, teniendo en cuenta las tecnologías de la Entidad y el propósito del perfil el cual tiene un rol importante de arquitecto de seguridad y de conocimientos de protocolos y pruebas de seguridad para los desarrollos, se incluyen las siguientes certificaciones: MICROSOFT CERTIFIED DEVOPS ENGINEER EXPERT y CERTIFIED SECURITY+ DE COMPTIA:

- DevOps seguro y automatizado:  
DevOps Engineer Expert permite integrar seguridad en el pipeline de CI/CD, aplicando prácticas como análisis estático de código, pruebas automatizadas y despliegues seguros.
- Cultura de seguridad en todo el ciclo:  
Security+ y otras certificaciones fomentan una cultura de seguridad entre desarrolladores, testers, arquitectos y líderes de proyecto.

Por lo anterior, se ajusta el requerimiento del Perfil de Especialista de Seguridad de la Información, el cual quedará así:

| Perfil                                      | Formación Académica                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Experiencia Mínima                                                                                                                                                                                 |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Especialista de Seguridad de la Información | <p>Ingeniero de Sistemas, de Telecomunicaciones, Electrónico o ingenierías afines según el NBC del SNIES, con Maestría en Seguridad de la Información o afines según el NBC del SNIES</p> <p>Deberá contar con por lo menos cinco (5) de las siguientes certificaciones vigentes:</p> <ul style="list-style-type: none"> <li>• LEAD IMPLEMENTER ISO 27001 v.2022</li> <li>• CISM - CERTIFIED INFORMATION SECURITY MANAGEMENT</li> <li>• CERTIFIED ETHICAL HACKER (CEH).</li> <li>• ECIH EC-COUNCIL CERTIFIED INCIDENT HANDLER</li> <li>• CISSP - CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL</li> <li>• CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER</li> <li>• MANAGER CYBERSECURITY ISO/IEC 27032</li> <li>• MICROSOFT CERTIFIED DEVOPS ENGINEER EXPERT</li> <li>• CERTIFIED SECURITY+ DE COMPTIA</li> </ul> | <p>Experiencia específica de al menos diez (10) años en proyectos relacionados con seguridad de la información, en roles de Líder, Consultor, Asesor u Oficial en Seguridad de la Información.</p> |





## 6. EYC INGENIEROS SAS

### OBSERVACIÓN 1

| DOCUMENTO | REQUERIMIENTO                                                                                                                                                                                                           | OBSERVACIÓN                                                                                    |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| ANEXOS    | Soporte Post-Entrega: Después de la entrega e implementación de los productos, el contratista brindará soporte técnico para estabilizar los sistemas y corregir posibles incidencias en un periodo acordado con la FGN. | Solicitamos a la entidad aclarar: ¿ Este tiempos esta contemplado en la duración del proyecto? |

### RESPUESTA 1

La Fiscalía General de Nación , Aclara que Sí, el tiempo destinado al soporte técnico post-entrega para la estabilización de los desarrollos e identificación/corrección de posibles incidencias está contemplado dentro del plazo de ejecución del contrato.

Este periodo forma parte integral de la metodología de trabajo que implica:

- El paso a producción de las funcionalidades.
- La estabilización funcional y técnica de los desarrollos.
- El acompañamiento post-despliegue para garantizar que los productos cumplen adecuadamente con los requisitos definidos por la FGN.

Asimismo, de acuerdo con el numeral 2.6 del Estudio Previo, el contratista también debe garantizar el funcionamiento de las funcionalidades entregadas durante un periodo adicional de 12 meses posterior a la finalización del contrato, lo cual se debe respaldar mediante garantía, más no implica una extensión de la duración del contrato como tal.

### OBSERVACIÓN 2

| DOCUMENTO | REQUERIMIENTO                                                                                                                                                                                                                                                                                  | OBSERVACIÓN                                                                                                                              |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| ANEXOS    | Despliegue en Ambientes de Preproducción: Antes de que cualquier funcionalidad sea desplegada en producción, será implementada en un entorno de preproducción, donde se realizarán pruebas finales para asegurar que el sistema funcione correctamente en un entorno similar al de producción. | Solicitamos a la entidad aclarar: ¿ Este entorno lo entregara la entidad o nosotros como contratistas debemos implementar este ambiente? |

### RESPUESTA 2

La Fiscalía General de Nación , Aclara que el entorno de preproducción será provisto **por la Fiscalía General de la Nación tal** como se establece en la respuesta previamente brindada a una observación anterior del proceso, los ambientes tecnológicos requeridos para el desarrollo, pruebas y despliegue incluidos licencias, accesos, plataformas y recursos de infraestructura serán suministrados por la FGN.

Esto incluye:

- Entorno de desarrollo.
- Entorno de pruebas y preproducción.
- Entorno de producción.
- Accesos y configuraciones necesarias para la integración con sistemas existentes.

El contratista no debe implementar ni proveer el entorno de preproducción, la FGN proporcionará los ambientes tecnológicos, conforme a las condiciones del proceso. El contratista deberá hacer uso de dichos entornos para desplegar, validar y estabilizar las funcionalidades antes de pasar a producción.

- El contratista deberá realizar la configuración técnica, instalación, pruebas, despliegue y adecuación funcional de los aplicativos dentro de los ambientes proporcionados por la entidad y alineados con los procesos y procedimientos que la subdirección de tecnologías, estos serán de obligatorio cumplimiento y el contratista debe adherirse a la metodología actual y la evolución tecnológica que este enmarcada en el plan de transformación digital de la Entidad.





- Asimismo, deberá coordinar con el equipo técnico de la FGN para la correcta utilización de estos entornos, respetando los lineamientos de seguridad, control de acceso, auditoría y uso de recursos definidos por la Subdirección de Sistemas de Información.

### OBSERVACIÓN 3

| DOCUMENTO | REQUERIMIENTO                                                                                                                                      | OBSERVACIÓN                                                                                                  |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| ANEXOS    | Se realizará una evaluación continua de la efectividad de la transferencia de conocimiento, a través de encuestas, entrevistas y pruebas prácticas | Solicitamos a la entidad aclarar: ¿Estas evaluaciones las realizará al entidad o nosotros como contratistas? |

### RESPUESTA 3

La Fiscalía General de Nación, Aclara que el requisito las evaluaciones sobre la efectividad de la transferencia de conocimiento serán coordinadas y aplicadas directamente por la Fiscalía General de la Nación, en ejercicio de sus funciones de supervisión y aseguramiento de la calidad del servicio contratado.

Estas evaluaciones pueden incluir:

- Aplicación de encuestas a los funcionarios y contratistas de la Subdirección TIC receptores de la capacitación.
- Entrevistas y retroalimentación cualitativa sobre el desempeño del equipo formador.
- Pruebas prácticas o técnicas, que validen la apropiación efectiva del conocimiento impartido.

El contratista, por su parte, debe garantizar que las sesiones de capacitación cumplan con:

- El contenido requerido.
- La intensidad horaria definida.
- La disposición de material de apoyo (presentaciones, guías, manuales, etc.).
- La participación de formadores con competencias técnicas y habilidades pedagógicas.

**Responsable de evaluación:** Fiscalía General de la Nación. **Responsable de ejecución de la capacitación:** Contratista. **Objetivo de las evaluaciones:** Verificar que el equipo de la FGN haya comprendido y apropiado el conocimiento necesario para la continuidad de los desarrollos y operación de los sistemas intervenidos.

### OBSERVACIÓN 4

| DOCUMENTO                                                           | REQUERIMIENTO                                                                                                                                                                                                                                                                           | OBSERVACIÓN                                                     |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| ANEXO<br>TECNICO1_CONDICIONES_MINIMAS_DEL_PRODUC<br>TO_DEL_SOFTWARE | Soporte, Actualización y Mantenimiento (SAM): Prestación de servicios de soporte preventivo y correctivo a los sistemas de información nuevos o actuales que posea la Fiscalía, asegurando la estabilidad, seguridad y optimización de los mismos, con disponibilidad de atención 7x24. | Solicitamos a la entidad aclarar: ¿Esto será en sitio o remoto? |

### RESPUESTA 4

La Fiscalía General de Nación, Aclara que la prestación del servicio de soporte técnico preventivo y correctivo, según lo establecido en el Anexo Técnico 1, se realizará de forma remota, salvo en aquellos casos excepcionales en los que la Subdirección de Tecnologías de la Información (Subdirección TIC) de la Fiscalía General de la Nación requiera explícitamente la presencia en sitio

ER





por motivos de seguridad, acceso restringido o soporte a infraestructura local que no pueda ser operada de forma remota, las condiciones específicas son:

- Modalidad predominante: Remota.
- Intervenciones presenciales: Se realizarán únicamente bajo solicitud formal de la FGN.
- Cobertura del servicio: 7 días a la semana, 24 horas al día (7x24), aplicando a ambos tipos de intervención (preventiva y correctiva).
- Criterio de seguridad: Se atenderán las políticas y protocolos internos definidos por la Fiscalía para el acceso a ambientes sensibles.

#### OBSERVACIÓN 5

| DOCUMENTO                                                           | REQUERIMIENTO                                                                                                                                         | OBSERVACIÓN                                                                                                                       |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| ANEXO<br>TECNICO1_CONDICIONES_MINIMAS_DEL<br>_PRODUCTO_DEL_SOFTWARE | <ul style="list-style-type: none"><li>• Revisión y retrospectiva al final del sprint.</li><li>• Despliegue en ambiente productivo de la FGN</li></ul> | Solicitamos a la entidad aclarar: ¿ los despliegues a producción se encuentran contemplados dentro de la ejecución del proyecto ? |

#### RESPUESTA 5

La Fiscalía General de Nación , Aclara que Sí, los despliegues a ambiente productivo de la Fiscalía General de la Nación se encuentran contemplados dentro de la ejecución del proyecto, conforme a la metodología ágil adoptada para la ejecución contractual, en la cual cada Sprint culmina con una entrega potencialmente desplegable.

El contratista debe realizar los despliegues a producción de las funcionalidades desarrolladas durante el proyecto, siguiendo los procedimientos y protocolos establecidos por la FGN, estos despliegues forman parte integral del ciclo de desarrollo y son responsabilidad del contratista hasta la estabilización del componente liberado.

El flujo contempla desarrollo, pruebas, despliegue a preproducción, validación funcional y técnica, y finalmente, despliegue a producción, los despliegues deberán ser planificados, documentados y ejecutados con previa autorización de la FGN, conforme al cronograma de iteraciones o Sprints.

El contratista deberá realizar la configuración técnica, instalación, pruebas, despliegue y adecuación funcional de los aplicativos dentro de los ambientes proporcionados por la entidad y alineados con los procesos y procedimientos que la subdirección de tecnologías, estos serán de obligatorio cumplimiento y el contratista debe adherirse a la metodología actual y la evolución tecnológica que este enmarcada en el plan de transformación digital de la Entidad.

Asimismo, deberá coordinar con el equipo técnico de la FGN para la correcta utilización de estos entornos, respetando los lineamientos de seguridad, control de acceso, auditoría y uso de recursos definidos por la Subdirección de Sistemas de Información.

#### OBSERVACIÓN 6

| DOCUMENTO | REQUERIMIENTO | OBSERVACIÓN |
|-----------|---------------|-------------|
|-----------|---------------|-------------|





|                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                     |
|-------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| ANEXO<br>TECNICO1_CONDICIONES_MINIMAS_<br>DEL_<br>PRODUCTO_DEL_SOFTWARE | <ul style="list-style-type: none"><li>• Ambientes de Desarrollo y Preproducción: El contratista deberá proporcionar un ambiente de desarrollo y pruebas seguro para los aplicativos encargados por la FGN, asegurando que estos ambientes estén aislados del entorno de producción y cumplan con las políticas de seguridad.</li></ul> <p>Los despliegues en entornos de preproducción deberán estar debidamente planificados y documentados, asegurando que se realicen todas las pruebas de seguridad antes del despliegue final en producción.</p> | Solicitamos a la entidad aclarar: ¿ Estos ambiente donde estaran desplegados en la entidad o en la infraestructura del contratista? |
|-------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|

#### RESPUESTA 6

La Fiscalía General de Nación , Aclara que los ambientes de desarrollo, pruebas, preproducción y producción serán **proporcionados y administrados por la Fiscalía General de la Nación (FGN)**. El contratista no debe implementar ni alojar estos entornos en su propia infraestructura.

- Aunque en el Anexo Técnico 1 se menciona que el contratista debe asegurar ambientes seguros, esta obligación se refiere a las **condiciones técnicas y operativas** bajo las cuales el contratista debe trabajar, **no a la provisión física o lógica de los entornos**.
- Tal como se ha indicado en otras observaciones previas resueltas, **todas las plataformas, licencias, ambientes y accesos serán proporcionados por la FGN**, permitiendo al contratista desarrollar, probar y desplegar funcionalidades en entornos controlados por la entidad.
- **La responsabilidad del contratista se limita a operar sobre los ambientes proporcionados por la FGN**, aplicando prácticas seguras de desarrollo, pruebas y despliegue.
- No se debe interpretar que el contratista deba instalar o mantener ambientes en su infraestructura propia.

Los ambientes donde estarán desplegadas las funcionalidades serán **infraestructura de la FGN**, y el contratista deberá asegurar que su uso sea conforme con las políticas de seguridad de la entidad. Esta precisión será incluida como parte de las aclaraciones al proceso sin modificar el alcance técnico general.

#### OBSERVACIÓN 7

| DOCUMENTO                                                           | REQUERIMIENTO                                                                                                                                                                                                                                                                                                                                             | OBSERVACIÓN                                                                                                                                                                      |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ANEXO<br>TECNICO1_CONDICIONES_MINIMAS_DEL_PRODUC<br>TO_DEL_SOFTWARE | Transferencia de Infraestructura:<br>En el caso de que el contrato llegue a su fin o se realice una transición hacia otro proveedor, el contratista deberá realizar la transferencia completa de la infraestructura técnica relacionada con los desarrollos, incluyendo las configuraciones de los ambientes, licencias y documentación técnica asociada. | Solicitamos a la entidad aclarar: ¿ Si ustedes poseen protocolos de este tipo de trasnferencia ya que es un tema complejo que requerira el acompañamiento por parte de ustedes ? |

#### RESPUESTA 7

ER





La Fiscalía General de Nación , Aclara que Sí, la Fiscalía General de la Nación cuenta con lineamientos y procedimientos internos establecidos para realizar procesos de transferencia técnica y operativa al cierre de contratos o ante cambios de proveedor. Por lo tanto, el contratista contará con **acompañamiento técnico y administrativo de la entidad** durante todo el proceso de transición.

Durante el proceso de transferencia, la Subdirección de Tecnología de la Información y las comunicaciones asignará personal técnico responsable de guiar, revisar y validar los entregables asociados. Este acompañamiento garantiza que la información técnica, configuraciones, documentación y accesos queden formalmente entregados y validados.

La FGN proporcionará al contratista los documentos **oficiales** para la transferencia técnica asociada a los desarrollos. El contenido mínimo esperado incluye: manuales de instalación, arquitectura, configuración de ambientes, uso de licencias, integración con servicios existentes, y trazabilidad de versiones.

La obligación de entrega se limita exclusivamente a los elementos **relacionados con los desarrollos y configuraciones realizadas por el contratista** durante la ejecución del contrato. No se requiere la entrega de infraestructura física, ya que esta pertenece a la FGN y es administrada por la entidad.

La transferencia técnica al finalizar el contrato se desarrollará bajo protocolos definidos por la FGN y con acompañamiento institucional. El contratista no se encuentra solo en este proceso, y recibirá apoyo para garantizar una transición ordenada y documentada.

#### OBSERVACIÓN 8

| DOCUMENTO                                                           | REQUERIMIENTO                                                                                                                                                                                                                                                                                                                                                                                                                                                               | OBSERVACIÓN                                                                                                                   |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| ANEXO<br>TECNICO1_CONDICIONES_MINIMAS_DEL_PRODU<br>CTO_DEL_SOFTWARE | <ul style="list-style-type: none"><li>● Cierre de Ambientes de Desarrollo: El contratista deberá proceder a dismantelar o devolver los ambientes de desarrollo utilizados para la ejecución del contrato, asegurando que toda la información confidencial o sensible de la FGN ha sido debidamente eliminada de estos entornos. Antes de su cierre, se deberá asegurar que todos los datos y configuraciones relevantes han sido migrados o transferidos a la FGN</li></ul> | Solicitamos a la entidad aclarar: ¿ El tiempo para el cierre de estos ambientes esta contemplado en la duración del proyecto? |

#### RESPUESTA 8

La Fiscalía General de Nación , Aclara que Sí, el tiempo requerido para el cierre técnico, dismantelamiento o devolución de los ambientes de desarrollo está contemplado dentro del plazo de ejecución del contrato. Este cierre hace parte del ciclo final de actividades previstas, alineado con el proceso de entrega final y transferencia técnica a la Fiscalía General de la Nación.

El contratista debe planificar e incluir dentro del cronograma del proyecto las actividades relacionadas con la eliminación de datos sensibles, respaldo de configuraciones y generación de documentación técnica sobre el entorno de desarrollo. Las actividades de cierre no podrán extenderse más allá del plazo contractual establecido.

La Subdirección de Tecnología de la Información y las comunicaciones de la FGN realizará el acompañamiento y validación del proceso de cierre de ambientes, asegurando que se cumplan los estándares de seguridad y trazabilidad requeridos. Se validará que





todos los entregables asociados al ambiente (scripts, configuraciones, bases de datos, versiones, documentación) estén debidamente entregados.

Se sugiere al contratista definir en su propuesta un cronograma detallado que contemple una fase de cierre y transferencia, de tal forma que dichas actividades no interfieran con la operación ni excedan el tiempo previsto de ejecución.

El proceso de cierre y desmantelamiento de ambientes debe ejecutarse dentro del término total del contrato. No se contemplarán tiempos adicionales fuera del plazo contractual para esta actividad. La entidad realizará seguimiento para asegurar que la transferencia y eliminación de datos se cumpla conforme a los lineamientos de seguridad y confidencialidad establecidos.

El contratista debe implementar los procesos y procedimientos internos de seguridad y gestión de TI, que estén relacionados con el requerimiento solicitado, incluyendo los cambios que se realicen durante la vigencia del contrato y que sean de carácter obligatorio para los procesos internos de la Subdirección de Tecnología.

#### OBSERVACIÓN 9

| DOCUMENTO                                        | REQUERIMIENTO                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | OBSERVACIÓN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7.<br>Complemento<br>al Pliego de<br>Condiciones | <p>Para el ítem No. 2. Se otorgarán 20,25 puntos, a la oferta que incluya un especialista en seguridad y vulnerabilidades que garantice que los desarrollos cumplan con las mejores prácticas en materia de seguridad de la información, de acuerdo con el siguiente perfil:</p> <p>Perfil<br/>Especialista de Seguridad de la Información</p> <p>Formación Académica<br/>Ingeniero de Sistemas, de Telecomunicaciones, Electrónico o ingenierías afines con Maestría en Seguridad de la Información .....</p> | <p>Solicitamos a la entidad incluir las siguientes certificaciones con el fin de asegurar la pluralidad de oferentes al rol puntuable:</p> <ol style="list-style-type: none"><li>1. MICROSOFT CERTIFIED CYBERSECURITY ARCHITECT EXPERT</li><li>2. MICROSOFT CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT</li><li>3. MICROSOFT CERTIFIED DEVOPS ENGINEER EXPERT</li><li>4. CRISC - CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL DE ISACA</li><li>5. CERTIFIED SECURITY+ DE COMPTIA</li><li>6. CERTIFIED SECURITY ENGINEER GOLD DE IPV6 FORUM</li></ol> |

#### RESPUESTA 9

La Fiscalía General de Nación acepta parcialmente la observación, teniendo en cuenta las tecnologías de la Entidad y el propósito del perfil el cual tiene un rol importante de arquitecto de seguridad y de conocimientos de protocolos y pruebas de seguridad para los desarrollos, se incluyen las siguientes certificaciones: MICROSOFT CERTIFIED DEVOPS ENGINEER EXPERT y CERTIFIED SECURITY+ DE COMPTIA:

DevOps seguro y automatizado:

- DevOps Engineer Expert permite integrar seguridad en el pipeline de CI/CD, aplicando prácticas como análisis estático de código, pruebas automatizadas y despliegues seguros.

Cultura de seguridad en todo el ciclo:

- Security+ y otras certificaciones fomentan una cultura de seguridad entre desarrolladores, testers, arquitectos y líderes de proyecto.

Por lo anterior, se ajusta el requerimiento del Perfil de Especialista de Seguridad de la Información, el cual quedará así:

|        |                     |                    |
|--------|---------------------|--------------------|
| Perfil | Formación Académica | Experiencia Mínima |
|--------|---------------------|--------------------|

EE





|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                             |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Especialista de Seguridad de la Información | <p>Ingeniero de Sistemas, de Telecomunicaciones, Electrónico o ingenierías afines según el NBC del SNIES, con Maestría en Seguridad de la Información o afines según el NBC del SNIES</p> <p>Deberá contar con por lo menos cinco (5) de las siguientes certificaciones vigentes:</p> <ul style="list-style-type: none"> <li>• LEAD IMPLEMENTER ISO 27001 v.2022</li> <li>• CISM - CERTIFIED INFORMATION SECURITY MANAGEMENT</li> <li>• CERTIFIED ETHICAL HACKER (C EH).</li> <li>• ECIH EC-COUNCIL CERTIFIED INCIDENT HANDLER</li> <li>• CISSP - CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL</li> <li>• CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER</li> <li>• MANAGER CYBERSECURITY ISO/IEC 27032</li> <li>• MICROSOFT CERTIFIED DEVOPS ENGINEER EXPERT</li> <li>• CERTIFIED SECURITY+ DE COMPTIA</li> </ul> | Experiencia específica de al menos diez (10) años en proyectos relacionados con seguridad de la información, en roles de Líder, Consultor, Asesor u Oficial en Seguridad de la Información. |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### 7. INTEGRA S.A.S - BIC

#### OBSERVACION 1

OBSERVACIÓN No. 1. NUMERAL 6.2 FACTOR TÉCNICO Respecto del requerimiento previsto en el ítem 1 "Certificación CMMI DATA y/o DEV NIVEL 3 o CMMI NIVEL 5", se solicita a la entidad eliminar ese ítem como factor ponderable toda vez que dicha certificación corresponde a un sistema de gestión calidad en el desarrollo de software y gestión de datos. Certificaciones que de conformidad al artículo 5 parágrafo 2 de la ley 1150 de 2007 están prohibidas ya que limitan la participación y pluralidad de oferentes. Al respecto la ley indica:

PARÁGRAFO 2o. Las certificaciones de sistemas de gestión de calidad no serán objeto de calificación, ni podrán establecerse como documento habilitante para participar en licitaciones o concursos. El legislador quiso evitar la imposición de requisitos subjetivos tendientes a limitar la libre concurrencia y libre competencia pues en el mercado de compras públicas no pueden existir restricciones a la participación o evaluación de las condiciones técnicas en los proceso de contratación limitándolas a que los oferentes tengan certificaciones en sistemas de gestión de calidad que no evalúan las capacidades o aptitudes técnicas del oferente o del servicio que ofrece, pues en el sector TIC existen muchas empresas que a pesar de no contar con las certificaciones CMMI, cuentan con la capacidad para prestar servicios con óptimos estándares en el desarrollo de software y existen otros criterios técnicos para evaluar esa capacidad por parte de la entidad contratante.

Es pertinente aclarar que las certificaciones CMMI, aunque reconocidas internacionalmente como modelos de madurez para la mejora de procesos, no constituyen una norma técnica

obligatoria ni forman parte del marco regulatorio aplicable al desarrollo de software en Colombia. En el contexto jurídico colombiano, los estándares y normas técnicas de obligatorio cumplimiento para este sector son aquellos expedidos por organismos como el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) o establecidos en reglamentos técnicos expedidos por la



autoridad competente. En consecuencia, la exigencia de una certificación CMMI como criterio para otorgar puntaje en el factor técnico de un proceso de selección carece de legitimidad legal por no estar sustentada en una norma de carácter vinculante y de pertinencia técnica al no constituir un requisito indispensable para garantizar la calidad o idoneidad del software conforme a las normas nacionales. Ahora bien, no existe una justificación objetiva en los documentos que hacen parte de los estudios previos que le permitan a la entidad contratante justificar jurídica y técnicamente las razones por cuales considera por un lado que la inclusión de tales certificaciones como criterio puntuable le permite evaluar la calidad del servicio a contratar y por otro lado las razones que sustentan incluir requisitos prohibidos expresamente por la ley, pues si bien la entidad tiene libertad para configurar el pliego de condiciones esta se encuentra limitada por la ley, en este caso por el artículo 5 parágrafo 2 de la ley 1150 de 2007. Al respecto Colombia Compra Eficiente, en los conceptos del 8 de julio, 13 y 29 de agosto, 25 de septiembre, 15 de noviembre y 16 de diciembre de 2019 – radicados Nos. 2201913000004727, 2201913000005855, 2201913000006343, 2201913000007131, 2201913000008520 y 2201913000009295–, analizó el alcance del artículo 5, parágrafo 2, de la Ley 1150 de 2007. Igualmente, mediante el concepto C-166 de 2020, esta Agencia se pronunció en relación con la posibilidad de exigir certificaciones de gestión de calidad como requisito habilitante o como requisito ponderable, concluyendo que: (...) “El artículo 5, parágrafo 2, de la Ley 1150 de 2007 establece que las «certificaciones de sistemas de gestión de calidad no serán objeto de calificación, ni podrán establecerse como documento habilitante para participar en licitaciones o concursos». Es del caso precisar que esta prohibición comprende los requisitos habilitantes y, además, los requisitos puntuables, pues la norma prohíbe expresamente que dichas certificaciones sean objeto de calificación. En efecto, el parágrafo en mención establece:

PARÁGRAFO 2o. Las certificaciones de sistemas de gestión de calidad no serán objeto de calificación, ni podrán establecerse como documento habilitante para participar en licitaciones o concursos. (Cursivas fuera de texto) Ese es el criterio actual en el Consejo de Estado. En efecto, en concepto del 20 de mayo del 2010, la Sala de Consulta y Servicio Civil de dicha Corporación aclaró que «[...] Los certificados de gestión de calidad no se pueden solicitar a los proponentes, ni como requisito habilitante para participar en los procesos de selección, ni para otorgar puntaje»<sup>1</sup>. Es del caso precisar que, a juicio de la Agencia Nacional de Contratación Pública, tal prohibición no se restringe a la exigencia de la certificación o el documento como tal, sino que debe entenderse en relación con la implementación de un sistema de gestión de calidad en sí mismo. En ese sentido, lo que prohíbe el legislador es que la entidad les exija a los proponentes, a título de requisito habilitante o calificable, la implementación de un sistema de gestión de calidad. Ese es el efecto útil de la norma sub examine, pues, aceptar una lectura exegética del parágrafo, implicaría asumir que una entidad está autorizada para exigir como requisito habilitante el cumplimiento de normas que hacen parte de sistemas de gestión de la calidad, verbi gracia ISO o ICONTEC, entre otras, sin pedir expresamente el documento o certificado que se expide al verificar estos estándares de calidad, lo cual, por un lado, le resta efectos prácticos a la prohibición establecida por el legislador y, por el otro, desconoce la finalidad perseguida por la norma”.

#### RESPUESTA 1

La Fiscalía General de Nación No acepta la observación, la razón por la cual CMMI (Capability Maturity Model Integration) no se considera una certificación de gestión de calidad radica en su enfoque, propósito y estructura.

- CMMI es un modelo de mejora de procesos que ayuda a las organizaciones a evaluar y mejorar la madurez de sus procesos en áreas como desarrollo de software, ingeniería de sistemas y gestión de servicios.
- CMMI busca optimizar procesos internos para mejorar el rendimiento organizacional, la eficiencia y la capacidad de entrega.
- CMMI se organiza en niveles de madurez (del 1 al 5), que indican el grado de sofisticación y control de los procesos de una organización. No siempre implica una certificación externa, sino una evaluación interna o por terceros autorizados
- Aunque CMMI incluye prácticas de aseguramiento de calidad, su enfoque es más amplio y técnico, orientado a la madurez organizacional
- En contraposición con lo anterior, las certificaciones de gestión de calidad:
- Generalmente son una norma de gestión de calidad que establece requisitos para implementar un sistema de gestión de calidad (SGC) aplicable a cualquier tipo de organización
- Se enfocan en garantizar la calidad del producto o servicio entregado al cliente, asegurando la satisfacción del cliente y el cumplimiento de requisitos legales y reglamentarios
- Requieren de una auditoría externa por parte de un organismo certificador acreditado, que verifica el cumplimiento de los requisitos del estándar y otorga una certificación oficial





- Están diseñadas como un sistema de gestión de calidad, con requisitos específicos para la mejora continua, enfoque al cliente y gestión de riesgos
- En conclusión CMMI no es una certificación de gestión de calidad porque:
- No está centrado exclusivamente en la calidad del producto o servicio.
- No sigue el esquema de certificación formal
- Su propósito es mejorar la madurez de los procesos, no necesariamente certificar la calidad organizacional.

#### 8. TIKKA TECHNOLOGY S.A.S.

##### OBSERVACION 1

###### 1. REQUISITO TÉCNICO HABILITANTE ADICIONAL

En el numeral 5.3.2 REQUISITO TÉCNICO HABILITANTE ADICIONAL del documento Complemento al **Pliego de Condiciones** la entidad establece:

###### 5.3.2 REQUISITO TÉCNICO HABILITANTE ADICIONAL:

El proponente (Si es proponente plural lo podrá acreditar uno de sus integrantes) deberá acreditar que cuenta con la Certificación CMMI NIVEL 3 la que debe estar vigente mínimo durante la ejecución del contrato.

**NOTA:** Respecto del certificado aportado por el proponente, la FGN realizará la comprobación en la página oficial de evaluación del Modelo en el link:

<https://cmminstitute.com/pars/?StateId=722fc265-61bf-436f-9ab5-c7a2d3c1a42f>

En caso en el cual el oferente no se encuentre listado en la página oficial de evaluación conforme a los anteriores criterios, será inhabilitado

###### SOLICITUD:

Dado lo anterior solicitamos muy respetuosamente a la entidad adicione al texto la palabra **mínimo**, quedando de la siguiente manera:

*El proponente (Si es proponente plural lo podrá acreditar uno de sus integrantes) deberá acreditar que cuenta como **mínimo** con la Certificación CMMI NIVEL 3 la que debe estar vigente mínimo durante la ejecución del contrato.*

Teniendo en cuenta que la certificación CMMI Nivel 5 incluye todos los procesos del Nivel 3.

Adicionalmente en el pliego de condiciones se exige que la Certificación CMMI NIVEL 3 debe estar vigente mínimo durante la ejecución del contrato., lo cual se valora como parte del cumplimiento de requisitos habilitantes.

Sin embargo, esta exigencia puede generar ambigüedades en su aplicación, considerando que:

- Las certificaciones CMMI® tienen una vigencia determinada (por lo general de 3 años).
- Existen escenarios en los que la certificación puede expirar durante la ejecución del contrato, sin que ello implique la pérdida de las capacidades organizacionales adquiridas.
- Un proveedor responsable puede encontrarse en proceso de renovación de dicha certificación, y continuar garantizando las buenas prácticas de desarrollo bajo el modelo CMMI®.

El Capability Maturity Model Integration (CMMI®) es un modelo de mejora continua de procesos, no un sistema de gestión con recertificación automática. La vigencia de la certificación CMMI-DEV depende del ciclo de evaluación SCAMPI (Standard CMMI Appraisal Method for Process Improvement), que tiene una duración determinada. Su renovación implica un proceso interno de mejora continua, pero la expiración momentánea del certificado no implica pérdida inmediata de capacidad organizacional.

Por lo tanto, el enfoque adecuado no debe ser únicamente la fecha de vigencia del certificado, sino el compromiso del proveedor de mantener vigente la certificación durante la ejecución del contrato, ya sea a través de renovación o mantenimiento de la evaluación formal.

Con fundamento en lo anterior, se solicita modificar el pliego para incluir la posibilidad de que:

"En caso de que la certificación CMMI ofrecida tenga una fecha de expiración dentro del período de ejecución del contrato, el proponente seleccionado deberá presentar una carta firmada por su representante legal en la que se compromete a mantener vigente dicha certificación durante todo el período de ejecución, incluyendo su renovación o recertificación del modelo CMMI "

##### RESPUESTA 1

La Fiscalía General de Nación acepta la observación, se incluirá el texto dentro de los documentos definitivos de la así:





En caso de que la certificación CMMI ofrecida tenga una fecha de expiración dentro del periodo de ejecución del contrato, el proponente seleccionado deberá presentar una carta firmada por su representante legal en la que se compromete a mantener vigente dicha certificación durante todo el periodo de ejecución, incluyendo su renovación o recertificación del modelo CMMI

## OBSERVACION 2

### 2. FACTOR TÉCNICO - Certificación CMMI DATA y/o DEV NIVEL 3 o CMMI NIVEL 5

En el numeral 6.2 FACTOR TÉCNICO del documento Complemento al Pliego de Condiciones la entidad establece:

#### 6.2 FACTOR TÉCNICO

La oferta técnica tiene un puntaje de hasta 43.25 puntos, y se calculará de acuerdo con los siguientes criterios.

Tabla. Factor Técnico

| item | Criterio                                               | Puntaje      |
|------|--------------------------------------------------------|--------------|
| 1    | Certificación CMMI DATA y/o DEV NIVEL 3 o CMMI NIVEL 5 | 23           |
| 2    | Especialista en seguridad de la información            | 20,25        |
|      | <b>TOTAL</b>                                           | <b>43,25</b> |

**Para el ítem No. 1.** Se otorgarán 23 puntos, al proponente (Si es proponente plural lo podrá acreditar uno de sus integrantes) que acredite la Certificación CMMI DATA y/o DEV NIVEL 3 o CMMI NIVEL 5

**NOTA 1:** Respecto del certificado aportado por el proponente, la FGN realizará la comprobación en la página oficial de evaluación del Modelo en el link <https://cmmiinstitute.com/pars/?StateId=722fc265-61bf-436f-9ab5-c7a2d3c1a42f>

**NOTA 2:** El proveedor debe estar listado en la página oficial del CMMI, aplicable para el país ("Country") "Colombia".

### 1.1 OBSERVACIÓN

El modelo CMMI (Capability Maturity Model Integration), desarrollado por el CMMI Institute, define cinco niveles de madurez que reflejan la capacidad de una organización para gestionar y mejorar sus procesos.

| Nivel                   | Descripción                                                                                      | Capacidades Típicas                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Nivel 3 –<br>Defined    | Procesos están documentados, estandarizados y se siguen en toda la organización.                 | Buen nivel de consistencia y control en procesos; sin embargo, aún no hay control estadístico ni optimización continua.    |
| Nivel 5 –<br>Optimizing | Procesos están continuamente mejorados mediante la medición cuantitativa y la retroalimentación. | Uso de métricas estadísticas, análisis de causa raíz, mejora continua y predictiva; capacidad altamente madura de gestión. |

La diferencia técnica y de madurez organizacional entre los niveles 3 y 5 es profunda y significativa:

- CMMI Nivel 3 demuestra una organización que ha definido e implementado procesos estándar.
- CMMI Nivel 5 demuestra una organización que no solo tiene procesos definidos, sino que también mide, controla y mejora continuamente sus procesos mediante métodos estadísticos avanzados, lo que garantiza mayor calidad, predictibilidad y eficiencia en la prestación de servicios.

Por lo tanto, desde un punto de vista técnico y de madurez organizacional:

- La certificación CMMI Nivel 5 incluye todos los procesos del Nivel 3 y añade prácticas de gestión cuantitativa de procesos, análisis de causas raíces y mejora continua basada en datos. Por tanto, una organización certificada en Nivel 5 cumple plenamente, y con mayor rigor, los estándares exigidos para Nivel 3.
- Tratar ambos niveles como equivalentes para efectos de la puntuación desconoce la diferencia sustancial entre niveles de madurez y desincentiva la participación de proponentes con niveles superiores de calidad, quienes han hecho inversiones significativamente mayores en sus procesos.





#### SOLICITUD:

Solicito respetuosamente a la entidad contratante ajustar el criterio de evaluación, diferenciando el puntaje otorgado según el nivel de certificación CMMI, de forma proporcional al nivel de madurez, por ejemplo:

- CMMI DEV o DATA Nivel 3: hasta 15 puntos
- CMMI DEV o DATA Nivel 5: hasta 23 puntos

Este ajuste promoverá un tratamiento equitativo entre proponentes, basado en la capacidad real y el esfuerzo organizacional demostrado mediante dichas certificaciones.

#### RESPUESTA 2

La Fiscalía General de Nación No acepta la observación, la certificaciones exigidas para el factor técnico ponderable corresponden a:

- CMMI DATA Nivel 3 o superior
- CMMI (cualquier representación) Nivel 5

El estándar definido en el proceso, CMMI DEV o DATA Nivel 3, ha sido establecido como criterio habilitante y puntuable con base en su reconocimiento internacional, aplicabilidad técnica y suficiencia para garantizar la calidad y madurez de los procesos de desarrollo.

Si bien los niveles superiores del modelo CMMI (niveles 4 y 5) representan una mayor madurez organizacional, su inclusión como diferenciador de puntaje podría generar una restricción injustificada de la competencia, al favorecer únicamente a organizaciones con capacidades avanzadas que no necesariamente son requeridas para el cumplimiento del objeto contractual.

En consecuencia, mantener un puntaje uniforme para las certificaciones CMMI a partir del nivel 3 permite garantizar la pluralidad de oferentes, sin desmedro de la calidad técnica exigida, y en concordancia con los principios de objetividad, proporcionalidad y libre concurrencia que rigen la contratación pública.

#### 9. BIS@ CORPORATION

#### OBSERVACION 1

Los pliegos de condiciones establecen:

##### 5.3.2 REQUISITO TÉCNICO HABILITANTE ADICIONAL:

El proponente (Si es proponente plural lo podrá acreditar uno de sus integrantes) deberá acreditar que cuenta con la Certificación CMMI NIVEL 3 la que debe estar vigente mínimo durante la ejecución del contrato.

**NOTA:** Respecto del certificado aportado por el proponente, la FGN realizará la comprobación en la página oficial de evaluación del Modelo en el link.

<https://cmmiinstitute.com/pars/?Statelid=722fc265-61bf-436f-9ab5-c7a2d3c1a42f>

En caso en el cual el oferente no se encuentre listado en la página oficial de evaluación conforme a los anteriores criterios, será inhabilitado

#### Solicitud 1:

Con el fin de garantizar la participación amplia y competitiva en el presente proceso, se considera necesario incluir la certificación ITmark dentro de los requisitos técnicos habilitantes adicionales. Actualmente, se encuentra definido como habilitante y puntuable el estándar CMMI Nivel 3; sin embargo, esta condición genera una restricción para las empresas que han alcanzado niveles superiores, como CMMI Nivel 5, ya que estas no emitirán certificación en un nivel inferior al que poseen, dado que lo han superado. En consecuencia, si se mantiene únicamente el requisito de CMMI Nivel 3, se estaría limitando la participación de organizaciones que cuentan con mejores prácticas y un mayor nivel de madurez, lo cual va en contravía del principio de pluralidad de oferentes y libre concurrencia.

La certificación ITmark, reconocida por el Ministerio TIC y en línea con las políticas nacionales de fortalecimiento de la industria de software y TI, permite acreditar prácticas en calidad, gestión y desarrollo, fomentando la competitividad de las empresas que aún no alcanzan CMMI Nivel 3, pero que cumplen estándares aceptados a nivel internacional. Por lo anterior, se solicita la inclusión de





ITmark como requisito técnico habilitante adicional, permitiendo la participación tanto de empresas certificadas en CMMI Nivel 3 o superior, como aquellas que cuentan con ITmark, promoviendo la igualdad de condiciones, la pluralidad de oferentes y la transparencia en la contratación.

#### Sustento legal y técnico

- Ley 80 de 1993 (art. 24): Principio de pluralidad de oferentes.
- Ley 1150 de 2007 (art. 5): Selección objetiva.
- Decreto 1082 de 2015: Permite a las entidades establecer requisitos adicionales siempre que no restrinjan la libre concurrencia.
- La inclusión de ITmark evita la restricción indirecta a empresas certificadas en CMMI Nivel 5, que no presentan certificación en Nivel 3 por haberlo superado, y a empresas con procesos de calidad consolidados pero que han optado por modelos equivalentes reconocidos.

Lo anterior garantiza la pluralidad y transparencia

- Garantiza igualdad de oportunidades entre empresas con altos niveles de madurez (CMMI 3, 4 o 5) y aquellas con certificaciones alternativas reconocidas (ITmark).
- Fomenta la competencia efectiva, ampliando el universo de oferentes sin reducir el estándar técnico exigido.
- Evita interpretaciones restrictivas que puedan generar nulidad del proceso por limitación injustificada de la participación.

#### RESPUESTA 1

La Fiscalía General de Nación No acepta la observación, con relación a la solicitud de incluir la certificación ITmark como requisito técnico habilitante adicional en el presente proceso, se considera no viable dicha modificación.

La certificación actualmente definida como habilitante y puntuable, CMMI Nivel 3, responde a estándares internacionales ampliamente reconocidos en la industria del desarrollo de software, especialmente en procesos de contratación pública y privada de alto impacto.

Por su parte, aunque ITmark representa una iniciativa valiosa para la mejora de procesos en PYMEs del sector TIC, su alcance, profundidad y nivel de exigencia no son equivalentes al modelo CMMI. ITmark integra elementos de CMMI, ISO 9001 e ISO 27000, pero está diseñado como un esquema de entrada para empresas en etapas iniciales de madurez, con un enfoque más simplificado. En consecuencia, mantener como habilitante el estándar CMMI Nivel 3 garantiza la participación de organizaciones con procesos robustos, medibles y alineados con las mejores prácticas internacionales, lo cual es esencial para asegurar la calidad y competitividad en el desarrollo del objeto contractual.

#### OBSERVACIÓN 2

El pliego indica

##### 5.3.1. Experiencia

El oferente deberá acreditar en el Registro Único de Proponentes hasta cinco (5) contratos ejecutados, identificados con al menos tres de los códigos del Clasificador de Bienes y Servicios de Naciones Unidas relacionados en la siguiente tabla, una experiencia igual o mayor a 5.620 SMLMV, para el proceso, que experiencia relacionada con el SERVICIO DE DESARROLLO, IMPLEMENTACIÓN, SOPORTE Y MANTENIMIENTO ADAPTATIVO Y EVOLUTIVO PARA LA

MEJORA CONTINUA DE SOLUCIONES DE SOFTWARE PARA LA FISCALÍA GENERAL DE LA NACIÓN, MEDIANTE EL MODELO DE FÁBRICA DE SOFTWARE.

#### Solicitud 2:

Se solicita amablemente a la entidad eliminar la palabra "adaptativo" de la experiencia habilitante y sustituir la expresión "mantenimiento adaptativo y evolutivo" por "mantenimiento" o, en su defecto, "mantenimiento evolutivo y correctivo", por las siguientes razones:

1. Restricción a la participación y afectación de la libre concurrencia El término "mantenimiento adaptativo" no es de uso generalizado en la industria nacional bajo la modalidad de fábrica de software, lo que puede generar confusión y desincentivar la participación de oferentes que interpretan este requerimiento como una condición adicional a los servicios

EL





estándar de mantenimiento. Esta situación contraviene el principio de pluralidad de oferentes consagrado en el artículo 24 de la Ley 80 de 1993.

2. Ambigüedad técnica y redundancia conceptual El mantenimiento adaptativo hace referencia a ajustes derivados de cambios en el entorno operativo (hardware, sistema operativo, plataforma base), actividades que generalmente se encuentran inmersas en la fase de desarrollo y soporte del modelo de fábrica de software. Por ello, mantener la palabra "adaptativo" genera ambigüedad y riesgos interpretativos que pueden afectar la claridad del alcance contractual.
3. Estándares y prácticas reconocidas por MinTIC y la industria Las mejores prácticas en mantenimiento de software, de acuerdo con el estándar ISO/IEC 14764 y lineamientos del MinTIC, agrupan las actividades en categorías como correctivo, perfecto y evolutivo. La mención exclusiva de "adaptativo" no corresponde a la terminología empleada en los lineamientos normativos nacionales, lo que podría inducir a interpretaciones erróneas en la etapa de evaluación.
4. Cumplimiento del principio de selección objetiva Incluir términos no esenciales ni uniformemente reconocidos en el sector puede ocasionar ofertas con alcances heterogéneos y costos adicionales injustificados, lo que afecta la comparación objetiva entre propuestas.

## RESPUESTA 2

La Fiscalía General de Nación, Aclara que, para evitar ese tipo de confusiones a la hora de la verificación del requisito de experiencia, verificará la experiencia con base en las siguientes características: EL SERVICIO DE DESARROLLO, IMPLEMENTACIÓN, SOPORTE Y MANTENIMIENTO PARA LA MEJORA CONTINUA DE SOLUCIONES DE SOFTWARE PARA LA FISCALÍA GENERAL DE LA NACIÓN, MEDIANTE EL MODELO DE FÁBRICA DE SOFTWARE.

## OBSERVACIÓN 3

El pliego establece:

**Para el ítem No. 2.** Se otorgarán **20,25 puntos**, a la oferta que incluya un especialista en seguridad y vulnerabilidades que garantice que los desarrollos cumplan con las mejores prácticas en materia de seguridad de la información, de acuerdo con el siguiente perfil:

| Perfil                                      | Formación Académica                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Experiencia Mínima                                                                                                                                                                          |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Especialista de Seguridad de la Información | Ingeniero de Sistemas, de Telecomunicaciones, Electrónico o Ingenierías afines con Maestría en Seguridad de la Información<br><br>Deberá contar con por lo menos cuatro (4) de las siguientes certificaciones vigentes: <ul style="list-style-type: none"><li>• LEAD IMPLEMENTER ISO 27001 y 2022</li><li>• CISM - CERTIFIED INFORMATION SECURITY MANAGEMENT</li><li>• CERTIFIED ETHICAL HACKER (CEH)</li><li>• EC-COUNCIL CERTIFIED INCIDENT HANDLER</li><li>• CISSP - CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL</li><li>• CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER</li><li>• MANAGER CYBERSECURITY ISO/IEC 27032</li></ul> | Experiencia específica de al menos diez (10) años en proyectos relacionados con seguridad de la información, en roles de Líder, Consultor, Asesor u Oficial en Seguridad de la Información. |

**NOTA.** Para acreditar este requisito ponderable, el proponente deberá adjuntar los documentos soporte del perfil solicitado, los cuales serán revisados por el comité evaluador, quien otorgará la totalidad de los puntos únicamente si se cumple con cada uno de los requisitos de formación académica y experiencia solicitados.

La experiencia profesional se contará según lo establecido en la ley 842 de 2003.

**Solicitud 3:** Con el fin de garantizar la pluralidad de oferentes y la libre concurrencia, solicitamos adicionar al perfil de la formación en especialización Seguridad de la Información de la siguiente manera:

1. Incluir la formación avanzada como requisito opcional o preferente:  
Especialización o Maestría en Seguridad de la Información Esto permitirá que los profesionales que cuenten con formación de posgrado específica puedan acreditar idoneidad técnica, alineándose con las buenas prácticas de la industria y los lineamientos del MinTIC en materia de ciberseguridad.
2. Ajustar el requisito de experiencia mínima a cinco (5) años en actividades relacionadas con gestión de seguridad de la información, ciberseguridad o auditoría en sistemas de información.





La experiencia solicitada en el texto actual (10 años) puede resultar excesiva frente a las dinámicas del mercado y las certificaciones técnicas que exigen actualización permanente, lo cual puede restringir la participación de profesionales altamente capacitados con formación especializada.

Justificación técnica y normativa:

1. Principio de pluralidad de oferentes y selección objetiva (Ley 80 de 1993, art. 24 y 25): Establecer requisitos proporcionales y relacionados con el objeto del contrato para evitar barreras injustificadas de acceso.
2. Buenas prácticas en seguridad de la información: La formación avanzada (Especialización o Maestría) y certificaciones como ISO 27001, CISM, CISSP, entre otras, son indicadores reconocidos internacionalmente de idoneidad profesional, los cuales pueden complementar la experiencia práctica.
3. Competitividad del proceso: Reducir el tiempo de experiencia exigido a 5 años y adicionar la formación especializada fomenta la participación de profesionales jóvenes altamente cualificados y actualizados en estándares internacionales.

Texto propuesto:

Título profesional en ingeniería de sistemas, telemática o carreras afines, con posgrado (Especialización o Maestría) en Seguridad de la Información. Experiencia mínima de cinco (5) años proyectos relacionados con seguridad de la información, en roles de profesional, líder, consultor, asesor u oficial de Seguridad de la Información.

### RESPUESTA 3

La Fiscalía General de Nación No acepta su observación, la maestría solicitada garantiza un nivel específico de conocimiento práctico y actualizado en áreas críticas de la seguridad de la información, lo anterior, permitirá identificar y mitigar riesgos de seguridad en cada etapa del desarrollo, aplicar principios de seguridad desde la fase de análisis y arquitectura, realizar revisiones de código seguras, entre otras actividades de seguridad informática.

En cuanto a la experiencia, la exigencia de experiencia específica responde a la complejidad técnica y el nivel de criticidad del objeto contractual, el cual involucra la protección de activos de información, la gestión de riesgos cibernéticos, la implementación de controles normativos (como ISO 27001, ISO 27032, entre otros) y la ejecución de auditorías en procesos críticos de TI.

En este caso, la experiencia mínima de 10 años se considera necesaria para garantizar la idoneidad técnica del profesional, dado que, la seguridad de la información requiere conocimientos avanzados y experiencia acumulada en múltiples dominios técnicos y normativos, la gestión de incidentes, auditorías, y diseño de políticas de seguridad exige madurez profesional y criterio experto, que se desarrolla con años de práctica, la experiencia en roles de liderazgo

10. INDRA COLOMBIA S.A.S

### OBSERVACIÓN 1

3.1. ANEXO TECNICO 1\_CONDICIONES\_MINIMAS\_DEL\_PRODUCTO\_DE\_SOFTWARE\_V2

1,3 METODOLOGÍAS DE DESARROLLO DE SOFTWARE PAG. 4

1. Modelo de Desarrollo Ágil (PMI Agile y/o Scrum)

Se utilizará (PMI Agile y/o Scrum u otras), como la metodología ágil principal, facilitando la entrega continua de valor mediante iteraciones o sprints cortos. Esto permite una mayor flexibilidad y adaptación a cambios en los requerimientos del proyecto. Cada sprint incluirá...

3. Gestión de Proyectos según PMI

Para la gestión global del proyecto se seguirá el estándar de PMI, que incluye la gestión del alcance, tiempo, costos, riesgos y calidad del proyecto. Esto se complementará con herramientas de gestión para asegurar el control efectivo del cronograma y los recursos.

Observación:

Agradecemos sea detallado el proceso "híbrido" de gestión PMI y proyectos ágiles en la entidad aplicado en este momento y cuáles son los entregables y KPIs de cada etapa en él.

EL





## RESPUESTA 1

La Fiscalía General de Nación ampliar la información sobre la aplicación del modelo híbrido de gestión de proyectos, compuesto por elementos de la guía PMBOK del Project Management Institute (PMI) y la metodología ágil Scrum como marco de trabajo operativo. El modelo híbrido adoptado por la Fiscalía busca maximizar la entrega continua de valor con un control riguroso del proyecto desde la planificación hasta el cierre. Se encuentra alineado con las mejores prácticas internacionales de dirección de proyectos y desarrollo ágil, asegurando trazabilidad, flexibilidad y cumplimiento técnico.

Frente a los KPI's establecidos para el modelo híbrido están enmarcados en el ANEXO\_TÉCNICO\_2\_ANS\_FGN en la primera hoja del archivo.

## OBSERVACIÓN 2

3.1. ANEXO TECNICO 1\_CONDICIONES\_MINIMAS\_DEL\_PRODUCTO\_DE\_SOFTWARE\_V2

1 CARACTERÍSTICAS DEL SERVICIO PARA LA FISCALÍA GENERAL DE LA NACIÓN -> Servicio Integral de Soporte, Actualización y Mantenimiento (SAM). PAG. 7

Niveles de Prioridad y Tiempos de Respuesta: Los incidentes y solicitudes de soporte serán clasificados en categorías de prioridad (alta, media y baja), y se atenderán según los tiempos de respuesta establecidos en los ANS, de la siguiente manera:

- Alta prioridad: Respuesta en un máximo de 2 horas y solución en un plazo de 8 horas.
- Media prioridad: Respuesta en un máximo de 4 horas y solución en 24 horas.
- Baja prioridad: Respuesta en un máximo de 9 horas y solución en 72 horas.

Observación:

Agradecemos sea detallado el criterio para clasificar la prioridad de los incidentes para el servicio integral de soporte, actualización y mantenimiento SAM.

## RESPUESTA 2

La Fiscalía General de Nación , Aclara que la clasificación de la prioridad de los incidentes en el marco del servicio SAM (Soporte, Actualización y Mantenimiento) de la Fiscalía General de la Nación se realiza conforme a criterios establecidos de impacto y urgencia, los cuales permiten definir la atención más adecuada según la criticidad del evento. Estos se encuentran establecidos en el ANEXO\_TÉCNICO\_2\_ANS\_FGN, en la segunda hoja denominada Tiempo de atención de incidente y relacionado en el ANEXO TECNICO 1\_CONDICIONES\_MINIMAS\_DEL\_PRODUCTO\_DE\_SOFTWARE\_V2, para este último, acogiendo la observación se realiza aclaración de los criterios de clasificación, detallando cada uno de ellos

## OBSERVACIÓN 3

3.1. ANEXO TECNICO 1\_CONDICIONES\_MINIMAS\_DEL\_PRODUCTO\_DE\_SOFTWARE\_V2

1 CARACTERÍSTICAS DEL SERVICIO PARA LA FISCALÍA GENERAL DE LA NACIÓN -> Servicio Integral de Soporte, Actualización y Mantenimiento (SAM) PAG. 7

Observación:

Con el fin de dimensionar el servicio adecuadamente, agradecemos proveer, si es posible, volumetría o históricos de soporte de aplicaciones de la entidad que hayan tenido este esquema de servicio de soporte.

## RESPUESTA 3

La Fiscalía General de Nación , aclara que comprende la importancia de contar con información de contexto que permita una adecuada planeación y dimensionamiento del servicio de soporte, actualización y mantenimiento. En este sentido, y en cumplimiento





con los principios de transparencia y libre concurrencia del proceso, se informa que, la volumetría de soporte puede variar dependiendo de la criticidad del sistema, el número de usuarios concurrentes, el tipo de tecnología involucrada y los cambios normativos o funcionales requeridos.

A modo de referencia, y sin que ello constituya una condición contractual, en proyectos similares ejecutados en vigencias anteriores bajo esquemas de soporte 7x24, se han registrado promedios mensuales de 280 a 350 casos reportados. Este dato es una aproximación y no debe interpretarse como un compromiso contractual de volúmenes. El comportamiento puede variar en función del contexto institucional, ciclos de implementación, necesidades normativas o evolución tecnológica. Para efectos del presente proceso, se recomienda al proponente tener en cuenta las características técnicas, funcionales y de cobertura del SAM descritas en los anexos técnicos. Cualquier ajuste o necesidad particular deberá ser gestionado conforme a los lineamientos del contrato y el modelo de gestión acordado con la FGN.

#### **OBSERVACIÓN 4**

3.1. ANEXO TÉCNICO 1\_CONDICIONES\_MINIMAS\_DEL\_PRODUCTO\_DE\_SOFTWARE\_V2

1 CARACTERÍSTICAS DEL SERVICIO PARA LA FISCALÍA GENERAL DE LA NACIÓN -> Servicio Integral de Soporte, Actualización y Mantenimiento (SAM) PAG. 7

Disponibilidad: El servicio de soporte se prestará bajo un esquema 7\*24, se garantizará que los sistemas de información desplegados en ambientes productivos de la Fiscalía mantengan su operatividad y funcionalidad durante estos horarios.

Observación:

¿Consideraría la entidad definir la disponibilidad (7x24, 5x8) del servicio de acuerdo a la criticidad de cada aplicación? O ¿necesariamente todas las aplicaciones asociadas al servicio deberán contar con soporte 7x24?

#### **RESPUESTA 4**

La Fiscalía General de Nación, se permite aclarar que, el Servicio Integral de Soporte, Actualización y Mantenimiento (SAM) contemplado en el Anexo Técnico 1 está diseñado para garantizar la operatividad continua y sin interrupciones de los sistemas de información desplegados en los entornos productivos de la entidad.

En consecuencia, la disponibilidad del servicio de soporte es obligatoriamente bajo el esquema 7x24 (7 días a la semana, 24 horas al día), sin excepción para todas las aplicaciones que estén dentro del alcance del contrato, independientemente de su nivel de criticidad o naturaleza funcional.

#### **OBSERVACIÓN 5**

3.1. ANEXO TÉCNICO 1\_CONDICIONES\_MINIMAS\_DEL\_PRODUCTO\_DE\_SOFTWARE\_V2

2 CARACTERÍSTICAS DEL SERVICIO PARA LA FISCALÍA GENERAL DE LA NACIÓN -> 2.

Bolsa de Horas a Monto

Agotable. PAG. 7

Observación:

Con el fin de dimensionar el servicio adecuadamente, agradecemos proveer, si es posible, la cantidad promedio de horas por mes que la entidad espera ejecutar bajo el servicio de "bolsa de horas".

#### **RESPUESTA 5**

La Fiscalía General de Nación, Aclara que, el servicio de Bolsa de Horas a Monto Agotable está diseñado para atender requerimientos no previstos, nuevos sistemas de información, ajustes funcionales, soporte evolutivo, mantenimiento correctivo menor y mejoras incrementales durante la ejecución del contrato. Por su naturaleza, el consumo puede variar mes a mes según la priorización de necesidades internas, la disponibilidad de ambientes y el volumen de solicitudes funcionales.

No obstante, la entidad estima un consumo promedio mensual entre 3.800 y 4.300 horas es importante tener en cuenta que esta bolsa de horas permite gestionar con flexibilidad la asignación de esfuerzos entre los diferentes perfiles requeridos, de acuerdo con la carga real de trabajo en cada etapa del contrato.





Asimismo, se recomienda que los proponentes contemplen en su propuesta mecanismos de control y seguimiento del consumo de horas, entregables parciales, validaciones por sprint, y reportes periódicos, con trazabilidad completa para la supervisión e interventoría.

#### **OBSERVACIÓN 6**

3.1. ANEXO TECNICO 1\_CONDICIONES MINIMAS DEL PRODUCTO DE SOFTWARE\_V2

3 CARACTERÍSTICAS DEL SERVICIO PARA LA FISCALÍA GENERAL DE LA NACIÓN -> 3. Desarrollo de Nuevas Funcionalidades, Mejoras y Nuevos Sistemas de Información. PAG. 7

##### **Observación:**

Con el fin de dimensionar el servicio adecuadamente, agradecemos proveer, si es posible, la cantidad promedio de horas por mes que la entidad espera ejecutar bajo el servicio de "desarrollo de funcionalidades. Mejoras y nuevos sistemas de información"

#### **RESPUESTA 6**

La Fiscalía General de Nación, Aclara que Tener en cuenta la respuesta relacionada en la anterior pregunta, La Fiscalía General de la Nación agradece su observación y se permite informar que, el servicio de Bolsa de Horas a Monto Agotable está diseñado para atender requerimientos no previstos, nuevos sistemas de información, ajustes funcionales, soporte evolutivo, mantenimiento correctivo menor y mejoras incrementales durante la ejecución del contrato. Por su naturaleza, el consumo puede variar mes a mes según la priorización de necesidades internas, la disponibilidad de ambientes y el volumen de solicitudes funcionales.

No obstante, la entidad estima un consumo promedio mensual entre 3.800 y 4.300 horas es importante tener en cuenta que esta bolsa de horas permite gestionar con flexibilidad la asignación de esfuerzos entre los diferentes perfiles requeridos, de acuerdo con la carga real de trabajo en cada etapa del contrato.

Asimismo, se recomienda que los proponentes contemplen en su propuesta mecanismos de control y seguimiento del consumo de horas, entregables parciales, validaciones por sprint, y reportes periódicos, con trazabilidad completa para la supervisión e interventoría.

#### **OBSERVACIÓN 7**

3.1. ANEXO TECNICO 1\_CONDICIONES MINIMAS DEL PRODUCTO DE SOFTWARE\_V2

7 CARACTERÍSTICAS DEL SERVICIO PARA LA FISCALÍA GENERAL DE LA NACIÓN -> 7. Gestión de Riesgos y Seguridad. PAG 9

##### **Observación:**

Agradecemos confirmar las herramientas y medios dispuestos por la entidad para la conectividad a los ambientes de esta por parte del equipo de Indra.

#### **RESPUESTA 7**

La Fiscalía General de Nación, Aclara que, la conectividad a los ambientes de la entidad por parte del contratista se realizará exclusivamente a través de los canales, mecanismos y medios autorizados por la Subdirección de Tecnologías de la Información y las comunicaciones de la Fiscalía, bajo los principios de seguridad, confidencialidad y control.

La FGN dispone de una infraestructura de red segura, que puede ser otorgado previa solicitud formal, validación de los requerimientos y firma de compromisos de confidencialidad y uso responsable. El acceso estará limitado únicamente a los entornos definidos en el contrato, mediante mecanismos como VPN, credenciales personalizadas, entre otros de acuerdo con la necesidad del servicio. Durante la etapa inicial del contrato, el equipo técnico de la FGN brindará la inducción y orientación sobre los procedimientos de acceso, así como el acompañamiento necesario para garantizar la correcta conexión a los entornos requeridos, según el cronograma y alcance aprobado.

Igualmente, si durante la vigencia del contrato se implementan técnicas para asegurar el acceso, tales como herramientas de acceso privilegiado, SASE entre otros, el contratista debe implementarlos y alinearse a los nuevos procesos y/o procedimientos que tenga la FGN.

#### **OBSERVACIÓN 8**

3.1. ANEXO TECNICO 1\_CONDICIONES MINIMAS DEL PRODUCTO DE SOFTWARE\_V2





N/A. RESTRICCIONES. PAG 13

- Facturación y Productos Parciales: No se permitirá la facturación de productos parciales. Solo se facturará aquellos productos que hayan sido completados, desplegados en el ambiente productivo y aprobados por la FGN de acuerdo con los criterios de aceptación.

**Observación:**

¿Consideraría la entidad la opción de una facturación parcial una vez finalizadas las pruebas de aceptación por parte de los usuarios clave y otra una vez el desarrollo sea entregado a satisfacción en producción? Esto teniendo en cuenta que la decisión de paso a producción puede tener otras variables asociadas al negocio y no al proceso de desarrollo como tal.

**RESPUESTA 8**

La Fiscalía General de Nación, Aclara que, de acuerdo con los lineamientos establecidos en el pliego de condiciones y en el Anexo Técnico 1, no se contempla la facturación por productos parciales, dado que se requiere garantizar que cada producto entregado cumpla integralmente con las siguientes condiciones:

- Finalización total del desarrollo conforme a los criterios funcionales y técnicos acordados.
- Despliegue exitoso en el ambiente productivo de la entidad.
- Aprobación formal por parte de la Fiscalía, en el marco de los criterios de aceptación definidos.

Este enfoque tiene como propósito asegurar la calidad final del entregable y la disponibilidad operativa del producto para su uso institucional. En ese sentido, la entidad reitera que la decisión de paso a producción y la aprobación del producto completo son condiciones necesarias y previas para que proceda cualquier proceso de facturación.

No obstante, en los procesos de planificación y seguimiento del contrato, se podrán establecer mecanismos internos de verificación, revisión y preaprobación que permitan al contratista realizar una adecuada gestión financiera y operativa, dentro de los parámetros definidos contractualmente.

**OBSERVACIÓN 9**

3.1. ANEXO TECNICO 1.CONDICIONES\_MINIMAS\_DEL\_PRODUCTO\_DE\_SOFTWARE\_V3

N/A. RESTRICCIONES. PAG 13.

- Responsabilidad por la Seguridad del Software: El contratista será responsable de garantizar que los productos desarrollados cumplan con los estándares de seguridad exigidos por la FGN, incluyendo la protección contra vulnerabilidades comunes y ataques cibernéticos, vulnerabilidades detectadas en las pruebas exhaustivas y de los análisis de vulnerabilidades efectuados.

**Observación:**

¿La entidad cuenta en sus ambientes de desarrollo y CI/CD con herramientas especializadas (p.j SonarQube o OWASP Zap) en el escaneo de vulnerabilidades? ¿El licenciamiento de este tipo de herramientas correrá por cuenta de la entidad?

**RESPUESTA 9**

La Fiscalía General de Nación, Aclara que la Entidad cuenta con herramientas de análisis de vulnerabilidades, sin embargo, este requerimiento es inherente a la responsabilidad de productos entregados por el contratista, quiere decir que el contratista debe asegurar que el código entregado este basado en las mejores prácticas como mínimo OWASP zap en su última versión y no solo el TOP 10, para web services WS-policy, y para análisis de código herramientas que el contratista implemente y que garantice que el código es seguro.

Si la FGN adquiere una herramienta de análisis de código, el contratista debe adherirse a los procedimientos y políticas de la FGN y permitir el análisis de código, de esa manera el contratista deberá implementar las recomendaciones e implementarlas como parte de la garantía.

**OBSERVACIÓN 10**

3.1. ANEXO TECNICO 1.CONDICIONES\_MINIMAS\_DEL\_PRODUCTO\_DE\_SOFTWARE\_V4

Transferencia de Conocimiento y Documentación de Sistemas para la FGN. PAG 44

**Observación:**

ER





¿La entidad cuenta con un proceso o tiene definido algún alcance para garantizar la transferencia de conocimiento al equipo al inicio, durante y/o al finalizar el mantenimiento de las aplicaciones, ya sea correctivo y/o evolutivo? Esto haciendo referencia a la entrega por parte de proveedores actuales con los que cuente la entidad.

¿Cuál será el tiempo previsto para esta etapa?

#### RESPUESTA 10

La Fiscalía General de Nación, Aclara que Sí. Tal como se ha indicado en respuestas anteriores, la entidad tiene previsto realizar el proceso de transferencia de conocimiento al inicio, durante y al finalizar el mantenimiento correctivo y/o evolutivo, conforme al alcance definido en el Anexo Técnico y alineado con los principios de aseguramiento de la continuidad del servicio.

El tiempo estimado para esta etapa será concertado con el contratista al inicio del contrato, en función del cronograma de trabajo acordado y garantizando que la documentación técnica y funcional esté completa y actualizada para el equipo de la FGN

#### OBSERVACIÓN 11

3.1. ANEXO TECNICO 1\_CONDICIONES\_MINIMAS\_DEL\_PRODUCTO\_DE\_SOFTWARE\_V5

**Observación:**

¿Qué asistentes de IA están autorizados para codificación y pruebas y cómo debe demostrarse su uso?

#### RESPUESTA 11

La Fiscalía General de Nación, Aclara que el documento de las políticas de uso adecuado de IA, una vez se firme el acta de inicio, las herramientas serán analizadas dentro de estas políticas y acordadas con el contratista.

#### OBSERVACIÓN 12

Anexo Téc. 3

Herramientas

Stack tecnológico

No esp.

"Java 17 o superior... OpenShift Docker y Kubernetes... IBM BAW/COGNOS/ESRI"

**Observación:**

Especificar versiones objetivo (JBoss/EAP, OpenShift/K8s, IBM BAW/Filnet/Cognos, Oracle 12c/19c), licenciamiento y entornos disponibles (dev/test/pre/producción).

#### RESPUESTA 12

La Fiscalía General de Nación, Aclara que de acuerdo con lo establecido previamente en las condiciones del proceso, la Fiscalía General de la Nación informa que, el stack tecnológico detallado, incluyendo versiones específicas de herramientas y plataformas (como JBoss, OpenShift, Kubernetes, IBM BAW, Cognos, Oracle, entre otras), será informado y validado durante la etapa de inicio del contrato. Esto permitirá garantizar que la información proporcionada esté actualizada y acorde con el entorno tecnológico vigente de la Entidad en el momento de ejecución.

El licenciamiento de las herramientas necesarias para el desarrollo, pruebas, despliegue y operación será provisto por la Fiscalía, por lo cual el contratista no deberá asumir costos por licencias o herramientas especializadas para conectividad, análisis, automatización o despliegue. En cuanto a los ambientes disponibles, la Fiscalía contará con los entornos requeridos para garantizar el ciclo completo de desarrollo, los cuales incluyen, Desarrollo (dev), Pruebas (test), Preproducción (pre), Producción (prod). Cada uno de estos entornos será habilitado y accesible bajo los lineamientos de seguridad y conectividad definidos por la Subdirección de Tecnología de la Información y las comunicaciones.

#### OBSERVACIÓN 13

Anexo Téc. 1 (DOCX)

Seguridad

Pruebas de penetración

s/p (DOCX)





"El contratista deberá realizar pruebas de penetración..."

Observación:

Especifiquen alcance (caja negra/gris/blanca), frecuencia y ambientes permitidos; criterio de cierre por severidad.

#### RESPUESTA 13

La Fiscalía General de la Nación informa que el alcance de las pruebas de penetración ha sido documentado en el Anexo Técnico 1 – Condiciones Mínimas del Producto de Software, conforme a lo requerido. En dicho anexo se especifican los lineamientos y condiciones bajo los cuales deben llevarse a cabo estas pruebas, incluyendo los aspectos relacionados con:

- El entorno permitido para su ejecución
- Los criterios de evaluación y remediación de hallazgos
- El rol del contratista en la planeación y ejecución técnica de las pruebas

Por tanto, se considera atendida y resuelta la observación con base en el contenido descrito en el anexo técnico mencionado.

#### OBSERVACIÓN 14

Anexo Técnico 1

Entregables

Lista mínima

s/p (DOCX)

No especificado

Observación:

Para estructurar costo fijo por entregable: faciliten lista mínima (p. ej., ADR, HLD/LLD, casos de prueba, manuales, SBOM).

#### RESPUESTA 14

La Fiscalía General de la Nación informa que los entregables esperados han sido documentados en cada una de las fases del ciclo de vida del desarrollo de software en el Anexo Técnico 1 – Condiciones Mínimas del Producto de Software. En dicho anexo se definen, entre otros, los siguientes productos mínimos por etapa:

- Documentos de levantamiento y análisis de requerimientos (por ejemplo, ADR – Architecture Decision Records).
- Diseños de alto y bajo nivel (HLD – High Level Design, LLD – Low Level Design).
- Casos de prueba funcionales y no funcionales.
- Manuales técnicos y de usuario.
- Bitácoras de pruebas de aceptación y paso a producción.
- Evidencia de ejecución de pruebas de seguridad y calidad.
- Documentación asociada al mantenimiento evolutivo y correctivo.
- SBOM (Software Bill of Materials) en los casos donde la solución lo amerite, especialmente cuando se utilicen componentes de terceros o librerías open source.
- Esta lista podrá ser complementada o ajustada según los requerimientos específicos del producto o sistema desarrollado, y según las necesidades técnicas y normativas de la FGN.

#### OBSERVACIÓN 15

Anexo Técnico 1

Seguridad

Herramientas mínimas

s/p (DOCX)

"alineado a OWASP/27001"

Observación:

Para cotizar licencias: ¿La Entidad proveerá SAST/DAST/SCA? (A: Sí, se usarán N herramientas; B: No, oferente las incluye).

#### RESPUESTA 15

EP





La Entidad cuenta con herramientas de análisis de vulnerabilidades, sin embargo, este requerimiento es inherente a la responsabilidad de productos entregados por el contratista, quiere decir que el contratista debe asegurar que el código entregado este basado en las mejores prácticas como mínimo OWASP zap en su última versión y no solo el TOP 10, para web services WS-policy, y para análisis de código herramientas que el contratista implemente y que garantice que el código es seguro.

Si la FGN adquiere una herramienta de análisis de código, el contratista debe adherirse a los procedimientos y políticas de la FGN y permitir el análisis de código, de esa manera el contratista deberá implementar las recomendaciones e implementarlas como parte de la garantía.

#### **OBSERVACIÓN 16**

Anexo Técnico 1

Formación

Capacitación mínima

s/p (DOCX)

"28 funcionarios; 4h por sesión"

**Observación:**

Para horas/cronograma de oferta: definan # sesiones esperadas (p. ej., 6-10), modalidad (remota/presencial), y temas prioritarios.

#### **RESPUESTA 16**

La Fiscalía General de la Nación confirma que, en concordancia con las respuestas previamente emitidas, la entidad proveerá las herramientas necesarias para garantizar el cumplimiento de los lineamientos de seguridad establecidos en el Anexo Técnico 1. La Modalidad mixta (presencial y remota) dependiendo de la naturaleza del tema y el público objetivo, algunas sesiones podrán desarrollarse de manera presencial (principalmente las que impliquen interacción directa con sistemas internos sensibles o prácticas en ambiente controlado), y otras de forma remota mediante herramientas institucionales de videoconferencia. La programación específica de las sesiones será definida en conjunto entre la entidad y el contratista, una vez iniciado el contrato, y conforme al cronograma general de entregables y disponibilidad del personal de la Fiscalía.

La Fiscalía General de la Nación informa que, conforme a lo indicado en el Anexo Técnico 1, se contempla la realización de jornadas de capacitación orientadas a garantizar la adecuada transferencia de conocimiento al equipo funcional y técnico de la entidad.

#### **OBSERVACIÓN 17**

Complemento al Pliego de Condiciones

Supuestos y Restricciones

Disponibilidad de Recursos Técnicos

s/p (DOCX – imagen)

"la FGN proporcionará todos los accesos... incluyendo bases de datos, plataformas de desarrollo, servidores y herramientas de gestión de proyectos."

**Observación:**

Para efectos de oferta, confirmar quién proveerá/operará los ambientes de desarrollo y pruebas: (A) la FGN los proporciona (accesos e infraestructura) o (B) el contratista debe proveerlos. Indicar opción.

#### **RESPUESTA 17**

La Fiscalía General de la Nación informa que tal como se ha indicado en respuestas anteriores y de acuerdo con lo establecido en el Anexo Técnico 1 y el Complemento al Pliego de Condiciones, la Fiscalía General de la Nación (FGN) proporcionará los ambientes necesarios para el desarrollo, pruebas y producción, así como el acceso correspondiente a las herramientas e infraestructura asociadas.





El contratista deberá hacer uso de estos ambientes, siguiendo las políticas y lineamientos definidos por la FGN en cuanto a seguridad, control de cambios, planificación de despliegues y buenas prácticas de desarrollo.

Cualquier requerimiento adicional que implique adecuaciones o ajustes sobre los entornos suministrados será coordinado y validado en conjunto con los equipos técnicos de la Fiscalía.

#### **OBSERVACIÓN 18**

Anexo Téc. 3

Herramientas y tecnologías

Stack

s/p (DOCX)

"Se determina de manera prioritaria pero no obligatoria..." / "Openshift Docker y Kubernetes, GitLab"

##### **Observación:**

Confirman si OpenShift/JBoss EAP (Red Hat) son obligatorios en el ambiente del contratista o solo compatibles con la plataforma FGN. Si obligatorios, ¿quién asume licenciamiento?

#### **RESPUESTA 18**

La Fiscalía General de la Nación aclara que, el licenciamiento mencionado será entregado por la Entidad.

#### **OBSERVACIÓN 19**

Anexo Téc. 1

Supuestos

Disponibilidad de recursos técnicos

s/p (DOCX)

"La FGN proporcionará todos los accesos... incluyendo bases de datos, plataformas de desarrollo, servidores y herramientas de gestión..."

##### **Observación:**

En términos de oferta, este supuesto ¿incluye que la FGN suministra plataformas dev/test? Si hay excepciones, listar tecnologías/licencias que esperen del contratista.

#### **RESPUESTA 19**

La Fiscalía General de la Nación confirma que suministra los ambientes de desarrollo y pruebas, junto con sus respectivos accesos, herramientas y licenciamientos, sin que se esperen aportes por parte del contratista en este sentido.

#### **OBSERVACIÓN 20**

ANEXO TÉCNICO 4 EQUIPO DE TRABAJO FGN

No especificado

Matriz de roles y perfiles

s/p (DOCX)

No especificado

##### **Observación:**

Para efectos de oferta, indiquen si la matriz de roles es (A) cerrada o (B) mínima (se permiten roles adicionales propuestos: p.ej. Líder DevSecOps, Arquitecto, Observabilidad, Release Manager). Seleccionar opción.

#### **RESPUESTA 20**

La Fiscalía General de la Nación informa que la matriz de roles definida en el Anexo Técnico 4 tiene carácter mínimo, por tanto, se permite la inclusión de roles adicionales por parte del proponente, siempre que estos contribuyan al cumplimiento integral de los objetivos contractuales, la calidad del producto entregado y la correcta operación de los servicios. Estos roles adicionales podrán ser

ER





incluidos en la propuesta técnica, junto con su justificación y articulación dentro del modelo operativo propuesto, sin que su ausencia en la matriz mínima represente una restricción para su incorporación.

#### **OBSERVACIÓN 21**

ANEXO TÉCNICO 4 EQUIPO DE TRABAJO FGN

No especificado

Sustitución / Reemplazos

s/p (DOCX)

No especificado

##### **Observación:**

Definan plazos máximos para reemplazo: presentar CV  $\leq$  (A) 5 / (B) 10 días hábiles y empalme de (A) 40 / (B) 80 horas. Indicar combinación aceptada y si aplica penalidad por incumplir.

#### **RESPUESTA 21**

La Fiscalía General de Nación, Aclara que como se indicó en respuestas anteriores sobre la gestión del equipo de trabajo y los lineamientos operativos definidos para garantizar la continuidad del servicio, la Fiscalía General de la Nación establece que, en caso de requerirse la sustitución de un recurso, el contratista deberá presentar la hoja de vida del nuevo profesional en un plazo no mayor a cinco (5) días hábiles a partir de la notificación de la necesidad de reemplazo, el nuevo recurso propuesto debe cumplir con el perfil y experiencia exigidos para el rol a reemplazar, lo cual será validado por la FGN. Se deberá garantizar un proceso de empalme mínimo de cuarenta (40) horas efectivas, de manera presencial o remota, según lo determine la entidad, con el objetivo de no afectar la continuidad de los servicios. El incumplimiento de estos tiempos o condiciones podrá ser objeto de evaluación en el seguimiento contractual y, si afecta la operación crítica del servicio, podría derivar en medidas contractuales conforme a la normatividad vigente y lo pactado en el contrato.

#### **OBSERVACIÓN 22**

ANEXO TÉCNICO 4 EQUIPO DE TRABAJO FGN

No especificado

Equivalencias

s/p (DOCX)

No especificado

##### **Observación:**

¿Se aceptan equivalencias? (A) certificación equivalente de organismo acreditado, (B) experiencia comprobable  $\geq$  5 años en la tecnología, o (C) ambas. Indicar opción.

#### **RESPUESTA 22**

La observación no es clara, no se especifica a que rol o a que hace referencia o ha que certificación pretende la equivalencia, por esta razón no emite una respuesta.

#### **OBSERVACIÓN 23**

ANEXO TÉCNICO 4 EQUIPO DE TRABAJO FGN

No especificado

Subsanación post-adjudicación

s/p (DOCX)

No especificado

##### **Observación:**

¿Se admite carta de compromiso para obtener la certificación post-adjudicación en (A) 30, (B) 60, o (C) 90 días calendario, sin afectar elegibilidad? Elegir plazo.

#### **RESPUESTA 23**





La Fiscalía General de Nación No acepta la observación las condiciones del equipo técnico de trabajo deberán ser acreditadas en su integridad como requisito de ejecución del contrato previo a la suscripción del acta de inicio

#### 11. EXSIS DIGITAL S.A.S

##### OBSERVACIÓN 1

Dentro de los criterios de asignación de puntaje establecidos por la entidad, en el numeral 6.2 del proyecto pliego de condiciones se indica para la obtención de 20,25 puntos lo siguiente: "Para el ítem No. 2. Se otorgarán 20,25 puntos, a la oferta que incluya un especialista en seguridad y vulnerabilidades que garantice que los desarrollos cumplan con las mejores prácticas en materia de seguridad de la información, de acuerdo con el siguiente perfil:

| Perfil                                      | Formación Académica                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Experiencia Mínima                                                                                                                                                                                 |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Especialista de Seguridad de la información | <p>Ingeniero de Sistemas de Telecomunicaciones, Electrónica o ingenierías afines con Maestría en Seguridad de la Información.</p> <p>Deberá contar con por lo menos cuatro (4) de las siguientes certificaciones vigentes:</p> <ul style="list-style-type: none"><li>• LEAD IMPLEMENTER ISO 27001 v.2022</li><li>• CISM - CERTIFIED INFORMATION SECURITY MANAGEMENT</li><li>• CERTIFIED ETHICAL HACKER (C EH).</li><li>• EC IH EC-COUNCIL CERTIFIED INCIDENT HANDLER</li><li>• CISSP - CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL</li><li>• CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER</li><li>• MANAGER CYBERSECURITY ISO/IEC 27032</li></ul> | <p>Experiencia específica de al menos diez (10) años en proyectos relacionados con seguridad de la información, en roles de Líder, Consultor, Asesor u Oficial en Seguridad de la Información.</p> |

**NOTA:** Para acreditar este requisito ponderable, el proponente deberá adjuntar los documentos soporte del perfil solicitado, los cuales serán revisados por el comité evaluador, quien otorgará la totalidad de los puntos únicamente si se cumple con cada uno de los requisitos de formación académica y experiencia solicitados.

De acuerdo con los requisitos establecidos para cumplir con el perfil Especialista de Seguridad de la Información en aras de obtener los 20,25 puntos, nos permitimos hacer un llamado a la entidad a modificar dichos requerimientos de la siguiente Manera:

Frente a los requisitos del perfil en mención, solicitamos a la entidad modificar lo siguiente:

1. Frente al requisito de posgrado solicitamos sea permitido especialización en seguridad de la información o afines y/o Maestría en seguridad de la información o afines.

2. Frente a la cantidad de certificaciones técnicas solicitadas solicitamos se reduzca la cantidad a dos (2) certificaciones y se incluyan otras opciones de certificación relacionadas con seguridad informática o seguridad de información así:

- Lead Auditor Certified 27001:2022
- Certified Information Systems Auditor CISA
- Auditor ISO 22301:2019 o superior
- Ethical Hacking Certified CEH EC-COUNCIL

3. Solicitamos reducir la experiencia específica así: al menos ocho (8) años en proyectos relacionados con seguridad de la información, en roles de Líder, Consultor, Asesor u Oficial en Seguridad de la Información.

Esta solicitud de modificación se hace teniendo en cuenta que el mercado de profesionales de TI en Colombia específicamente en temas relacionados con seguridad de la información es escaso, y se reduce aún más el número de profesionales existentes que cuente con cuatro (4) certificaciones del tipo que solicita la entidad para la obtención de puntaje, generando con esto que no se garantice en el proceso de selección la pluralidad de oferentes.

Sumado a lo anterior, es importante resaltar que según lo indica la entidad este perfil es requerido para garantizar que en los desarrollos que se realicen durante la ejecución del proyecto, se apliquen las mejores prácticas de seguridad de la información lo cual no se garantiza únicamente con las certificaciones y formación de posgrado que está estableciendo la entidad en los prepliegos, sino que también se pueden garantizar si el profesional cuenta con formación académico de otros programas de posgrado y otras certificaciones técnicas afines a seguridad de la información que existen en el mercado y las cuales sugerimos incluir anteriormente.

Es importante resaltar que, aunque estos requisitos corresponden a un aspecto puntuable la entidad no puede desconocer lo establecido por la Agencia Nacional de Contratación Pública Colombia Compra Eficiente como ente rector de la contratación pública en Colombia en sus guías de contratación pública, en las cuales indica que los estudios previos y del sector pretenden que las

ER





entidades tengan un panorama de los posibles proveedores que puedan satisfacer la necesidad a contratar, ello incluye que con base en la información obtenida de dichos estudios se puedan establecer los requisitos habilitantes y puntuables adecuados alineados al mercado garantizando con esto los principios de la contratación estatal.

Por todo lo anterior, amablemente solicitamos a la entidad modificar los requisitos establecidos para otorgar el puntaje por el criterio Especialista de Seguridad de la Información, estableciendo requisitos más competitivos y aterrizados al mercado, garantizando así la aplicación de los principios de igualdad y transparencia, así como promover la participación plural de oferentes.

#### **RESPUESTA 1**

La Fiscalía General de Nación No acepta su observación, la maestría solicitada garantiza un nivel específico de conocimiento práctico y actualizado en áreas críticas de la seguridad de la información, lo anterior, permitirá identificar y mitigar riesgos de seguridad en cada etapa del desarrollo, aplicar principios de seguridad desde la fase de análisis y arquitectura, realizar revisiones de código seguras, entre otras actividades de seguridad informática.

La Fiscalía General si bien se reconoce la importancia de garantizar la pluralidad de oferentes y la libre concurrencia en los procesos de contratación estatal, conforme a lo dispuesto en el artículo 5 de la Ley 1150 de 2007 y la jurisprudencia del Consejo de Estado, también es deber de la entidad garantizar la selección objetiva del contratista más idóneo, en función de la naturaleza especializada del objeto contractual. La exigencia de estas cuatro certificaciones no constituye una barrera injustificada, sino una medida proporcional y técnica que responde al análisis de riesgo del proceso, la criticidad de los servicios contratados y la necesidad de contar con personal altamente calificado en un campo que exige estándares internacionales de seguridad. Tal como lo establece el Concepto C-456 de 2025 de la Agencia Nacional de Contratación Pública, los requisitos técnicos pueden ser ponderables siempre que estén debidamente justificados y alineados con el objeto contractual. Adicionalmente, la jurisprudencia del Consejo de Estado ha señalado que la autonomía de la entidad para definir los requisitos técnicos está limitada por los principios de proporcionalidad, transparencia y selección objetiva. En este caso, la exigencia de cuatro certificaciones responde a la necesidad de asegurar un nivel mínimo de especialización en áreas complementarias de la seguridad informática (gestión, respuesta a incidentes, hacking ético, privacidad, etc.), sin que ello implique una restricción arbitraria o discriminatoria. Ahora, frente a la solicitud de experiencia, No acepta su observación, La exigencia de experiencia específica responde a la complejidad técnica y el nivel de criticidad del objeto contractual, el cual involucra la protección de activos de información, la gestión de riesgos cibernéticos, la implementación de controles normativos (como ISO 27001, ISO 27032, entre otros) y la ejecución de auditorías en procesos críticos de TI. En este caso, la experiencia mínima de 10 años se considera necesaria para garantizar la idoneidad técnica del profesional, dado que, la seguridad de la información requiere conocimientos avanzados y experiencia acumulada en múltiples dominios técnicos y normativos, la gestión de incidentes, auditorías, y diseño de políticas de seguridad exige madurez profesional y criterio experto, que se desarrolla con años de práctica, la experiencia en roles de liderazgo.

#### **12. TCI SOFTWARE SAS BIC**

##### **OBSERVACIÓN 1**

De acuerdo con el ítem "6.2 FACTOR TÉCNICO", para el ítem 2, la entidad solicita el Perfil de "Especialista de Seguridad de la Información" en donde manifiesta una formación académica así: "Ingeniero de Sistemas, de Telecomunicaciones, Electrónico o ingenierías afines con Maestría en Seguridad de la Información. Deberá contar con por lo menos cuatro (4) de las siguientes certificaciones vigentes:

- LEAD IMPLEMENTER ISO 27001 v.2022
- CISM - CERTIFIED INFORMATION SECURITY MANAGEMENT
- CERTIFIED ETHICAL HACKER (CEH). • ECIH EC-COUNCIL CERTIFIED INCIDENT HANDLER • CISSP - CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
- CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER • MANAGER CYBERSECURITY ISO/IEC 27032"

Amablemente solicitamos a la entidad incluir dentro de la formación postgrados y/o maestrías, adicionalmente, que dentro del requerimiento se añada el afín así, quedando el requerimiento así: "... con especialización y/o maestría en Seguridad de la Información, Ciberseguridad, y/o afines de acuerdo con el núcleo básico del conocimiento"





Ahora bien, agradecemos disminuir la cantidad de certificaciones requeridas y ampliando las opciones de certificaciones incluyendo:

- Certified Application Security Engineer (CASE)
- EC-Council - Certified Ethical Hacking (CEH)
- EC-Council - Offensive Security Certified Professional
- (OSCP) - Offensive Security - Certified Red Team Professional - (CRTP)
- Altered Security.
- Mobile Application Pentester (eMAPT) - eLearnSecurity
- ISO27001 Auditor Interno

#### RESPUESTA 1

La FGN no acoge su observación, teniendo en cuenta las tecnologías de la Entidad y el propósito del perfil el cual tiene un rol importante de arquitecto de seguridad y de conocimientos de protocolos y pruebas de seguridad para los desarrollos, se modificará el requerimiento del Perfil de Especialista de Seguridad de la Información, el cual quedará así:

| Perfil                                      | Formación Académica                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Experiencia Mínima                                                                                                                                                                          |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Especialista de Seguridad de la Información | <p>Ingeniero de Sistemas, de Telecomunicaciones, Electrónico o ingenierías afines según el NBC del SNIES, con Maestría en Seguridad de la Información o afines según el NBC del SNIES</p> <p>Deberá contar con por lo menos cinco (5) de las siguientes certificaciones vigentes:</p> <ul style="list-style-type: none"><li>• LEAD IMPLEMENTER ISO 27001 v.2022</li><li>• CISM - CERTIFIED INFORMATION SECURITY MANAGEMENT</li><li>• CERTIFIED ETHICAL HACKER (CEH).</li><li>• ECIH EC-COUNCIL CERTIFIED INCIDENT HANDLER</li><li>• CISSP - CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL</li><li>• CERTIFIED DATA PRIVACY SOLUTIONS ENGINEER</li><li>• MANAGER CYBERSECURITY ISO/IEC 27032</li><li>• MICROSOFT CERTIFIED DEVOPS ENGINEER EXPERT</li><li>• CERTIFIED SECURITY+ DE COMPTIA</li></ul> | Experiencia específica de al menos diez (10) años en proyectos relacionados con seguridad de la información, en roles de Lider, Consultor, Asesor u Oficial en Seguridad de la Información. |





#### **OBSERVACIÓN 1**

##### **7. Complemento al Pliego de Condiciones**

PAG. 38

##### **6.2 FACTOR TÉCNICO**

###### **Observación:**

Considerando el principio de pluralidad de oferentes y la habilitación de empresas multinacionales de alto nivel que puedan prestar los servicios con los más altos estándares de calidad, consideramos restrictiva la siguiente anotación, y agradecemos pueda ser eliminada: NOTA 2: El proveedor debe estar listado en la página oficial del CMMI, aplicable para el país ("Country") "Colombia".

#### **RESPUESTA 1**

La Fiscalía General de Nación No acepta la observación, Esta condición tiene como finalidad garantizar que el proveedor cuenta con presencia formal y capacidad operativa en el país donde se ejecutará el contrato. Si bien se reconoce la importancia del principio de pluralidad de oferentes, esta medida no restringe la participación de empresas multinacionales, siempre que estas cuenten con representación o habilitación en Colombia, lo cual es coherente con los principios de transparencia, trazabilidad y verificación técnica que rigen la contratación pública.

#### **OBSERVACIÓN 2**

##### **7. Complemento al Pliego de Condiciones**

PAG. 39

##### **6.2 FACTOR TÉCNICO**

###### **Observación:**

Considerando la finalidad del recurso solicitado, y teniendo en cuenta los estándares del mercado mas importantes, consideramos relevante incluir entre las opciones de certificaciones requeridas las siguientes:

- Certified Chief Information Security Officer C-CISO
- Auditor Líder ISO 31000: Gestión del riesgo 2017
- Auditor Líder ISO 22301 Gestión de la Continuidad del Negocio

#### **RESPUESTA 2**

La fiscalía general de la nación no acepta la observación, en razón a que, las certificaciones actualmente requeridas fueron definidas en función de las competencias específicas necesarias para el cumplimiento de las actividades técnicas contempladas.

Las certificaciones C-CISO, Auditor Líder ISO 31000 e ISO 22301 están orientadas a perfiles estratégicos y de gestión, más que a perfiles operativos o técnicos. En este caso, el recurso solicitado requiere conocimientos aplicados en áreas específicas de seguridad de la información, continuidad de negocio o gestión de riesgos, pero no necesariamente en niveles de liderazgo o auditoría.

#### **OBSERVACIÓN 3**

##### **8.1. Anexo Oferta Económica**

###### **Observación:**

Agradecemos confirmar si la "BOLSA DE HORAS A MONTO AGOTABLE" se definirá con base a la cantidad de horas establecidas en el formato económico, con base en el presupuesto asignado a este proceso.

#### **RESPUESTA 3**

La fiscalía general aclara que en atención a la observación estimada para la bolsa de horas a monto agotable, se informa que, la asignación de horas y su correspondiente monto económico será definida en el documento contractual, una vez consolidadas las necesidades funcionales, técnicas y presupuestales, en el marco del plan de trabajo inicial.

El valor total y la cantidad de horas correspondientes a la bolsa de horas estarán determinados por el presupuesto aprobado, así como por la planeación estratégica de requerimientos adicionales no cubiertos.

#### **OBSERVACIÓN 4**

##### **8.1. Anexo Oferta Económica**

###### **Observación:**





Agradecemos confirmar la fecha máxima en la que se pueden consumir el "monto agotable" para la ejecución de este proyecto.

#### RESPUESTA 4

La fiscalía general aclara que para la Bolsa de Horas a Monto Agotable, el número de horas exacto a consumir dependerá de las solicitudes que se generen y se irá agotando de acuerdo con la ejecución y la planeación realizada

#### OBSERVACIÓN 5

##### 3.4. ANEXO TÉCNICO 4 EQUIPO DE TRABAJO V2

PAG 1

##### CONFORMACIÓN DE EQUIPOS DE TRABAJO Y PERFILES REQUERIDOS

#### Observación:

Agradecemos confirmar a la entidad el stack tecnológico completo utilizado por la entidad, así como las arquitecturas estándar que se utilizarán en la ejecución del proyecto, de tal manera que se pueda realizar un adecuado dimensionamiento de desarrollo solicitado por la entidad como responsabilidad del contratista.

#### RESPUESTA 5

La fiscalía general de la Nación aclara que las arquitecturas serán entregadas una vez se tenga el acta de inicio del contrato, no obstante, para el conocimiento de oferente se aclara que el contratista debe tener capacidad de implementar DevOps (AZURE), GitHub, metodologías ágiles, Azure boards y/o metodologías de otras nubes como GCP y AWS, o pueden ser híbridas.

#### OBSERVACIÓN 6

##### 3.2. ANEXO TÉCNICO 2 ANS V2

PAG. 36

##### DESARROLLO E IMPLEMENTACIÓN PARA LA FISCALÍA GENERAL DE LA NACIÓN

#### Observación:

Agradecemos confirmar a la entidad el stack tecnológico completo utilizado por la entidad, así como las arquitecturas estándar que se utilizarán en la ejecución del proyecto, de tal manera que se pueda realizar un adecuado dimensionamiento de desarrollo solicitado por la entidad como responsabilidad del contratista.

#### RESPUESTA 6

La fiscalía general de la Nación aclara que las arquitecturas serán entregadas una vez se tenga el acta de inicio del contrato, no obstante, para el conocimiento de oferente se aclara que el contratista debe tener capacidad de implementar DevOps (AZURE), GitHub, metodologías ágiles, Azure boards y/o metodologías de otras nubes como GCP y AWS, o pueden ser híbridas.

#### OBSERVACIÓN 7

##### 3.1. ANEXO TECNICO 1 CONDICIONES MINIMAS DEL PRODUCTO DE SOFTWARE V2

#### Observación:

¿Cuál es el alcance exacto por dominios funcionales y sistemas priorizados en el primer trimestre, y qué catálogo de aplicaciones será cubierto por SAM y por bolsa de horas respectivamente?

#### RESPUESTA 7

La Fiscalía General de la Nación informa que, conforme a lo establecido en el Anexo Técnico 1, los servicios definidos en los componentes de **Soporte, Actualización y Mantenimiento (SAM)**, así como aquellos asociados a la **bolsa de horas**, serán distribuidos de acuerdo con las necesidades funcionales y estratégicas priorizadas por la Entidad, las cuales serán comunicadas formalmente al contratista al inicio del contrato y actualizadas de manera iterativa en el marco del ciclo de vida del proyecto.

Los sistemas incluidos en esta modalidad serán definidos de manera acorde a las prioridades establecidas por las áreas funcionales usuarias y autorizadas por la FGN. Este catálogo será dinámico y podrá ser ajustado por la FGN durante la ejecución contractual, conforme a las necesidades institucionales.

#### OBSERVACIÓN 8

ER





|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>3.1. ANEXO TECNICO 1_CONDICIONES_MINIMAS_DEL_PRODUCTO_DE_SOFTWARE_V2</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Observación:</b><br><br>¿Qué autoridad aprueba cambios de alcance y cuál es el flujo de control de cambios (herramienta, estados, SLA de decisión, criterios de aceptación del cambio)?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>RESPUESTA 8</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| La Fiscalía General de la Nación cuenta con un procedimiento definido para la gestión y aprobación de cambios de alcance durante la ejecución del contrato, conforme a los principios de trazabilidad, evaluación técnica y control contractual, la aprobación de la misma estará a cargo de la supervisión del contrato y el comité de cambios en los casos en que el producto ya se encuentre en ambiente productivo. Una vez aprobado el cambio por la autoridad competente, este se integrará al Plan de Trabajo, cronograma y entregables contractuales mediante el mecanismo correspondiente (acta de comité, actualización del plan, acta de reunión, historia de usuario). |
| <b>OBSERVACIÓN 9</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>3.1. ANEXO TECNICO 1_CONDICIONES_MINIMAS_DEL_PRODUCTO_DE_SOFTWARE_V2</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Observación:</b><br>¿Existe un Product Governance Board entre FGN y contratista para la priorización del backlog, con periodicidad y quorum definidos?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>RESPUESTA 9</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| La Fiscalía General de Nación , Aclara que Sí. De acuerdo con lo establecido en el Anexo Técnico 1, y como se ha mencionado en observaciones anteriores, la Fiscalía General de la Nación cuenta con mecanismos formales de articulación y seguimiento conjunto para garantizar la correcta planeación, seguimiento y priorización del backlog.                                                                                                                                                                                                                                                                                                                                    |
| <b>OBSERVACIÓN 10</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>3.1. ANEXO TECNICO 1_CONDICIONES_MINIMAS_DEL_PRODUCTO_DE_SOFTWARE_V2</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Observación:</b><br>Hay dos tablas distintas de tiempos (incidentes Alta/Media/Baja y clasificación Crítica/Moderada/Menor/Mantenimiento de emergencia) con SLA diferentes; ¿cuál prevalece y cómo se mapean exactamente las categorías entre sí?                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>RESPUESTA 10</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| La Fiscalía General de Nación , Aclara que las dos tablas referenciadas en el Anexo Técnico no son contradictorias ni excluyentes, sino complementarias entre sí. Cada una está diseñada para atender aspectos específicos de la gestión del servicio, conforme al enfoque integral definido en el modelo SAM (Soporte, Actualización y Mantenimiento).                                                                                                                                                                                                                                                                                                                            |
| <b>OBSERVACIÓN 11</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>3.1. ANEXO TECNICO 1_CONDICIONES_MINIMAS_DEL_PRODUCTO_DE_SOFTWARE_V2</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Observación:</b><br>¿Cómo se calculan la disponibilidad objetivo y las ventanas de mantenimiento planificado, y qué exclusiones aplican para indisponibilidades atribuibles a terceros/infraestructura FGN?                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>RESPUESTA 11</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| La fiscalía general de la Nación aclara que, el tiempo de las ventanas será verificado por los procesos de gestión de TI, como Gestión de cambios, Gestión de despliegue, entre otros que se implementen actualmente y dentro de la vigencia del contrato.                                                                                                                                                                                                                                                                                                                                                                                                                         |



**OBSERVACIÓN 12****3.1. ANEXO TECNICO 1\_CONDICIONES\_MINIMAS\_DEL\_PRODUCTO\_DE\_SOFTWARE\_V2****Observación:**

¿Cuál es el factor de productividad oficial en horas por UCP para este contrato, y bajo qué condiciones se actualiza (histórico, complejidad tecnológica, madurez del equipo)?

**RESPUESTA 12**

La Fiscalía General de Nación, Aclara que en el marco del contrato y conforme a lo establecido en el *Anexo Técnico 1 – Condiciones Mínimas del Producto de Software*, no se ha definido un factor de productividad oficial en horas por UCP (Use Case Points) de manera rígida o única. Sin embargo, se considera que este factor podrá ser determinado en conjunto con el contratista una vez se inicie la ejecución del contrato, y con base en variables técnicas y operativas observadas en el desarrollo real del servicio.

**OBSERVACIÓN 13****3.1. ANEXO TECNICO 1\_CONDICIONES\_MINIMAS\_DEL\_PRODUCTO\_DE\_SOFTWARE\_V2****Observación:**

Para historias de usuario, ¿cómo se medirá exactamente el conteo de “transacciones” al no usar Casos de Uso clásicos (definición operativa, ejemplos, reglas de conteo)?

**RESPUESTA 13**

La Fiscalía General de Nación, Aclara que de acuerdo con el enfoque de desarrollo ágil adoptado por la Fiscalía General de la Nación (FGN), y conforme a lo establecido en el *Anexo Técnico 1 – Condiciones Mínimas del Producto de Software*, la medición del esfuerzo de desarrollo se realiza mediante métricas funcionales adaptadas a metodologías modernas como User Stories (Historias de Usuario), sin depender estrictamente del modelo clásico de Casos de Uso. El conteo de transacciones no depende de Casos de Uso clásicos, sino de la definición funcional contenida en las historias de usuario, bajo una lógica estructurada de interacción funcional.

**OBSERVACIÓN 14****3.1. ANEXO TECNICO 1\_CONDICIONES\_MINIMAS\_DEL\_PRODUCTO\_DE\_SOFTWARE\_V2****Observación:**

¿Qué factores TCF/ECF y pesos están preestablecidos por FGN y cuáles pueden ser propuestos por el contratista, incluyendo rangos y justificación requerida?

**RESPUESTA 14**

La Fiscalía General de Nación, Aclara que respecto a la solicitud sobre los factores de ajuste TCF (Technical Complexity Factor) y ECF (Environmental Complexity Factor) utilizados en la estimación basada en Puntos de Caso de Uso (UCP), la Fiscalía General de la Nación (FGN) se permite informar que la FGN ha establecido valores de referencia para los factores TCF y ECF, pero permite ajustes justificados por parte del contratista dentro del marco del contrato. Dichos ajustes deberán ser técnicamente sustentados, aprobados por la entidad y registrados formalmente en la documentación técnica del proyecto.

**OBSERVACIÓN 15****3.1. ANEXO TECNICO 1\_CONDICIONES\_MINIMAS\_DEL\_PRODUCTO\_DE\_SOFTWARE\_V2**





**Observación:**

¿Cuál es el proceso de discrepancias de estimación (FGN vs contratista), tiempos de resolución y criterio de desempate?

**RESPUESTA 15**

La Fiscalía General de Nación , Aclara que definirá un proceso formal y colaborativo para la resolución de discrepancias el cual será documentado y acordado el inicio de la ejecución del contrato.

**OBSERVACIÓN 16**

**3.1. ANEXO TECNICO 1\_CONDICIONES\_MINIMAS\_DEL\_PRODUCTO\_DE\_SOFTWARE\_V2**

**Observación:**

¿Qué herramienta oficial de gestión del trabajo usará FGN (Jira/Dexón/GitLab Issues) para backlog, historias, defectos y cambios, y qué esquema de proyectos x áreas se adoptará?

**RESPUESTA 16**

La Fiscalía General de Nación , Aclara que definirá la herramienta formal al inicio de la ejecución del contrato, sin embargo, se aclara que en la actualidad se utiliza GitLab Issues el cual se informa como referencia.

**OBSERVACIÓN 17**

**3.1. ANEXO TECNICO 1\_CONDICIONES\_MINIMAS\_DEL\_PRODUCTO\_DE\_SOFTWARE\_V2**

**Observación:**

¿Cuál es el Definition of Ready y Definition of Done institucional, incluyendo requisitos minimos de seguridad, pruebas y documentación por historia?

**RESPUESTA 17**

La Fiscalía General de Nación , Aclara que ha definido un conjunto de requisitos institucionales tanto para el inicio como para la aceptación de historias de usuario que garantizan el control de calidad, la seguridad, la trazabilidad y el cumplimiento funcional del desarrollo. Estos criterios están alineados con las mejores prácticas ágiles y se encuentran descritos y aplicables conforme a lo establecido en el Anexo Técnico 1 del proceso.

Los criterios específicos de DoR y DoD pueden ajustarse según la naturaleza del producto o servicio involucrado, siempre alineados al marco definido en el **Anexo Técnico 1** y en las metodologías ágiles adoptadas. El contratista deberá ajustarse a estos lineamientos y podrá sugerir mejoras, que serán evaluadas por la FGN en los espacios de gobernanza técnica.

**OBSERVACIÓN 18**

**3.1. ANEXO TECNICO 1\_CONDICIONES\_MINIMAS\_DEL\_PRODUCTO\_DE\_SOFTWARE\_V2**

**Observación:**

¿Qué cadencia y formato tendrán planning, review, retro y refinamiento, y qué roles de FGN deben asistir con carácter obligatorio?

**RESPUESTA 18**

La Fiscalía General de Nación , Aclara que tal como se ha indicado en respuestas anteriores, la FGN proporciona los medios colaborativos, herramientas de gestión de proyectos y canales de comunicación necesarios para llevar a cabo estas ceremonias. La asistencia y participación activa de los roles definidos será obligatoria en las ceremonias principales (planning, review y refinement),