SOLICITUD DE MANIFESTACIONES DE INTERÉS
SERVICIOS DE CONSULTORÍA - OPERACIONES EJECUTADAS POR EL BANCO
PROCESO DE SELECCIÓN COMPETITIVO SIMPLIFICADO

NOMBRE DEL PROYECTO: Consultoría para la implementación y despliegue de la Plataforma de Gestión de Fondos de Ayuda Federal para la Seguridad Pública (FASP)
SELECCIÓN #: ME-T1552-P001
MÉTODO DE SELECCIÓN: Competitivo Simplificado
PAÍS: México
SECTOR OR DEPARTMENTO: IFD/CIS
NOMBRE DE LA CT: ME-T1552: Fortaleciendo la capacidad de gestión del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública
FINANCIAMIENTO – CT #: ATN/OC-22197-ME
ENLACE AL DOCUMENTO DE CT: HTTPS://WWW.IADB.ORG/ES/PROYECTO/ME-T1552

Atención Firmas Consultoras: Actualización Importante sobre el Registro en el Portal de Adquisiciones BEO

A partir del 1 de julio, todas las firmas consultoras, tanto nuevas como previamente registradas en el Portal de Adquisiciones BEO, deben agregar su **Número de Socio Comercial (Business Partner Number por sus siglas en inglés)** al perfil de su organización para participar o continuar participando en un proceso de adquisición BEO.

Por favor consulte las **Preguntas Frecuentes** (FAQs) en el Portal para más detalles sobre **"Cómo encontrar u obtener su Número BP".**

Evite retrasos, no espere hasta el último momento para completar esta actualización. Este proceso puede tardar hasta **48 horas** en completarse y podría impedir que su organización participe en un Proceso BEO.

Para preguntas o asistencia técnica, utilice el **chat en vivo** en la página del Portal de Adquisiciones BEO o envíenos un correo electrónico a: **ocs.procurement@iadb.org**

El Banco Interamericano de Desarrollo (el Banco) se creó en diciembre de 1959 para contribuir a acelerar el desarrollo económico y social de América Latina y el Caribe. En la actualidad, el Banco es un importante catalizador en la movilización de recursos para la región (Para más información sobre el Banco, consulte su sitio web en www.iadb.org).

Sección 1. Objeto de la presente Solicitud de Manifestaciones de Interés

1.1. El Banco ejecuta el proyecto mencionado. El Banco tiene la intención de contratar

los servicios de consultoría descritos en la presente Solicitud de Manifestaciones de Interés (REOI, por sus siglas en inglés). El propósito de esta REOI es obtener información suficiente que permita al Banco evaluar si las empresas consultoras (EC) elegibles poseen la experiencia y la competencia requeridas pertinentes para prestar los servicios de consultoría solicitados por el Banco.

1.2. Según se define en la Política de Adquisiciones Institucionales (GN-2303-33), las EC participantes deben ser de un País[1] o Territorio[2] miembro del Banco para poder presentar una Manifestación de Interés (EOI por sus siglas en inglés). Las EC que posean la experiencia requerida relevante para el encargo serán evaluadas. El Banco llevará a cabo la evaluación y clasificación (ranking) de las EOI presentadas por las EC que hayan manifestado su interés. El Banco invitará a las EC a presentar una propuesta en el orden en que se haya establecido la clasificación (ranking). Si la propuesta de la EC clasificada en primer lugar es aceptable, se le invitará a negociar un Contrato. Si fracasan las negociaciones con la primera EC, se podrá invitar a la siguiente EC clasificada a presentar una propuesta y negociar.

1.3. Esta REOI no debe interpretarse ni como una Solicitud de Propuesta ni como una oferta de contratación y no obliga en modo alguno al Banco a contratar a ninguna EC. El Banco se reserva el derecho de rechazar cualquiera y todas las EC participantes por cualquier motivo o sin motivo alguno, sin necesidad de dar explicaciones. El Banco no se compromete de modo alguno a seleccionar a una empresa consultora participante. El Banco no informará los motivos por los que cualquier EC participante haya o no sido incluida como parte de la lista corta.

Sección 2. Instrucciones para las empresas consultoras elegibles

2.1. Las manifestaciones de interés deberán enviarse utilizando el *Portal de Adquisiciones BEO del BID* (el Portal) (http://beo-procurement.iadb.org) antes del *23/04/2026* 5:00 PM. (**hora de Washington, D.C.**) en formato PDF (Max. 45MB).

2.2. Para acceder al Portal, la EC debe generar una cuenta de registro que incluya ***todos*** los datos solicitados por el Portal. En caso de que no se incluya alguno de los datos solicitados, la empresa consultora no podrá participar en este ni en

[1] **Países miembro:** Alemania, Argentina, Austria, Bahamas, Barbados, Bélgica, Belice, Bolivia, Brasil, Canadá, Colombia, Costa Rica, Chile, Croacia, Dinamarca, Ecuador, El Salvador, Eslovenia, España, Estados Unidos, Finlandia, Francia, Guatemala, Guyana, Haití, Honduras, Israel, Italia, Jamaica, Japón, México, Nicaragua, Noruega, Países Bajos, Panamá, Paraguay, Perú, Portugal, Reino Unido, República de Corea, República Dominicana, República Popular China, República Popular Democrática de Corea, Suecia, Suiza, Surinam, Trinidad y Tobago, Uruguay y Venezuela. Tobago, Reino Unido, Uruguay y Venezuela.

[2] **Territorios elegibles:** a) Guadalupe, Guayana Francesa, Martinica, Reunión - como Departamentos de Francia; b) Islas Vírgenes de los Estados Unidos, Puerto Rico, Guam - como Territorios de los EE.UU.; c) Aruba - como país constituyente de los Países Bajos; y Bonaire, Curaçao, San Martín, Saba, San Eustaquio - como Departamentos de los Países Bajos; d) Hong Kong - como Región Administrativa Especial de la República Popular China.

ningún otro proceso de selección que lleve a cabo el Banco. Si la empresa consultora se ha registrado previamente, verifique que tenga ***toda*** la información de la EC actualizada y completa antes de presentar una EOI.

2.3. Las EC elegibles podrán asociarse en forma de Consorcio/ Joint Venture (JV) para mejorar sus calificaciones. Dicho Consorcio/ JV designará a una de las EC como representante responsable de las comunicaciones, del registro en el Portal y de la presentación de los documentos correspondientes.

2.4. Las EC elegibles interesadas podrán obtener más información en horario de oficina, de 09:00 AM a 5:00 PM **(hora de Washington, D.C**.), enviando un correo electrónico a: Sergio Triana: *SERGIOTR@IADB.ORG*

Banco Interamericano de Desarrollo
División: División de Seguridad Ciudadana (IFD/CIS)
A la atención de: Sergio Triana
1300 New York Ave, NW
Washington DC 20577
Tel: +12026232325
Correo electrónico: *SERGIOTR@IADB.ORG*
Página web: www.iadb.org

2.5. Por la presente, el Banco invita a las EC elegibles a indicar su interés en prestar los servicios descritos a continuación en el borrador de Términos de Referencia para realizar los servicios de consultoría. Las EC interesadas deberán proporcionar información que demuestre que poseen la experiencia necesaria y están calificadas para prestar los servicios. Para que todas las respuestas puedan evaluarse adecuadamente, las EC elegibles deben incluir en sus presentaciones la información solicitada en la siguiente sección, con explicaciones completas y claras.

Sección 3. Servicios de consultoría

3.1. Los servicios de consultoría incluyen [la continuación del desarrollo, fortalecimiento, integración, despliegue y transferencia de plataforma digital nacional que permita gestionar, monitorear y auditar de forma segura, eficiente y trazable el ciclo completo de los Fondos de Ayuda Federal para la Seguridad Pública.

3.2. Aunque no existe un formato estándar para presentar una EOI, las EC elegibles deberán presentar una EOI que contenga la siguiente información:

a) Información básica: indique el nombre oficial de la EC, el nombre de la persona de contacto, la dirección de correo electrónico, los números de teléfono y la dirección de la oficina de la persona de contacto clave responsable de la EOI.
b) Antecedentes: Incluya una descripción de la EC. La EC puede incluir folletos o documentos que proporcionen información sobre su organización, historia, misión, estructura y número de empleados.
c) Experiencia relacionada con los servicios de consultoría solicitados: Proporcione todo tipo de pruebas que la EC considere apropiadas para demostrar su experiencia y conocimientos técnicos en la prestación de servicios similares a los descritos en el Anexo A, Términos de Referencia (por ejemplo, folletos, informes, estudios, descripción de encargos similares, referencias a casos en los que haya prestado servicios similares, experiencia en condiciones similares, disponibilidad de habilidades apropiadas entre el personal, etc.)

3.3. Presupuesto estimado: USD 115,000

Anexo A. Borrador de los Términos de Referencia

Tenga en cuenta que el Banco podrá modificar los Términos de Referencia adjuntos. Se notificarán estos cambios a las EC que hayan sido preseleccionadas.

Términos de Referencia

1. Antecedentes y justificación

1.1. La gestión de los Fondos de Ayuda Federal para la Seguridad Pública —incluyendo su asignación, aprobación, concertación, ejercicio y seguimiento— **se realiza mediante procesos manuales y poco trazables**. Las entidades federativas deben elaborar y enviar la documentación correspondiente en medios físicos (oficios impresos, firmados, escaneados y correspondencia física), lo que genera tiempos de atención prolongados y altos costos operativos.
1.2. Este modelo de operación **ha dificultado la vigilancia y seguimiento oportuno del ejercicio del presupuesto**, impidiendo que se cumplan plenamente con los objetivos definidos en los Programas con Prioridad Nacional para la Seguridad Pública. Aunado a la dispersión de procesos, baja trazabilidad del cumplimiento de metas y la limitada interoperabilidad entre instituciones federales y locales. Todo ello dificulta la supervisión estratégica y el control del ejercicio presupuestal a través de sus diferentes momentos contables.
1.3. En respuesta a este diagnóstico, el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP), en coordinación con la Agencia de Transformación Digital y Telecomunicaciones (ATDT), responsable de generar e implementar la política digital y tecnológica del Gobierno de México, han iniciado el **desarrollo de una nueva plataforma digital que permita reducir procesos manuales y basados en papel**. Esta herramienta busca digitalizar el proceso de concertación, así como mejorar el monitoreo, vigilancia y la rendición de cuentas del uso de los recursos asignados.
1.4. Dicha plataforma considera las **cuatro etapas** del ciclo de vida de los fondos de ayuda federal en materia de Seguridad Pública, a saber: **1)** presupuesto y estructuras programáticas; **2)**

convocatoria y concertación; **3)** seguimiento y verificación; **4)** vigilancia y cierre. La ATDT realizará dos entregas una para cada una de las primeras dos etapas.

2. Objetivos

2.1. El objetivo general de esta consultoría consiste en continuar el desarrollo e implementación de una plataforma digital nacional que permita gestionar, monitorear y auditar de forma segura, eficiente y trazable el ciclo completo de los Fondos de Ayuda Federal para la Seguridad Pública.

2.2. Los objetivos específicos consisten en:

a) Analizar y validar el estado actual de la plataforma digital desarrollada por la ATDT, y en su caso ajustar los requerimientos funcionales, flujos operativos y reglas de negocio ya definidos; asegurando su correcta implementación, incluyendo pero no limitado a: arquitectura, código fuente, integridad de datos, módulos funcionales existentes, documentación técnica y funcional, mapeo de procesos y las reglas de negocio correspondientes a las fases de presupuesto, estructuras programáticas, convocatoria y concertación.

b) Desarrollar, integrar y poner en operación los módulos correspondientes a las fases de seguimiento y verificación, vigilancia y cierre del ciclo de los Fondos de Ayuda Federal para la Seguridad Pública, asegurando la identificación de brechas funcionales y su interoperabilidad con los módulos ya existentes y su implementación conforme a los lineamientos técnicos, estándares de desarrollo, arquitectura y stack tecnológico definidos por la ATDT (véase “Anexo de Lineamientos Técnicos de Desarrollo y Arquitectura”).

c) Fortalecer las capacidades institucionales para la operación y sostenibilidad del sistema, mediante la elaboración de documentación técnica y funcional actualizada, así como la implementación de procesos de capacitación, acompañamiento y transferencia de conocimiento dirigidos al personal del SESNSP y a las y los enlaces de los Secretariados Ejecutivos Estatales

d) Garantizar que la solución cumpla con estándares verificables de seguridad, calidad, mantenibilidad y continuidad operativa.

3. Alcance de los servicios

3.1. La firma consultora deberá brindar acompañamiento al Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP), en un esfuerzo colaborativo con la Agencia de Transformación Digital y Telecomunicaciones (ATDT) para dar continuidad, completar y consolidar el desarrollo e implementación de la plataforma digital nacional de gestión del ciclo completo de los Fondos de Ayuda Federal para la Seguridad Pública.

3.2. El alcance se centra en la evaluación, fortalecimiento y evolución de una plataforma digital ya existente, desarrollada bajo la rectoría técnica de la ATDT, la cual cuenta con una primera entrega funcional correspondiente a las fases de presupuesto, estructuras programáticas, convocatoria y concertación. La firma consultora deberá trabajar sobre las directrices establecidas en el “Anexo de Lineamientos Técnicos de Desarrollo y Arquitectura” definidos por la ATDT.

3.3. El enfoque metodológico de esta consultoría deberá considerar las siguientes funcionalidades requeridas:

- Continuación del proceso de diseño y desarrollo de la plataforma, e identificación y priorización de funcionalidades y mejoras en el sistema de acuerdo a las

necesidades del SESNSP.

- Implementación de capacitaciones y acompañamiento para personal del Secretariado Ejecutivo del Sistema Nacional de Seguridad y entidades federativas que administren y operen el sistema.
- Implementación de capacitaciones y acompañamiento para personal de las entidades federativas que registren la información de su jurisdicción.

4. Actividades clave

4.1. Para cumplir con el objetivo del proyecto de consultoría, la firma a cargo deberá realizar las siguientes actividades, sin perjuicio de otras que se consideren necesarias:

Actividades	Tareas
a) Seguimiento del proyecto y gestión de recomendaciones	● Reuniones operativas y estratégicas sobre los avances y retos en la implementación. ● Elaboración de informes de actividades. ● Implementación de los cambios y recomendaciones. ● Resolución de incidencias ocurridas durante la implementación y/o evolución. ● Evaluación y priorización de deuda técnica. ● Gestión de dependencias con la ATDT. ● Prueba piloto de los módulos heredados (presupuesto y estructuras programáticas; convocatoria y concertación) en al menos tres entidades seleccionadas por el SESNSP.
b) Desarrollo de los módulos especificados para este nuevo alcance	● Análisis funcional y técnico de los módulos desarrollados por la ATDT (presupuesto y estructuras programáticas; convocatoria y concertación) con los que deberán integrarse los nuevos módulos desarrollados (seguimiento y verificación; vigilancia y cierre), considerando flujos existentes, reglas de negocio, estructura de datos y el flujo TO-BE definido por la ATDT. ● Diseño técnico y funcional, así como documentación de los flujos operativos de los módulos de seguimiento y verificación, vigilancia y cierre. ● Desarrollo, configuración e integración de los módulos mencionados, garantizando: interoperabilidad con los módulos heredados, trazabilidad de la información a lo largo del ciclo de vida de los fondos, control por roles y perfiles de usuario; y registro de eventos, validaciones y estados del proceso. ● Validación operativa de los módulos con un grupo de control de personas usuarias, mediante la realización de un ejercicio acotado de revisión funcional con personal del SESNSP y representantes de tres entidades federativas

	seleccionadas. ● Despliegue automatizado en la infraestructura de la nube que utiliza el SESNSP. ● Documentación técnica y funcional de los módulos desarrollados, incluyendo: descripción de funcionalidades, flujos operativos, reglas de negocio implementadas y la documentación obligatoria de entrega señalada en el "Anexo de Lineamientos Técnicos de Desarrollo y Arquitectura". ● Entrega de los módulos desarrollados en ambientes de prueba y su posterior liberación en ambientes productivos conforme al Anexo de Lineamientos Técnicos de Desarrollo y Arquitectura Definidos en coordinación con la ATDT y el SESNSP.
c) Control de calidad y pruebas del sistema (QA)	● Diseñar y ejecutar planes de prueba funcionales, de carga y de aceptación de personas usuarias, incluyendo criterios de éxito. ● Participar en la planificación de iteraciones y sprints, identificando riesgos de calidad en entregables técnicos. ● Pruebas de ciberseguridad, incluyendo, pero no limitando: pruebas de penetración (pentesting), auditoría de mejores prácticas de ciberseguridad y análisis de vulnerabilidades. ● Operación de una mesa de ayuda técnica durante las fases de pruebas, implementación y estabilización del sistema durante la vigencia del contrato.
d) Gestión del cambio, adopción del sistema y transferencia del conocimiento	● Elaborar un plan de gestión del cambio para facilitar la adopción del sistema en las entidades federativas. ● Elaboración de manuales operativos por rol y guías rápidas. ● Desarrollar materiales de capacitación, guías para las personas usuarias y manuales operativos en lenguaje claro. ● Sesiones de train-the-trainer y acompañamiento a replicadores estatales. ● Realizar sesiones de capacitación (virtuales) con los diferentes perfiles de personas usuarias. ● Documentación sobre la gestión del cambio, capacitaciones y retroalimentación.

5. Entregables

5.1. Plan de trabajo detallado

- Ruta estratégica dividida en etapas para definir los temas fundamentales en el desarrollo e implementación de los módulos faltantes y la interoperabilidad de los módulos heredados.
- Documento que defina el alcance del proyecto, objetivos por etapa del ciclo de los fondos; supuestos, dependencias y restricciones técnicas; así como criterios de aceptación generales del proyecto.
- Cronograma detallada por fases e iteraciones.

5.2. Diagnóstico técnico–funcional del sistema existente y backlog priorizado

- Documento de estado inicial y estado final del sistema, de acuerdo al Documento de Arquitectura Base del Sistema (DABS) que será entregado por la ATDT una vez firmado el contrato, que identifique los módulos heredados, los módulos desarrollados o ajustados durante la consultoría y las principales decisiones técnicas y funcionales adoptadas.
- Documentación técnica y funcional actualizada y consolidada de la plataforma, incluyendo arquitectura, flujos de procesos, reglas de negocio y descripción de funcionalidades por fase y por rol.
- Registro de incidencias, ajustes y mejoras priorizadas e implementadas por la consultora durante el periodo del contrato.
- Registro de la implementación de las mejoras en colaboración con la ATDT, incluyendo acuerdos técnicos y validaciones correspondientes.
- Backlog funcional priorizado de funcionalidades por módulo y rol de usuario.
- Plan de gestión de desarrollo de los módulos (seguimiento y verificación, vigilancia y cierre).

5.3. Implementación y capacitación de módulos heredados

- Plan de capacitación por perfil de persona usuaria e institución (visualizador, capturista, revisor y validador), materiales didácticos, presentaciones y video-tutoriales para el uso del sistema en las primeras fases del ciclo de fondos.

5.4. Documentación técnica obligatoria de entrega y código fuente

La documentación deberá incluir, por lo menos, la siguiente información:

- **README.md** por repositorio.
- **CHANGELOG.md** por repositorio o componente.
- OpenAPI del backend.
- Modelo lógico de datos o documentación equivalente.
- Diagrama de arquitectura actualizado.
- Instrucciones de construcción local.
- Manual de configuración por ambiente.
- Inventario de variables y secretos referenciados.
- Evidencia de pruebas ejecutadas.
- Relación de decisiones de arquitectura y desviaciones aprobadas.
- Repositorio de código fuente en Git con permisos de administración y transferencia de propiedad.
- Código fuente completo y comentado, diferenciando los componentes heredados, los módulos desarrollados y los ajustes realizados durante la consultoría.
- Guía de despliegue, operación y mantenimiento técnico del sistema.

5.5. Plan y ejecución de pruebas de calidad (QA)

- Plan de pruebas funcionales, de carga y de aceptación de personas usuarias.

- Registro de casos de prueba, resultados obtenidos y documentación de hallazgos.
- Informe de verificación de calidad y recomendaciones de mejora.
- Estándar de verificación de seguridad adoptado (alineado a buenas prácticas internacionales).
- Adopción del marco **OWASP** como referencia mínima para el desarrollo seguro.
- Lineamientos de arquitectura obligatorios para garantizar escalabilidad, mantenibilidad e interoperabilidad.
- Política de calidad de código (estructura, convenciones, documentación mínima requerida).
- Reglas de versionado y control de cambios.
- Lineamientos de trazabilidad entre requerimientos, desarrollo, pruebas y liberación.
- Política de revisión automatizada de dependencias.
- Uso obligatorio de herramientas de análisis estático de código.

5.6. Productos de gestión del cambio y capacitación para entidades federativas

- Plan de Gestión del Cambio que incluya las tareas para la implementación de la herramienta en las entidades federativas.
- Plan de Comunicaciones que defina la información y los actores relevantes en relación con la herramienta.
- Plan de capacitación, mallas curriculares por perfil de persona usuaria, materiales didácticos, presentaciones y video-tutoriales para el uso del sistema en las distintas fases del ciclo de los fondos.
- Instrumentos de evaluación del aprendizaje y definición de métricas básicas de adopción y uso del sistema.
- Manuales por rol, guías rápidas, checklists, procedimientos operativos estándar (SOPs), preguntas frecuentes (FAQ) y glosario.
- Materiales de capacitación: presentaciones, guías operativas y videotutoriales en lenguaje claro.
- Manuales para personas usuarias del sistema por roles.
- Informe de ejecución de sesiones de capacitación y retroalimentación de personas usuarias.

5.7. Informe de cierre y transferencia de conocimiento

- Informe final que consolide los aprendizajes, entregables y buenas prácticas derivadas del acompañamiento al desarrollo del sistema.
- Repositorio estructurado con toda la documentación técnica, funcional y operativa generada durante el contrato.
- Recomendaciones para futuras fases de desarrollo, sostenibilidad técnica y backlog para incorporación de nuevas funcionalidades, así como actualización de reglas de negocio.

6. Calendario del Proyecto e Hitos

6.1. La consultoría tendrá una duración de 12 meses, con el siguiente cronograma:

Calendario de entrega de productos de la consultoría

Entregable	Fecha de entrega
Entregable 1. Plan de trabajo detallado	30 días luego de la firma del contrato
Entregable 2. Diagnóstico técnico–funcional del sistema existente; e implementación y capacitación de módulos heredados	75 días luego de la firma del contrato
Entregable 3. Productos de gestión del cambio	150 días luego de la firma del contrato
Entregable 4. Documentación técnica obligatoria de entrega; y plan y ejecución de pruebas de calidad (QA) del **módulo de seguimiento y verificación**	200 días luego de la firma del contrato
Entregable 5. Documentación técnica obligatoria de entrega; y plan y ejecución de pruebas de calidad (QA) del **módulo de vigilancia y cierre**	260 días luego de la firma del contrato
Entregable 6. Informe de cierre y transferencia de conocimiento	335 días luego de la firma del contrato

7. Requisitos de los Informes

7.1. Todos los entregables serán presentados en español en los formatos requeridos. Los informes serán presentados en las fechas consignadas en el cuadro "Calendario de entrega de productos de la consultoría". Después de cada entrega, se realizarán reuniones específicas de explicación del detalle de cada producto y se levantará un acta de recepción a satisfacción del producto respectivo. El Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP) y la supervisión del BID podrán pedir presentaciones especiales del producto entregado a equipos técnicos o grupos de trabajo relacionados con la temática tratada.

8. Criterios de aceptación

8.1. La empresa consultora mantendrá una comunicación periódica con el punto de contacto del BID y del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP), a lo largo de todo el proceso de la realización de las actividades y de desarrollo de todos los entregables descritos en este contrato. La empresa consultora deberá obtener la aprobación del BID de cada entrega previo al procesamiento de los pagos asociados.

8.2. Los entregables de esta consultoría deberán ser enviados por la firma consultora al BID y deberán contar con el visto bueno del beneficiario (punto de contacto del SESNSP) y del

especialista del BID a cargo de esta consultoría, a fin de procesar el pago por cada entregable.

8.3. La propiedad intelectual del desarrollo de los componentes, así como de todos los materiales y repositorios generados en el marco de esta consultoría será transferida al Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública y a la Agencia de Transformación Digital y Telecomunicaciones como donación del Banco Interamericano de Desarrollo.

9. Requisitos de la empresa consultora y equipo clave

9.1. La empresa consultora debe tener y acreditar al menos 5 años de experiencia en colaboraciones con gobiernos nacionales o locales. Asimismo, es deseable que la empresa tenga experiencia relevante trabajando con instituciones multilaterales de desarrollo. De igual manera, demostrar experiencia acreditada en el tema específico de la consultoría.

10. Supervisión e informes

10.1. La firma consultora deberá presentar los entregables de esta consultoría a Sergio Triana, Especialista Principal en Seguridad Ciudadana (*SERGIOTR@IADB.ORG*), y David Ortigosa, Especialista en Transformación Digital (davidor@iadb.org), quienes serán los supervisores de esta consultoría y quienes para todos los efectos realizarán seguimiento a la ejecución de la consultoría y podrán recomendar revisiones al proceso de ejecución, hacer comentarios a los entregables, aceptar o no los mismos.

11. Calendario de pagos

11.1. Las condiciones de pago se basarán en los hitos o entregables del proyecto. El Banco no espera hacer pagos por adelantado en virtud de contratos de consultoría a menos que se requiera una cantidad significativa de viajes. El Banco desea recibir la propuesta de costos más competitiva para los servicios descritos en el presente documento.

11.2. La Tasa de Cambios Oficial del BID indicada en el SDP se aplicará para las conversiones necesarias de los pagos en moneda local.

Plan de Pagos	
Entregables	**%**
1. Plan de trabajo detallado	**10%**
2. Diagnóstico técnico–funcional del sistema existente y backlog priorizado; e implementación y capacitación de módulos heredados	**20%**
3. Productos de gestión del cambio	**10%**
4. Documentación técnica obligatoria de entrega; y plan y ejecución de pruebas de calidad (QA) del módulo de seguimiento y verificación	**25%**
5. Documentación técnica obligatoria de entrega; y plan y ejecución de pruebas de calidad (QA) del módulo de vigilancia y cierre	**25%**
6. Informe de cierre y transferencia de conocimiento	**10%**
TOTAL	**100%**

Anexo 1

Anexo de Lineamientos Técnicos de Desarrollo y Arquitectura

1. Objetivo

- Objetivo: Establecer las reglas técnicas obligatorias para el diseño, construcción, pruebas, despliegue, documentación y transferencia de soluciones institucionales basadas en frontend SPA, backend API y repositorio de base de datos/migraciones.

2. Criterios normativos

Las reglas de este anexo se interpretan con el siguiente nivel de exigencia:

- Obligatorio:
  - Debe cumplirse sin excepción, salvo aprobación formal de la Agencia de Transformación Digital y Telecomunicaciones (ATDT).
- Recomendado:
  - Debe adoptarse por defecto; una alternativa requiere justificación técnica.
- Prohibido:
  - No debe implementarse bajo ninguna circunstancia sin autorización expresa.

3. Lineamientos transversales

3.1. Diseño y construcción

- Obligatorio:
  - Mantener una separación clara entre presentación, aplicación, dominio, persistencia e infraestructura.
  - Diseñar componentes con responsabilidades acotadas y dependencias explícitas.
  - Favorecer modularidad, bajo acoplamiento y alta cohesión.
  - Documentar cualquier decisión técnica relevante que afecte la mantenibilidad, seguridad, despliegue o adopción futura.
- Prohibido:
  - Mezclar lógica de negocio, acceso a datos y lógica de presentación en un mismo componente.
  - Introducir dependencias circulares entre módulos, features o capas.
  - Implementar soluciones ad hoc sin trazabilidad documental cuando afecten la arquitectura base.

3.2. Estándares de nomenclatura y estructura

- Obligatorio:
  - Mantener nombres consistentes, semánticos y alineados con la responsabilidad real de cada archivo, paquete o carpeta.
  - Conservar una estructura de proyecto predecible para facilitar mantenimiento y traspaso.
  - Colocar las pruebas adjuntas al código o en una estructura claramente relacionada.
- Prohibido:
  - Crear carpetas o paquetes genéricos como misc, helpers, temp, varios o equivalentes sin responsabilidad definida.

3.3. Control de dependencias

- Obligatorio:
  - Justificar el uso de librerías externas cuando afecten seguridad, autenticación, UI base, persistencia u observabilidad.

- Encapsular las integraciones con terceros mediante adaptadores, facades o servicios internos.
- Mantener inventario de dependencias críticas y su propósito.

- Prohibido:
  - Acoplar la lógica de negocio a APIs concretas de proveedores externos sin una capa de abstracción.

3.4. Transferencia y continuidad operativa

- Obligatorio:
  - Entregar código, documentación, scripts, configuraciones de ejemplo y evidencia de pruebas suficientes para continuidad interna.
  - Evitar conocimiento tácito como dependencia del proveedor.
  - Mantener la solución en estado reproducible desde cero por un equipo distinto al desarrollador original.

4. Lineamientos backend

4.1. Stack base

- Obligatorio:
  - Java 21.
  - Spring Boot 3.5.x.
  - Maven como sistema de construcción.
  - API REST sobre HTTP/HTTPS.
  - Validación con Jakarta Bean Validation.
  - Persistencia con Spring Data JPA o equivalente aprobado.
  - Documentación de API con OpenAPI.
- Recomendado:
  - Uso de MapStruct para mapeos de DTOs.
  - ProblemDetail o estándar equivalente para manejo homogéneo de errores.
  - @ConfigurationProperties para configuración tipada.

4.2. Organización del proyecto

- Obligatorio:
  - Organizar el backend, como mínimo, con paquetes o módulos equivalentes a:
    - controller
    - service
    - service.impl
    - repository
    - entity
    - dto
    - mapper
    - config
    - exception
    - validation
    - util
  - Usar domain cuando el modelo de negocio requiera encapsular reglas y comportamiento.
  - Mantener componentes técnicos transversales separados de los componentes funcionales.
- Prohibido:
  - Acceder a repository directamente desde controller.
  - Colocar lógica de negocio en clases de configuración, filtros o controladores.
  - Exponer entidades JPA como contrato externo.

4.3. Controladores

- Obligatorio:
  - Exponer endpoints coherentes con el contrato OpenAPI.
  - Validar entradas con @Valid y restricciones declarativas en DTOs.
  - Limitar el controlador a orquestación ligera, validación básica y delegación.
  - Devolver códigos HTTP consistentes con el resultado funcional y técnico.
- Recomendado:
  - Definir DTOs diferenciados para request y response cuando el caso lo requiera.
  - Anotar endpoints críticos con metadatos OpenAPI suficientes para consumidores y soporte.
- Prohibido:
  - Implementar reglas de negocio complejas en controladores.
  - Retornar entidades persistentes directamente al frontend.

4.4. Servicios y dominio

- Obligatorio:
  - Modelar los servicios como casos de uso o capacidades de negocio.
  - Separar interfaz e implementación cuando la solución lo amerite o cuando sea parte del estándar de arquitectura.
  - Declarar transaccionalidad de forma explícita en operaciones que modifican estado.
  - Ubicar la lógica de negocio en servicios o en dominio, no en repositorios.
- Recomendado:
  - Encapsular reglas complejas en objetos de dominio o servicios especializados.
  - Mantener servicios orquestadores delgados cuando exista un dominio más rico.
- Prohibido:
  - Convertir los servicios en simples wrappers de repositorio sin intención de negocio.

4.5. Persistencia

- Obligatorio:
  - Usar entidades JPA solo para representar el modelo persistente.
  - Limitar los repositorios a operaciones de acceso a datos.
  - Mantener spring.jpa.hibernate.ddl-auto=none en ambientes compartidos y productivos.
  - Trazar la compatibilidad entre versión del backend y versión mínima del esquema.
- Recomendado:
  - Ubicar consultas complejas en especificaciones, consultas tipadas o adaptadores claramente identificados.
- Prohibido:
  - Incrustar reglas de negocio, autorización o integración externa dentro del repositorio.
  - Confiar en generación automática del esquema como mecanismo de despliegue.

4.6. DTOs y mapeo

- Obligatorio:
  - Definir DTOs estables y orientados al contrato.
  - Mantener los mapeos fuera de controladores y repositorios.
  - Hacer explícitos los cambios de contrato entre versiones.
- Recomendado:
  - Usar MapStruct para mapeos repetitivos y tipados.
- Prohibido:

- Reutilizar un DTO para contextos incompatibles si eso degrada claridad o seguridad.

4.7. Validaciones

- Obligatorio:
  - Aplicar Bean Validation en entradas externas.
  - Centralizar validaciones reutilizables en un paquete o módulo de validación.
  - Diferenciar validaciones sintácticas, de negocio y de autorización.
- Recomendado:
  - Usar validadores especializados para reglas que requieran acceso a repositorios o servicios.
- Prohibido:
  - Persistir, modificar estado o disparar integraciones desde validadores.

4.8. Manejo de errores

- Obligatorio:
  - Centralizar la traducción de excepciones a respuestas HTTP.
  - Definir un contrato homogéneo para errores funcionales, de validación, seguridad e infraestructura.
  - Proporcionar mensajes útiles para soporte sin revelar datos sensibles.
- Recomendado:
  - Adoptar ProblemDetail como estándar base.
- Prohibido:
  - Retornar trazas, secretos, consultas SQL o mensajes internos al cliente final.

4.9. Seguridad backend

- Obligatorio:
  - Centralizar la configuración de seguridad en componentes dedicados.
  - Aplicar autenticación y autorización a nivel de endpoint y, cuando corresponda, a nivel de servicio o política de dominio.
  - Restringir endpoints operativos, de documentación y depuración según ambiente.
  - Configurar CORS por lista controlada de orígenes y nunca como apertura irrestricta en producción.
  - Considerar defensa en profundidad, aunque exista API Gateway o proveedor de identidad externo.
- Recomendado:
  - Encapsular la integración con proveedores de identidad y federación.
  - Versionar y documentar permisos, roles y reglas de autorización.
- Prohibido:
  - Confiar en cabeceras o tokens provenientes del perímetro sin validaciones mínimas esperadas.
  - Exponer /actuator, Swagger u otras superficies técnicas sin endurecimiento por ambiente.

4.10. Configuración y propiedades

- Obligatorio:
  - Externalizar la configuración por ambiente.
  - Modelar propiedades de aplicación mediante clases tipadas.
  - Separar parámetros públicos, parámetros internos y secretos.
  - Documentar cada variable requerida por la aplicación.
- Recomendado:
  - Utilizar .env.example o equivalente como guía, sin valores reales sensibles.
- Prohibido:
  - Versionar credenciales, tokens, secretos o certificados privados.

4.11. Calidad y pruebas backend

- Obligatorio:
  - Mantener pruebas unitarias e integración para flujos críticos.
  - Ejecutar validaciones de arquitectura automatizadas cuando se establezca una estructura por capas.
  - Incorporar pruebas de seguridad o integración para mecanismos de autenticación/autorización relevantes.
  - Garantizar que la construcción falle cuando fallen pruebas o reglas de calidad.
- Recomendado:
  - Usar ArchUnit para verificar dependencias permitidas entre capas.
  - Usar PIT en módulos críticos.
- Prohibido:
  - Desactivar permanentemente pruebas o reglas arquitectónicas para facilitar la entrega.

5. Lineamientos frontend

5.1. Stack base

- Obligatorio:
  - Angular 20.
  - TypeScript 5.9 en modo estricto.
  - Node.js 20+ y npm 10+ para desarrollo y CI.
  - Estructura SPA con componentes standalone, routing y servicios HTTP tipados.
- Recomendado:
  - Uso de Angular Testing Library para pruebas de comportamiento.

5.2. Estructura del proyecto

- Obligatorio:
  - Organizar la aplicación, como mínimo, en:
    - core
    - features
    - shared
    - environments
    - public
  - Ubicar en core toda capacidad transversal: configuración, guards, interceptores, servicios singleton, adaptadores, logging y utilidades técnicas.
  - Ubicar en features las capacidades funcionales desacopladas entre sí.
  - Ubicar en shared elementos reutilizables y libres de dependencia funcional específica.
- Recomendado:
  - Mantener aliases de paths consistentes para reducir imports frágiles.
- Prohibido:
  - Permitir que una feature dependa directamente de otra.
  - Colocar componentes o servicios de propósito global dentro de una feature.

5.3. Componentes y servicios

- Obligatorio:
  - Diseñar componentes con responsabilidades claras.
  - Mantener componentes de presentación desacoplados de detalles de infraestructura cuando sea viable.
  - Ubicar servicios transversales en core y servicios de caso de uso dentro de la feature correspondiente.
- Recomendado:

- Separar componentes contenedores y de presentación cuando la complejidad lo justifique.
- Prohibido:
  - Introducir lógica de integración HTTP o autenticación directamente en templates o componentes sin una capa de servicio.

5.4. Estado y flujo de datos

- Obligatorio:
  - Definir explícitamente la estrategia de manejo de estado.
  - Limitar el estado global a información realmente transversal.
  - Mantener el estado de pantalla o feature dentro de su contexto funcional.
- Recomendado:
  - Usar signals para estado local o de mediana complejidad.
  - Evaluar un store global solo cuando exista una necesidad transversal real.
- Prohibido:
  - Introducir múltiples patrones de estado sin criterio ni documentación.

5.5. Integración HTTP

- Obligatorio:
  - Centralizar el comportamiento común en interceptores.
  - Implementar clientes o servicios HTTP por dominio o feature.
  - Normalizar el manejo de errores de red y de backend.
  - Controlar timeouts, reintentos y degradación de experiencia según criticidad.
- Recomendado:
  - Implementar un interceptor de base URL y uno de normalización de errores.
- Prohibido:
  - Repetir lógica de headers, endpoints base o manejo de errores en cada componente.

5.6. Configuración runtime

- Obligatorio:
  - Cargar configuración pública no sensible mediante un servicio centralizado.
  - Permitir parametrizar endpoints, banderas de entorno y nivel de logging sin recompilar cuando el caso lo requiera.
  - Validar y normalizar la configuración recibida.
- Recomendado:
  - Implementar un patrón similar a ConfigService con inicialización controlada y fallbacks seguros.
- Prohibido:
  - Publicar secretos, tokens privados o credenciales en archivos JSON públicos o environment.*.

5.7. Seguridad frontend

- Obligatorio:
  - Tratar al frontend como cliente no confiable.
  - Proteger rutas mediante guards y flujos de sesión claramente definidos.
  - Encapsular integraciones con librerías externas de identidad o sesión.
  - Documentar el manejo de expiración de sesión, cierre de sesión y errores de autorización.
- Recomendado:
  - Minimizar persistencia local de tokens o datos sensibles.
- Prohibido:
  - Tomar decisiones definitivas de autorización exclusivamente en frontend.

5.8. UX técnica, accesibilidad y escalabilidad

- Obligatorio:

- Considerar accesibilidad mínima, navegación clara, manejo de estados vacíos y mensajes de error comprensibles.
- Diseñar la aplicación para crecimiento de features sin degradar la mantenibilidad.

- Recomendado:
  - Usar lazy loading cuando el tamaño de la solución lo amerite.
  - Formalizar lineamientos de componentes reutilizables y sistema visual.

5.9. Calidad y pruebas frontend

- Obligatorio:
  - Mantener pruebas unitarias y de integración para componentes, servicios e interceptores críticos.
  - Ejecutar lint, pruebas y build productivo en CI.
  - Conservar cobertura mínima global igual o superior al umbral institucional definido.
- Recomendado:
  - Mantener un umbral base de 80% cuando no exista una política distinta.
  - Incorporar pruebas de routing y autenticación para flujos principales.
- Prohibido:
  - Entregar features sin pruebas mínimas cuando afecten negocio, seguridad o configuración.

5.10. Linting, formateo y convenciones

- Obligatorio:
  - Aplicar Biome para revisión/formato general del código.
  - Aplicar ESLint sobre templates HTML.
  - Mantener scripts de lint, test y build funcionales desde línea de comandos.
  - Ejecutar hooks locales o equivalentes de calidad antes de la integración.
- Recomendado:
  - Mantener pre-commit y pre-push con verificaciones automáticas.

6. Lineamientos para base de datos y migraciones

6.1. Repositorio de base de datos

- Obligatorio:
  - Mantener un repositorio dedicado o una estructura claramente separada para la evolución del esquema.
  - Incluir, como mínimo:
    - migrations
    - seed
    - docs
  - Incluir rollback cuando la estrategia lo permita y sea segura.
  - Documentar motor objetivo, versión soportada y pre requisitos.
- Prohibido:
  - Operar cambios de esquema directamente en ambiente sin control de versiones, trazabilidad ni registro formal dentro del sistema de gestión de cambios.

6.2. Herramienta y estrategia de migraciones

- Obligatorio:
  - Usar herramienta de migración estandarizada, preferentemente Flyway o Liquibase.
  - Adoptar migraciones incrementales, inmutables y auditables.
  - Mantener una convención de nombres consistente, por ejemplo V001__descripcion.sql.
  - Crear una nueva migración para corregir o ampliar cambios ya ejecutados.
- Recomendado:

- Definir reglas claras para datos de referencia, catálogos y cargas iniciales.
- Prohibido:
  - Modificar migraciones ya aplicadas en ambientes compartidos.

6.3. Compatibilidad y despliegue

- Obligatorio:
  - Mantener trazabilidad entre versión de backend y versión mínima del esquema.
  - Validar migraciones en pipeline o procedimiento controlado antes del despliegue.
  - Documentar orden de ejecución y pre requisitos.
- Prohibido:
  - Desplegar backend sin confirmar compatibilidad con el esquema objetivo.

6.4. Datos sensibles y administración

- Obligatorio:
  - Mantener usuarios, contraseñas y parámetros de conexión fuera de scripts versionados.
  - Aplicar principios de mínimo privilegio.
  - Definir estrategia de respaldo, recuperación y protección de datos sensibles.

7. Lineamientos de seguridad transversal

7.1. Gestión de secretos

- Obligatorio:
  - Gestionar secretos mediante variables de entorno, gestores de secretos o mecanismos institucionales equivalentes.
  - Separar claramente secretos de configuraciones públicas.
- Prohibido:
  - Versionar secretos reales en repositorios.

7.2. Exposición técnica y endurecimiento

- Obligatorio:
  - Restringir por ambiente documentación técnica, endpoints operativos, paneles y herramientas auxiliares.
  - Definir listas de origen permitidas para CORS y políticas de publicación seguras.
  - Alinear headers, certificados y endurecimiento con la política de infraestructura institucional.

7.3. Trazabilidad y auditoría

- Obligatorio:
  - Registrar eventos técnicos y de seguridad relevantes.
  - Mantener trazabilidad de versiones y despliegues.
  - Definir auditoría funcional cuando la naturaleza del sistema o los datos lo requiera.

8. Configuración, entornos y parametrización

- Obligatorio:
  - Mantener configuración separada por ambiente.
  - Documentar todas las variables requeridas para levantar la solución.
  - Distinguir entre:
    - configuración pública,
    - configuración interna,
    - secretos,
    - parámetros de operación.
  - Asegurar que el frontend pueda consumir solo información pública.

- Asegurar que el backend exponga únicamente configuraciones públicas que hayan sido aprobadas para consumo externo.
- Recomendado:
  - Entregar archivos de ejemplo como .env.example, environment.example.ts o equivalentes.
- Prohibido:
  - Usar archivos locales no documentados como requisito implícito para construir o ejecutar la solución.

9. Calidad, pruebas y control de cambios

9.1. Reglas mínimas de calidad

- Obligatorio:
  - El código debe compilar y ejecutar pruebas de forma reproducible.
  - Toda contribución debe pasar revisiones automáticas de calidad antes de integrarse.
  - Los umbrales de cobertura, cuando existan, deben hacerse cumplir automáticamente.
  - Todo repositorio entregable deberá integrarse con SonarQube o una plataforma equivalente aprobada por la institución.
  - Ningún cambio podrá promoverse a ambientes compartidos si falla el Quality Gate establecido para código nuevo.

9.2. SonarQube y Quality Gate

- Obligatorio:
  - Ejecutar análisis de SonarQube en cada pipeline aplicable a backend, frontend y, cuando proceda, scripts o artefactos versionados de base de datos.
  - Configurar el análisis sobre New Code como criterio mínimo de aceptación técnica.
  - Publicar el resultado del análisis como evidencia del pipeline.
  - Tratar el Quality Gate como control bloqueante de integración y promoción.
- Quality Gate mínimo para código nuevo:
  - Security Hotspots Reviewed = 100%.
  - Coverage > 70%.
  - Duplicated Lines (%) <= 3%.
  - Maintainability Rating = A.
  - Reliability Rating = A.
  - Security Rating = A.
  - Blocker Issues = 0.
  - Bugs = 0.
  - Code Smells = 0.
  - Critical Issues = 0.
  - Major Issues = 0.
  - Vulnerabilities = 0.
- Recomendado:
  - Definir perfiles diferenciados por tipo de repositorio cuando la institución lo apruebe, manteniendo como base el gate anterior.
  - Monitorear tendencia de deuda técnica, cobertura, duplicidad y hotspots de seguridad además del resultado puntual del gate.
- Prohibido:
  - Ignorar resultados del Quality Gate como parte del proceso de aceptación.
  - Desactivar reglas para permitir una liberación sin aprobación formal.
  - Cerrar hallazgos sin evidencia técnica o sin justificación aprobada.

9.3. Estrategia de pruebas

- Obligatorio:
  - Definir estrategia de pruebas por tipo:
    - unitarias,
    - integración,
    - arquitectura,
    - seguridad,
    - regresión,
    - despliegue.
  - Cubrir al menos los flujos críticos, reglas de negocio clave, seguridad, configuración y errores relevantes.
- Recomendado:
  - Incorporar pruebas end-to-end para procesos principales cuando la criticidad lo justifique.

9.4. Control de cambios

- Obligatorio:
  - Mantener CHANGELOG.md o artefacto equivalente.
  - Usar versionamiento claro y trazable en backend, frontend y base de datos.
  - Registrar impacto de cambios que modifiquen contratos, seguridad, estructura o despliegue.
- Recomendado:
  - Adoptar una convención consistente de commits, idealmente basada en Conventional Commits.

10. CI/CD y despliegue

10.1. Pipeline mínimo obligatorio

- Backend:
  - test
  - verify
  - análisis SonarQube
  - package
- Frontend:
  - lint
  - test
  - análisis SonarQube
  - build
- Base de datos:
  - validación de migraciones,
  - análisis estático o validación equivalente cuando aplique,
  - empaquetado o publicación del artefacto correspondiente,
  - ejecución controlada en el ambiente objetivo.

10.2. Reglas de automatización

- Obligatorio:
  - Los pipelines deben ser reproducibles y no depender del estado local de un desarrollador.
  - Cualquier falla de lint, pruebas, seguridad o build debe bloquear la promoción del artefacto.
  - Cualquier falla del Quality Gate de SonarQube debe bloquear la integración y la promoción.
  - Deben generarse artefactos versionados y rastreables.
- Recomendado:

- Publicar evidencias de calidad, cobertura, resultado de SonarQube y resultados de pruebas como parte del pipeline.

11. Documentación obligatoria de entrega
El proveedor deberá entregar y mantener actualizados, como mínimo:

- README.md por repositorio.
- CHANGELOG.md por repositorio o componente.
- OpenAPI del backend.
- Modelo lógico de datos o documentación equivalente.
- Diagrama de arquitectura actualizado.
- Instrucciones de construcción local.
- Instrucciones de despliegue.
- Manual de configuración por ambiente.
- Inventario de variables y secretos referenciados.
- Evidencia de pruebas ejecutadas.
- Relación de decisiones de arquitectura y desviaciones aprobadas.

12. Criterios de aceptación para transferencia a la institución
Una entrega se considerará técnicamente aceptable cuando:

- El código sea construible, ejecutable y desplegable por un equipo distinto al proveedor.
- Existan repositorios completos, consistentes y con estructura gobernable.
- La arquitectura implementada coincida con el DABS o documente sus desviaciones.
- La configuración por ambiente esté documentada y separada de secretos.
- Las APIs, migraciones y versiones compatibles estén claramente trazadas.
- Existan pruebas suficientes para sostener el mantenimiento y evolución.
- Se entregue evidencia del cumplimiento del Quality Gate de SonarQube.
- La solución no dependa de conocimiento tácito no documentado.

13. Gobernanza de excepciones

- Cualquier excepción a este anexo deberá:
  - documentarse,
  - justificarse,
  - evaluarse por la ATDT ,
  - incluir impacto técnico,
  - incluir plan de mitigación,
  - incluir vigencia o criterio de retiro.
- Ninguna excepción debe asumirse como permanente por omisión.

Anexo 2

El flujo TO-BE del Fondo de Aportaciones a la Seguridad Pública (FASP), diseñado por la ATDT en coordinación con el SESNSP, puede ser consultado en el archivo “TO-BE Fondos Federales-Flujo general.pdf”