

**PLIEGO DE BASES Y CONDICIONES**

---

Convocante:

**Policia Nacional / Ministerio del Interior  
Policia Nacional**

Nombre de la Licitación:

**ADQUISICIÓN DE SERVICIOS DE INFORMÁTICA Y LICENCIAS  
SOFTWARE**  
(versión 1)

ID de Licitación:

**462484**



Modalidad:

**Subasta a la baja electrónica nacional**

Publicado el:

**21/10/2025**

*"Pliego para la Adquisición de Bienes y/o Servicios - SBE - Ley N° 7021/22."  
Versión 3*

## RESUMEN DEL LLAMADO

### Datos de la Convocatoria

ID de Licitación:	462484	Nombre de la Licitación:	ADQUISICIÓN DE SERVICIOS DE INFORMÁTICA Y LICENCIAS SOFTWARE
Convocante:	Policia Nacional / Ministerio del Interior	Categoría:	81000000 - Tecnologías de Informacion, Telecomunicaciones y Radiodifusiones
Unidad de Contratación:	Policia Nacional	Tipo de Procedimiento:	SBEN - Subasta a la baja electrónica nacional

### Etapas y Plazos

Lugar para Realizar Consultas:	Consulta Virtual a través del Sistema de Información de Contrataciones Públicas	Fecha Límite de Consultas:	27/10/2025 12:00
Lugar de Entrega de Ofertas:		Fecha de Presentación de Ofertas Electrónicas e Inicio de la Etapa Competitiva:	31/10/2025 08:00
Lugar de Apertura de Ofertas:		Fecha de Apertura de Ofertas Electrónicas:	03/11/2025 09:00

### Adjudicación y Contrato

Sistema de Adjudicación:	Lote	Anticipo:	20.0%
Vigencia del Contrato:	Los contratos abiertos definen su fecha de vigencia en el pliego		

### Datos del Contacto

Nombre:	IGNACIA BRITZ DE MORENO	Cargo:	Jefa Interina Departamento UOC
Teléfono:	0983862908	Correo Electrónico:	uoc.policia@gmail.com

## DATOS DE LA CONVOCATORIA

Los Datos de la Licitación constituye la información proporcionada por la convocante para establecer las condiciones a considerar del proceso particular, y que sirvan de base para la elaboración de las ofertas por parte de los potenciales oferentes.

### Datos de la Convocatoria

Los datos de la licitación serán consignados en esta sección y en el Sistema de Información de Contrataciones Públicas (SICP), los mismos forman parte de los documentos del presente procedimiento de contratación.

### Difusión de los documentos de la Convocatoria

Todos los datos y documentos de este procedimiento de contratación deben ser obtenidos directamente del Sistema de Información de Contrataciones Públicas (SICP). Es responsabilidad del oferente examinar todos los documentos y la información de la convocatoria que obren en el mismo.

### Contratación Pública Sostenibles - CPS

Las compras públicas juegan un papel fundamental en el desarrollo sostenible, así como en la promoción de estilos de vida sostenibles.

El Estado, por medio de las actividades de compra de bienes y servicios sostenibles, busca incentivar la generación de nuevos emprendimientos, modelos de negocios innovadores y el consumo sostenible. La introducción de criterios y especificaciones técnicas con consideraciones sociales, ambientales y económicas tiene como fin contribuir con el Desarrollo Sostenible en sus tres dimensiones.

El símbolo "CPS" en este pliego de bases y condiciones, es utilizado para indicar criterios o especificaciones sostenibles.

#### Criterios sociales y económicos:

- Los oferentes deberán garantizar la no contratación de menores, de conformidad a lo establecido en las normativas legales vigentes, conforme a lo indicado en el formulario de oferta.
- Los oferentes deberán cumplir con las disposiciones legales vigentes, garantizando a sus trabajadores condiciones de trabajo dignas y justas. Esto incluye el pago de salarios adecuados, el cumplimiento de cargas sociales, la provisión de uniformes y equipos de protección individual, la bonificación familiar cuando corresponda, el respeto a la jornada laboral y la aplicación de condiciones especiales para quienes desempeñan trabajos insalubres o peligrosos, así como la remuneración correspondiente por jornada nocturna, conforme a lo indicado en el formulario de oferta.
- Los oferentes adjudicados deberán adoptar medidas para la creación de empleo local y el uso de suministros locales, siempre y cuando exista viabilidad técnica y económica.

#### Criterios ambientales:

- El oferente adjudicado deberá cumplir con los lineamientos ambientales, incluidos en el ordenamiento jurídico o dictado por la institución.
- El oferente adjudicado deberá asegurar que todos los residuos generados por sus actividades sean adecuadamente gestionados (identificados, segregados y destinados) y buscar su minimización en la fuente, por medio de prácticas como la modificación de los procesos de producción, manutención y de las instalaciones utilizadas, además de la sustitución, conservación, reciclaje o reutilización de materiales.

#### Conducta empresarial responsable:

Los oferentes deberán observar los más altos niveles de integridad, así como altos estándares de conducta de negocios, ya sea durante el procedimiento de licitación o la ejecución de un contrato. En tal sentido, se comprometen a:

- Abstenerse de ofrecer, prometer, entregar o solicitar, de manera directa o indirecta, pagos ilícitos, a funcionarios públicos, con el fin de obtener o mantener un contrato, en todos los casos sea o no una ventaja ilegítima o indebida.
- Abstenerse de solicitar, recibir o aceptar ventajas indebidas de funcionarios públicos o de empleados de sus socios comerciales.
- Promover o fomentar políticas, programas o códigos de conducta orientados a la prevención de la corrupción, promoción de la integridad y fomento de la transparencia dentro de todas sus actividades, sean comerciales o no. Asimismo, podrá promover mecanismos de monitoreo y evaluación de cumplimiento de los mismos.
- Asegurar que todos los recursos destinados a la ejecución de un contrato público provengan de fuentes lícitas.
- Promover estándares de conducta responsable en sus propios proveedores, creando una cadena de suministro ética y sostenible.
- Garantizar que los fondos derivados de una licitación no serán utilizados para fines ilícitos.

### Aclaración de los documentos de la convocatoria

### 1. Consultas electrónicas

Todo potencial oferente que necesite alguna aclaración sobre la convocatoria o el pliego de bases y condiciones podrá solicitarla a la convocante a través del Sistema de Información de las Contrataciones Públicas (SICP) desde el día de la publicación de la convocatoria o de sus adendas, y hasta el plazo establecido por la convocante. Las consultas recibidas deberán ser respondidas y publicadas directamente a través del SICP.

### 2. Respuestas y aclaraciones

Las aclaraciones realizadas durante los procedimientos de contratación no serán consideradas modificaciones a las bases de la contratación. Sin embargo, a los efectos legales, la aclaración será considerada parte integrante del documento cuyo contenido aclare.

### 3. Adendas y prórrogas del tope para consultas.

Cuando la Convocante modifique especificaciones técnicas, criterios de evaluación u otros aspectos sustanciales del pliego de bases y condiciones, deberá prorrogar de manera obligatoria el tope para la realización de consultas, a fin de garantizar los plazos de difusión mínimos establecidos en la reglamentación de la DNCP.

### 4. Emisión de aclaraciones sobre Adendas

Cuando se prorrogue el plazo tope de consultas debido a una adenda modificatoria de las bases y condiciones, la convocante deberá analizar únicamente las consultas que se refieran al contenido de la adenda. En caso de recibir consultas relacionadas con lo establecido en las bases originalmente, la convocante no estará obligada a analizarlas, debiendo el oferente remitirse a las bases originales.

### 5. Junta de aclaraciones

La convocante podrá establecer una Junta de Aclaraciones para la evacuación de consultas sobre la convocatoria y los pliegos de bases y condiciones, de forma adicional a las consultas realizadas, debiendo fijar la fecha, hora y lugar de realización en el SICP.

La convocante podrá optar por responder las consultas en la Junta de Aclaraciones o diferirlas para responderlas conforme a los plazos de respuesta o emisión de adendas. En todos los casos, se deberá levantar un acta circunstanciada.

La inasistencia a la Junta de Aclaraciones no será motivo de descalificación de la oferta.

## Reserva de Información en respuestas y aclaraciones.

En las respuestas a las solicitudes de aclaración, los oferentes deberán indicar si la información suministrada es de carácter reservado, debiendo precisar la norma legal que la establece como secreta o de carácter reservado, de conformidad a lo estipulado en la Ley N° 5282/14 "DE LIBRE ACCESO CIUDADANO A LA INFORMACIÓN PÚBLICA Y TRANSPARENCIA GUBERNAMENTAL".

## Fraude y Corrupción

1. La convocante exige que los participantes en los procedimientos de contratación, observen los más altos niveles éticos, ya sea durante el proceso de licitación o de ejecución de un contrato. La convocante actuará frente a cualquier hecho o reclamación que se considere fraudulento o corrupto.

2. Si se comprueba que un funcionario público, o quien actúe en su lugar, y/o el oferente o adjudicatario propuesto en un proceso de contratación, hayan incurrido en prácticas fraudulentas o corruptas, la convocante deberá:

- (i) En la etapa de oferta, se descalificará cualquier oferta del oferente y/o rechazará cualquier propuesta de adjudicación relacionada con el proceso de adquisición o contratación de que se trate; y/o
- (ii) Durante la ejecución del contrato, se rescindirá el contrato por causa imputable al proveedor;
- (iii) Se remitirán los antecedentes del oferente o proveedor directamente involucrado en las prácticas fraudulentas o corruptivas, a la Dirección Nacional de Contrataciones Públicas, a los efectos de la aplicación de las sanciones previstas.
- (iv) Se presentará la denuncia ante las instancias correspondientes si el hecho conocido se encontrare tipificado en la legislación penal.

Fraude y corrupción comprenden actos como:

- (i) Ofrecer, dar, recibir o solicitar, directa o indirectamente, cualquier cosa de valor para influenciar las acciones de otra parte;
- (ii) Cualquier acto u omisión, incluyendo la tergiversación de hechos y circunstancias, que engañen, o intenten engañar, a alguna parte para obtener un beneficio económico o de otra naturaleza o para evadir una obligación;
- (iii) Perjudicar o causar daño, o amenazar con perjudicar o causar daño, directa o indirectamente, a cualquier parte o a sus bienes para influenciar las acciones de una parte;
- (iv) Colusión o acuerdo entre dos o más partes realizado con la intención de alcanzar un propósito inapropiado, incluyendo influenciar en forma inapropiada las acciones de otra parte.
- (v) Cualquier otro acto considerado como tal en la legislación vigente.

3. Los oferentes deberán declarar que por sí mismos o a través de interpósita persona, se abstendrán de adoptar conductas orientadas a que los funcionarios o empleados de la convocante induzcan o alteren las evaluaciones de las propuestas, el resultado del procedimiento u otros aspectos que les otorguen condiciones más ventajosas con relación a los demás participantes.

## Formato y firma de la oferta

1. El formulario de oferta será presentado a través del Módulo de ofertas electrónicas, firmado electrónicamente por el oferente o por las personas debidamente facultadas para firmar en nombre del oferente.
2. No serán descalificadas las ofertas que no hayan sido firmadas en documentos considerados no sustanciales.
3. Cuando la Garantía de Mantenimiento de Oferta sea instrumentada mediante una Declaración Jurada, la misma estará exenta del requerimiento de certificación de firma por Escribano Público y será presentado a través del Módulo de Oferta Electrónica junto con el formulario de oferta.

## Plazo para presentar las ofertas

Las ofertas electrónicas podrán ser cargadas y presentadas desde la publicación de la convocatoria hasta la fecha y hora límite de presentación de ofertas electrónicas e inicio de la etapa competitiva indicadas en el SICP.

La convocante podrá, extender el plazo originalmente establecido para la presentación de ofertas mediante la prórroga de fecha tope o la postergación de la presentación de ofertas electrónicas e inicio de la etapa competitiva.

En este caso todos los derechos y obligaciones de la convocante y de los oferentes previamente sujetos a la fecha límite original para presentar las ofertas, quedarán sujetos a la nueva fecha prevista. La oferta podrá ser modificada o retirada hasta antes de la fecha y hora límite de presentación de ofertas electrónicas e inicio de la etapa competitiva

## Oferentes en consorcio

Dos o más interesados podrán unirse temporalmente para presentar una oferta sin crear una persona jurídica distinta y deberán designar a uno de sus integrantes como líder quien suscribirá la oferta y los documentos relativos al procedimiento de contratación. La inscripción en el Registro de Proveedores del Estado por parte de todos los miembros del consorcio, constituye requisito previo para la presentación de las ofertas, los cuales deberán encontrarse activos en el Registro. Se deberá realizar el procedimiento de activación del consorcio directamente a través del Registro de Proveedores.

Para ello deberán presentar una escritura pública de constitución que reúna las características previstas en el Decreto reglamentario o un acuerdo de intención de participación en contrato de consorcio, el cual se deberá formalizar por escritura pública en caso de resultar adjudicados, antes de la firma del contrato.

Los integrantes de un consorcio no podrán presentar ofertas individuales ni conformar más de un consorcio para un mismo lote o ítem, lo que no impide que puedan presentarse en diferentes partidas de manera individual o como miembro de otro consorcio.

En todo lo demás deberán ajustarse a lo dispuesto en la normativa legal vigente.

## Idioma de la oferta

La oferta deberá ser presentada en idioma castellano.

La convocante permitirá con la oferta, la presentación de catálogos, anexos técnicos o folletos en idioma distinto al castellano y su traducción:

No Aplica

Cuando se admitiera la presentación de anexos técnicos y folletos en idioma distinto al español, su traducción deberá ser realizada por un traductor público matriculado en la República del Paraguay.

## Lista de Precios

1. Para la cotización el oferente deberá ajustarse a los requerimientos que se indican a continuación:

- a) En el caso del sistema de adjudicación por la totalidad de los bienes y/o servicios requeridos, el oferente deberá cotizar en la lista de precios todos los ítems, con sus precios unitarios y totales correspondientes.
- b) En el caso del sistema de adjudicación por lotes, el oferente cotizará en la lista de precios uno o más lotes, e indicará todos los ítems del lote ofertado con sus precios unitarios y totales correspondientes. En caso de no cotizar uno o más lotes, los lotes no cotizados no requieren ser incorporados al listado de ítems.
- c) En el caso del sistema de adjudicación por ítems, el oferente podrá ofertar por uno o más ítems, en cuyo caso deberá cotizar el precio unitario y total de cada uno o más ítems, los ítems no cotizados no requieren ser incorporados al listado de ítems.
- d) En todos los casos, independiente al sistema de adjudicación, el oferente deberá indicar el CPEN respectivo al ítem ofertado, en caso de contar. Dicho atributo tendrá carácter formal siendo susceptible de aclaraciones por parte del comité de evaluación.

2. En caso de que se establezca en las bases de la contratación, los precios indicados en el listado de precios serán consignados separadamente de la siguiente manera:

- a) El precio de bienes y/o servicios cotizados, incluidos todos los derechos de aduana, los impuestos al valor agregado o de otro tipo pagados o por pagar sobre los componentes y materia prima utilizada en la fabricación o ensamblaje de los bienes;

b) Todo impuesto al valor agregado u otro tipo de impuesto que obligue a la República del Paraguay a pagar sobre los bienes en caso de ser adjudicado el contrato; además, se deberá indicar los ítems exentos de IVA, cuando los hubiere y;

c) El precio de otros servicios conexos (incluyendo su impuesto al valor agregado), si los hubiere, enumerados en los datos de la licitación.

3. En caso de indicarse en el SICP, que se utilizará el atributo de contrato abierto, cuando se realice por montos mínimos y máximos deberán indicarse el precio unitario de los bienes y/o servicios ofertados; y en caso de realizarse por cantidades mínimas y máximas, deberán cotizarse los precios unitarios y los totales se calcularán multiplicado los precios unitarios por la cantidad máxima correspondiente.

4. El precio del contrato que perciba el proveedor por los bienes y/o servicios suministrados en virtud del contrato no podrá ser diferente a los precios unitarios cotizados en su oferta, excepto por cualquier ajuste previsto en el mismo.

5. En caso que se requiera el desglose de los componentes de los precios será con el propósito de facilitar a la convocante la comparación de las ofertas.

6. Una vez generada el Acta de Sesión Pública Virtual, el oferente, toda vez que haya realizado lances durante la etapa competitiva, deberá ajustar su listado de ítems al precio final de la competencia electrónica, a través del módulo de ofertas electrónicas, debiendo confirmar el precio ajustado de la oferta, hasta la fecha y hora prevista para el acto de apertura de ofertas electrónicas, para el efecto el SICP habilitará únicamente la modificación del precio unitario, los demás campos del ítem se mantendrán invariables.

7. En las contrataciones internacionales los oferentes no domiciliados en el territorio de la República deberán manifestar en su oferta que los precios que presentan en su propuesta económica no se cotizan en condiciones de prácticas desleales de comercio internacional en su modalidad de discriminación de precios o subsidios.

## Abastecimiento simultáneo

En caso de que se opte por el sistema de abastecimiento simultaneo, en éste apartado se deberá indicar la manera de distribución de los mismos:

No Aplica

## Moneda de la oferta y pago

La moneda de la oferta y pago será

En guaraníes para todos los oferentes

La cotización en moneda diferente de la indicada en este apartado será causal de rechazo de la oferta. Si la oferta seleccionada es en guaraníes, la oferta se deberá expresar en números enteros, no se aceptarán cotizaciones en décimos y céntimos.

## Documentos de la oferta

El pliego, sus adendas y aclaraciones no forman parte de la oferta, por lo que no se exigirá la presentación de copias de los mismos con la oferta.

### 1. Constancia de perfil del proveedor.

No se admitirá la presentación de la constancia de perfil del proveedor. El proveedor deberá proceder a la vinculación de los documentos del Registro de Proveedores del Estado a través del Módulo de Ofertas Electrónicas, según lo dispuesto en las disposiciones vigentes.

### 2. Confidencialidad de documentos.

Los oferentes deberán indicar en su oferta, qué documentos que forman parte de la misma son de carácter reservado e invocar la norma que ampara dicha reserva, para así dar cumplimiento a lo estipulado en la Ley N° 5282/14 "DE LIBRE ACCESO CIUDADANO A LA INFORMACIÓN PÚBLICA Y TRANSPARENCIA GUBERNAMENTAL". Si el oferente no hace pronunciamiento expreso amparado en la Ley, se entenderá que toda su oferta y documentación es pública.

## Periodo de validez de las ofertas

Las ofertas deberán mantenerse válidas por:

60

días corridos.

Las ofertas se deberán mantener válidas por el periodo indicado en el presente apartado, a partir de la fecha límite para la presentación de ofertas, establecido por la convocante. Toda oferta con un periodo menor será rechazada.

La convocante en circunstancias excepcionales podrá solicitar, por escrito, al oferente que extienda el periodo de validez de la oferta, por lo tanto la Garantía de Mantenimiento de la Oferta deberá ser también prorrogada.

El oferente puede rehusarse a tal solicitud sin que se le haga efectiva su Garantía de Mantenimiento de Oferta. A los oferentes que acepten la solicitud de prórroga no se les solicitará ni permitirá que modifiquen sus ofertas.

## Garantías: instrumentación, plazos y ejecución

### 1. Instrumentación y porcentaje

1.1 La Garantía de Mantenimiento de Oferta deberá expedirse por el equivalente 5% (cinco por ciento) del monto total de la oferta. El oferente debe adoptar cualquiera de las siguientes formas:

- Garantía bancaria emitida por un banco establecido en la República del Paraguay, la que deberá ajustarse a las condiciones establecidas por la DNCP.
- Póliza de seguros emitida por una compañía autorizada a operar y emitir pólizas de seguros de caución en la República del Paraguay. La póliza deberá ajustarse a las condiciones establecidas por la DNCP.
- En las SBE inferiores a los dos mil (2.000) jornales mínimos, se admitirá la instrumentación de las garantías de mantenimiento de ofertas a través de Declaraciones juradas, que será presentada directamente a través del módulo de ofertas electrónicas, junto al formulario de oferta, suscripta electrónicamente. La garantía instrumentada mediante declaración jurada estará exenta del requerimiento de certificación de firmas.

1.2 En los casos de contratos abiertos las garantías se registrarán por lo dispuesto en el Decreto Reglamentario y la reglamentación emitida por la DNCP para el efecto.

1.3 En caso de instrumentarse las garantías a través de Garantía Bancaria, deberá estar sustancialmente de acuerdo con el formulario incluido en la Sección "Formularios".

### 2. Garantía de mantenimiento de ofertas en consorcios

2.1. En caso de consorcios, la garantía de mantenimiento de ofertas deberá ser presentada de la siguiente manera:

- Consortio constituido por escritura pública: deberán emitir a nombre del consorcio legalmente constituido por escritura pública o del gestor y representante del consorcio (Empresa líder), designado en la escritura pública.
- Consortio con acuerdo de intención de participación en contrato de consorcio: deberán emitir a nombre del gestor y representante del consorcio (empresa líder), designado en el acuerdo.

### 3. Ejecución de la Garantía de mantenimiento de ofertas

3.1. La Garantía de Mantenimiento de Ofertas podrá ser ejecutada:

- La garantía de mantenimiento de ofertas será ejecutada y los antecedentes del caso serán remitidos a la DNCP, cuando un oferente susceptible de ser adjudicado, hubiere realizado lances y no hubiera confirmado el precio ajustado de la oferta, de acuerdo al acta de sesión pública virtual.
- Si el oferente altera las condiciones de su oferta,
- Si el oferente retira su oferta durante el periodo de validez de ofertas,
- Si no acepta la corrección aritmética del precio de su oferta, en caso de existir, o
- Si el adjudicatario no procede, por causa imputable al mismo a:
  - Firmar el contrato,
  - Suministrar los documentos indicados en las bases de la contratación para la firma del contrato,
  - Suministrar en tiempo y forma la garantía de cumplimiento de contrato,
  - Cuando se comprare que las declaraciones juradas presentadas por el oferente adjudicado con su oferta sean falsas,
  - No se formaliza el consorcio por escritura pública antes de la firma del contrato.

4. En caso de configuración de Siniestro, la convocante deberá solicitar la ejecución de la garantía. El proceso de ejecución será según el tipo de garantía que haya sido suministrada.

## Período de Validez de la Garantía de Mantenimiento de Oferta

El plazo de validez de la Garantía de Mantenimiento de Oferta será de:

90

días corridos

El oferente deberá presentar como parte de su oferta una Garantía de Mantenimiento de acuerdo al porcentaje indicado para ello en el SICP y por el plazo indicado en este apartado.

En el caso de que la competencia se desarrolle por más de un día, la garantía de mantenimiento de oferta deberá cubrir a partir del primer día del inicio de la etapa competitiva.

## Subcontratación

El porcentaje permitido para la subcontratación será de:

No Aplica

El oferente podrá indicar junto con la oferta las personas a ser subcontratadas, o, en la etapa contractual previa a la autorización por parte de la contratante. El formulario de personas a subcontratar/subcontratadas, deberá ser presentado de acuerdo a la etapa en la que se indique la subcontratación, siendo susceptible de evaluación respecto a las inhabilidades del Art 21 de la Ley N° 7021/22.

### Método de presentación

La carga y presentación de ofertas electrónicas se regirán por las disposiciones emitidas por la DNCP. Las ofertas electrónicas podrán ser cargadas y presentadas desde la publicación de la convocatoria hasta la fecha y hora límite de presentación de ofertas electrónicas e inicio de la etapa competitiva indicadas en el SICP.

En SBE no se admitirá el método de presentación de ofertas en doble sobre

### Retiro, sustitución y modificación de las ofertas electrónicas

Un oferente podrá retirar, sustituir o modificar su oferta presentada, hasta antes de la fecha límite de presentación e inicio de etapa competitiva, para ello deberá sujetarse a la reglamentación pertinente.

### Ajuste de Precios de Oferta Electrónica

El ajuste de precios se formaliza con la confirmación del precio ajustado de la oferta de acuerdo al acta de sesión pública virtual, constituyéndose el mismo una condición sustancial, caso contrario la oferta será rechazada.

### Apertura de ofertas

Culminada la etapa de ajustes de precios de la oferta electrónica, se procederá a la apertura de las ofertas electrónicas, en el día y hora fijados en el SICP de conformidad a las disposiciones establecidas en la normativa vigente. La apertura de ofertas electrónicas podrá establecerse desde el día siguiente hábil al cierre de la etapa de competitiva y hasta tres (03) días hábiles posteriores al mismo.

### Postergación de Presentación o Suspensión de la Etapa Competitiva

**1. Postergación de la presentación de ofertas electrónicas:** Las convocantes podrán postergar la fecha de presentación de ofertas electrónicas e inicio de la etapa competitiva, hasta en dos (02) oportunidades, cuando llegada la fecha límite fijada para la presentación de ofertas e inicio de etapa competitiva no se hayan presentado oferta alguna.

**2. Suspensión de la etapa competitiva:** La DNCP podrá disponer la suspensión de la etapa competitiva por motivos de fuerza mayor, con el fin de salvaguardar la prosecución del procedimiento. A dicho efecto, se procederá a la suspensión de la competencia y se publicará un aviso en el SICP con la información pertinente. La etapa competitiva será reanudada en el plazo que resulte conveniente para el desarrollo de la Subasta, con el grupo que no haya finalizado. Los demás plazos de la competencia serán prorrogados proporcionalmente, las nuevas fechas serán difundidas mediante un aviso en el SICP, de lo cual quedará constancia en el Acta de Sesión Pública Virtual

### Visita al sitio de ejecución del contrato

La convocante dispone la realización de una visita al sitio con las siguientes indicaciones:

No Aplica



### 1. Difusión de la visita

La visita o inspección técnica deberá fijarse de forma previa a la fecha tope de consulta, previendo como mínimo el plazo de difusión de (02) dos días hábiles. En todos los casos, el procedimiento para su realización deberá difundirse en las bases de la contratación.

Cuando la convocante haya establecido la visita o inspección técnica, en las bases de la contratación, el oferente que conozca el sitio podrá declarar bajo fe de juramento conocer el sitio y que cuenta con la información suficiente para preparar la oferta y ejecutar el contrato.

Cuando por la naturaleza o complejidad de la contratación sea imprescindible la realización de la visita técnica, la convocante podrá establecer la obligatoriedad de dicha visita a través del SICP. En estos casos no se aceptará la presentación de la declaración jurada.

### 2. Desarrollo de la visita.

Se registrará en acta los asistentes, la fecha, lugar, hora de realización y funcionarios participantes. Los representantes de los oferentes que asistan a la visita podrán contar con una autorización, bastando para ello la presentación de una nota del oferente. La falta de presentación de esta autorización no impide su participación en la visita o inspección técnica.

Los gastos relacionados con dicha visita correrán por cuenta del oferente.

## Incoterms

La edición de incoterms para esta licitación será:

No Aplica

Las expresiones DDP, CIP, FCA, CPT y otros términos afines, se regirán por las normas prescriptas en la edición vigente de los Incoterms publicada por la Cámara de Comercio Internacional.

Durante la ejecución contractual, el significado de cualquier término comercial, así como los derechos y obligaciones de las partes serán los prescritos en los Incoterms, a menos que sea inconsistente con alguna disposición del Contrato.

## Autorización del Fabricante

Los ítems a los cuales se le requerirá Autorización del Fabricante son los indicados a continuación:

SI APLICA

Cuando la convocante lo requiera, el oferente deberá acreditarse la cadena de autorizaciones, hasta el fabricante, productor o prestador de servicios.

La autorización deberá ser presentada en idioma castellano o en su defecto acompañada de su traducción oficial, realizada por un traductor público matriculado en la República del Paraguay. Así también cada autorización debe indicar a que ítem corresponde.

## Muestras

Se requerirá la presentación de muestras de los siguientes ítems y en las siguientes condiciones:

No Aplica

En caso de ser solicitadas, las muestras serán consideradas requisito indispensable para la evaluación de la oferta y deberán ser presentadas junto con la oferta, o bien en el momento y plazo fijado por la convocante en este apartado. La falta de presentación en la forma y plazo establecido por la convocante será causal de descalificación de la oferta.

## Tiempo de funcionamiento de los bienes

El periodo de tiempo estimado de funcionamiento de los bienes, para los efectos de repuestos será de:

No Aplica

## Plazo de reposición de bienes

El plazo de reposición de bienes para reparar o reemplazar será de:

3 (tres) días hábiles, contados a partir de la comunicación del rechazo

El proveedor garantiza que todos los bienes suministrados están libres de defectos derivados de actos y omisiones que este hubiera incurrido, o derivados del diseño, materiales o manufactura, durante el uso normal de los bienes en las condiciones que imperen en la República del Paraguay.

1. La Contratante comunicará al proveedor la naturaleza de los defectos y proporcionará toda evidencia disponible, inmediatamente después de haberlos descubierto. La contratante otorgará al proveedor facilidades razonables para inspeccionar tales defectos.

Tan pronto reciba ésta comunicación, y dentro del plazo establecido en este apartado, deberá reparar o reemplazar los bienes defectuosos, o sus partes sin ningún costo para la contratante.

2. Si el proveedor después de haber sido notificado, no cumple dentro del plazo establecido, la contratante, procederá a tomar medidas necesarias para remediar la situación, por cuenta y riesgo del proveedor y sin perjuicio de otros derechos que la contratante pueda ejercer contra el proveedor en virtud del contrato.

## Periodo de validez de la Garantía de los bienes

El plazo de validez de la Garantía de los bienes será el siguiente:

Para el Lote 1: Se requiere una garantía de buen funcionamiento del software por el tiempo que dure la suscripción  
Para los Lotes 2, 3, 4, 5 y 6 se requiere una garantía de buen funcionamiento del software por al menos 24 meses luego de la implementación total.

## Cobertura de Seguro de los bienes

La cobertura de seguro requerida a los bienes será:

No Aplica

A menos que se disponga otra cosa en este apartado, los bienes suministrados deberán estar completamente asegurados en guaraníes, contra riesgo de extravío o daños incidentales ocurridos durante la fabricación, adquisición, transporte, almacenamiento y entrega, de acuerdo a los incoterms aplicables.

# REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN

Esta sección contiene los criterios que la convocante utilizará para evaluar la oferta y determinar si un oferente cuenta con las calificaciones requeridas. Ningún otro factor, método o criterio será utilizado.

## Condición de Participación

Podrán participar de este procedimiento, las personas físicas, jurídicas y/o Consorcio, constituidos o con acuerdo de intención, inscriptos en el Registro de Proveedores del Estado.

Los oferentes domiciliados en la República del Paraguay, que pretendan participar en un procedimiento de contratación, no deberán estar comprendidos en las prohibiciones o limitaciones para presentar propuestas y contratar con el Estado, establecidas en el artículo 21 de la Ley N° 7021/22 "DE SUMINISTROS Y CONTRATACIONES PUBLICAS".

## Sucursales

En los casos de procedimientos de contratación de carácter nacional podrán participar las sucursales de las matrices internacionales constituidas en la República del Paraguay. Solo serán admitidas como criterios de adjudicación las capacidades, experiencia y aptitudes de la sucursal recabadas desde su constitución, sin admitirse la utilización de las cualidades de la casa matriz u otras filiales o sucursales.

## Conflicto de Interés

**1. Deber de Abstención del funcionario ante un posible conflicto de interés.** El funcionario público que participe en el procedimiento de contratación deberá abstenerse de intervenir, de manera directa o indirecta, en los asuntos en los que su actuación esté comprendida en alguno de los supuestos del artículo 17 de la Ley N° 7021/22. A tales efectos, deberá comunicar a su superior jerárquico o a la máxima autoridad institucional que se encuentra inmerso en uno de los supuestos legales, detallando la situación particular. En caso que corresponda, el superior jerárquico o la máxima autoridad institucional tendrá por aceptada la abstención apartando al funcionario y, de ser necesario, designará al sustituto. Se deberá dejar constancia por escrito de todo lo actuado.

**2. Apartamiento del funcionario por la Entidad Convocante.** Enterada la Convocante de que existe un conflicto de interés respecto a un funcionario público que ha sido designado o requerido para intervenir o que interviene en alguna de las etapas de la fase de contratación del suministro público, y no mediando la abstención expresa del funcionario, deberá apartarlo del asunto particular, detallando la situación que configura el conflicto de interés. La Convocante deberá dejar constancia por escrito de todo lo actuado. Se procederá a la designación del sustituto, en los casos que correspondiere.

**3. Actuaciones tras la detección de un conflicto de interés.** Si la Entidad Convocante detectare que un funcionario público comprendido en alguno de los supuestos del artículo 17 de la Ley N° 7021/22 tuvo intervención en alguna de las etapas de la fase de contratación del suministro público, adoptará las medidas que correspondan. La Convocante podrá subsanar las actuaciones en sede administrativa o revocarlas, según corresponda. Deberá dejarse constancia por escrito de todo lo actuado y comunicarse a la DNCP. La DNCP podrá, de oficio o por denuncia fundada, realizar las investigaciones que resulten pertinentes, a fin de verificar presuntos hechos que podrían constituir conflicto de intereses y/o irregularidades en contravención con el artículo 17 de la Ley N° 7021/22, conforme las atribuciones conferidas en el artículo 132 de la Ley.

**4. Declaración jurada de conocimiento de la existencia de un conflicto de intereses respecto a los funcionarios públicos intervinientes en el procedimiento.** La convocante deberá verificar la "Declaración jurada de conocimiento de la existencia de un conflicto de intereses respecto a los funcionarios públicos intervinientes en el procedimiento" presentada por el oferente al momento de la oferta en cumplimiento de su obligación de comunicar o denunciar la existencia de posibles conflictos de intereses, de conformidad al artículo 17 de la Ley 7021/22. De comprobarse la omisión, falsedad o inexactitud de la información proporcionada y declarada en la Declaración la Convocante analizará si se configura un conflicto de interés en los términos del artículo 17 de la Ley 7021/22 y emitirá las directrices que correspondan acorde a la etapa del procedimiento de contratación. Además, la Convocante podrá resolver la descalificación de la oferta y/o rescisión del contrato respectivo.

## Confidencialidad de la etapa de evaluación de ofertas.

No deberá darse a conocer información alguna acerca del análisis, aclaración y evaluación de las ofertas, mientras dure el mismo de conformidad con el artículo N° 52 de la Ley N° 7021/22 "De Suministro y Contrataciones Públicas", ni sobre las recomendaciones relativas a la adjudicación, después de la apertura en público de las ofertas, a los oferentes ni a personas no involucradas en el proceso de evaluación, hasta que haya sido dictada la resolución de adjudicación cuando se trate de un solo sobre. Cuando se trate de dos sobres, la confidencialidad de la primera etapa será hasta la emisión del acto administrativo de selección de ofertas técnicas, reanudándose la confidencialidad después de la apertura en público de las ofertas económicas hasta la emisión de la resolución de adjudicación.

## Requisitos de Calificación

**Calificación Legal.** Los oferentes deberán declarar que no se encuentran comprendidos en las limitaciones o prohibiciones para contratar con el Estado, según lo establecido en el artículo 21 de la Ley N° 7021/22. Esta declaración forma parte del formulario de oferta.

Serán rechazadas las ofertas de los oferentes que se encuentren comprendidos en las prohibiciones o limitaciones para presentar propuesta y contratar con el Estado, a la hora y fecha límite de presentación de ofertas o a la fecha de firma del contrato.

A los efectos de la verificación de la existencia de prohibiciones o limitaciones contenidas en el artículo 21 de la Ley N° 7021/22, el comité de evaluación realizará el siguiente análisis:

1° Verificará que el oferente haya proporcionado el formulario de ofertas, el cual comprende la declaración jurada de no estar comprendido en las prohibiciones y limitaciones para presentar propuesta y contratar.

2° Además, deberá verificar la presentación de la declaración jurada de conocimiento de la existencia de un conflicto de intereses respecto a los funcionarios públicos intervinientes en el procedimiento, y de las constancias de registro de estructura jurídica y de beneficiarios finales, a fin de verificar que los oferentes no se encuentren incurso en las causales previstas en el Art 21 de la Ley N° 7021/22.

3° Verificará por los medios disponibles, si el oferente y los demás sujetos individualizados en las prohibiciones o limitaciones contenidas en los incisos d) y e) del artículo 21 de la Ley, aparecen en la base de datos del SINARH del VICE MINISTERIO DE CAPITAL HUMANO Y GESTION ORGANIZACIONAL.

4° Si se constata que alguna de las personas mencionadas en el párrafo anterior figura en la base de datos del SINARH del VICE MINISTERIO DE CAPITAL HUMANO Y GESTION ORGANIZACIONAL, el comité analizará acabadamente si tal situación le impedirá contratar con el Estado, exponiendo los motivos para aceptar o rechazar la oferta, según sea el caso.

5° Verificará que el oferente haya proporcionado el formulario de Declaración de Personas, debidamente firmado, en el Registro de Proveedores del Estado, conforme a los estándares establecidos, y cotejará los datos con las personas físicas inhabilitadas que constan en el registro de “Sanciones a Proveedores” del SICP. Con el objeto de verificar si los directores, gerentes, socios gerentes, quienes ejerzan la administración, accionistas, cuotapartistas o propietarios se encuentren dentro de los criterios contemplados en los incisos h), i), y j) de la Ley 7021/22, además la convocante se encuentra facultada de solicitar informes internos institucionales para el cotejo de la información con respecto a los incisos mencionados. La declaración jurada deberá contar con información vigente al momento de la presentación de las ofertas y el oferente será responsable de la actualización del documento que obre en el registro de proveedores del Estado. En caso de que el oferente no cuente con dicho Formulario en su registro, la Convocante procederá a solicitarlo durante la etapa de evaluación de ofertas. Si el oferente no responde el pedido o no remite el citado Formulario, se procederá al rechazo de la oferta.

6° El comité podrá recurrir a fuentes públicas o privadas de información, para verificar los datos proporcionados por el oferente y las obrantes en el registro de sancionados de la DNCP.

7° El comité verificará en fuentes públicas de información de libre acceso, si el oferente o sus integrantes, se encuentran en los demás supuestos contenidos en el artículo 21 de la Ley N° 7021/22, pudiendo utilizar como guía instructiva el documento aprobado por la DNCP. En caso de requerirse, el comité podrá solicitar aclaración al oferente sobre la vigencia de la información obrante en las fuentes respectivas.

8° En caso de que aplique la subcontratación y que el oferente haya presentado el formulario de personas a subcontratar/subcontratadas junto con la oferta, el Comité de Evaluación de Ofertas deberá evaluar el contenido del formulario a los efectos de constatar que el subcontratista no se encuentra comprendido en alguna de las causales de prohibición previstas en el Art. 21 de la Ley N° 7021/22, pudieron requerir al oferente la información que sea necesaria.

Si el Comité confirma que el oferente o sus integrantes poseen impedimentos en virtud a lo dispuesto en el artículo 21 de la Ley N° 7021/22, la oferta será rechazada y se remitirán los antecedentes a la DNCP para los fines pertinentes.

## Método de Evaluación

El método de evaluación del presente procedimiento de contratación será basado únicamente en precio.

## Análisis de los precios ofertados

**Para evaluación de ofertas con el criterio basado únicamente en precio.**

Luego de haber realizado la corrección de errores aritméticos y de ordenar las ofertas presentadas de menor a mayor, el Comité de Evaluación procederá a solicitar a los oferentes una explicación detallada de la composición del precio ofertado de cada ítem, rubro o partida adjudicable, conforme al siguiente parámetro:

En contrataciones en general: cuando la diferencia entre el precio ofertado y el precio referencial sea 25% por debajo del precio referencial y 15% por encima del referencial establecido por la convocante y difundido con el llamado a contratación.

Si el oferente no respondiese la solicitud, o la respuesta no sea suficiente para justificar el precio ofertado del bien o servicio, el precio será declarado inaceptable y la oferta rechazada.

El análisis de los precios, con esta metodología, será aplicado a cada ítem, rubro o partida que componga la oferta y en cada caso deberá ser debidamente fundada la decisión adoptada por la Convocante en el ejercicio de su facultad discrecional.

## Composición de Precios

La estructura mínima del desglose de composición de los precios, será:

Contar mínimamente de: costo del bien/servicio, gastos administrativos y financieros y otros, cargas laborales, rentabilidad, cargas impositivas y el precio final.

El oferente podrá presentar junto con su oferta el desglose de composición de precios, cuando su oferta se encuentre fuera de los parámetros establecidos en la cláusula anterior.

Cuando la Convocante requiera el desglose con el propósito de facilitar el análisis y comparación de las ofertas, el oferente deberá ajustarse a la estructura mínima establecida y, en caso de considerarlo pertinente, podrá complementarla e incluir una explicación detallada o parámetros que permitan aclarar aspectos puntuales de su composición y/o sustentar la razonabilidad de sus precios.

## Certificado de Producto y Empleo Nacional - CPS

**a) Oferentes.** A los efectos de acogerse al beneficio de la aplicación del margen de preferencia, el oferente deberá contar con el Certificado de Producto y Empleo Nacional (CPEN). El certificado debe ser emitido como máximo a la fecha y hora tope de presentación de ofertas. La falta del CPEN no será motivo de descalificación de la oferta, sin embargo, el oferente no podrá acogerse al beneficio.

El comité de evaluación verificará en el portal oficial indicado por el Ministerio de Industria y Comercio (MIC) la emisión en tiempo y forma del CPEN declarado por los oferentes. No será necesaria la presentación física del Certificado de Producto y Empleo Nacional.

Independientemente al sistema de adjudicación, el margen de preferencia será aplicado a cada bien o servicio objeto de contratación que se encuentre indicado en la planilla de precios.

### b) Oferentes en Consorcio:

b.1. Provisión de Bienes. El CPEN debe ser expedido a nombre del oferente que fabrique o produzca los bienes objeto de la contratación. En el caso que ninguno de los oferentes consorciados fabrique o produzca los bienes ofrecidos, el consorcio deberá contar con el CPEN correspondiente al bien ofertado, debiendo encontrarse debidamente autorizado por el fabricante. Esta autorización podrá ser emitida a nombre del consorcio o de cualquiera de los integrantes del mismo.

b.2. Provisión de Servicios. (se entenderá por el término "servicio" aquello que comprende a los servicios en general, las consultorías, obras públicas y servicios relacionados a obras públicas).

Todos los integrantes del consorcio deben contar con el CPEN.

Excepcionalmente se admitirá que no todos los integrantes del consorcio cuenten con el CPEN para aplicar el margen de preferencia, cuando el servicio específico se encuentre detallado en uno de los ítems de la planilla de precios, y de los documentos del consorcio (acuerdo de intención o consorcio constituido) se desprenda que el integrante del consorcio que cuenta con el CPEN será el responsable de ejecutar el servicio licitado

## Margen de preferencia en procedimientos de contratación de carácter internacional

En los procedimientos de contratación de carácter internacional, las convocantes otorgarán el beneficio de margen de preferencia del 10% (diez por ciento), a las ofertas que incorporen:

1 - El empleo de los recursos humanos del país.

2 - La adquisición y locación de bienes producidos en la República del Paraguay.

Para el otorgamiento del beneficio, los Oferentes deberán acreditar como mínimo el porcentaje de contenido nacional establecido en la reglamentación vigente en la materia.

El oferente podrá acogerse al beneficio del margen de preferencia con la obtención del CPEN, o en su defecto, aquél que disponga el MIC.

## Requisitos documentales para evaluación de las condiciones de participación

### Requisitos documentales para evaluación de las condiciones de participación

<b>1. Formulario de Oferta (*)</b> <i>[El formulario de oferta, deberá ser generado en el módulo de oferta electrónica y se considerará que el listado de ítems forma parte del formulario de oferta electrónica, y deberá sujetarse en todo lo demás a la reglamentación vigente.]</i>
<b>2. Garantía de Mantenimiento de Oferta (*)</b> <i>[La garantía de mantenimiento de oferta debe ser extendida, bajo la forma establecida en el SICP.]</i>
<b>3. Certificado de Cumplimiento con la Seguridad Social (**)</b>
<b>4. Declaración jurada de conocimiento de la existencia de un conflicto de intereses respecto a los funcionarios públicos intervinientes en el procedimiento. (**)</b>

5. Certificado de Producto y Empleo Nacional emitido por el MIC, en formato físico, solo en caso de imposibilidad de certificación electrónica. (**)
6. Certificado de Cumplimiento Tributario. (**)
7. Patente comercial del municipio en donde esté asentado el establecimiento del oferente. (**)
8. Declaración Jurada de "Declaración de Personas", de conformidad con el formulario estándar – Sección Formularios, cuando no se encuentre en el Registro de Proveedores (**)
<b>9. Documentos legales. Oferentes</b>
<b>9.1. Personas Físicas.</b>
a. Fotocopia simple de la Cédula de Identidad del firmante de la oferta. (*)
b. Constancia de inscripción en el Registro Único de Contribuyentes – RUC (*)
c. En el caso que suscriba la oferta otra persona en su representación, deberá acompañar una fotocopia simple de su cédula de identidad y una fotocopia simple del poder suficiente otorgado por Escritura Pública para presentar la oferta y representarlo en los actos de la licitación. No es necesario que el poder esté inscripto en el Registro de Poderes. (*)
<b>9.2. Personas Jurídicas.</b>
a. Fotocopia simple de los documentos que acrediten la existencia legal de la persona jurídica tales como la Escritura Pública de Constitución, según el tipo de sociedad y protocolización de los Estatutos Sociales. Los estatutos deberán estar inscriptos en la Sección Personas Jurídicas de la Dirección de Registros Públicos. (*)
b. Constancia de inscripción en el Registro Único de Contribuyentes. (**)
c. Fotocopia simple de los documentos de identidad de los representantes o apoderados de la sociedad. (*)
d. Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al oferente. Estos documentos pueden consistir en: un poder suficiente en el que conste que el apoderado posee facultades suficientes para representar y obligar a la persona jurídica, otorgado por Escritura Pública (no es necesario que esté inscripto en el Registro de Poderes); o los documentos societarios que justifiquen la representación del firmante, tales como las actas de asamblea y de directorio en el caso de las sociedades anónimas. (*)
<b>9.3. Oferentes en Consorcio en formación.</b>
a. Original o fotocopia del acuerdo de intención de constituir el consorcio, en caso de resultar adjudicados y antes de la firma del contrato. (*)

- b. Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al consorcio en formación y que acrediten las facultades de los firmantes del acuerdo de intención para consorciarse. Estos documentos pueden consistir en (\*):
  - I. Original o fotocopia del acuerdo de intención de constituir el consorcio en caso de resultar adjudicados y antes de la firma del contrato, instrumentado por escritura pública, o
  - II. Original o fotocopia del acuerdo de intención de constituir el consorcio en caso de resultar adjudicados y antes de la firma del contrato, instrumentado por acuerdo privado. Cada integrante del consorcio que sea persona física domiciliada en la República del Paraguay deberá presentar los documentos requeridos para Oferentes Individuales especificados en el apartado Oferentes. (Personas Físicas) y, las personas jurídicas domiciliadas en Paraguay deberán presentar los documentos requeridos para Oferentes (Personas Jurídicas).
  - III. Un poder en el que conste que el apoderado posee facultades suficientes para representar y obligar al Consorcio, otorgado por escritura pública (no es necesario que esté inscripto en el Registro de Poderes) (\*).

#### 9.4. Oferentes en Consorcios constituidos o formalizados.

- a. Original o fotocopia del instrumento público (escritura pública) de constitución del consorcio. (\*)
- b. Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al consorcio. Estos documentos pueden consistir en (\*):
  - i. Original o fotocopia del instrumento público (escritura pública) de constitución del consorcio.
  - ii. Un poder en el que conste que el apoderado posee facultades suficientes para representar y obligar al Consorcio, otorgado por escritura pública (no es necesario que esté inscripto en el Registro de Poderes).

En el Módulo de Oferta Electrónica, el oferente deberá cargar los datos en el Formulario de oferta electrónica de conformidad a la normativa vigente.

Las formalidades de los acuerdos de intención y de los consorcios serán determinadas por la Dirección Nacional de Contrataciones Públicas (DNCP).

Los documentos indicados con asterisco (\*) son considerados documentos sustanciales a ser presentados con la oferta de conformidad al Decreto Reglamentario.

Los documentos indicados con doble asterisco (\*\*) deberán estar vigentes a la fecha y hora tope de presentación de ofertas electrónicas e inicio de la etapa competitiva.

La falta de firma en documentos formales no será un motivo de descalificación, salvo que expresamente se disponga la exigencia de la firma del oferente en cuyo caso la omisión o disconformidad deberá analizarse conforme a los Artículos 77, 78 y 80 del Decreto 2264/24.

Respecto al punto 3, cuando el oferente se encuentre activo sin movimiento, deberá presentar la documentación respaldatoria expedida por autoridad competente. En caso de no contar con personal subordinado por tratarse de un consultor individual, el oferente deberá presentar el certificado de no hallarse inscripto en el IPS.

## Capacidad Financiera

Con el objetivo de calificar la situación financiera del oferente, se considerarán los siguientes índices:

#### a. Para contribuyente de IRACIS/IRE.

Con el objetivo de calificar la situación financiera del oferente, se considerarán los siguientes índices: Para contribuyente de IRACIS/IRE GENERAL, IRPC/IRE SIMPLE, IRP e IVA GENERAL. AÑOS 2022, 2023, 2024.-

Deberán cumplir con el siguiente parámetro:

1- Para contribuyentes de IRACIS/IRE GENERAL: Deberá cumplir con el siguiente parámetro de los años ( 2022, 2023, 2024).-

a. Ratio de Liquidez: activo corriente / pasivo corriente

Deberá ser igual o mayor que 1, en promedio, en los 3 últimos años

b. Endeudamiento: pasivo total / activo total

No deberá ser mayor a 0,80 en promedio, en los 3 últimos años

c. Rentabilidad: Porcentaje de utilidad después de impuestos o pérdida con respecto al Capital.

El promedio en los 3 últimos años, no deberá ser negativo.

2- Para contribuyentes de IRPC/IRE SIMPLE: Deberá cumplir el siguiente parámetro.

Eficiencia: (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio de los años 2022, 2023, 2024.

3- Para contribuyentes de IRP/IRP-RSP, Deberá cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio de los años 2022, 2023, 2024.

4- Para contribuyentes exclusivamente del IVA General. Deberá cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio de los últimos (36) treinta y seis meses.

Para los consorcios: todos los integrantes deberán cumplir los índices financieros solicitados.

Observación: para hallar el promedio de los 3 años se calculará el índice de cada año y luego se sumarán estos índices y se dividirán entre la cantidad de años.

## Requisitos documentales para la evaluación de la capacidad financiera

Para evaluar el presente criterio, el oferente deberá presentar las siguientes documentaciones:

- a Balance General y Estado de Resultados de los años 2022, 2023, 2024 para contribuyente de IRACIS/IRE GENERAL.
- b Presentación del Formulario N° 501 años 2022, 2023, 2024 para los contribuyentes IRPC/IRE/IRE SIMPLE.-
- c Presentación del Formulario N° 515 años 2022, 2023, 2024 para los contribuyentes del IRP/IRP-RSP.-
- d Para contribuyentes de IVA Formularios IVA General: de los 36 treinta y seis últimos meses.

## Experiencia requerida

Con el objetivo de calificar la experiencia del oferente, se considerarán los siguientes índices:

### Lote 1

- 1- Demostrar la experiencia en la provisión e Implementación de los objetos del llamado, a organizaciones públicas y/o privadas con facturaciones de venta y/o recepciones finales, de los 2 (dos) últimos años (2023-2024) en un porcentaje equivalente del 30% del monto total ofertado. No se considerarán contratos y/o facturas que no estén acompañadas de la recepción final o certificado de buen cumplimiento de Contrato.
- 2- Existencia legal de por lo menos 2 (años) años de antigüedad.

### Lotes 2,3,4, 5 y 6

- 1-El proveedor debe tener como actividad principal Tecnologías de la Información y Comunicación (TIC), específicamente servicios de desarrollo de software.
- 2-Para Licitaciones, Concursos o Contrataciones a nivel local, se requiere un mínimo de 2 años de experiencia demostrable en dicho rubro operando en nuestro país y deberá corresponder a trabajos de desarrollo de software, totalizando un mínimo del 30% del monto total ofertado

La actividad comercial, industrial o de servicios debe estar vinculada con el tipo de bienes o servicios a contratar.

## Requisitos documentales para la evaluación de la experiencia

### Lote 1

- 1. Copia de contratos con sus respectivos certificados de buen cumplimiento de Contrato y/o facturaciones con sus respectivas remisiones, pudiendo presentarse los que fueren necesarios para acreditar el volumen (30% de la oferta)
- 2- Constancia de Inscripción en el Registro Único de Contribuyente emitida por la DNIT

### Lotes 2,3,4, 5 y 6

- 1- Constancia de Inscripción en el Registro Único de Contribuyente emitida por la DNIT
- 2- Documentos respaldatorios, ya sean contratos, constancias firmadas por el contratante o su representante, u otro documento que sea respaldatorio de justificación, totalizando un mínimo del 30% del monto total ofertado..

Se deberá acreditar que el giro comercial de la empresa corresponde al procedimiento de contratación ofertado, para lo cual deberá presentar copia simple y legible del documento que acredite la actividad comercial, industrial o de servicio, pudiendo ser: la constancia de RUC, patente municipal o documentos constitutivos, siempre que de la documentación se desprenda su actividad comercial y la correspondencia al procedimiento objetado. Cuando no resulte aplicable la constancia de RUC, la patente municipal o los documentos constitutivos, el oferente deberá manifestar y justificar esta condición en su oferta y presentar otra documentación a los efectos de acreditar el giro comercial.

## Capacidad Técnica

El oferente deberá proporcionar evidencia documentada que demuestre su cumplimiento con los siguientes requisitos de capacidad técnica:

\*El Oferente deberá preparar una ficha de las Especificaciones Técnicas del producto que oferta.

\*El oferente Debe pertenecer a rubros relacionados a Tecnologías de la Información y Comunicación, específicamente a desarrollo, mantenimiento y/o implementación de software. En caso de tratarse de una persona jurídica, esto deberá verificarse en el objeto de su Constitución siendo una de las actividades principales.



\*Mínimo de 3 referencias de clientes.

Al menos 3 referencias deben ser de clientes distintos.

Al menos 2 referencias deben corresponder a trabajos realizados en el Paraguay para organizaciones públicas o privadas radicadas en nuestro país.

La sumatoria de los montos de las referencias presentadas que cumplan los criterios deberá ser como mínimo el 30% del monto referencial de la adquisición.

\*Perfiles técnicos del proveedor

Para llevar adelante las tareas técnicas en el marco de la presente licitación, el oferente pondrá a disposición los siguientes perfiles:

1) Un ingeniero en informática o Lic. en análisis de sistemas.

2) Un desarrollador de software.

## Requisitos documentales para evaluar el criterio de capacidad técnica

Los siguientes documentos serán los considerados para la evaluación del presente criterio:

\*Ficha de las Especificaciones Técnicas del producto que ofertado por el oferente

\*Constancia de Inscripción en el Registro Único del Contribuyente.

\*Referencias de clientes, conforme a la exigencia de los criterios.

\*Se deberá presentar CV de cada uno de los RR.HH. propuestos, que deberán estar firmados por cada uno de ellos, y deberán declarar su compromiso a formar parte del equipo de trabajo en caso de

resultar adjudicado En caso de que uno de los recursos no participe al inicio o deje de formar parte durante el proceso de desarrollo por algún motivo, para dichos casos el oferente deberá

reemplazarlo por otro de equivalente perfil al solicitado o superior y notificar por nota el cambio realizado, adjuntando nuevamente el CV del recurso que se incorpora al equipo de desarrollo

conforme a lo requerido anteriormente.

## Aclaración de las ofertas

Con el objeto de realizar la revisión, evaluación, comparación y posterior calificación de ofertas, el Comité de Evaluación podrá solicitar a los oferentes, aclaraciones respecto de sus ofertas, dichas solicitudes y las respuestas de los oferentes se realizarán por escrito.

A los efectos de confirmar la información o documentación suministrada por el oferente, el Comité de Evaluación, podrá solicitar aclaraciones a cualquier fuente pública o privada de información.

Las aclaraciones de los oferentes que no sean en respuesta a aquellas solicitadas por la convocante, no serán consideradas.

No se solicitará, ofrecerá, ni permitirá ninguna modificación a los precios ni a la sustancia de la oferta, excepto para confirmar la corrección de errores aritméticos.

El comité de evaluación podrá solicitar aclaración respecto al CPEN, cuando se deba a omisiones o errores formales en la lista de precio, debiendo el oferente limitarse a responder a la solicitud de aclaración remitiendo el formulario respectivo anexo al Pliego.

## Disconformidad, errores y omisiones

Siempre y cuando una oferta se ajuste sustancialmente a las bases de la contratación, el Comité de Evaluación, requerirá que cualquier disconformidad u omisión que no constituya una desviación significativa, sea subsanada en cuanto a la información o documentación que permita al Comité de Evaluación realizar la calificación de la oferta.

A tal efecto, el Comité de Evaluación emplazará por escrito al oferente a que presente la información o documentación necesaria, dentro de un plazo razonable no menor a un día hábil, bajo apercibimiento de rechazo de la oferta. El Comité de Evaluación podrá reiterar el pedido cuando la respuesta no resulte satisfactoria, toda vez que no se viole el principio de igualdad.

Para los casos de ajustes de precios de las ofertas electrónicas, toda vez que se hayan realizado lances durante la etapa competitiva, el oferente deberá ajustar su listado de ítems al precio final de la competencia electrónica, a través del módulo de ofertas electrónicas.

Si como consecuencia del resultado de la división del precio total subastado respecto a la cantidad, se obtuviere una cifra con decimales, se deberá realizar el redondeo del mismo hacia abajo, de modo a que el precio total no supere al que figure en el Acta de Sesión Pública Virtual como precio final, conforme al sistema de adjudicación establecido (ítem, lote, total).

En la consignación de los precios unitarios finales, el oferente no podrá aumentar el precio unitario cargado inicialmente para la presentación de ofertas electrónicas e inicio de la etapa competitiva.

En caso de que el oferente no haya realizado lance durante la etapa competitiva, los precios permanecerán invariables.

## Criterios de desempate de ofertas

En caso de que existan dos o más oferentes solventes que cumplan con todos los requisitos establecidos en el pliego de bases y condiciones del procedimiento de

contratación, igualen en precio y sean sus ofertas las más bajas, el vencedor de cada grupo subastado será el que lo haya ingresado primero.

Siempre que el criterio de desempate establecido, no sea aplicable, el comité de evaluación determinará cuál de ellas es la mejor calificada para ejecutar el contrato utilizando los criterios dispuestos para el efecto por la DNCP en la reglamentación pertinente.

## Notificación del resultado

La notificación del resultado se realizará a través del SICP de manera automática, desde la publicación de los documentos en el SICP, a los correos declarados en el Registro de Proveedores del Estado de los oferentes presentados. A efectos de la notificación oficial, solo serán considerados tales correos electrónicos. Dicha notificación, al tiempo de la publicación de los documentos en el SICP, comprenderá la Resolución del resultado de la adjudicación y el informe de evaluación respectivo.

En casos excepcionales regulados por la DNCP, las Convocantes podrán dar a conocer el resultado por otros medios físicos o electrónicos a cada uno de los oferentes, remitiendo junto a la notificación, la copia íntegra de la resolución de adjudicación y del informe de evaluación, de conformidad al artículo 82 del Decreto.

En caso de que la convocante opte por la notificación física a los oferentes participantes, ésta deberá contar con la mención de haberse acompañado el informe de evaluación y la resolución de adjudicación correspondientes y con el acuse de recibo. De no contar con este último, se considerará que la notificación fue realizada en la fecha de publicación de los documentos relativos al resultado en el SICP.

En caso de que la convocante opte por la notificación por correo electrónico, se considerará que el oferente ha sido debidamente notificado desde el día siguiente de la notificación, en consecuencia, no se requerirá del acuse de recibo por parte del oferente.

La solicitud del Informe de Evaluación suspende el plazo para formular protestas hasta tanto la convocante haga entrega de dicha copia al oferente solicitante.

Las cancelaciones o declaraciones desiertas deberán ser notificadas a todos los oferentes, según el procedimiento indicado precedentemente.

Las notificaciones realizadas en virtud al contrato, deberán ser por escrito y dirigirse a la dirección indicada en el contrato.

## Criterios de Adjudicación

De acuerdo con el mercado, el objeto del contrato y el ciclo de vida del bien o servicio, podrá usarse uno o la combinación de varios criterios, previstos en el artículo 52 de la Ley N° 7021/22 "De Suministro y Contrataciones Públicas".

La adjudicación de la oferta solo podrá fundamentarse en la evaluación de los criterios señalados en los documentos del procedimiento de contratación.

La convocante adjudicará el contrato al oferente cuya oferta haya sido evaluada como la más baja y cumpla sustancialmente con los requisitos de las bases y condiciones, siempre y cuando la convocante determine que el oferente está calificado para ejecutar el contrato satisfactoriamente.

1. La adjudicación en los procedimientos de contratación en los cuales se aplique el atributo de contrato abierto, se efectuará por las cantidades o montos máximos solicitados en el procedimiento de contratación, sin que ello implique obligación de la convocante de requerir la provisión de esa cantidad o monto durante de la vigencia del contrato, obligándose sí respecto de las cantidades o montos mínimos establecidos.

2. En caso de que la convocante no haya adquirido la cantidad o monto mínimo establecido, deberá consultar al proveedor si desea ampliarlo para el siguiente ejercicio fiscal, hasta cumplir el mínimo.

3. Al momento de adjudicar el contrato, la convocante se reserva el derecho a disminuir la cantidad de Bienes y/o Servicios requeridos, por razones de disponibilidad presupuestaria u otras razones debidamente justificadas. Estas variaciones no podrán alterar los precios unitarios u otros términos y condiciones de la oferta y de los documentos de la licitación.

En aquellos procedimientos de contratación en los cuales se aplique el atributo de contrato abierto, cuando la Convocante deba disminuir cantidades o montos a ser adjudicados, no podrá modificar el monto o las cantidades mínimas establecidas en las bases de la contratación.

## Audiencia Informativa

Una vez notificado el resultado del proceso, el oferente tendrá la facultad de solicitar una audiencia a fin de que la convocante explique los fundamentos que motivan su decisión.

La solicitud de audiencia informativa no suspenderá ni interrumpirá el plazo para la interposición de protestas.

El procedimiento de realización de la misma deberá ajustarse a las reglamentaciones vigentes para el efecto.

# SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS

Esta sección constituye el detalle de los bienes con sus respectivas especificaciones técnicas - EETT, de manera clara y precisa para que el oferente elabore su oferta. Salvo aquellas EETT de productos ya determinados por plantillas aprobadas por la DNCP.

## Suministros y Especificaciones técnicas.

Esta sección constituye el detalle de los bienes con sus respectivas especificaciones técnicas - EETT, de manera clara y precisa para que el oferente elabore su oferta. Salvo aquellas EETT de productos ya determinados por plantillas aprobadas por la DNCP.

El Suministro deberá incluir todos aquellos ítems que no hubiesen sido expresamente indicados en la presente sección, pero que pueda inferirse razonablemente que son necesarios para satisfacer el requisito de suministro indicado, por lo tanto, dichos bienes y servicios serán suministrados por el Proveedor como si hubiesen sido expresamente mencionados, salvo disposición contraria en el Contrato.

Los bienes y servicios suministrados deberán ajustarse a las especificaciones técnicas y las normas estipuladas en este apartado. En caso de que no se haga referencia a una norma aplicable, la norma será aquella que resulte equivalente o superior a las normas oficiales de la República del Paraguay. Cualquier cambio de dichos códigos o normas durante la ejecución del contrato se aplicará solamente con la aprobación de la contratante y dicho cambio se registrará de conformidad a la cláusula de adendas y cambios convenios modificatorios.

El Proveedor tendrá derecho a rehusar responsabilidad por cualquier diseño, dato, plano, especificación u otro documento, o por cualquier modificación proporcionada o diseñada por o en nombre de la Contratante, mediante notificación a la misma de dicho rechazo.

## Identificación de la unidad solicitante y justificaciones

En este apartado la convocante deberá indicar los siguientes datos:

Identificar el nombre, cargo y la dependencia de la Institución de quien solicita el procedimiento de contratación a ser publicado.

- Comisario Principal MCP. JESÚS M. BAEZ , Tesorero Habilitado Pagador Actividad 09 Servicio de Operaciones Especiales y de Contención - LOTE 6
- Comisario Principal MCP. GREGORIO R. FLOR CÁCERES , Tesorero Habilitado Pagador Actividad 02 Gestión de los Recursos Policía Nacional - LOTE 1
- Comisario Principal MCP. LENNY SILVANA DANEI PEREIRA, Tesorero Habilitado Pagador Actividad Act. 05 Investigación de Hechos Punibles - LOTE 2
- Comisario Principal MCP. HUGO NOGUERA ARROYO, Tesorero Habilitado Pagador Actividad 06 Formación y Capacitación de Oficiales y Suboficiales- LOTE 4 Y 5
- Comisario Principal MCP. MIRIAN C. AÑASCO V., Tesorero Habilitado Pagador Actividad 08 Servicio de Identificación de Personas - LOTE 3

Justificación de la necesidad que se pretende satisfacer mediante la contratación a ser realizada.

Este pedido obedece, a la necesidad de renovar licencias y adquirir softwares para el mejoramiento de las gestiones de datos de las distintas dependencias solicitantes, componentes de la

Institución  
Policial.

Justificación de la planificación, si se trata de un procedimiento de contratación periódico o sucesivo, o si el mismo responde a una necesidad temporal.

Esta planificación responde a una necesidad temporal.

Justificación de las especificaciones técnicas establecidas.

Se han elaborado las Especificaciones Técnicas de acuerdo a la necesidad de los hardwares actualmente utilizados. (ver dictamen técnico)

## Especificaciones Técnicas "CPS"

Los productos y/o servicios a ser requeridos cuentan con las siguientes especificaciones técnicas:

El propósito de la Especificaciones Técnicas (EETT), es el de definir las características técnicas de los bienes que la convocante requiere. La convocante preparará las EETT detalladas teniendo en cuenta que:

- Las EETT sirven de referencia para verificar el cumplimiento técnico de las ofertas y posteriormente evaluarlas. Por lo tanto, unas EETT bien definidas facilitarán a los oferentes la preparación de ofertas que se ajusten a los documentos de licitación, y a la convocante el examen, evaluación y comparación de las ofertas.
- En las EETT se deberá estipular que todos los bienes o materiales que se incorporen en los bienes deberán ser nuevos, sin uso y del modelo más reciente o actual, y que contendrán todos los perfeccionamientos recientes en materia de diseño y materiales, a menos que en el contrato se disponga otra cosa.
- En las EETT se utilizarán las mejores prácticas. Ejemplos de especificaciones de adquisiciones similares satisfactorias en el mismo sector podrán proporcionar bases concretas para redactar las EETT.
- Las EETT deberán ser lo suficientemente amplias para evitar restricciones relativas a manufactura, materiales, y equipo generalmente utilizados en la fabricación de bienes similares.
- Las normas de calidad del equipo, materiales y manufactura especificadas en los Documentos de Licitación no deberán ser restrictivas. Se deberán evitar referencias a marcas, números de catálogos u otros detalles que limiten los materiales o artículos a un fabricante en particular. Cuando sean inevitables dichas descripciones, siempre deberá estar seguida de expresiones tales como "o sustancialmente equivalente" u "o por lo menos equivalente", remitiendo la aclaración respectiva. Cuando en las ET se haga referencia a otras normas o códigos de práctica particulares, éstos solo serán aceptables si a continuación de los mismos se agrega un enunciado indicando otras normas emitidas por autoridades reconocidas que aseguren que la calidad sea por lo menos sustancialmente igual.
- Asimismo, respecto de los tipos conocidos de materiales, artefactos o equipos, cuando únicamente puedan ser caracterizados total o parcialmente mediante nomenclatura, simbología, signos distintivos no universales o marcas, únicamente se hará a manera de referencia, procurando que la alusión se adecue a estándares internacionales comúnmente aceptados.

- Las EETT deberán describir detalladamente los siguientes requisitos con respecto a por lo menos lo siguiente:
    - (a) Normas de calidad de los materiales y manufactura para la producción y fabricación de los bienes.
    - (b) Lista detallada de las pruebas requeridas (tipo y número).
    - (c) Otro trabajo adicional y/o servicios requeridos para lograr la entrega o el cumplimiento total.
    - (d) Actividades detalladas que deberá cumplir el proveedor, y consiguiente participación de la convocante.
    - (e) Lista detallada de avaluos de funcionamiento cubiertas por la garantía, y las especificaciones de las multas aplicables en caso de que dichos avaluos no se cumplan.
  - Las EETT deberán especificar todas las características y requisitos técnicos esenciales y de funcionamiento, incluyendo los valores máximos o mínimos aceptables o garantizados, según corresponda. Cuando sea necesario, la convocante deberá incluir un formulario específico adicional de oferta (como un Anexo a la de Oferta), donde el oferente proporcionará la información detallada de dichas características técnicas o de funcionamiento con relación a los valores aceptables o garantizados.
- Quando la convocante requiera que el oferente proporcione en su oferta datos sobre una parte de o todas las Especificaciones Técnicas, cronogramas técnicos, u otra información técnica, la convocante deberá detallar la información requerida y la forma en que deberá ser presentada por el oferente en su oferta.
- Si se debe proporcionar un resumen de las EETT, la convocante deberá insertar la información en la tabla siguiente. El oferente preparará un cuadro similar para documentar el cumplimiento con los requerimientos.

## Detalle de los bienes y/o servicios

Los bienes y/o servicios deberán cumplir con las siguientes especificaciones técnicas y normas:

### Disposiciones Generales:

Se deberá aplicar la línea gráfica gubernamental en los Lotes pertinentes, según el uso y finalidad de cada sistema, en especial los utilizados por la ciudadanía. Dicha línea gráfica se puede encontrar en el siguiente enlace:

<https://www.mitic.gov.py/materiales/norma-de-gobierno-linea-grafic>

LOTE N° 1 LICENCIA FORTINET- ACTIVIDAD 2

### LISTA DE PRECIOS BIENES Y SERVICIOS

Ítem	Código de Catálogo	Nombre	Unidad de Medida	Cantidad
1	43232901-9999	Renovación de Licencia Fortinet: Modelo: FORTIGATE 101E Serial N°: FC101ETK18004554, por 2 (dos) años como mínimo.		
unidad	1			

Modalidad de incorporación del software

Adquisición de software con licencia de propiedad de terceros Organismo y Entidad del Estado

Policía Nacional Tesorería de la Actividad 02 Gestión de los Recursos Nombre del Llamado Proceso de contratación

Renovación de Licencia Fortinet

Ítems a ser Licitados, Contratados o Adquiridos

Renovación de la Licencia Fortinet Comandancia de la Policía Nacional

**IMPORTANTE:** En caso de que la Policía Nacional necesite la adquisición o compra de productos de software con licencia de propiedad de terceros, deberá hacerlo de lotes diferentes Software Lista y especificación de software

[Por cada software de terceros que la Policía Nacional necesite adquirir, se debe especificar una tabla de datos.]

Datos del software con licencia de propiedad de terceros

Renovación de la Licencia Fortinet Comandancia de la Policía Nacional.

Software	Especificar
Año	2.000
Número de	N/A
identificación	
de compra	
Nombre del	Licencia para Fortinet: Modelo: FORTIGATE 101E
software	Serial N°: FC101ETK18004554.
Objetivo del	Distribución y Seguridad en la RED de la Comandancia de la Policía
software	Nacional.
Justificación	Es utilizado en la distribución y seguridad de la Red de la Comandancia de
la Policía	la Policía Nacional. Se requiere la renovación, ya que el equipo se
Nacional	encuentra en funcionamiento.
Versión del	Fortinet: Modelo: FORTIGATE 101E
software	Serial N°: FC101ETK18004554.
Modalidad	Software especializado

Tipo de No aplica

software

utilitario (para

esta

modalidad)

Tipo de Seguridad de Red.

software

utilitario (para

esta

modalidad)

Tipo de No aplica

software

especializado

(para esta

modalidad)

Año de 2.000

creación del

software

País de origen Estados Unidos

del software

Compras - Renovación de licencia Fortinet, en el año 2021, por el monto de

relacionadas 48.200.000 Gs.

Tipo de Especificar si se trata de licencia o suscripción:

adquisición

Licencia

Detalle del Para el equipo Fortinet

tipo de

adquisición

Vigencia de Anual (2 años) como mínimo.

titularidad

Infraestructura Requiere únicamente infraestructura dla Policía Nacional.

requerida

Consultoría de NO

especialistas

Fabricante

Fabricante. Fortinet

Nombre legal

Año de En el año 2.000

constitución

del fabricante

País de origen Estados Unidos.

del fabricante

Utilización en la Policía Nacional

Responsable [Responsable TIC que realiza la solicitud del software.]

TIC

Áreas internas Departamento de Informática Comandancia de la Policía Nacional.

usuarias dla

Policía

Nacional

Cantidad de Uno

usuarios dla

Policia

Nacional

**Autorización** El oferente deberá acreditarse como representante oficial o distribuidor del Fabricante, autorizado del software y sus respectivas licencias, según se detalla:

**Representante**

**o Distribuidor** El oferente deberá acreditarse como representante oficial o distribuidor autorizado por el fabricante del software ofertado

manifestando que posee la capacidad para proveer la cantidad ofertada en el tiempo solicitado. En la misma, deberá constar que se encuentra en condiciones para proveer, instalar, configurar y soportar el software, según lo solicitado en la planilla de especificaciones técnicas, en caso de resultar adjudicatario.

Las cartas presentadas deben ser originales, estar dirigidas a la Policía Nacional y hacer referencia en forma específica a la licitación. Las mismas deben estar firmadas por alguna autoridad del fabricante con injerencia comercial con potestades sobre nuestra región o país. En caso la propuesta sea presentada con la integración de varias empresas nacionales o regionales, todas ellas deberán contar con esta certificación.

A estos efectos, se deberá considerar lo siguiente:

Los representantes deberán presentar la documentación expedida por el fabricante que lo acredite como representante oficial o distribuidor autorizado de la marca ofertada.

En el caso de los distribuidores, deberán presentar la autorización del representante, distribuidor y/o resellers para Paraguay y/o Latinoamérica extendida al oferente participante de la licitación y que lo acredite como distribuidor de la marca ofertada. Asimismo, se deberá demostrar documentalmente el vínculo entre el representante, distribuidor o resellers y el fabricante.

Entregables

Definido en el Estándar de Software

Especificar

Documentación técnica.

N/A

Licencias (in extenso, es decir, todo el contrato que rige la adquisición de la licencia y las condiciones que rigen sobre los usos o formas de explotación de las mismas).

Contrato en donde se especifica la valides de la licencia.



Manuales de uso u otros requeridos para la utilización del software adquirido.

N/A

Los derechos de las licencias o suscripciones deberán estar a favor de la Policía Nacional utilizando su respectiva cuenta.  
Licencia.

A nombre de la Policía Nacional

SE HACE MENCIÓN QUE EN EL DICTAMEN TÉCNICO SE JUSTIFICA LA DEPENDENCIA TECNOLÓGICA DE LA MARCA.

LOTE N° 2 ADQUISICIÓN DE SOFTWARE PARA EL DEPARTAMENTO ESPECIALIZADO EN EL CONTROL Y FISCALIZACIÓN DE EMPRESAS DE SEGURIDAD PRIVADA Y AFINES.  
ACTIVIDAD 5

DESARROLLO DEL SISTEMA WEB DE GESTIÓN DE EMPRESAS DE SEGURIDAD, GUARDIAS, ARMAS Y OTROS. (Submodalidad de desarrollo de software con requerimientos definidos ítems específicos para su contratación).

#### Introducción y justificación

La finalidad del presente proceso de adquisición, Desarrollo del Sistema Web de Gestión de empresas de seguridad, guardias, armas y otros, es a fin de almacenar, cambiar y administrar datos. De modo a permitir diseñar un almacenamiento de datos personalizado para satisfacer las necesidades de análisis e informes. El diseño de software de base de datos también permitirá la creación, implementación y mantenimiento de un sistema de gestión de datos en toda la organización.

1. Submodalidad de adquisición La submodalidad de adquisición será:

Software con requerimientos definidos

2. Objetivo general

Lograr permitir diseñar un almacenamiento de datos personalizado para satisfacer las necesidades de análisis e informes.

3. Objetivos específicos

Facilitar la gestión de los datos de las empresas de seguridad para su posterior utilización Obtener una forma segura de administración y almacenamiento de datos  
Brindar un mejor servicio a las empresas de seguridad

4. Definiciones, acrónimos y abreviaturas

Sistema Web de Gestión de Empresas de Seguridad, Guardias, Armas SGESEA.

5. Antecedentes

La modernización del departamento de seguridad privada y afines a través de la obtención de un sistema que permita mayor seguridad en cuanto a administración y almacenamiento de los datos de las

empresas privadas.

6. Marco legal

Ley N° 5424 Regula la prestación de servicios de vigilancia y seguridad de las personas y bienes patrimoniales en el ámbito de seguridad privada.

7. Beneficiarios

Empresas de seguridad privada, personal administrativo.

8. Infraestructura para el software Infraestructura para el software

Para la implementación y operación del sistema, objeto de este procedimiento de definición y compra, no serán necesarios nuevos equipos de hardware, serán utilizados los equipos que conforman el parque actual de equipos del Departamento de Informática de la Policía Nacional destinados a Seguridad privada y afines.

Servidores: SERVIDOR DELL PowerEdge R820

Máquinas Virtuales y Contenedores: Virtualizador Proxmox V.8.2 (estable) Sistemas Operativos: Linux distribución Debian v.12

Sistema de Virtualización: Proxmox Estaciones de trabajo:

Cantidad aproximada de estaciones de trabajo (PC, notebook, dispositivos móviles) que tiene la Policía Nacional destinada para el uso de los sistemas a adquirir, para ello se destaca que los usuarios acceden desde sus dispositivos particulares (notebook, celular, etc) siendo de 600 usuarios simultáneamente, con conexión dispar de usuarios aproximadamente a 1.200 usuarios en total.

Datacenter: Ubicado en el Departamento de Informática de la Policía Nacional (Datacenter tipo Contenedor), con generador, UPS para los Servidores, Dispositivos sensor de Humedad, humos, llamas, extintores de incendios con polvo seco (para electrónicas).

El responsable del datacenter es la División TIC del Departamento de Informática de la Policía Nacional, bajo la supervisión de un Oficial Superior con diligencia en el área técnica-tecnológica y quien trabaja en coordinación directa con la jefatura del Departamento de Informática.

Se utilizan los dominios de la Institución Policial administrados por el Departamento de Informática y se encuentra abierta para trabajar en conexión externa a dominios generados por terceros. Los servicios de dominios se establecen por medio de una IP Publica.

## 9. Confidencialidad

Con la intención de proteger la información que la entidad contratante proporciona a los proveedores (oferentes adjudicados), una vez adjudicado el contrato, debe especificar el grado de privacidad de la información. Es importante precisar la confidencialidad de la información que se entrega para la realización de los estudios o trabajos, diferenciando el tipo de información en caso de requerir aplicar distintos niveles de confidencialidad o publicidad de la información. Así también, respecto de la información que se genere durante la realización de las actividades, y la información producida una vez que se haya concluido el servicio. Deberá incluir, como mínimo, lo siguiente:

- a. El oferente reconoce que la información y documentación que \_\_\_\_\_ como entidad contratante le proporcione, así como los datos y resultados obtenidos de la prestación de los servicios, son propiedad exclusiva de la entidad contratante, como el carácter confidencial y/o reservado en términos de la normativa aplicable y las disposiciones del contrato.

El oferente se obliga a mantener absoluta confidencialidad sobre las creaciones realizadas, incluyendo todos los algoritmos y toda la información sobre el código fuente y código objeto de las mismas, como respecto de todos sus manuales, incluyendo la documentación preparatoria, su descripción técnica, manuales de uso y cualquier otra documentación relacionada con cualquier actividad realizada por el Desarrollador en virtud del contrato.

Cualquier información, fuese cual fuere su naturaleza (técnica, comercial, financiera, operacional o de otro tipo), contenida en cualquier forma y soporte (ya sea verbal, escrita, grabada o de cualquier otro tipo), que pudiera ser facilitada por la Policía Nacional, será considerada como Información Confidencial, incluyéndose en esta categoría aquella información generada a partir de la propia Información Confidencial.

El desarrollador, se obliga asimismo a:

- b. tratar la Información Confidencial como estrictamente secreta.
- c. custodiar y guardar la Información Confidencial, bien sea escrita, grabada o en cualquier otro tipo de soporte, separada de cualquier otra información de la que pudiera disponer.
- d. utilizar o transmitir la Información Confidencial exclusivamente para los fines del proyecto.
- e. utilizar procedimientos de control de dicho uso o transmisión de la Información Confidencial. El desarrollador no realizará copia de la Información Confidencial sin el previo consentimiento escrito de la Policía Nacional, excepto aquellas copias que sean necesarias por el desarrollador para su estudio interno.
- f. restringir el acceso a la Información Confidencial únicamente a aquellos empleados suyos que necesiten conocerla para los fines convenidos, y asegurarse que dichos empleados conocen las obligaciones que les resultan aplicables en virtud de lo establecido en el presente documento. Todos los contratos que el Desarrollador celebrará con empleados, trabajadores y prestadores de servicios que podrían participar en el desarrollo del contrato, incluirán cláusulas sobre confidencialidad y transferencia que producen iguales efectos y sujetan a dichas personas a las mismas obligaciones que el Desarrollador se ha obligado.
- g. no facilitar Información Confidencial a tercero alguno sin el previo consentimiento escrito de la Policía Nacional, y asegurarse de que, en caso de haber obtenido dicha autorización, dicho tercero firme un compromiso de confidencial con la Policía Nacional en términos equivalentes a los de la presente cláusula.

La Policía Nacional será en todo momento el titular exclusivo de la información confidencial, la cual será protegida por todos los medios legales a su alcance. En ningún caso se entenderá implícito en modo alguno, que el hecho de que la Policía Nacional facilite la Información Confidencial significa la concesión de licencia o la cesión de cualquier naturaleza a favor del desarrollador de cualesquiera derechos de patentes, marca, modelo de utilidad, diseño, derechos de autor, o derecho alguno de propiedad intelectual. Ninguna de las partes utilizará el nombre, marca, nombre comercial, o cualesquiera otros derechos de propiedad industrial o intelectual de la otra Parte, sin el previo consentimiento por escrito de ésta, salvo aquellos expresa y contractualmente cedidos.

Toda información que ostente algún derecho de propiedad intelectual de conformidad al derecho positivo que rige a ambas partes, a pesar de ser compartida entre estas, no implicará renuncia alguna a tales derechos, los cuales permanecerán vigentes sobre toda utilización que haga la otra parte de tal información.

La interpretación del concepto de propiedad intelectual no podrá ir más allá de lo establecido en la legislación respectiva. Lo incluido en tales derechos dependerá de lo que le ha sido expresamente reconocido por la autoridad de aplicación, no pudiendo invocarse de lo contrario, derecho alguno.

El desarrollador no podrá utilizar la información y los desarrollos o análisis funcionales elaborados en el cumplimiento de la contratación, para terceros o en beneficio de terceras partes. No podrá utilizar esta información en otras implementaciones que lo coloquen en situación privilegiada. Toda infracción a esta obligación, lo hará responsable de responder de los daños y perjuicios que pudieran derivarse, así como las sanciones administrativas que correspondan.

### Sección 1

Submodalidad de desarrollo de software con requerimientos definidos ítems específicos para su contratación La Policía Nacional deberá indicar explícitamente las especificaciones generales del software, definidos en los ítems comunes para la contratación de empresas de software, y adicionalmente los descritos a continuación. Requerimientos

DESARROLLO DEL SISTEMA WEB DE GESTION DE EMPRESAS DE SEGURIDAD, GUARDIAS, ARMAS Y OTROS.

#### 1. MODULOS QUE TENDRA EL SISTEMA

1. Módulo de Empresas de seguridad.
  - Actualización y modificación de datos generales de empresas de seguridad.
  - Acceso a documentos escaneados y su actualización.
  - Consultas sobre empresas e seguridad.
  - Reportes varios.
  - Acceso web.
  - Generación de bases de datos desde información almacenada en Excel.
  - Enlace a archivos escaneados.

2. Módulo de situación de empresas de seguridad.
  - Renovación de constancias.

- Sumarios
  - Notificaciones.
  - Cancelaciones.
  - Consultas.
  - Reportes.
- 3. Módulo del personal.
  - Registro de datos de Guardias de seguridad.
  - Registro de datos de carnet de habilitación.
  - Actualización de registro de Vinculación/desvinculación.
- Informes y resoluciones sobre el personal de empresas de seguridad.
- Consultas.
- Reportes.
- 4. Módulo de Armas.
  - Registro y actualización de datos de armas, marca, calibre, registro Dimabel, etc.
  - Incorporaciones, bajas de armas.
  - Notificaciones, actas, eventos relacionados al uso de las mismas.
  - Web service de verificación con Dimabel.
  - Consultas.
  - Reportes.
  - Carga de documentación de respaldo PDF.
- 5. Módulo de Vehículos.
  - Datos generales sobre vehículos usados por las empresas de seguridad, marca, modelo, Chasis, etc.
  - Notificaciones, eventos relacionados al uso de estos vehículos.
  - Altas y retiros de vehículos.
  - Consultas.
  - Reportes.
  - Carga de documentación de respaldo PDF.
- 6. Módulo de equipos de comunicaciones.
  - Registro y actualizaciones de equipos de comunicación, marca, modelo, frecuencia, habilitación Conatel.
  - Registro de celulares de uso por personal de empresas de seguridad.
  - Notificaciones, actas, eventos relacionados al uso de los mismos.
  - Consultas.
  - Reportes.
- 7. Sistema de administración de usuarios y seguridad.
  - Creación de usuarios y pines.
  - Permisos de accesos por rol o perfil de lectura.
  - Pistas de auditorías de los diferentes usuarios.
  - Copia de seguridad automática.
  - Acceso web.

Entrenamiento y capacitación del personal a operar el sistema.

El sistema será desarrollado en software libre (open Source), con licencia perpetua y todos los derechos. Tener licencias necesarias.

Requerimientos no funcionales

El sistema deberá contar con alta capacidad de integración que posibilite intercambios de información a través del Sistema de Intercambio de Información (SII) provisto por el MITIC. Arquitectura general

El Sistema ofrecido debe tener la capacidad de correr sobre un Sistema Operativo Linux Red Hat o Windows Server. Su arquitectura debe ser en 3 capas:

Presentación o capa web en aplicaciones web (interfaz de usuario). Lógica de negocio o capa aplicativa (servidor de aplicaciones).

La Capa de Datos: Esto comprende el servidor de base de datos. Esta capa se requiere que sea en uno de los motores de base de datos de la Policía Nacional (MySQL, PostgreSQL). Tecnología

El Sistema ofrecido debe tener la capacidad de correr sobre un Sistema Operativo Linux Red Hat o Windows Server.

Seguridad

CRITERIOS MINIMOS DE SEGURIDAD PARA EL DESARROLLO Y LA ADQUISICION DE SOFTWARE.

-Soporte y gestión continua del software:

1. Todo el software desarrollado debe contar con soporte de software del fabricante. Al momento de la adquisición se debe establecer claramente el tiempo de vida mínimo que se requiere para el software o sistema, y el fabricante debe ofrecer un tiempo de soporte igual o superior a dicho tiempo de vida.
2. En caso de que no sea posible contar con soporte de software del fabricante, el modelo de

licenciamiento y la disponibilidad del código fuente debe ser tal que permita a la institución o a otra empresa o desarrollador de software nacional asumir dicho soporte.

3. El fabricante o servicio de soporte debe tener un canal de comunicación y/o mecanismo de reporte de vulnerabilidades o bugs de programación, de manera a que el cliente pueda contactarlo en caso de descubrimiento de vulnerabilidades. En caso de que el reporte ocurra dentro de la ventana de tiempo de vida solicitado, el fabricante o servicio soporte debe ser

capaz de proporcionar una corrección a la vulnerabilidad de manera oportuna, según el acuerdo del nivel del servicio (por sus siglas en inglés, Service Level Agreement o SLA) especificado en el contrato o pliego de bases y condiciones.

4. El software debe poder ser inventariado por herramientas estándar automatizadas de inventario de software basados en el estándar *Common Platform Enumeration* (CPE), debiendo incluir como mínimo la información del nombre, versión, autor y fecha de instalación del mismo.

- Gestión de usuarios, sesiones y privilegios:

1. El software debe permitir una gestión de usuarios de acuerdo a los requerimientos de la

institución, con niveles de privilegios de acuerdo a los roles que éstos requieran (administrador, editor, usuario, etc.), basados en el principio de mínima necesidad de conocimiento.

2. El software debe permitir la revocación de acceso de usuarios, mediante un estado desactivado o similar.
3. Debe ser posible establecer una fecha de expiración para las cuentas de usuarios, a partir de la cual la cuenta deberá entrar a un estado desactivado o similar, hasta tanto se apruebe la continuidad de la misma. El parámetro de fecha de expiración podrá ser fijo o configurable por la institución, de acuerdo a sus requerimientos de negocio.
4. El software debe contemplar la expiración de sesiones de acuerdo a parámetros temporales. Estos parámetros pueden ser fijos o configurables por la institución, de acuerdo a sus requerimientos de negocio.

El software debe poder ser inventariado por herramientas estándar automatizadas de inventario de software basados en el estándar Common Platform Enumeration (CPE), debiendo incluir como mínimo la información del nombre, versión, autor y fecha de instalación del mismo.

- Autenticación y gestión de credenciales:

1. El software debe permitir la gestión individual eficaz de credenciales, debiendo permitir que cada usuario sea capaz de cambiar su propia contraseña. Se debe contemplar también mecanismos de recuperación de contraseñas, ya sea a través de un usuario de mayores privilegios o de mecanismos de auto-gestión por parte del usuario. Preferentemente, debe ser posible que al momento de la creación de cuentas permita forzar el cambio de contraseña luego del primer inicio de sesión.

3/62. El software que almacene y/o procese información crítica y/o que se utilice para un proceso crítico de la institución debe soportar autenticación de doble factor para los usuarios de privilegios elevados.

3. El software debe permitir establecer políticas de contraseña, que incluyan, como mínimo, la posibilidad de establecer los siguientes parámetros:

- longitud mínima de la contraseña
- complejidad de contraseña (mayúsculas, minúsculas, números y caracteres especiales, etc.)

Los mencionados parámetros serán configurables por la institución, preferentemente, o en su defecto, deberán ajustarse a los lineamientos y estándares mínimos indicados por la institución.

4. Las contraseñas no deben almacenarse en texto claro, sino mediante la aplicación de funciones hash o funciones resumen. Para el almacenamiento de las contraseñas se debe utilizar funciones criptográficas seguras no reversibles de hash combinadas con salt aplicadas a las contraseñas. Algoritmos aprobados son los siguientes:

- Argon2
- PBKDF2
- scrypt
- bcrypt

5. De manera alternativa, se puede cifrar las contraseñas utilizando técnicas criptográficas

reversibles únicamente en aquellos casos en que la clave secreta y/o privada de cifrado quede bajo el poder exclusivo del usuario dueño de la contraseña.

- Gestión de registros de auditoría:

1. El software debe ser capaz de generar registros de auditoría de todos los eventos relevantes, con los detalles suficientes para permitir una trazabilidad adecuada, que abarque como mínimo los siguientes eventos:

- inicios de sesión de usuarios (exitosos y fallidos)
- delegación/impersonificación de cuentas de usuarios
- modificación de parámetros del sistema
- gestión de usuarios (cambio de contraseña, creación/eliminación/modificación de usuarios y/o grupos)
- acciones críticas llevadas a cabo por usuarios en el marco del proceso de negocio del sistema (edición de datos sensibles, eliminación de datos, etc.)

2. El software debe contemplar un mecanismo configurable de rotación de registros de auditoría, de acuerdo al parámetro de cantidad de tiempo (diario, semanal, mensual, etc.), como mínimo.

• Cifrado:

1. El software debe cifrar toda la información sensible en tránsito, especialmente aquella información de carácter confidencial y/o cuya integridad deba asegurarse. Para ello se deberán utilizar protocolos de red cifrados, tales como HTTPS, SSH, SCP, SFTP/FTPS, etc.

2. Para sistemas basados en web, se adoptará el modelo SSL/TLS para el cifrado del tráfico. Los protocolos aprobados son TLS v.1.2 o superiores. Los protocolos TLS v.1.1 e inferiores y SSLv3 4/6e inferiores no deben ser utilizados. Se deben seleccionar suites de cifrado robustos; una guía de referencia es:

[https://cheatsheetseries.owasp.org/cheatsheets/TLS\\_Cipher\\_String\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html) Se deben evitar las suites de categoría C o inferiores.

3. Las claves de cifrado deben ser robustas. Se recomienda una longitud de 2048 bits para RSA o equivalente, de acuerdo al estándar NIST SP 800-57. La clave privada debe quedar en poder de la institución, exclusivamente.

• Codificación del software:

1. Se debe utilizar estándares de buenas prácticas seguras de programación, la cual debe ser seleccionada e implementada de acuerdo al lenguaje de programación y el entorno de desarrollo utilizado. Guías de referencia recomendadas son las siguientes:

- SEI CERT Coding Standards <https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards>
- OWASP Secure Coding Practices y OWASP Secure Coding Cheat Sheet [https://www.owasp.org/index.php/OWASP\\_Secure\\_Coding\\_Practices\\_-\\_Quick\\_Reference\\_Guide](https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide)

[https://www.owasp.org/index.php/Secure\\_Coding\\_Cheat\\_Sheet](https://www.owasp.org/index.php/Secure_Coding_Cheat_Sheet)

- Oracle Secure Coding Guidelines for Java SE <http://www.oracle.com/technetwork/java/seccodeguide-139067.html>

2. El software debe contemplar un manejo seguro de errores. Se debe realizar y documentar la verificación explícita de errores para todas las entradas, comprobando el tamaño, el tipo de datos, los rangos de valores y/o formatos aceptables de modo a que éstos sean válidos para la operación que están por realizar.

3. Todos los componentes de terceros utilizados para el desarrollo del software deben estar actualizados a la última versión estable disponible, contar con soporte por un periodo igual o

superior al exigido para el proyecto y ser de confianza. Esto es aplicable, pero no limitante, a librerías, *frameworks*, *scripts*, funciones, *plugins*, plantillas, generadores de código, compiladores, entre otros.

4. Se debe realizar y documentar las pruebas de vulnerabilidades de código, incluyendo análisis estático y dinámico de vulnerabilidades para verificar que se cumplan los estándares mínimos de codificación segura, utilizando herramientas y/o guías de testing de seguridad estándar y aceptados por la industria. Guías de referencia recomendadas son las siguientes:

- OWASP Testing Project: [https://www.owasp.org/index.php/OWASP\\_Testing\\_Project](https://www.owasp.org/index.php/OWASP_Testing_Project)
- Open Source Security Testing Methodology Manual (OSSTMM) <http://www.isecom.org/research/>
- Microsoft Security Development Lifecycle (SDL) - Pasos 10 a 13 <https://www.microsoft.com/es-es/download/details.aspx?id=12379>  
<https://www.microsoft.com/en-us/securityengineering/sdl/practices>

Plan de trabajo

CRONOGRAMA Y PLAN DE TRABAJO

DESCRIPCIÓN DE LA	SEM	SEM	SEM	SEM	SEM	SEM	SEM	SEM	SEM	SEM
-------------------	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----

TAREA	1	2	3	4	5	6	7	7	9
-------	---	---	---	---	---	---	---	---	---

*Análisis y Relevamiento de Software*

*Módulo en entorno*

*Modulo de registro de empresas de seguridad*

*Módulo de actualización y documentación de empresas de seguridad*

*Módulo de registro de guardias*

*Módulo de registro de armas*

*Módulo de registro de vehiculos*

*Módulo de registro de elementos de comunicacion*

*Plataforma de verificación (uso interno)*

*Plan de Capacitación y utilización del sistema*

El oferente deberá presentar en su oferta técnica un cronograma detallado y propuesta de metodología de trabajo que mejor se adecue a lo solicitado en el cronograma general, incluyendo la lista de personal proponente por cada actividad. Según lo dispuesto en la sección [Perfiles técnicos del personal](#).

Entregables

El oferente adjudicado deberá obligatoriamente realizar la entrega de los siguientes ítems a la Policía Nacional, quien emitirá un certificado de recepción satisfactoria. Este certificado se constituye en un documento donde la Policía Nacional deja constancia que el oferente adjudicado ha brindado los servicios contratados, y que ha entregado los siguientes:

Documentación del Proceso de Análisis.

Se requiere la presentación del Listado de casos de uso, descripción de casos de uso, diagrama de cada caso de uso, documento de especificación de requerimientos, documento de arquitectura, entre otros

El código fuente versionado deberá estar alojado en los repositorios oficiales de la Policía Nacional. Adicionalmente el oferente adjudicado deberá realizar una copia del código fuente versionado definido por la contratante en los repositorios de código fuente del MITIC

Informe de entrega y evidencias de control de calidad.

Corresponde a un documento donde el oferente declara haber realizado las pruebas necesarias y detalla las funcionalidades entregadas. Deberá estar firmado por el oferente adjudicado o coordinador del mismo e incluir evidencias de las pruebas realizadas.

Manuales:

Manual de instalación para ambiente en desarrollo: Paso a paso de la instalación del software en ambiente de desarrollo

Manual de instalación para ambiente en producción: Paso a paso de la instalación del software en ambiente de producción. Manual del usuario

Otra documentación requerida y especificada por la Policía Nacional.

Instaladores:

En caso de que requiera software no contemplado en los manuales entregados

#### Soporte y asistencia técnica

El oferente adjudicado deberá suministrar asistencia técnica por vía telefónica, e-mail, chat, virtual y/o atención in situ en las oficinas que designe la Policía Nacional para restablecer y corregir el servicio en caso de fallas.

El tiempo mínimo de soporte técnico a ser tenidos en cuenta a partir de la entrega e instalación satisfactoria, será como mínimo de 6 (seis) meses.

El oferente adjudicado indicará cómo realizará el servicio de operación de la asistencia técnica por el tiempo especificado a partir de la emisión del certificado de recepción satisfactoria por parte de la Policía Nacional. El oferente adjudicado, deberá detallar los niveles de servicio (soporte técnico) a ser utilizados para la operación y asistencia técnica del software, y de todo lo que implica la supervisión y el monitoreo.

Durante dicho periodo, igualmente el oferente adjudicado se compromete al suministro de actualizaciones de nuevas versiones del software, como así también la aplicación de parches si es necesario, sin costo adicional para la Policía Nacional.

-Propiedad intelectual y definición de licencias:

Todo código fuente del software o versión de software resultante del proceso licitatorio será de libre disposición por parte de la POLICÍA NACIONAL quien se constituye en propietario / titular del mismo. Quien establecerá el uso, distribución, reproducción, incluyendo además derechos como: extraer partes, copiar, modificar, fusionar y todo aquel uso lícito, a favor de todo o parte del sector público, constituyéndose en licencia de software libre con propiedad intelectual del Estado

#### 12. Criterios de Selección de Oferentes

El oferente debe ser una persona física o jurídica radicada o constituida legalmente en el país.

#### 13. Rubro

Debe pertenecer a rubros relacionados a Tecnologías de la Información y Comunicación, específicamente a desarrollo, mantenimiento y/o implementación de software. En caso de tratarse de una persona jurídica, esto deberá verificarse en el objeto de su Constitución siendo una de las actividades principales

#### 15. Restricciones mínimas de tipo y cantidad de las referencias presentadas Cada referencia deberá corresponder a trabajos de desarrollo de software.

Deberá acompañar evidencia

comprobable, sean contratos, constancias firmadas por el contratante o su representante, u otro documento que respaldatorio de justificación. Mínimo de 3 referencias de clientes.

Al menos 3 referencias deben ser de clientes distintos.

Al menos 2 referencias deben corresponder a trabajos realizados en el Paraguay para organizaciones públicas o privadas radicadas en nuestro país.

#### 16. Restricciones mínimas de montos de las referencias presentadas

La sumatoria de los montos de las referencias presentadas que cumplan los criterios deberá ser como mínimo el 30% del monto referencial de la adquisición.

#### 17. Perfiles técnicos del personal

Para llevar adelante las tareas técnicas en el marco de la presente licitación pondrá a disposición los siguientes perfiles:

1. Un ingeniero en informática o analista de sistemas funcional informática
2. Un desarrollador de software

#### LOTE N° 3 LICENCIA SOFTWARE- ACTIVIDAD 8 DESARROLLO DE SOFTWARE A MEDIDA \_ACT 8

La Policía Nacional deberá indicar explícitamente las especificaciones comunes o generales del software definidas en esta sección, al momento de confeccionar los pliegos de bases y condiciones para la respectiva contratación.

#### Introducción y justificación

La finalidad del presente proceso de adquisición es contar con un sistema de control de las recaudaciones de todas las Oficinas Regionales y casa central. Para la elaboración de cuentas de ingreso para el informe solicitado por el Ministerio de Economía, así como datos estadísticos para la generación de otros informes como el POI, ejecución de metas y otras.

La adquisición Software es a fin de obtener información para generar informe de rendición de cuenta de los ingresos proveniente de las solicitudes de Cédula de Identidad, Pasaporte Policial y Certificado de Antecedentes que son requeridos por el Ministerio de Economía y finanzas y otros entes de control.

#### Submodalidad de adquisición

La su modalidad de adquisición será: Software con requerimientos definidos

#### Objetivo general

Lograr un control preciso de las recaudaciones, trazabilidad de depósitos o transferencias y contar con un mecanismo de auditoria. Objetivos específicos

Facilitar la gestión de las diferentes Oficinas Regionales y Sede Central, facilitar el control y cierre de cajas, control de los depósitos de las recaudaciones y tener informes actualizados de dichos movimientos.

Definiciones, acrónimos y abreviaturas Sistema de gestión de recaudación SGR Antecedentes

El creciente aumento de las transacciones monetarias y aumento en los usuarios de Identificaciones exige tener un mejor y más preciso control de recaudaciones, además de tener automatizados los informes requeridos por el Ministerio de Economía y Finanzas y otros entes de control.

#### Marco legal

La Ley 7280 /2024 de Reforma y Modernización de la Policía Nacional, en su Art.6 inciso 8 Expedir Cédulas de Identidad, Pasaportes, Certificado de Antecedentes, Certificado de Vida y Residencia, permiso de portación de armas de fuego y otros documentos relacionados con sus funciones.

Ley N° 1535/99 de Administración Financiera del Estado y su decreto 8127/00 por la cual se establecen las disposiciones legales y administrativas que reglamentan la implementación de la ley. Ley 6562/2020 DE LA REDUCCIÓN DE LA UTILIZACIÓN DE PAPEL EN LA GESTIÓN PÚBLICA Y SU REEMPLAZO POR EL FORMATO DIGITAL, conocida como Papel Cero.

#### Beneficiarios

Personal de la División Tesorería con 20 usuarios

Usuarios de las 81 Oficinas Regionales y casa central del Departamento de Identificaciones.

Los ciudadanos atreves de la Ley N° 5282 / Libre Acceso Ciudadano a la Información Pública y Transparencia Gubernamental.

#### Infraestructura para el software

Para la implementación y operación del sistema, objeto de este procedimiento de definición y compra, no serán necesarios nuevos equipos de hardware, serán utilizados los equipos que conforman el parque actual de equipos de Institución.

Pc windows 11, hhd 1 tb, 16 Gb RAM Red local conectados con 4pc.

Disco externo de 1 TB para copias de seguridad. Alojado en el Datacenter

#### Confidencialidad

Con la intención de proteger la información que la entidad contratante proporciona a los proveedores (oferentes adjudicados), una vez adjudicado el contrato, debe especificar el grado de privacidad de la información. Es importante precisar la confidencialidad de la información que se entrega para la realización de los estudios o trabajos, diferenciando el tipo de información en caso de requerir aplicar distintos niveles de confidencialidad o publicidad de la información. Así también, respecto de la información que se genere durante la realización de las actividades, y la información producida una vez que se haya concluido el servicio. Deberá incluir, como mínimo, lo siguiente:

- f. El oferente reconoce que la información y documentación que como entidad contratante le proporcione, así como los datos y resultados obtenidos de la prestación de los servicios, son propiedad exclusiva de la entidad contratante, como el carácter confidencial y/o reservado en términos de la normativa aplicable y las disposiciones del contrato.

El oferente se obliga a mantener absoluta confidencialidad sobre las creaciones realizadas, incluyendo todos los algoritmos y toda la información sobre el código fuente y código objeto de las mismas, como respecto de todos sus manuales, incluyendo la documentación preparatoria, su descripción técnica, manuales de uso y cualquier otra documentación relacionada con cualquier actividad realizada por el Desarrollador en virtud del contrato.

Cualquier información, fuese cual fuere su naturaleza (técnica, comercial, financiera, operacional o de otro tipo), contenida en cualquier forma y soporte (ya sea verbal, escrita, grabada o de cualquier otro tipo), que pudiera ser facilitada por la Policía Nacional, será considerada como Información Confidencial, incluyéndose en esta categoría aquella información generada a partir de la propia Información Confidencial.

El desarrollador, se obliga asimismo a:

- g. tratar la Información Confidencial como estrictamente secreta.
- h. custodiar y guardar la Información Confidencial, bien sea escrita, grabada o en cualquier otro tipo de soporte, separada de cualquier otra información de la que pudiera disponer.
- a. utilizar o transmitir la Información Confidencial exclusivamente para los fines del proyecto.

j. utilizar procedimientos de control de dicho uso o transmisión de la Información Confidencial. El desarrollador no realizará copia de la Información Confidencial sin el previo consentimiento escrito dla Policía Nacional, excepto aquellas copias que sean necesitadas por el desarrollador para su estudio interno.

k. restringir el acceso a la Información Confidencial únicamente a aquellos empleados suyos que necesiten conocerla para los fines convenidos, y asegurarse que dichos empleados conocen las obligaciones que les resultan aplicables en virtud de lo establecido en el presente documento. Todos los contratos que el Desarrollador celebrará con empleados, trabajadores y prestadores de servicios que podrían participar en el desarrollo del contrato, incluirán cláusulas sobre confidencialidad y transferencia que producen iguales efectos y sujetan a dichas personas a las mismas obligaciones que el Desarrollador se ha obligado.

no facilitar Información Confidencial a tercero alguno sin el previo consentimiento escrito dla Policía Nacional, y asegurarse de que, en caso de haber obtenido dicha autorización, dicho tercero firme un compromiso de confidencial con la Policía Nacional en términos equivalentes a los de la presente cláusula.

La Policía Nacional será en todo momento el titular exclusivo de la información confidencial, la cual será protegida por todos los medios legales a su alcance. En ningún caso se entenderá implícito en modo alguno, que el hecho de que la Policía Nacional facilite la Información Confidencial significa la concesión de licencia o la cesión de cualquier naturaleza a favor del desarrollador de cualesquiera derechos de patentes, marca, modelo de utilidad, diseño, derechos de autor, o derecho alguno de propiedad intelectual. Ninguna de las partes utilizará el nombre, marca, nombre comercial, o cualesquiera otros derechos de propiedad industrial o intelectual de la otra Parte, sin el previo consentimiento por escrito de ésta, salvo aquellos expresa y contractualmente cedidos.

Toda información que ostente algún derecho de propiedad intelectual de conformidad al derecho positivo que rige a ambas partes, a pesar de ser compartida entre estas, no implicará renuncia alguna a tales derechos, los cuales permanecerán vigentes sobre toda utilización que haga la otra parte de tal información.

La interpretación del concepto de propiedad intelectual no podrá ir más allá de lo establecido en la legislación respectiva. Lo incluido en tales derechos dependerá de lo que le ha sido expresamente reconocido por la autoridad de aplicación, no pudiendo invocarse de lo contrario, derecho alguno.

El desarrollador no podrá utilizar la información y los desarrollos o análisis funcionales elaborados en el cumplimiento de la contratación, para terceros o en beneficio de terceras partes. No podrá utilizar esta información en otras implementaciones que lo coloquen en Situación privilegiada. Toda infracción a esta obligación, lo hará responsable de responder de los daños y perjuicios que pudieran derivarse, así como las sanciones administrativas que correspondan.

La Policía Nacional deberá indicar explícitamente las especificaciones generales del software, definidos en los ítems comunes para la contratación de empresas de software, y adicionalmente los descritos a continuación. Requerimientos

INGRESO bancario.	- Registrar en línea la rendición de los movelistas y cajeros. MOVILISTAS	- Registrar en línea los depósitos en cajero automatizado y/o
<ul style="list-style-type: none"><li>• Generar la planilla de ingresos por comprobantes.</li><li>• Llevar un registro en línea de las diferencias de depósitos (casos monedas o billetes en mal estado).</li><li>• Generar los informes y planillas de recepción.</li><li>• Generar las planillas excel requeridas para control.</li></ul>		
VERIFICACION.	- Programa para verificación de cargas de planillas, se utilizan los datos cargados por movelistas y cajeros en recepción.	
<ul style="list-style-type: none"><li>• Ajustes, modificaciones, observaciones de las recaudaciones en planilla.</li><li>• Programa de consolidación por fechas (días, mes, año).</li><li>• Con capacidad de exportación a Excel.</li><li>• Formulario de carga en forma manual, para casos no previstos.</li></ul>		
VALIDACION informes.	- Generación de reportes para el Ministerio de Economía y Hacienda y otros entes de control. INFORMES	- Estadísticas varias para control e
FINALES.		
<ul style="list-style-type: none"><li>• Informe de auditoría y gestión del mes.</li><li>• Firma con Qr, clave y/o ipad.</li></ul>		
CARGA REMOTA DE	- Link para carga remota de formulario de planilla de rendición. PLANILLAS.	- Validación con depósitos en Banco.
<ul style="list-style-type: none"><li>• Informe de cruzamiento de datos.</li></ul>		
MODULO DE	- Cruce de datos entre rendición de recaudación y depósito bancario y/o cajero automatizado. AUDITORIA.	- Conciliación de cuentas.

MÓDULO GENERAL - Multi usuario.

DEL SISTEMA. - Multi ejercicio fiscal.

- La plataforma tecnológica debe brindar respuestas rápidas y precisas con grandes volúmenes de datos (Big Data). Se solicita que el almacenamiento de datos sea en alta velocidad y permita ejecutar cualquier consulta en forma no planeada para resolver problemas en tiempo real.

#### Requerimientos no funcionales

El sistema deberá contar con alta capacidad de integración que posibiliten los intercambios de información en tiempo y forma: con otros sistemas informáticos de la Policía Nacional, entre otros. El sistema deberá escalable, portable y accesible como también contar con las medidas de seguridad y facilidad de uso y buen rendimiento.

#### Arquitectura general

El Sistema ofrecido debe tener la capacidad de correr sobre un Sistema Operativo Linux Red Hat o Windows Server. Su arquitectura debe ser en 3 capas:

- Presentación o capa web en aplicaciones web (Front end).
- Lógica de negocio o capa aplicativa (Back end).
- La Capa de Datos: Esto comprende el servidor de base de datos. Esta capa se requiere que sea en uno de los motores de base de datos de la Policía Nacional (MySQL, POSTGRESQL)



## Tecnología

El Sistema ofrecido debe tener la capacidad de correr sobre un Sistema Operativo Linux Red Hat o Windows Server.

## Seguridad

CRITERIOS MINIMOS DE SEGURIDAD PARA EL DESARROLLO Y LA ADQUISICION DE SOFTWARE.

1. Todo el software desarrollado debe contar con soporte de software del fabricante. Al momento de la adquisición se debe establecer claramente el tiempo de vida mínimo que se requiere para el software o sistema, y el fabricante debe ofrecer un tiempo de soporte igual o superior a dicho tiempo de vida.
2. En caso de que no sea posible contar con soporte de software del fabricante, el modelo de licenciamiento y la disponibilidad del código fuente debe ser tal que permita a la institución o a otra empresa o desarrollador de software nacional asumir dicho soporte.
3. El fabricante o servicio de soporte debe tener un canal de comunicación y/o mecanismo de reporte de vulnerabilidades o bugs de programación, de manera a que el cliente pueda contactarlo en caso de descubrimiento de vulnerabilidades. En caso de que el reporte ocurra dentro de la ventana de tiempo de vida solicitado, el fabricante o servicio soporte debe ser

capaz de proporcionar una corrección a la vulnerabilidad de manera oportuna, según el acuerdo del nivel del servicio (por sus siglas en inglés, Service Level Agreement o SLA) especificado en el contrato o pliego de bases y condiciones.

4. El software debe poder ser inventariado por herramientas estándar automatizadas de inventario de software basado en el estándar *Common Platform Enumeration* (CPE), debiendo incluir como mínimo la información del nombre, versión, autor y fecha de instalación del mismo.

- Gestión de usuarios, sesiones y privilegios:

1. El software debe permitir una gestión de usuarios de acuerdo a los requerimientos de la

institución, con niveles de privilegios de acuerdo a los roles que éstos requieran (administrador, editor, usuario, etc.), basados en el principio de mínima necesidad de conocimiento.

2. El software debe permitir la revocación de acceso de usuarios, mediante un estado desactivado o similar.
3. Debe ser posible establecer una fecha de expiración para las cuentas de usuarios, a partir de la cual la cuenta deberá entrar a un estado desactivado o similar, hasta tanto se apruebe la continuidad de la misma. El parámetro de fecha de expiración podrá ser fijo o configurable por la institución, de acuerdo a sus requerimientos de negocio.
4. El software debe contemplar la expiración de sesiones de acuerdo a parámetros temporales. Estos parámetros pueden ser fijos o configurables por la institución, de acuerdo a sus requerimientos de negocio.

- Autenticación y gestión de credenciales:

1. El software debe permitir la gestión individual eficaz de credenciales, debiendo permitir que cada usuario sea capaz de cambiar su propia contraseña. Se debe contemplar también mecanismos de recuperación de contraseñas, ya sea a través de un usuario de mayores privilegios o de mecanismos de auto-gestión por parte del usuario. Preferentemente, debe ser posible que al momento de la creación de cuentas permita forzar el cambio de contraseña luego del primer inicio de sesión.

3/62. El software que almacene y/o procese información crítica y/o que se utilice para un proceso crítico de la institución debe soportar autenticación de doble factor para los usuarios de privilegios elevados.

3. El software debe permitir establecer políticas de contraseña, que incluyan, como mínimo, la posibilidad de establecer los siguientes parámetros:
  - a. longitud mínima de la contraseña
  - b. complejidad de contraseña (mayúsculas, minúsculas, números y caracteres especiales, etc.)

Los mencionados parámetros serán configurables por la institución, preferentemente, o en su defecto, deberán ajustarse a los lineamientos y estándares mínimos indicados por la institución.

4. Las contraseñas no deben almacenarse en texto claro, sino mediante la aplicación de funciones hash o funciones resumen. Para el almacenamiento de las contraseñas se debe utilizar funciones criptográficas seguras no reversibles de hash combinadas con salt aplicadas a las contraseñas. Algoritmos aprobados son los siguientes:
  - a. Argon2
  - b. PBKDF2

- c. scrypt
- d. bcrypt

5. De manera alternativa, se puede cifrar las contraseñas utilizando técnicas criptográficas

reversibles únicamente en aquellos casos en que la clave secreta y/o privada de cifrado quede bajo el poder exclusivo del usuario dueño de la contraseña.

- Gestión de registros de auditoría:

1. El software debe ser capaz de generar registros de auditoría de todos los eventos relevantes, con los detalles suficientes para permitir una trazabilidad adecuada, que abarque como mínimo los siguientes eventos:
  - a. inicios de sesión de usuarios (exitosos y fallidos)
  - b. delegación/impersonificación de cuentas de usuarios
  - c. modificación de parámetros del sistema
  - d. gestión de usuarios (cambio de contraseña, creación/eliminación/modificación de usuarios y/o grupos)
  - e. acciones críticas llevadas a cabo por usuarios en el marco del proceso de negocio del sistema (edición de datos sensibles, eliminación de datos, etc.)
2. El software debe contemplar un mecanismo configurable de rotación de registros de auditoría, de acuerdo al parámetro de cantidad de tiempo (diario, semanal, mensual, etc.), como mínimo.

- Cifrado:

1. El software debe cifrar toda la información sensible en tránsito, especialmente aquella información de carácter confidencial y/o cuya integridad deba asegurarse. Para ello se deberán utilizar protocolos de red cifrados, tales como HTTPS, SSH, SCP, SFTP/FTPS, etc.
2. Para sistemas basados en web, se adoptará el modelo SSL/TLS para el cifrado del tráfico. Los protocolos aprobados son TLS v.1.2 o superiores. Los protocolos TLS v.1.1 e inferiores y SSLv3 4/6e inferiores no deben ser utilizados. Se deben seleccionar suites de cifrado robustos; una guía de referencia es:

[https://cheatsheetseries.owasp.org/cheatsheets/TLS\\_Cipher\\_String\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html) Se deben evitar las suites de categoría C o inferiores.

4. Las claves de cifrado deben ser robustas. Se recomienda una longitud de 2048 bits para RSA o equivalente, de acuerdo al estándar NIST SP 800-57. La clave privada debe quedar en poder de la institución, exclusivamente.

- Codificación del software:

1. Se debe utilizar estándares de buenas prácticas seguras de programación, la cual debe ser seleccionada e implementada de acuerdo al lenguaje de programación y el entorno de desarrollo utilizado. Guías de referencia recomendadas son las siguientes:
  - a. SEI CERT Coding Standards <https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards>
  - b. OWASP Secure Coding Practices y OWASP Secure Coding Cheat Sheet [https://www.owasp.org/index.php/OWASP\\_Secure\\_Coding\\_Practices\\_-\\_Quick\\_Reference\\_Guide](https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide)

[https://www.owasp.org/index.php/Secure\\_Coding\\_Cheat\\_Sheet](https://www.owasp.org/index.php/Secure_Coding_Cheat_Sheet)

- c. Oracle Secure Coding Guidelines for Java SE <http://www.oracle.com/technetwork/java/seccodeguide-139067.html>
2. El software debe contemplar un manejo seguro de errores. Se debe realizar y documentar la verificación explícita de errores para todas las entradas, comprobando el tamaño, el tipo de datos, los rangos de valores y/o formatos aceptables de modo a que éstos sean válidos para la operación que están por realizar.
  3. Todos los componentes de terceros utilizados para el desarrollo del software deben estar actualizados a la última versión estable disponible, contar con soporte por un periodo igual o superior al exigido para el proyecto y ser de confianza. Esto es aplicable, pero no limitante, a librerías, *frameworks*, *scripts*, funciones, *plugins*, plantillas, generadores de código, compiladores, entre otros.
  4. Se debe realizar y documentar las pruebas de vulnerabilidades de código, incluyendo análisis estático y dinámico de vulnerabilidades para verificar que se cumplan los estándares mínimos de codificación segura, utilizando herramientas y/o guías de testing de seguridad estándar y aceptados por la industria. Guías de referencia recomendadas son las siguientes:
    - a. OWASP Testing Project: [https://www.owasp.org/index.php/OWASP\\_Testing\\_Project](https://www.owasp.org/index.php/OWASP_Testing_Project)
    - b. Open Source Security Testing Methodology Manual (OSSTMM) <http://www.isecom.org/research/>
    - c. Microsoft Security Development Lifecycle (SDL) - Pasos 10 a 13 <https://www.microsoft.com/es-ES/download/details.aspx?id=12379> <https://www.microsoft.com/en-us/securityengineering/sdl/practices> Plan de trabajo

El oferente deberá presentar en su oferta técnica un cronograma detallado y propuesta de metodología de trabajo que mejor se adecue a lo solicitado en el cronograma general, incluyendo la lista de personal proponente por cada actividad. Según lo dispuesto en la sección [Perfiles técnicos del personal](#).

Entregables

El oferente adjudicado deberá obligatoriamente realizar la entrega de los siguientes ítems a la Policía Nacional, quien emitirá un certificado de recepción satisfactoria. Este certificado se constituye en un documento donde

La Policía Nacional deja constancia que el oferente adjudicado ha brindado los servicios contratados, y que ha entregado los siguientes:

Documentación del Proceso de Análisis.

Se requiere la presentación del Listado de casos de uso, descripción de casos de uso, diagrama de cada caso de uso, documento de especificación de requerimientos, documento de arquitectura, entre otros

El código fuente versionado deberá estar alojado en los repositorios oficiales de la Policía Nacional. Adicionalmente el oferente adjudicado deberá realizar una copia del código fuente versionado definido por la contratante en los repositorios de código fuente del MITIC

Informe de entrega y evidencias de control de calidad.

Corresponde a un documento donde el oferente declara haber realizado las pruebas necesarias y detalla las funcionalidades entregadas. Deberá estar firmado por el oferente

adjudicado o coordinador del mismo e incluir evidencias de las pruebas realizadas.

Manuales:

Manual de instalación para ambiente en desarrollo: Paso a paso de la instalación del software en ambiente de desarrollo

Manual de instalación para ambiente en producción: Paso a paso de la instalación del software en ambiente de producción. Manual del usuario

Otra documentación requerida y especificada por la Policía Nacional.

Instaladores:

En caso de que requiera software no contemplado en los manuales entregados Soporte y asistencia técnica

El oferente adjudicado deberá suministrar asistencia técnica 24/7 por vía telefónica, e-mail, chat, virtual y/o atención in situ en las oficinas que designe la Policía Nacional para restablecer y corregir el servicio en caso de fallas.

El tiempo mínimo de soporte técnico a ser tenidos en cuenta a partir de la entrega e instalación satisfactoria, será como mínimo de 24 meses.

El oferente adjudicado indicará cómo realizará el servicio de operación de la asistencia técnica por el tiempo especificado a partir de la emisión del certificado de recepción satisfactoria por parte de la Policía Nacional. El oferente adjudicado, deberá detallar los niveles de servicio (soporte técnico) a ser utilizados para la operación y asistencia técnica del software, y de todo lo que implica la supervisión y el monitoreo.

Durante dicho periodo, igualmente el oferente adjudicado se compromete al suministro de actualizaciones de nuevas versiones del software, como así también la aplicación de parches si es necesario, sin costo adicional para la Policía Nacional.

-Propiedad intelectual y definición de licencias:

Todo código fuente del software o versión de software resultante del proceso licitatorio será de libre disposición por parte de la POLICÍA NACIONAL quien se constituye en propietario / titular del mismo. Quien establecerá el uso, distribución, reproducción, incluyendo además derechos como: extraer partes, copiar, modificar, fusionar y todo aquel uso lícito, a favor de todo o parte del sector público, constituyéndose en licencia de software libre con propiedad intelectual del Estado

#### Criterios de Selección de Oferentes

El oferente debe ser una persona física o jurídica radicada o constituida legalmente en el país.

#### Rubro

Debe pertenecer a rubros relacionados a Tecnologías de la Información y Comunicación, específicamente a desarrollo, mantenimiento y/o implementación de software. En caso de tratarse de una persona jurídica, esto deberá verificarse en el objeto de su Constitución siendo una de las actividades principales

Restricciones mínimas de tipo y cantidad de las referencias presentadas Cada referencia deberá corresponder a trabajos de desarrollo de software.

La sumatoria de los montos de las referencias presentadas que cumplan los criterios deberá ser como mínimo el 30% del monto referencial de la adquisición.

Para llevar adelante las tareas técnicas en el marco de la presente licitación pondrá a disposición los siguientes perfiles:

1. Un ingeniero en informática o Lic. en análisis de sistemas.
2. Un desarrollador de software.

#### Documentación del Proceso de Análisis.

Se requiere la presentación del Listado de casos de uso, descripción de casos de uso, diagrama de cada caso de uso, documento de especificación de requerimientos, documento de arquitectura, entre otros

El código fuente versionado deberá estar alojado en los repositorios oficiales de la Policía Nacional. Adicionalmente el oferente adjudicado deberá realizar una copia del código fuente versionado definido por la contratante en los repositorios de código fuente del MITIC

Informe de entrega y evidencias de control de calidad.

Corresponde a un documento donde el oferente declara haber realizado las pruebas necesarias y detalla las funcionalidades entregadas. Deberá estar firmado por el oferente adjudicado o coordinador del mismo e incluir evidencias de las pruebas realizadas.

Manuales:

Manual de instalación para ambiente en desarrollo: Paso a paso de la instalación del software en ambiente de desarrollo

Manual de instalación para ambiente en producción: Paso a paso de la instalación del software en ambiente de producción. Manual del usuario

Otra documentación requerida y especificada por la Policía Nacional.

Instaladores:

En caso de que requiera software no contemplado en los manuales entregados

#### LOTE N° 4 ADQUISICIÓN DE SERVICIO DE AMPLIACIÓN Y ACTUALIZACIÓN DE SISTEMAS DE ADMISIÓN Y COBRANZAS - ISEPOL- ACTIVIDAD 6

La Policía Nacional deberá indicar explícitamente las especificaciones comunes o generales del software definidas en esta sección, al momento de confeccionar los pliegos de bases y condiciones para la respectiva contratación.

## Introducción y justificación

La finalidad del presente proceso de adquisición de SERVICIO DE AMPLIACIÓN Y ACTUALIZACIÓN DE SISTEMAS DE ADMISIÓN Y COBRANZAS es a modo de permitir la agilización en el sistema de cobranzas para satisfacer las necesidades de análisis e informes. El diseño de software de base de datos también permitirá la creación, implementación y mantenimiento de un sistema de gestión de datos en toda la organización, como ser los diferentes cursos y sus alumnos.

## Submodalidad de adquisición

La submodalidad de adquisición será: Software con requerimientos definidos

## Objetivo general

Lograr mejorar y actualizar el sistema de cobranzas en línea dando transparencia al proceso, como así también la lista de cursos y sus alumnos.

## Objetivos específicos

Facilitar la gestión de los Cobros a través de pasarelas de pagos, definir y llevar la lista de cursos y sus alumnos, programar las clases a través de las plataformas virtuales.

**Definiciones, acrónimos y abreviaturas** Sistema de Admisión y Cursantes. SAC.

## Antecedentes

El creciente número de estudiantes quienes año tras año se vuelcan a formarse en las diversas disciplinas dictadas en el ISEPOL obliga a establecer procedimientos y facilidades para el cobro de los aranceles, como así también llevar el control de cursos y alumnos.

## Marco legal

Decreto N° 361 POR EL CUAL SE REGLAMENTA LA LEY N° 7110/2023 «DE SIMPLIFICACIÓN DE TRÁMITES PARA LA GESTIÓN Y EXPEDICIÓN DE TÍTULOS EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR DEL PARAGUAY Y REGISTROS DE TÍTULOS ANTE EL VICEMINISTRO DE EDUCACIÓN SUPERIOR Y CIENCIAS»

LEY 6562 DE LA REDUCCIÓN DE LA UTILIZACIÓN DE PAPEL EN LA GESTIÓN PÚBLICA Y SU REEMPLAZO POR EL FORMATO DIGITAL

## Beneficiarios

Estudiantes en General, Tesorería, Cajeros, Administración Académica.

## Infraestructura para el software

necesarios nuevos equipos de hardware, serán utilizados los equipos que conforman el parque actual de equipos de la ISEPOL. Detalle y tipo de servidores (máquinas virtuales, contenedores, sistemas operativos, sistemas de virtualización, entre otros), Servidores: SERVIDOR DELL PowerEdge R820

Máquinas Virtuales y Contenedores: Virtualizador Proxmox V.8.2 (estable) Sistemas Operativos: Linux distribución Debian v.12

Sistema de Virtualización: Proxmox Estaciones de trabajo:

Cantidad aproximada de estaciones de trabajo (PC, notebook, dispositivos móviles) que tiene la Policía Nacional destinada para el uso de los sistemas a adquirir, para ello se destaca que los usuarios acceden desde sus dispositivos particulares (notebook, celular, etc) siendo de 600 usuarios simultáneamente, con conexión dispar de usuarios aproximadamente a 1.200 usuarios en total.

La Policía Nacional deberá definir y describir dónde estará alojada la solución y los equipos necesarios para su correcto funcionamiento, especificando mínimamente:

Datacenter: Ubicado en el Departamento de Informática de la Policía Nacional (Datacenter tipo Contenedor), con generador, UPS para los Servidores, Dispositivos sensor de Humedad, humos, llamas, extintores de incendios con polvo seco (para electrónicas).

El responsable del datacenter es la División TIC del Departamento de Informática de la Policía Nacional, bajo la supervisión de un Oficial Superior con diligencia en el área técnica y quien trabaja en coordinación directa con la jefatura del Departamento de Informática.

Se utilizan los dominios de la Institución y se encuentra abierta para trabajar en conexión externa a dominios generados por terceros. Los servicios de dominios se establecen por medio de una IP Pública.

## Confidencialidad

Con la intención de proteger la información que la entidad contratante proporciona a los proveedores (oferentes adjudicados), una vez adjudicado el contrato, debe especificar el grado de privacidad de la información. Es importante precisar la confidencialidad de la información que se entrega para la realización de los estudios o trabajos, diferenciando el tipo de información en caso de requerir aplicar distintos niveles de confidencialidad o publicidad de la información. Así también, respecto de la información que se genere durante la realización de las actividades, y la información producida una vez que se haya concluido el servicio. Deberá incluir, como mínimo, lo siguiente:

El oferente reconoce que la información y documentación que como entidad contratante le proporcione, así como los datos y resultados obtenidos de la prestación de los servicios, son propiedad exclusiva de la entidad contratante, como el carácter confidencial y/o reservado en términos de la normativa aplicable y las disposiciones del contrato.

El oferente se obliga a mantener absoluta confidencialidad sobre las creaciones realizadas, incluyendo todos los algoritmos y toda la información sobre el código fuente y código objeto de las mismas, como respecto de todos sus manuales, incluyendo la documentación preparatoria, su descripción técnica, manuales de uso y cualquier otra documentación relacionada con cualquier actividad realizada por el Desarrollador en virtud del contrato.

Cualquier información, fuese cual fuere su naturaleza (técnica, comercial, financiera, operacional o de otro tipo), contenida en cualquier forma y soporte (ya sea verbal, escrita, grabada o de cualquier otro tipo), que pudiera ser facilitada por la Policía Nacional, será considerada como Información Confidencial, incluyéndose en esta categoría aquella información generada a partir de la propia Información Confidencial.

El desarrollador, se obliga asimismo a:

- a. tratar la Información Confidencial como estrictamente secreta.
- b. custodiar y guardar la Información Confidencial, bien sea escrita, grabada o en cualquier otro tipo de soporte, separada de cualquier otra información de la que pudiera disponer.

- a. utilizar o transmitir la Información Confidencial exclusivamente para los fines del proyecto.
- b. utilizar procedimientos de control de dicho uso o transmisión de la Información Confidencial. El desarrollador no realizará copia de la Información Confidencial sin el previo consentimiento escrito dla Policía Nacional, excepto aquellas copias que sean necesitadas por el desarrollador para su estudio interno.
- c. restringir el acceso a la Información Confidencial únicamente a aquellos empleados suyos que necesiten conocerla para los fines convenidos, y asegurarse que dichos empleados conocen las obligaciones que les resultan aplicables en virtud de lo establecido en el presente documento. Todos los contratos que el Desarrollador celebrará con empleados, trabajadores y prestadores de servicios que podrían participar en el desarrollo del contrato, incluirán cláusulas sobre confidencialidad y transferencia que producen iguales efectos y sujetan a dichas personas a las mismas obligaciones que el Desarrollador se ha obligado.
- d. no facilitar Información Confidencial a tercero alguno sin el previo consentimiento escrito dla Policía Nacional, y asegurarse de que, en caso de haber obtenido dicha autorización, dicho tercero firme un compromiso de confidencial con la Policía Nacional en términos equivalentes a los de la presente cláusula.

La Policía Nacional será en todo momento el titular exclusivo de la información confidencial, la cual será protegida por todos los medios legales a su alcance. En ningún caso se entenderá implícito en modo alguno, que el hecho de que la Policía Nacional facilite la Información Confidencial significa la concesión de licencia o la cesión de cualquier naturaleza a favor del desarrollador de cualesquiera derechos de patentes, marca, modelo de utilidad, diseño, derechos de autor, o derecho alguno de propiedad intelectual. Ninguna de las partes utilizará el nombre, marca, nombre comercial, o cualesquiera otros derechos de propiedad industrial o intelectual de la otra Parte, sin el previo consentimiento por escrito de ésta, salvo aquellos expresa y contractualmente cedidos.

Toda información que ostente algún derecho de propiedad intelectual de conformidad al derecho positivo que rige a ambas partes, a pesar de ser compartida entre estas, no implicará renuncia alguna a tales derechos, los cuales permanecerán vigentes sobre toda utilización que haga la otra parte de tal información.

La interpretación del concepto de propiedad intelectual no podrá ir más allá de lo establecido en la legislación respectiva. Lo incluido en tales derechos dependerá de lo que le ha sido expresamente reconocido por la autoridad de aplicación, no pudiendo invocarse de lo contrario, derecho alguno.

El desarrollador no podrá utilizar la información y los desarrollos o análisis funcionales elaborados en el cumplimiento de la contratación, para terceros o en beneficio de terceras partes. No podrá utilizar esta información en otras implementaciones que lo coloquen en

situación privilegiada. Toda infracción a esta obligación, lo hará responsable de responder de los daños y perjuicios que pudieran derivarse, así como las sanciones administrativas que correspondan.

La Policía Nacional deberá indicar explícitamente las especificaciones generales del software, definidos en los ítems comunes para la contratación de empresas de software, y adicionalmente los descritos a continuación. [Requerimientos](#)

- MOODLE.
- Actualización Plataforma E-Learning.
- Actualización de contraseñas Moodle, administradores gestores.
- Pre grado.
* Habilitación de Filiales.
* Habilitación de cursos.
* Habilitación de Materias por cursos.
* Habilitación y carga de lista de Profesores.
* Habilitación y carga de Alumnos.
* Renovación de Dominio.

* Capacitación.
- Post grado.
* Habilitación de Filiales.
* Habilitación de Cursos.
* Habilitación de Materias por cursos.
* Habilitación y carga de lista de Profesores.
* Habilitación y carga de Alumnos.
* Capacitación.
- Grado.
* Habilitación de Filiales.
* Habilitación de Cursos.
* Habilitación de Materias por cursos.
* Habilitación y carga de lista de Profesores.
* Habilitación y carga de Alumnos.
* Renovación de Dominio.
* Capacitación.
- Soporte permanente durante 1 año.
PAGINA WEB ISEPOL.

- Ajuste y actualización de la pagina Web Isepol.
- Inclusión de nuevos botones de acceso a sistemas varios.
- Soporte permanente durante 1 año.
ADMISION DE POSTULANTES.
Desarrollo de Nueva Plataforma a modo de Separar ADMISION del SISTEMA de ALMNOS PERMANENTES (CURSANTES)
- Puesta a punto del sistema de Admisión para el periodo 2026
- Actualización de Láminas 2026.
- Actualización de cartillas 2026.
- Reinicio de Base de Datos para postulantes 2026.
- Desbloqueo del Sistema.
- Planificación de periodos de carga, verificación y aprobación de postulantes.
- Modificación del Web Service 1 para los nuevos costos de aranceles.
- Reinicio de Base de datos a cero para el nuevo periodo de Inscripciones.
- Organización y preparación del equipo de soporte.
- Confección de nuevos informes estadísticos.
- Capacitación de verificadores y equipo de soporte.
- Administración de las nuevas contraseñas para verificadores.

- Seguimiento 24/7 desde el inicio del proceso hasta los exámenes de ingreso.

- Verificación y seguimiento a copias de seguridad.

- Entrega de todos los fuentes modificados y desarrollados para el Sistema.

- Soporte durante 1 año.

- Contar con las Licencias necesarias.

#### ALUMNOS PERMANENTES (CURSANTES)

- Reingeniería Total del Sistema de Cursantes pasará de ser plataforma de pago a plataforma de Pago y seguimiento Académico.

- Relevamiento y re diseño de la Base de Datos.

- Modificaciones de todos los programas para la nueva versión (80 programas aproximadamente).

- Carga de Datos en forma masiva desde planillas.

- Transferencia de Datos de la actual BD a la Nueva, con su correspondiente control de calidad.

- Modificación del Web Service 2 para la inclusión de nuevos aranceles con multas.

- Modificación del Web Service 2 para ajustar los nuevos costos de aranceles.

- Capacitación de la nueva versión.

- Soporte durante 1 año.



- Contar con las Licencias necesarias.

#### Requerimientos no funcionales

El sistema deberá contar con alta capacidad de integración que posibiliten los intercambios de información en tiempo y forma: con otros sistemas informáticos de la Policía Nacional, Registro Civil, proveedores, contratistas, entre otros.

#### Arquitectura general

El Sistema ofrecido debe tener la capacidad de correr sobre un Sistema Operativo Linux Red Hat o Windows Server. Su arquitectura debe ser en 3 capas:

La Capa de Datos: Esto comprende el servidor de base de datos. Esta capa se requiere que sea en uno de los motores de base de datos de la Policía Nacional (MySQL, POSTGRESQL).

#### Tecnología

El Sistema ofrecido debe tener la capacidad de correr sobre un Sistema Operativo Linux Red Hat o Windows Server.

#### Seguridad

##### CRITERIOS MINIMOS DE SEGURIDAD PARA EL DESARROLLO Y LA ADQUISICION DE SOFTWARE.

##### -Soporte y gestión continua del software:

1. Todo el software desarrollado debe contar con soporte de software del fabricante. Al momento de la adquisición se debe establecer claramente el tiempo de vida mínimo que se requiere para el software o sistema, y el fabricante debe ofrecer un tiempo de soporte igual o superior a dicho tiempo de vida.
2. En caso de que no sea posible contar con soporte de software del fabricante, el modelo de

licenciamiento y la disponibilidad del código fuente debe ser tal que permita a la institución o a otra empresa o desarrollador de software nacional asumir dicho soporte.

3. El fabricante o servicio de soporte debe tener un canal de comunicación y/o mecanismo de reporte de vulnerabilidades o bugs de programación, de manera a que el cliente pueda contactarlo en caso de descubrimiento de vulnerabilidades. En caso de que el reporte ocurra dentro de la ventana de tiempo de vida solicitado, el fabricante o servicio soporte debe ser

capaz de proporcionar una corrección a la vulnerabilidad de manera oportuna, según el acuerdo del nivel del servicio (por sus siglas en inglés, Service Level Agreement o SLA) especificado en el contrato o pliego de bases y condiciones.

4. El software debe poder ser inventariado por herramientas estándar automatizadas de inventario de software basados en el estándar *Common Platform Enumeration* (CPE), debiendo incluir como mínimo la información del nombre, versión, autor y fecha de instalación del mismo.

##### - Gestión de usuarios, sesiones y privilegios:

1. El software debe permitir una gestión de usuarios de acuerdo a los requerimientos de la

institución, con niveles de privilegios de acuerdo a los roles que éstos requieran (administrador, editor, usuario, etc.), basados en el principio de mínima necesidad de conocimiento.

2. El software debe permitir la revocación de acceso de usuarios, mediante un estado desactivado o similar.
3. Debe ser posible establecer una fecha de expiración para las cuentas de usuarios, a partir de la cual la cuenta deberá entrar a un estado desactivado o similar, hasta tanto se apruebe la continuidad de la misma. El parámetro de fecha de expiración podrá ser fijo o configurable por la institución, de acuerdo a sus requerimientos de negocio.
4. El software debe contemplar la expiración de sesiones de acuerdo a parámetros temporales. Estos parámetros pueden ser fijos o configurables por la institución, de acuerdo a sus requerimientos de negocio.

##### - Autenticación y gestión de credenciales:

1. El software debe permitir la gestión individual eficaz de credenciales, debiendo permitir que cada usuario sea capaz de cambiar su propia contraseña. Se debe contemplar también mecanismos de recuperación de contraseñas, ya sea a través de un usuario de mayores privilegios o de mecanismos de auto-gestión por parte del usuario. Preferentemente, debe ser posible que al momento de la creación de cuentas permita forzar el cambio de contraseña luego del primer inicio de sesión.

3/62. El software que almacene y/o procese información crítica y/o que se utilice para un proceso crítico de la institución debe soportar autenticación de doble factor para los usuarios de privilegios elevados.

3. El software debe permitir establecer políticas de contraseña, que incluyan, como mínimo, la posibilidad de establecer los siguientes parámetros:
  - a. longitud mínima de la contraseña
  - b. complejidad de contraseña (mayúsculas, minúsculas, números y caracteres especiales, etc.)

Los mencionados parámetros serán configurables por la institución, preferentemente, o en su defecto, deberán ajustarse a los lineamientos y estándares mínimos indicados por la institución.

4. Las contraseñas no deben almacenarse en texto claro, sino mediante la aplicación de funciones hash o funciones resumen. Para el almacenamiento de las contraseñas se debe utilizar funciones criptográficas seguras no reversibles de hash combinadas con salt aplicadas a las contraseñas. Algoritmos aprobados son los siguientes:
  - a. Argon2
  - b. PBKDF2
  - c. scrypt
  - d. bcrypt
5. De manera alternativa, se puede cifrar las contraseñas utilizando técnicas criptográficas

reversibles únicamente en aquellos casos en que la clave secreta y/o privada de cifrado quede bajo el poder exclusivo del usuario dueño de la contraseña.

#### Gestión de registros de auditoría:

1. El software debe ser capaz de generar registros de auditoría de todos los eventos relevantes, con los detalles suficientes para permitir una trazabilidad adecuada, que abarque como mínimo los siguientes eventos:
  - a. inicios de sesión de usuarios (exitosos y fallidos)
  - b. delegación/impersonificación de cuentas de usuarios
  - c. modificación de parámetros del sistema
  - d. gestión de usuarios (cambio de contraseña, creación/eliminación/modificación de usuarios y/o grupos)
  - e. acciones críticas llevadas a cabo por usuarios en el marco del proceso de negocio del sistema (edición de datos sensibles, eliminación de datos, etc.)
2. El software debe contemplar un mecanismo configurable de rotación de registros de auditoría, de acuerdo al parámetro de cantidad de tiempo (diario, semanal, mensual, etc.), como mínimo.

#### Cifrado:

1. El software debe cifrar toda la información sensible en tránsito, especialmente aquella información de carácter confidencial y/o cuya integridad deba asegurarse. Para ello se deberán utilizar protocolos de red cifrados, tales como HTTPS, SSH, SCP, SFTP/FTPS, etc.
2. Para sistemas basados en web, se adoptará el modelo SSL/TLS para el cifrado del tráfico. Los protocolos aprobados son TLS v.1.2 o superiores. Los protocolos TLS v.1.1 e inferiores y SSLv3 4/6e inferiores no deben ser utilizados. Se deben seleccionar suites de cifrado robustos; una guía de referencia es:

[https://cheatsheetseries.owasp.org/cheatsheets/TLS\\_Cipher\\_String\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html)

3. Se deben evitar las suites de categoría C o inferiores.

Las claves de cifrado deben ser robustas. Se recomienda una longitud de 2048 bits para RSA o equivalente, de acuerdo al estándar NIST SP 800-57. La clave privada debe quedar en poder de la institución, exclusivamente.

#### Codificación del software:

1. Se debe utilizar estándares de buenas prácticas seguras de programación, la cual debe ser seleccionada e implementada de acuerdo al lenguaje de programación y el entorno de desarrollo utilizado. Guías de referencia recomendadas son las siguientes:
  - a. SEI CERT Coding Standards <https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards>
  - b. OWASP Secure Coding Practices y OWASP Secure Coding Cheat Sheet [https://www.owasp.org/index.php/OWASP\\_Secure\\_Coding\\_Practices\\_-\\_Quick\\_Reference\\_Guide](https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide)

[https://www.owasp.org/index.php/Secure\\_Coding\\_Cheat\\_Sheet](https://www.owasp.org/index.php/Secure_Coding_Cheat_Sheet)

- c. Oracle Secure Coding Guidelines for Java SE <http://www.oracle.com/technetwork/java/seccodeguide-139067.html>
2. El software debe contemplar un manejo seguro de errores. Se debe realizar y documentar la verificación explícita de errores para todas las entradas, comprobando el tamaño, el tipo de datos, los rangos de valores y/o formatos aceptables de modo a que éstos sean válidos para la operación que están por realizar.
  3. Todos los componentes de terceros utilizados para el desarrollo del software deben estar actualizados a la última versión estable disponible, contar con soporte por un periodo igual o superior al exigido para el proyecto y ser de confianza. Esto es aplicable, pero no limitante, a librerías, *frameworks*, *scripts*, funciones, *plugins*, plantillas, generadores de código, compiladores, entre otros.
  4. Se debe realizar y documentar las pruebas de vulnerabilidades de código, incluyendo análisis estático y dinámico de vulnerabilidades para verificar que se cumplan los estándares mínimos de codificación segura, utilizando herramientas y/o guías de testing de seguridad estándar y aceptados por la industria. Guías de referencia recomendadas son las siguientes:
    - a. OWASP Testing Project: [https://www.owasp.org/index.php/OWASP\\_Testing\\_Project](https://www.owasp.org/index.php/OWASP_Testing_Project)
    - b. Open Source Security Testing Methodology Manual (OSSTMM) <http://www.isecom.org/research/>
    - c. Microsoft Security Development Lifecycle (SDL) - Pasos 10 a 13 <https://www.microsoft.com/es-ES/download/details.aspx?id=12379>  
<https://www.microsoft.com/en-us/securityengineering/sdl/practices> Plan de trabajo

El oferente deberá presentar en su oferta técnica un cronograma detallado y propuesta de metodología de trabajo que mejor se adecue a lo solicitado en el cronograma general, incluyendo la lista de personal proponente por cada actividad. Según lo dispuesto en la sección [Perfiles técnicos del personal](#).

#### Entregables

El oferente adjudicado deberá obligatoriamente realizar la entrega de los siguientes ítems a la Policía Nacional, quien emitirá un certificado de recepción satisfactoria. Este certificado se constituye en un documento donde la Policía Nacional deja constancia que el oferente adjudicado ha brindado los servicios contratados, y que ha entregado los siguientes:

Documentación del Proceso de Análisis.

La Policía Nacional deberá establecer la documentación y nivel de detalle que requiera. Ejemplo: Listado de casos de uso, descripción de casos de uso, diagrama de cada caso de uso, documento de especificación de requerimientos, documento de arquitectura, entre otros.

Código Fuente en los repositorios oficiales de la Policía Nacional. Informe de entrega y evidencias de control de calidad.

Corresponde a un documento donde el oferente declara haber realizado las pruebas necesarias y detalla las funcionalidades entregadas. Deberá estar firmado por el oferente adjudicado o coordinador del mismo e incluir evidencias de las pruebas realizadas.

Manuales:

Manual de instalación para ambiente en desarrollo: Paso a paso de la instalación del software en ambiente de desarrollo. Manual de instalación para ambiente en producción: Paso a paso de la instalación del software en ambiente de producción. Manual del usuario. La Policía Nacional deberá especificar el detalle del manual requerido. Ej: por tipo de perfil.

Otra documentación requerida y especificada por la Policía Nacional. Instaladores:

En caso de que requiera software no contemplado en los manuales entregados.

#### Soporte y asistencia técnica

El oferente adjudicado deberá suministrar asistencia técnica por vía telefónica, e-mail, chat, virtual y/o atención in situ en las oficinas que designe la Policía Nacional para restablecer y corregir el servicio en caso de fallas.

El tiempo mínimo de soporte técnico a ser tenidos en cuenta a partir de la entrega e instalación satisfactoria, será como mínimo de 6 (seis) meses.

El oferente adjudicado indicará cómo realizará el servicio de operación de la asistencia técnica por el tiempo especificado a partir de la emisión del certificado de recepción satisfactoria por parte de la Policía Nacional. El oferente adjudicado, deberá detallar los niveles de servicio (soporte técnico) a ser utilizados para la operación y asistencia técnica del software, y de todo lo que implica la supervisión y el monitoreo.

Durante dicho periodo, igualmente el oferente adjudicado se compromete al suministro de actualizaciones de nuevas versiones del software, como así también la aplicación de parches si es necesario, sin costo adicional para la Policía Nacional.

- Condiciones sobre propiedad intelectual, derechos de autor y otros derechos asociados al Desarrollo del Software

La titularidad de los derechos de propiedad intelectual y en especial de los derechos de autor que existan respecto al software desarrollado se considera y establece, a efectos de la contratación realizada, que es cedida por los autores materiales del mismo enteramente a favor de Estado Paraguayo en la persona jurídica o entidad/organismo contratante, por haber sido creados en cumplimiento de una relación laboral de la institución con requerimientos definidos

El desarrollador debe garantizar que todo el producto desarrollado no infringe derechos de propiedad intelectual de terceros y es cedido en su totalidad, incluyendo todos sus componentes, al organismo contratante.

Se establece que el Desarrollador (ya sea funcionario, contratado, firma unipersonal o empresa) transfiere en forma exclusiva y perpetua a la Policía Nacional todos los derechos de propiedad intelectual, propiedad industrial y cualquier otro derecho cuya titularidad y propiedad corresponda al Desarrollador, sobre programas computacionales, obras, creaciones, invenciones, ideas, conocimientos, knowhow, productos, objetos, elementos, tecnología o información que no habiendo sido especialmente desarrollada, creada, realizada o concebida por el Desarrollador para el cumplimiento de este contrato, haya sido utilizada por el Desarrollador en el cumplimiento del contrato

- Definición de licencias de software de titularidad del Estado por parte de la Policía Nacional

Todo el software y asociados al mismo resultante serán propiedad del Ministerio del Interior quien en su carácter de titular de dicho software establecerá el uso y/o disposición.

- Criterios de Selección de Oferentes

El oferente debe ser una persona física o jurídica radicada o constituida legalmente en el país.

- Rubro

Debe pertenecer a rubros relacionados a Tecnologías de la Información y Comunicación, específicamente a desarrollo, mantenimiento y/o implementación de software. En caso de tratarse de una persona jurídica, esto deberá verificarse en el objeto de su Constitución siendo una de las actividades principales

- Restricciones mínimas de tipo y cantidad de las referencias presentadas Cada referencia deberá corresponder a trabajos de desarrollo de software.

Deberá acompañar evidencia

comprobable, sean contratos, constancias firmadas por el contratante o su representante, u otro documento que respaldatorio de justificación. Mínimo de 3 referencias de clientes.

Al menos 3 referencias deben ser de clientes distintos.

Al menos 2 referencias deben corresponder a trabajos realizados en el Paraguay para organizaciones públicas o privadas radicadas en nuestro país.

- Restricciones mínimas de montos de las referencias presentadas

La sumatoria de los montos de las referencias presentadas que cumplan los criterios deberá ser como mínimo el 30% del monto referencial de la adquisición.

- Perfiles técnicos del personal

Para llevar adelante las tareas técnicas en el marco de la presente licitación pondrá a Disposición los siguientes perfiles:

1. Un líder o coordinador TIC del proyecto.
2. Al menos un analista funcional con perfil técnico del área de análisis de software. Tipo de Perfil técnico del oferente

Disposición los siguientes perfiles:

1. Un ingeniero en informática
2. Un técnico-desarrollador de software.

Debiendo presentar CV de cada uno de los RR.HH. propuestos, que deberán estar firmados por cada uno de ellos, y deberán declarar su compromiso a formar parte del equipo de trabajo en caso de resultar adjudicado En caso de que uno de los recursos no participe al inicio o deje de formar parte durante el proceso de desarrollo por algún motivo, para dichos casos el oferente deberá reemplazarlo por otro de equivalente perfil al solicitado o superior y notificar por nota el cambio realizado, adjuntando nuevamente el CV del recurso que se incorpora al equipo de desarrollo conforme a lo requerido anteriormente.

-Propiedad intelectual y definición de licencias:

Todo código fuente del software o versión de software resultante del proceso licitatorio será de libre disposición por parte de la POLICÍA NACIONAL quien se constituye en propietario / titular del mismo. Quien establecerá el uso, distribución, reproducción, incluyendo además derechos como: extraer partes, copiar, modificar, fusionar y todo aquel uso lícito, a favor de todo o parte del sector público, constituyéndose en licencia de software libre con propiedad intelectual del Estado

Documentación del Proceso de Análisis.

Se requiere la presentación del Listado de casos de uso, descripción de casos de uso, diagrama de cada caso de uso, documento de especificación de requerimientos, documento de arquitectura, entre otros

El código fuente versionado deberá estar alojado en los repositorios oficiales de la Policía Nacional. Adicionalmente el oferente adjudicado deberá realizar una copia del código fuente versionado definido por la contratante en los repositorios de código fuente del MITIC

Informe de entrega y evidencias de control de calidad.

Corresponde a un documento donde el oferente declara haber realizado las pruebas necesarias y detalla las funcionalidades entregadas. Deberá estar firmado por el oferente adjudicado o coordinador del mismo e incluir evidencias de las pruebas realizadas.

Manuales:

Manual de instalación para ambiente en desarrollo: Paso a paso de la instalación del software en ambiente de desarrollo

Manual de instalación para ambiente en producción: Paso a paso de la instalación del software en ambiente de producción.

Manual del usuario

Otra documentación requerida y especificada por la Policía Nacional.

Instaladores:

En caso de que requiera software no contemplado en los manuales entregados

LOTE N° 5 DESARROLLO DEL SISTEMA DE GESTION DE CERTIFICADOS, ANTECEDENTES E INFORME DE HISTORIAL ACADEMICO Y MESA DE ENTRADAS - ISEPOL- ACTIVIDAD 6

Especificaciones Técnicas

1. Análisis, definición y desarrollo de una BD, para integración con el sistema de alumnos permanentes (Cursantes).

- Bd para reportes de novedades de alumnos.
- Validaciones de datos.

2. Plataforma de acceso publico para solicitud de antecedente académico

- Bd para solicitud de antecedente academicos.

\* Link para acceso pu

isepol.edu.py.

\* Acceso a través de

- Modificación de la página de Isepol.edu.ý a modo de agregar el boton de acceso al nuevo

link.

\* Modulo de carga de datos del s

- Modulo de carga de documentos digitales solicitados.
- Pago de arancel vía plataforma de pago, ajuste del web service entre isepol y la pasarela de pago.

\* Recepción del certificado a través del correo registrado por el solicitante.

3. Plataforma de acceso oficial para solicitud de antecedentes académicos (uso interno)

- Acceso a través de usuario y contraseña y administración de las mismas.
- Módulo para revisión de solicitudes de antecedentes Académicos.
- Aprobación de documentos y generación automática de deuda para pasarela de pago.
- Carga y generación del antecedente académico.
- Envío automático del antecedente académico.
- Carga de novedades académicas por parte de las diferentes unidades.
- Reportes diarios y semanales.
- Estadísticas varias.

#### 4. Criterios mínimos de seguridad para el Desarrollo y Adquisición de Software.

##### Soporte y gestión continua del software:

1. Todo el software desarrollado debe contar con soporte de software del fabricante. Al momento de la adquisición se debe establecer claramente el tiempo de vida mínimo que se requiere para el software o sist igual o superior a dicho tiempo de vida.

2. En caso de que no sea posible contar con soporte de software del fabricante, el modelo de

licenciamiento y la disponibilidad del código fuente debe ser tal que permita a la institución o a otra empresa o desarrollador de software nacional asumir dicho soporte.

3. El fabricante o servicio de soporte debe tener un canal de comunicación y/o mecanismo de

reporte de vulnerabilidades o bugs de programación, de manera a que el cliente pueda

contactarlo en caso de descubrimiento de vulnerabilidades. En caso de que el reporte ocurra

dentro de la ventana de tiempo de vida solicitado, el fabricante o servicio soporte debe ser

capaz de proporcionar una corrección a la vulnerabilidad de manera oportuna, según el acuerdo del nivel del servicio (por sus siglas en inglés, Service Level Agreement o SLA) especificado en el contrato o pliego

4. El software debe poder ser inventariado por herramientas estándar automatizadas de inventario de software basados en el estándar Common Platform Enumeration (CPE), debiendo incluir como mínimo la in instalación del mismo.

##### Gestión de usuarios, sesiones y privilegios:

1. El software debe permitir una gestión de usuarios de acuerdo a los requerimientos de la

institución, con niveles de privilegios de acuerdo a los roles que éstos requieran (administrador, editor, usuario, etc.), basados en el principio de mínima necesidad de conocimiento.

2. El software debe permitir la revocación de acceso de usuarios, mediante un estado

desactivado o similar.

3. Debe ser posible establecer una fecha de expiración para las cuentas de usuarios, a partir de la cual la cuenta deberá entrar a un estado desactivado o similar, hasta tanto se apruebe la continuidad de la misma configurable por la institución, de acuerdo a sus requerimientos de negocio.

4. El software debe contemplar la expiración de sesiones de acuerdo a parámetros temporales.

Estos parámetros pueden ser fijos o configurables por la institución, de acuerdo a sus

requerimientos de negocio.

Autenticación y gestión de credenciales:

1. El software debe permitir la gestión individual eficaz de credenciales, debiendo permitir que cada usuario sea capaz de cambiar su propia contraseña. Se debe contemplar también mecanismos de recuperación mayores privilegios o de mecanismos de auto-gestión por parte del usuario. Preferentemente, debe ser posible que al momento de la creación de cuentas permita forzar el cambio de contraseña luego del primer

3/62. El software que almacene y/o procese información crítica y/o que se utilice para un proceso crítico de la institución debe soportar autenticación de doble factor para los usuarios de privilegios elevados.

3. El software debe permitir establecer políticas de contraseña, que incluyan, como mínimo, la posibilidad de establecer los siguientes parámetros:

a. longitud mínima de la contraseña

b. complejidad de contraseña (mayúsculas, minúsculas, números y caracteres especiales,

etc.)

Los mencionados parámetros serán configurables por la institución, preferentemente, o en su

defecto, deberán ajustarse a los lineamientos y estándares mínimos indicados por la institución.

4. Las contraseñas no deben almacenarse en texto claro, sino mediante la aplicación de funciones hash o funciones resumen. Para el almacenamiento de las contraseñas se debe utilizar funciones criptográficas aplicadas a las contraseñas. Algoritmos aprobados son los siguientes:

a. Argon2

b. PBKDF2

c. scrypt

d. bcrypt

5. De manera alternativa, se puede cifrar las contraseñas utilizando técnicas criptográficas

reversibles únicamente en aquellos casos en que la clave secreta y/o privada de cifrado quede bajo el poder exclusivo del usuario dueño de la contraseña.

Gestión de registros de auditoría:

1. El software debe ser capaz de generar registros de auditoría de todos los eventos relevantes, con los detalles suficientes para permitir una trazabilidad adecuada, que abarque como mínimo los siguientes even

a. inicios de sesión de usuarios (exitosos y fallidos)

b. delegación/impersonificación de cuentas de usuarios

c. modificación de parámetros del sistema

d. gestión de usuarios (cambio de contraseña, creación/eliminación/modificación de

usuarios y/o grupos)

e. acciones críticas llevadas a cabo por usuarios en el marco del proceso de negocio del

sistema (edición de datos sensibles, eliminación de datos, etc.)

2. El software debe contemplar un mecanismo configurable de rotación de registros de auditoría, de acuerdo al parámetro de cantidad de tiempo (diario, semanal, mensual, etc.), como mínimo.

Cifrado:

1. El software debe cifrar toda la información sensible en tránsito, especialmente aquella

información de carácter confidencial y/o cuya integridad deba asegurarse. Para ello se deberán

utilizar protocolos de red cifrados, tales como HTTPS, SSH, SCP, SFTP/FTPS, etc.

2. Para sistemas basados en web, se adoptará el modelo SSL/TLS para el cifrado del tráfico. Los protocolos aprobados son TLS v.1.2 o superiores. Los protocolos TLS v.1.1 e inferiores y SSLv3 4/6e inferiores no de cifrado robustos; una guía de referencia es:

[https://cheatsheetseries.owasp.org/cheatsheets/TLS\\_Cipher\\_String\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html)

Se deben evitar las suites de categoría C o inferiores.

3. Las claves de cifrado deben ser robustas. Se recomienda una longitud de 2048 bits para RSA o equivalente, de acuerdo al estándar NIST SP 800-57. La clave privada debe quedar en poder de la institución, exclu

Codificación del software:

1. Se debe utilizar estándares de buenas prácticas seguras de programación, la cual debe ser seleccionada e implementada de acuerdo al lenguaje de programación y el entorno de

desarrollo utilizado. Guías de referencia recomendadas son las siguientes:

- a. SEI CERT Coding Standards

<https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards>

- b. OWASP Secure Coding Practices y OWASP Secure Coding Cheat Sheet

[https://www.owasp.org/index.php/OWASP\\_Secure\\_Coding\\_Practices\\_-\\_Quick\\_Reference\\_Guide](https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide)

ce\_Guide

[https://www.owasp.org/index.php/Secure\\_Coding\\_Cheat\\_Sheet](https://www.owasp.org/index.php/Secure_Coding_Cheat_Sheet)

- c. Oracle Secure Coding Guidelines for Java SE

<http://www.oracle.com/technetwork/java/seccodeguide-139067.html>

2. El software debe contemplar un manejo seguro de errores. Se debe realizar y documentar la verificación explícita de errores para todas las entradas, comprobando el tamaño, el tipo de

datos, los rangos de valores y/o formatos aceptables de modo a que éstos sean válidos para la operación que están por realizar.



3. Todos los componentes de terceros utilizados para el desarrollo del software deben estar

actualizados a la última versión estable disponible, contar con soporte por un periodo igual o

superior al exigido para el proyecto y ser de confianza. Esto es aplicable, pero no limitante, a

librerías, frameworks, scripts, funciones, plugins, plantillas, generadores de código,

compiladores, entre otros.

4. Se debe realizar y documentar las pruebas de vulnerabilidades de código, incluyendo análisis estático y dinámico de vulnerabilidades para verificar que se cumplan los estándares mínimos de codificación seg seguridad estándar y aceptados por la industria. Guías de referencia recomendadas son las siguientes:

a. OWASP Testing Project: [https://www.owasp.org/index.php/OWASP\\_Testing\\_Project](https://www.owasp.org/index.php/OWASP_Testing_Project)

b. Open Source Security Testing Methodology Manual (OSSTMM)

<http://www.isecom.org/research/>

c. Microsoft Security Development Lifecycle (SDL) - Pasos 10 a 13

<https://www.microsoft.com/es-ES/download/details.aspx?id=12379>

<https://www.microsoft.com/en-us/securityengineering/sdl/practices>

5/6 Generadores de código:

1. Todo software generado mediante el uso de tecnologías de generación automatizada de código debe cumplir con los criterios mínimos de seguridad de la presente guía.

5 Capacitación.

Capacitación del personal operador.

Capacitación de los encargados del área informática para administración de las bases de datos.

## Introducción y justificación

La finalidad del presente proceso de adquisición, Sistema de Solicitud en Línea de Antecedentes Académicos, es a fin de brindar, por un lado, un servicio más integral al Estudiante de ISEPOL y por otro lado, descongestionar la acción presente de la gestión de estas solicitudes en forma presencial, dado la gran cantidad de estudiantes y la limitada infraestructura para atenderlos debidamente, generar los certificados en forma masiva y además contar con medidas de seguridad y verificación de los certificados y/o diplomas.

## Submodalidad de adquisición

La submodalidad de adquisición será: Software con requerimientos definidos

## Objetivo general

Lograr descongestionar, con la incorporación de un Sistema de Solicitud en Línea, la presencia de estudiantes que se aglomeran para una gestión, muy necesaria, pero que dada la limitada infraestructura física y de personal, lo vuelven tedioso y obsoleto.

## Objetivos específicos

Facilitar la gestión de los Antecedentes Académicos del estudiantado del ISEPOL. Reducir los tiempos de gestión de la solicitud y retiro de los Antecedentes Académicos. Brindar un mejor servicio al estudiantado del ISEPOL.

## Definiciones, acrónimos y abreviaturas

Sistema de Solicitud en Línea de Antecedentes Académicos SSLAA

## Antecedentes

El creciente número de estudiantes quienes año tras año se vuelcan a formarse en las diversas disciplinas dictadas en el ISEPOL obliga a establecer procedimientos y facilidades que agilicen la gestión que requieren los diversos estudiantes entre lo que se destaca la gestión, solicitud, pago y retiro de sus Antecedentes Académicos.

## Marco legal

En esta sección se deberán indicar leyes, decretos, resoluciones, ordenanzas, acordadas u otras normativas que versen sobre el servicio, trámite o función a ser implementada por la Policía Nacional a través del software, sistema o plataforma tecnológica, o bien hacen directa referencia a estos, en caso de que hubiere. Asimismo, el marco legal que da sustento a la adquisición objeto del llamado, en atención a las competencias legales establecidas dla Policía Nacional.

Decreto N° 361 POR EL CUAL SE REGLAMENTA LA LEY N° 7110/2023 «DE SIMPLIFICACIÓN DE TRÁMITES PARA LA GESTIÓN Y EXPEDICIÓN DE TÍTULOS EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR DEL PARAGUAY Y REGISTROS DE TÍTULOS ANTE EL VICEMINISTRO DE EDUCACIÓN SUPERIOR Y CIENCIAS»

LEY 6562 DE LA REDUCCION DE LA UTILIZACION DE PAPEL EN LA GESTION PUBLICA Y SU REEMPLAZO POR EL FORMATO DIGITAL.

## Beneficiarios

Estudiantes en General, Tesorería, Cajeros, Administración Académica.

## Infraestructura para el software

necesarios nuevos equipos de hardware, serán utilizados los equipos que conforman el parque actual de equipos de la ISEPOL. Detalle y tipo de servidores (máquinas virtuales, contenedores, sistemas operativos, sistemas de virtualización, entre otros), Servidores: SERVIDOR DELL PowerEdge R820

Máquinas Virtuales y Contenedores: Virtualizador Proxmox V.8.2 (estable)

Sistemas Operativos: Linux distribución Debían v.12 Sistema de Virtualización: Proxmox

Estaciones de trabajo:

Cantidad aproximada de estaciones de trabajo (PC, notebook, dispositivos móviles) que tiene la Policía Nacional destinada para el uso de los sistemas a adquirir, para ello se destaca que los usuarios acceden desde sus dispositivos particulares (notebook, celular, etc) siendo de 600 usuarios simultáneamente, con conexión dispar de usuarios aproximadamente a 1.200 usuarios en total.

La Policía Nacional deberá definir y describir dónde estará alojada la solución y los equipos necesarios para su correcto funcionamiento, especificando mínimamente:

Datacenter: Ubicado en el Departamento de Informática de la Policía Nacional (Datacenter tipo Contenedor), con generador, UPS para los Servidores, Dispositivos sensor de Humedad, humos, llamas, extintores de incendios con polvo seco (para electrónicas).

El responsable del datacenter es la División TIC del Departamento de Informática de la Policía Nacional, bajo la supervisión de un Oficial Superior con diligencia en el área técnica y quien trabaja en coordinación directa con la jefatura del Departamento de Informática.

Se utilizan los dominios de la Institución y se encuentra abierta para trabajar en conexión externa a dominios generados por terceros. Los servicios de dominios se establecen por medio de una IP Publica.

## Confidencialidad

Con la intención de proteger la información que la entidad contratante proporciona a los proveedores (oferentes adjudicados), una vez adjudicado el contrato, debe

especificar el grado de privacidad de la información. Es importante precisar la confidencialidad de la información que se entrega para la realización de los estudios o trabajos, diferenciando el tipo de información en caso de requerir aplicar distintos niveles de confidencialidad o publicidad de la información. Así también, respecto de la información que se genere durante la realización de las actividades, y la información producida una vez que se haya concluido el servicio. Deberá incluir, como mínimo, lo siguiente:

El oferente reconoce que la información y documentación que como entidad contratante le proporcione, así como los datos y resultados obtenidos de la prestación de los servicios, son propiedad exclusiva de la entidad contratante, como el carácter confidencial y/o reservado en términos de la normativa aplicable y las disposiciones del contrato.

El oferente se obliga a mantener absoluta confidencialidad sobre las creaciones realizadas, incluyendo todos los algoritmos y toda la información sobre el código fuente y código objeto de las mismas, como respecto de todos sus manuales, incluyendo la documentación preparatoria, su descripción técnica, manuales de uso y cualquier otra documentación relacionada con cualquier actividad realizada por el Desarrollador en virtud del contrato.

Cualquier información, fuese cual fuere su naturaleza (técnica, comercial, financiera, operacional o de otro tipo), contenida en cualquier forma y soporte (ya sea verbal, escrita, grabada o de cualquier otro tipo), que pudiera ser facilitada por la Policía Nacional, será considerada como Información Confidencial, incluyéndose en esta categoría aquella información generada a partir de la propia Información Confidencial.

El desarrollador, se obliga asimismo a:

- c. tratar la Información Confidencial como estrictamente secreta.
- d. custodiar y guardar la Información Confidencial, bien sea escrita, grabada o en cualquier otro tipo de soporte, separada de cualquier otra información de la que pudiera disponer.
- e. utilizar o transmitir la Información Confidencial exclusivamente para los fines del proyecto.
- f. utilizar procedimientos de control de dicho uso o transmisión de la Información Confidencial. El desarrollador no realizará copia de la Información Confidencial sin el previo consentimiento escrito de la Policía Nacional, excepto aquellas copias que sean necesitadas por el desarrollador para su estudio interno.
- g. restringir el acceso a la Información Confidencial únicamente a aquellos empleados suyos que necesiten conocerla para los fines convenidos, y asegurarse que dichos empleados conocen las obligaciones que les resultan aplicables en virtud de lo establecido en el presente documento. Todos los contratos que el Desarrollador celebrará con empleados, trabajadores y prestadores de servicios que podrían participar en el desarrollo del contrato, incluirán cláusulas sobre confidencialidad y transferencia que producen iguales efectos y sujetan a dichas personas a las mismas obligaciones que el Desarrollador se ha obligado.
- h. no facilitar Información Confidencial a tercero alguno sin el previo consentimiento escrito de la Policía Nacional, y asegurarse de que, en caso de haber obtenido dicha autorización, dicho tercero firme un compromiso de confidencial con la Policía Nacional en términos equivalentes a los de la presente cláusula.

La Policía Nacional será en todo momento el titular exclusivo de la información confidencial, la cual será protegida por todos los medios legales a su alcance. En ningún caso se entenderá implícito en modo alguno, que el hecho de que la Policía Nacional facilite la Información Confidencial significa la concesión de licencia o la cesión de cualquier naturaleza a favor del desarrollador de cualesquiera derechos de patentes, marca, modelo de utilidad, diseño, derechos de autor, o derecho alguno de propiedad intelectual. Ninguna de las partes utilizará el nombre, marca, nombre comercial, o cualesquiera otros derechos de propiedad industrial o intelectual de la otra Parte, sin el previo consentimiento por escrito de ésta, salvo aquellos expresa y contractualmente cedidos.

Toda información que ostente algún derecho de propiedad intelectual de conformidad al derecho positivo que rige a ambas partes, a pesar de ser compartida entre estas, no implicará renuncia alguna a tales derechos, los cuales permanecerán vigentes sobre toda utilización que haga la otra parte de tal información.

La interpretación del concepto de propiedad intelectual no podrá ir más allá de lo establecido en la legislación respectiva. Lo incluido en tales derechos dependerá de lo que le ha sido expresamente reconocido por la autoridad de aplicación, no pudiendo invocarse de lo contrario, derecho alguno.

El desarrollador no podrá utilizar la información y los desarrollos o análisis funcionales elaborados en el cumplimiento de la contratación, para terceros o en beneficio de terceras partes. No podrá utilizar esta información en otras implementaciones que lo coloquen en

situación privilegiada. Toda infracción a esta obligación, lo hará responsable de responder de los daños y perjuicios que pudieran derivarse, así como las sanciones administrativas que correspondan.

La Policía Nacional deberá indicar explícitamente las especificaciones generales del software, definidos en los ítems comunes para la contratación de empresas de software, y Adicionalmente los descritos a continuación. [Requerimientos](#)

- Análisis, definición y desarrollo de una BD, para integración con el sistema de alumnos permanentes (Cursantes).

Bd para solicitud de antecedente académicos. Bd para reportes de novedades de alumnos.

Validaciones de datos.

- Plataforma de acceso público.

Link para acceso público desde el portal web de isepol.edu.py

Modificación de la página de Isepol.edu.ý a modo de agregar el botón de acceso al nuevo link. Módulo de carga de datos del solicitante de antecedentes Académico.

Módulo de carga de documentos digitales solicitados.

Pago de arancel vía plataforma de pago, ajuste del web service entre Isepol y la pasarela de pago. Recepción del certificado a través del correo registrado por el solicitante.

- Plataforma de acceso oficial (uso interno)

Acceso a través de usuario y contraseña y administración de las mismas. Módulo para revisión de solicitudes de antecedentes Académicos.

Aprobación de documentos y generación automática de deuda para pasarela de pago. Carga y generación del antecedente académico.

Envío automático del antecedente académico.

Carga de novedades académicas por parte de las diferentes unidades. Reportes diarios y semanales.

Estadísticas varias.

Confección por parámetros del certificado.

Generación masiva de certificados desde los datos de cursantes. Envío masivo por correo (mail)

Contar con las licencias necesarias.

-

#### Requerimientos no funcionales

El sistema deberá contar con alta capacidad de integración que posibiliten los intercambios de información en tiempo y forma: con otros sistemas informáticos de la Policía Nacional, Registro Civil, proveedores, contratistas, entre otros.

#### Arquitectura general

El Sistema ofrecido debe tener la capacidad de correr sobre un Sistema Operativo Linux Red Hat o Windows Server. Su arquitectura debe ser en 3 capas:

La Capa de Datos: Esto comprende el servidor de base de datos. Esta capa se requiere que sea en uno de los motores de base de datos de la Policía Nacional (MySQL, POSTGRESQL).

#### Tecnología

El Sistema ofrecido debe tener la capacidad de correr sobre un Sistema Operativo Linux Red Hat o Windows Server.

#### Seguridad

##### CRITERIOS MINIMOS DE SEGURIDAD PARA EL DESARROLLO Y LA ADQUISICION DE SOFTWARE.

##### - Soporte y gestión continua del software:

1. Todo el software desarrollado debe contar con soporte de software del fabricante. Al momento de la adquisición se debe establecer claramente el tiempo de vida mínimo que se requiere para el software o sistema, y el fabricante debe ofrecer un tiempo de soporte igual o superior a dicho tiempo de vida.
2. En caso de que no sea posible contar con soporte de software del fabricante, el modelo de

licenciamiento y la disponibilidad del código fuente debe ser tal que permita a la institución o a otra empresa o desarrollador de software nacional asumir dicho soporte.

3. El fabricante o servicio de soporte debe tener un canal de comunicación y/o mecanismo de reporte de vulnerabilidades o bugs de programación, de manera a que el cliente pueda contactarlo en caso de descubrimiento de vulnerabilidades. En caso de que el reporte ocurra dentro de la ventana de tiempo de vida solicitado, el fabricante o servicio soporte debe ser

capaz de proporcionar una corrección a la vulnerabilidad de manera oportuna, según el acuerdo del nivel del servicio (por sus siglas en inglés, Service Level Agreement o SLA) especificado en el contrato o pliego de bases y condiciones.

4. El software debe poder ser inventariado por herramientas estándar automatizadas de inventario de software basados en el estándar *Common Platform Enumeration* (CPE), debiendo incluir como mínimo la información del nombre, versión, autor y fecha de instalación del mismo.

##### - Gestión de usuarios, sesiones y privilegios:

1. El software debe permitir una gestión de usuarios de acuerdo a los requerimientos de la

institución, con niveles de privilegios de acuerdo a los roles que éstos requieran (administrador, editor, usuario, etc.), basados en el principio de mínima necesidad de conocimiento.

2. El software debe permitir la revocación de acceso de usuarios, mediante un estado desactivado o similar.
3. Debe ser posible establecer una fecha de expiración para las cuentas de usuarios, a partir de la cual la cuenta deberá entrar a un estado desactivado o similar, hasta tanto se apruebe la continuidad de la misma. El parámetro de fecha de expiración podrá ser fijo o configurable por la institución, de acuerdo a sus requerimientos de negocio.
4. El software debe contemplar la expiración de sesiones de acuerdo a parámetros temporales. Estos parámetros pueden ser fijos o configurables por la institución, de acuerdo a sus requerimientos de negocio.

##### - Autenticación y gestión de credenciales:

1. El software debe permitir la gestión individual eficaz de credenciales, debiendo permitir que cada usuario sea capaz de cambiar su propia contraseña. Se debe contemplar también mecanismos de recuperación de contraseñas, ya sea a través de un usuario de mayores privilegios o de mecanismos de auto-gestión por parte del usuario. Preferentemente, debe ser posible que al momento de la creación de cuentas permita forzar el cambio de contraseña luego del primer inicio de sesión.

3/62. El software que almacene y/o procese información crítica y/o que se utilice para un proceso crítico de la institución debe soportar autenticación de doble factor para los usuarios de privilegios elevados.

3. El software debe permitir establecer políticas de contraseña, que incluyan, como mínimo, la posibilidad de establecer los siguientes parámetros:
  - a. longitud mínima de la contraseña
  - b. complejidad de contraseña (mayúsculas, minúsculas, números y caracteres especiales, etc.)

Los mencionados parámetros serán configurables por la institución, preferentemente, o en su defecto, deberán ajustarse a los lineamientos y estándares mínimos indicados por la institución.

4. Las contraseñas no deben almacenarse en texto claro, sino mediante la aplicación de funciones hash o funciones resumen. Para el almacenamiento de las contraseñas se debe utilizar funciones criptográficas seguras no reversibles de hash combinadas con salt aplicadas a las contraseñas. Algoritmos aprobados son los siguientes:
  - a. Argon2
  - b. PBKDF2
  - c. scrypt
  - d. bcrypt
5. De manera alternativa, se puede cifrar las contraseñas utilizando técnicas criptográficas

reversibles únicamente en aquellos casos en que la clave secreta y/o privada de cifrado quede bajo el poder exclusivo del usuario dueño de la contraseña.

#### Gestión de registros de auditoría:

1. El software debe ser capaz de generar registros de auditoría de todos los eventos relevantes, con los detalles suficientes para permitir una trazabilidad adecuada, que abarque como mínimo los siguientes eventos:
  - a. inicios de sesión de usuarios (exitosos y fallidos)
  - b. delegación/impersonificación de cuentas de usuarios
  - c. modificación de parámetros del sistema
  - d. gestión de usuarios (cambio de contraseña, creación/eliminación/modificación de

usuarios y/o grupos)

- e. acciones críticas llevadas a cabo por usuarios en el marco del proceso de negocio del sistema (edición de datos sensibles, eliminación de datos, etc.)
2. El software debe contemplar un mecanismo configurable de rotación de registros de auditoría, de acuerdo al parámetro de cantidad de tiempo (diario, semanal, mensual, etc.), como mínimo.

#### Cifrado:

1. El software debe cifrar toda la información sensible en tránsito, especialmente aquella información de carácter confidencial y/o cuya integridad deba asegurarse. Para ello se deberán utilizar protocolos de red cifrados, tales como HTTPS, SSH, SCP, SFTP/FTPS, etc.
2. Para sistemas basados en web, se adoptará el modelo SSL/TLS para el cifrado del tráfico. Los protocolos aprobados son TLS v.1.2 o superiores. Los protocolos TLS v.1.1 e inferiores y SSLv3 4/6e inferiores no deben ser utilizados. Se deben seleccionar suites de cifrado robustos; una guía de referencia es:

[https://cheatsheetseries.owasp.org/cheatsheets/TLS\\_Cipher\\_String\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html)

3. Se deben evitar las suites de categoría C o inferiores.

Las claves de cifrado deben ser robustas. Se recomienda una longitud de 2048 bits para RSA o equivalente, de acuerdo al estándar NIST SP 800-57. La clave privada debe quedar en poder de la institución, exclusivamente.

#### Codificación del software:

1. Se debe utilizar estándares de buenas prácticas seguras de programación, la cual debe ser seleccionada e implementada de acuerdo al lenguaje de programación y el entorno de desarrollo utilizado. Guías de referencia recomendadas son las siguientes:
  - a. SEI CERT Coding Standards <https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards>
  - b. OWASP Secure Coding Practices y OWASP Secure Coding Cheat Sheet [https://www.owasp.org/index.php/OWASP\\_Secure\\_Coding\\_Practices\\_-\\_Quick\\_Reference\\_Guide](https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide)

[https://www.owasp.org/index.php/Secure\\_Coding\\_Cheat\\_Sheet](https://www.owasp.org/index.php/Secure_Coding_Cheat_Sheet)

- c. Oracle Secure Coding Guidelines for Java SE <http://www.oracle.com/technetwork/java/seccodeguide-139067.html>
2. El software debe contemplar un manejo seguro de errores. Se debe realizar y documentar la verificación explícita de errores para todas las entradas, comprobando el tamaño, el tipo de datos, los rangos de valores y/o formatos aceptables de modo a que éstos sean válidos para la operación que están por realizar.
3. Todos los componentes de terceros utilizados para el desarrollo del software deben estar actualizados a la última versión estable disponible, contar con soporte por un periodo igual o superior al exigido para el proyecto y ser de confianza. Esto es aplicable, pero no limitante, a librerías, *frameworks*, *scripts*, funciones, *plugins*, plantillas, generadores de código, compiladores, entre otros.
4. Se debe realizar y documentar las pruebas de vulnerabilidades de código, incluyendo análisis estático y dinámico de vulnerabilidades para verificar que se cumplan los estándares mínimos de codificación segura, utilizando herramientas y/o guías de testing de seguridad estándar y aceptados por la industria. Guías de referencia recomendadas son las siguientes:
  - a. OWASP Testing Project: [https://www.owasp.org/index.php/OWASP\\_Testing\\_Project](https://www.owasp.org/index.php/OWASP_Testing_Project)
  - b. Open Source Security Testing Methodology Manual (OSSTMM) <http://www.isecom.org/research/>
  - c. Microsoft Security Development Lifecycle (SDL) - Pasos 10 a 13 <https://www.microsoft.com/es-ES/download/details.aspx?id=12379>  
<https://www.microsoft.com/en-us/securityengineering/sdl/practices>

#### Plan de trabajo

El oferente deberá presentar en su oferta técnica un cronograma detallado y propuesta de metodología de trabajo que mejor se adecue a lo solicitado en el cronograma general, incluyendo la lista de personal proponente por cada actividad. Según lo dispuesto en la sección [Perfiles técnicos del personal](#).

## Entregables

El oferente adjudicado deberá obligatoriamente realizar la entrega de los siguientes ítems a la Policía Nacional, quien emitirá un certificado de recepción satisfactoria. La Policía Nacional deja constancia que el oferente adjudicado ha brindado los servicios contratados, y que ha entregado los siguientes:

Documentación del Proceso de Análisis.

La Policía Nacional deberá establecer la documentación y nivel de detalle que requiera. Ejemplo: Listado de casos de uso, descripción de casos de uso, diagrama de cada caso de uso, documento de especificación de requerimientos, documento de arquitectura, entre otros.

Código Fuente en los repositorios oficiales de la Policía Nacional. Informe de entrega y evidencias de control de calidad.

Corresponde a un documento donde el oferente declara haber realizado las pruebas necesarias y detalla las funcionalidades entregadas. Deberá estar firmado por el oferente adjudicado o coordinador del mismo e incluir evidencias de las pruebas realizadas.

Manuales:

Manual de instalación para ambiente en desarrollo: Paso a paso de la instalación del software en ambiente de desarrollo. Manual de instalación para ambiente en producción: Paso a paso de la instalación del software en ambiente de producción. Manual del usuario. La Policía Nacional deberá especificar el detalle del manual requerido. Ej: por tipo de perfil.

Otra documentación requerida y especificada por la Policía Nacional. Instaladores:

En caso de que requiera software no contemplado en los manuales entregados.

## Soporte y asistencia técnica

El oferente adjudicado deberá suministrar asistencia técnica por vía telefónica, e-mail, chat, virtual y/o atención in situ en las oficinas que designe la Policía Nacional para restablecer y corregir el servicio

en caso de fallas.

El tiempo mínimo de soporte técnico a ser tenidos en cuenta a partir de la entrega e instalación satisfactoria, será como mínimo de 6 (seis) meses.

El oferente adjudicado indicará cómo realizará el servicio de operación de la asistencia técnica por el tiempo especificado a partir de la emisión del certificado de recepción satisfactoria por parte de la Policía Nacional. El oferente adjudicado, deberá detallar los niveles de servicio (soporte técnico) a ser utilizados para la operación y asistencia técnica del software, y de todo lo que implica la supervisión y el monitoreo.

Durante dicho periodo, igualmente el oferente adjudicado se compromete al suministro de actualizaciones de nuevas versiones del software, como así también la aplicación de parches si es necesario, sin costo adicional para la Policía Nacional.

- Condiciones sobre propiedad intelectual, derechos de autor y otros derechos asociados al Desarrollo del Software

La titularidad de los derechos de propiedad intelectual y en especial de los derechos de autor que existan respecto al software desarrollado se considera y establece, a efectos de la contratación realizada, que es cedida por los autores materiales del mismo enteramente a favor de Estado Paraguayo en la persona jurídica o entidad/organismo contratante, por haber sido creados en cumplimiento de una relación laboral de la institución con requerimientos definidos

El desarrollador debe garantizar que todo el producto desarrollado no infringe derechos de propiedad intelectual de terceros y es cedido en su totalidad, incluyendo todos sus componentes, al contratante.

Se establece que el Desarrollador (ya sea funcionario, contratado, firma unipersonal o empresa) transfiere en forma exclusiva y perpetua a la Policía Nacional todos los derechos de propiedad intelectual, propiedad industrial y cualquier otro derecho cuya titularidad y propiedad corresponda al Desarrollador, sobre programas computacionales, obras, creaciones, invenciones, ideas, conocimientos, knowhow, productos, objetos, elementos, tecnología o información que no habiendo sido especialmente desarrollada, creada, realizada o concebida por el Desarrollador para el cumplimiento de este contrato, haya sido utilizada por el Desarrollador en el cumplimiento del contrato

## Definición de licencias de software de titularidad del Estado por parte de la Policía Nacional

Todo el software y asociados al mismo resultante serán propiedad del Ministerio del Interior quien en su carácter de titular de dicho software establecerá el uso y/o disposición.

## Criterios de Selección de Oferentes

El oferente debe ser una persona física o jurídica radicada o constituida legalmente en el país.

## Rubro

Debe pertenecer a rubros relacionados a Tecnologías de la Información y Comunicación, específicamente a

desarrollo, mantenimiento y/o implementación de software. En caso de tratarse de una persona jurídica, esto deberá verificarse en el objeto de su Constitución siendo una de las actividades principales

- Restricciones mínimas de tipo y cantidad de las referencias presentadas Cada referencia deberá corresponder a trabajos de desarrollo de software.

Deberá acompañar evidencia

comprobable, sean contratos, constancias firmadas por el contratante o su representante, u otro documento que respaldatorio de justificación. Mínimo de 3 referencias de clientes.

Al menos 3 referencias deben ser de clientes distintos.

Al menos 2 referencias deben corresponder a trabajos realizados en el Paraguay para organizaciones públicas o privadas radicadas en nuestro país.

#### Restricciones mínimas de montos de las referencias presentadas

La sumatoria de los montos de las referencias presentadas que cumplan los criterios deberá ser como mínimo el 30% del monto referencial de la adquisición. [Perfiles técnicos del personal](#)

Para llevar adelante las tareas técnicas en el marco de la presente licitación pondrá a Disposición los siguientes perfiles:

1. Un líder o coordinador TIC del proyecto.
2. Al menos un analista funcional con perfil técnico del área de análisis de software. Tipo de Perfil técnico del oferente

Disposición los siguientes perfiles:

1. Un ingeniero en informática
2. Un técnico-desarrollador de software.

Debiendo presentar CV de cada uno de los RR.HH. propuestos, que deberán estar firmados por cada uno de ellos, y deberán declarar su compromiso a formar parte del equipo de trabajo en caso de resultar adjudicado En caso de que uno de los recursos no participe al inicio o deje de formar parte durante el proceso de desarrollo por algún motivo, para dichos casos el oferente deberá reemplazarlo por otro de equivalente perfil al solicitado o superior y notificar por nota el cambio realizado, adjuntando nuevamente el CV del recurso que se incorpora al equipo de desarrollo conforme a lo requerido anteriormente.

#### -Propiedad intelectual y definición de licencias:

Todo código fuente del software o versión de software resultante del proceso licitatorio será de libre disposición por parte de la POLICÍA NACIONAL quien se constituye en propietario / titular del mismo. Quien establecerá el uso, distribución, reproducción, incluyendo además derechos como: extraer partes, copiar, modificar, fusionar y todo aquel uso lícito, a favor de todo o parte del sector público, constituyéndose en licencia de software libre con propiedad intelectual del Estado

#### Documentación del Proceso de Análisis.

Se requiere la presentación del Listado de casos de uso, descripción de casos de uso, diagrama de cada caso de uso, documento de especificación de requerimientos, documento de arquitectura, entre otros

El código fuente versionado deberá estar alojado en los repositorios oficiales de la Policía Nacional. Adicionalmente el oferente adjudicado deberá realizar una copia del código fuente versionado definido por la contratante en los repositorios de código fuente del MITIC

Informe de entrega y evidencias de control de calidad.

Corresponde a un documento donde el oferente declara haber realizado las pruebas necesarias y detalla las funcionalidades entregadas. Deberá estar firmado por el oferente adjudicado o coordinador del mismo e incluir evidencias de las pruebas realizadas.

#### Manuales:

Manual de instalación para ambiente en desarrollo: Paso a paso de la instalación del software en ambiente de desarrollo

Manual de instalación para ambiente en producción: Paso a paso de la instalación del software en ambiente de producción. Manual del usuario

Otra documentación requerida y especificada por la Policía Nacional.

#### Instaladores:

En caso de que requiera software no contemplado en los manuales entregados

#### LOTE N° 6 RENOVACION Y ACTUALIZACIÓN DE LICENCIA SOFTWARE- ACTIVIDAD 9

Item	Descripción del Bien	Cantidad
------	----------------------	----------

1	Renovación, Actualización y Soporte Técnico de los Dispositivos con Software Forense UFED TOUCH (Inseyets Pro UFED) y PHYSICAL ANALYZER (InsEYets Pro PA), para Llave / Dongle Serie N° 218776161 (Departamento Contra el Crimen Organizado), Llave / Dongle 886021208 (Departamento Antisecuestro de Personas) y Llave / Dongle 7210903 (Departamento Antisecuestro de Personas)	2
2	Soporte y Actualización InsEYets Online Limited Unlocks 120	1

#### Introducción y justificación

La finalidad del presente proceso tiene como finalidad la actualización de licencias y adquisición de software para las agrupaciones dependientes de la Dirección de Apoyo Táctico y las Unidades Tácticas de las Direcciones de Policía Departamentales.

Este equipamiento permitirá atender la alta demanda actual de análisis y valoración de dispositivos incautados (celulares, computadores, tablets, discos), derivada de los procedimientos realizados o acompañados por las unidades solicitantes, las cuales dependen administrativamente de esta Tesorería.

El objetivo es garantizar el acceso integral a la información contenida en dichos dispositivos, optimizando así los procesos periciales.

1. Submodalidad de adquisición La submodalidad de adquisición será:

Software con requerimientos definidos

2. Objetivo general

El objetivo es garantizar el acceso integral a la información contenida en dichos dispositivos, optimizando así los procesos periciales.

3. Objetivos específicos

Desbloquear dispositivos soportados con facilidad, para la extracción de datos de una amplia gama de dispositivos, con capacidad de desbloqueo dispositivos de alta gama IOS y/o ANDROID. Extraer datos de teléfonos móviles, drones, tarjetas SIM, tarjetas SD, dispositivos GPS y más.

Realizar extracciones del sistema lógico completo de archivos y extracciones físicas para obtener la mayor cantidad de datos de los dispositivos incautados. Contar con métodos de recuperación sin igual (Cargadores de arranque exclusivos, capacidades automáticas exclusivas para cada dispositivo soportado). Posibilitar la extracción selectiva para recuperar tokens en la nube y seleccionar datos de aplicaciones.

Acceder a la mayor cantidad de datos y metadatos de los dispositivos extraídos y analizados.

Procesar datos dos veces más rápido que abarcan diversas aplicaciones, dispositivos y formatos de archivos.

Obtener datos más completos, para una comprensión más profunda, incluida la ubicación geográfica, los detalles criptográficos, el origen de los medios y los datos de la nube. Descubrir evidencia crucial, explorando los datos sin esfuerzo y validando los hallazgos mediante un análisis integral del dispositivo.

Agilizar los exámenes, desde el acceso y el análisis.

Revelar sin esfuerzo evidencia crucial y mejora la eficiencia de sus investigaciones.

Posibilitar el intercambio de evidencia crucial con organismos de seguridad, mediante un formato estandarizado. Acelerar la resolución de casos y ahorrar tiempo valioso.

4. Definiciones, acrónimos y abreviaturas

Inseyets Pro UFED, Inseyets Pro PA/CLOUD, InsEYets Online Limited Unlocks, iOS/Android, Llave/Dongle

5. Antecedentes

La Actividad 09 "Servicio de Operaciones Especiales y de Contención", en su calidad de área requirente, solicita el inicio del presente proceso debido a la necesidad atender los requerimientos operativos de las Agrupaciones dependientes de la Dirección de Apoyo Táctico y de las Unidades Tácticas de las Direcciones de Policía Departamentales, quienes requieren herramientas tecnológicas actualizadas que fortalezcan sus capacidades en el cumplimiento de sus funciones especializadas.

La solicitud se enmarca en la necesidad de garantizar el acceso a tecnologías de vanguardia que optimicen los procesos de análisis forense, gestión de información y apoyo táctico, en línea con los estándares institucionales y las demandas actuales del servicio policial.

6. Marco legal

Ley N° 1286 CÓDIGO PROCESAL PENAL, ARTÍCULO 320. ANTICIPO JURISDICCIONAL DE PRUEBA. Ley N° 645/95 DE LAS TELECOMUNICACIONES, ARTÍCULO 89 Y 90.

7. Beneficiarios

Departamentos Especializados de la Policía Nacional.

8. Infraestructura para el software



Para la implementación y operación del sistema sujeto a este proceso de adquisición, no se requerirá hardware adicional, ya que se utilizará la infraestructura tecnológica actual de los Departamentos Especializados de la Policía Nacional.

Estaciones de trabajo: Deben cumplir con los requisitos técnicos exigidos por el software ya instalado en los Departamentos Especializados de la Policía Nacional.

## 9. Confidencialidad

Con la intención de proteger la información que la entidad contratante proporciona a los proveedores (oferentes adjudicados), una vez adjudicado el contrato, debe especificar el grado de privacidad de la información.

### Sección 1

#### Adquisición de Servicios de Informática y Licencias Software

La Policía Nacional deberá indicar explícitamente las especificaciones de licencias de soporte de software, descritas a continuación. Requerimientos

Renovación, Actualización y Soporte Técnico de los Dispositivos con Software Forense UFED TOUCH (Inseyets Pro UFED) y PHYSICAL ANALYZER (InsEYets Pro PA), para Llave / Dongle Serie N° 218776161 (Departamento Contra el Crimen Organizado), Llave / Dongle 886021208 (Departamento Antisecuestro de Personas) y Llave / Dongle 7210903 (Departamento Antisecuestro de Personas)

UFED TOUCH / 4PC (InsEYets Pro UFED)

El soporte, deberá permitir la Actualización y/o Renovación del Hardware y Software del Dispositivo InsEYets Pro UFED (UFED 4PC) para la Llave / Dongle Serie N° 218776161 (Departamento Contra el Crimen Organizado), la Llave / Dongle Serie N° 886021208 (Departamento Antisecuestro de Personas) y la Llave / Dongle Serie N° 7210903 (Departamento Antisecuestro de Personas), conforme a las últimas actualizaciones realizadas por el fabricante.

La actualización deberá permitir realizar extracciones colaborativas de manera ilimitada, tanto físicas como completas del sistema de archivos, durante la vigencia. La actualización deberá contar con la capacidad de acceder a áreas y aplicaciones altamente seguras, incluyendo eliminados.

La actualización deberá mantenerse actualizada de manera periódica, durante la vigencia.

La actualización deberá ser compatible con las herramientas de análisis Physical Analyzer o InsEYets Pro PA/CLOUD, existentes en la institución.

El soporte, deberá permitir la Actualización y/o Renovación de los Conectores, para los dispositivos, conforme a los requerimientos de las actualizaciones a ser recibidas. El soporte, deberá incluir las capacitaciones necesarias y el acompañamiento por parte del Fabricante y/o representante de la misma.

Deberá contar con una interfaz de uso compartido con la herramienta InsEYets Online Limited Unlocks. Deberá contar con funcionalidades que permitan procesos de Autonomía, Coordinación, Priorización, Obtención de Información Preliminar de Interés y Capacidades de Colaboración.

La Renovación, Actualización y Soporte Técnico, deberán tener una vigencia de 12 meses. UFED PHYSICAL ANALYZER (InsEYets Pro PA/CLOUD)

El soporte, deberá permitir la Actualización del Software UFED Physical Analyzer / InsEYets Pro PA/CLOUD con Llave / Dongle Serie N° 218776161 (Departamento Contra el Crimen Organizado), Llave / Dongle Serie N° 886021208 (Departamento Antisecuestro de Personas) y Llave / Dongle Serie N° 7210903 (Departamento Antisecuestro de Personas), conforme a las últimas actualizaciones realizadas por el fabricante.

Se deberá permitir las siguientes funcionalidades conforme a las última actualizaciones del fabricante:

- Creación de casos y para cada caso la asignación de fuentes digitales específicas.
- Visualización de los datos descriptados de las múltiples aplicaciones soportadas.
- Visualización de la información de las extracciones en orden cronológico en el formato de línea de tiempo timeline, a fin de investigar la secuencia lógica y cronológica de los hechos.
- Identificación y clasificación automática de imágenes y videos en varias categorías predefinidas según el respectivo contenido de imágenes y videos como mínimo en las siguientes categorías: Armas, Drogas, Tatujes, Automóviles, Capturas de Pantalla, Documentos, Rostros, Desnudez, Abuso Infantil o Abuso de menores.
- Identificar automáticamente a un dueño de una fuente de datos digital según los identificadores presentes en la extracción, como email, IMEI, número de teléfono, etc.
- Visualización de geolocalización de los dispositivos, conforme al uso de aplicaciones y/o conexiones.
- Exportar la totalidad de contactos y dueños identificados de las fuentes de datos digitales.
- Extracción, decodificación y análisis de datos de teléfonos celulares y dispositivos móviles no debe limitarse tan solo a la extracción de datos y evidencias almacenadas localmente en los dispositivos móviles, sino también deberá ejecutar la extracción y análisis de datos almacenados en sitios remotos de internet, de las aplicaciones en nube.
- Suministrar condiciones para que se extraigan los datos almacenados en nube relativos a las aplicaciones instaladas en los dispositivos móviles.
- Proveer condiciones para que se acceda, extraiga y haga análisis de forma forense de informaciones almacenadas remotamente en servidores de aplicaciones en nube relacionadas a las aplicaciones instaladas, bajo las credenciales del usuario del dispositivo.
- Permitir que se obtengan las credenciales completas y válidas (o tokens) de acceso a las aplicaciones en nube instalados en el dispositivo móvil, a través de la extracción física de datos del dispositivo móvil realizadas por la herramienta InsEYets Pro UFED (UFED 4PC), con llave (dongle) serie N° 218776161 y 886021208.
- Proveer condiciones para que a través del módulo cloud, con las respectivas credenciales cargadas, se acceda a las aplicaciones y su contenido almacenado en la nube sin la necesidad de poner usuario y contraseña.
- Proveer condiciones para que se obtenga las informaciones en nube de las aplicaciones del usuario también a través de la inserción manual del usuario y contraseña de los mismos en el módulo de cloud de la plataforma, para aplicaciones que no estén instalados en el teléfono, o que no tengan las credenciales completas y válidas.
- Capacidad de acceder a las informaciones en servidores de almacenamiento en nube, incluso cuando los mismos tienen factores de seguridad de las aplicaciones almacenadas en la nube, tales como factor de autenticación doble.
- Soportar en lo mínimo 10 (diez) informaciones de login y credenciales de dispositivos IOS
- Soportar en lo mínimo 11 (once) informaciones de login y credenciales de dispositivos Android sin la necesidad del dispositivo estar rooteado.
- Proveer condiciones para la obtención de informaciones almacenadas remotamente de en lo mínimo las siguientes aplicaciones en nube: Facebook, Instagram, Twitter, Instagram, Snapchat, V Kontakte, oovoo, Dropbox, Google Drive, Microsoft Onedrive, Gmail, Yahoo, Outlook., Kik, Google Contacts, Google Location History, Google Search e Web History, entre otras.
- Proveer condiciones que permitan extraer datos en periodos de tiempo específicos seleccionables individualmente para cada servicio en la nube.
- Permitir que el contenido a ser extraído de cada servicio sea seleccionado previamente.
- Visualización de los datos en línea de tiempo y mapas.
- Búsqueda en el contenido extraído por palabras clave.
- Contar con un manual Web disponible para todos los usuarios en español.
- Generación de informes completos en formato PDF de los datos extraídos de los servicios en nube.
- Exportación de datos de informe para otros softwares a fin de ejecutar una lectura digital en softwares de terceros.
- Proveer condiciones para que se haga la extracción y análisis de mensajes de correo electrónico no leídas
- Capacidad de proveer una tabla conteniendo la lista de eventos y sus respectivas ubicaciones.
- Navegación en los puntos de ubicación de la lista de eventos en el mapa utilizándose el teclado.
- Rastreo de los datos de geoposición, filtrando y exhibiendo fácilmente las localizaciones más frecuentes del dispositivo móvil.
- La Renovación y el soporte técnico deberán ser proveídos por 12 meses, que permita la descarga de las actualizaciones disponibles durante el periodo de vigencia.

Soporte y Actualización InsEYEtS Online Limited Unlocks 120, hasta 12 meses.

- El soporte y actualización deberán contar con la capacidad de desbloquear u omitir códigos de bloqueo de al menos 120 (ciento veinte) dispositivos iOS y/o Android, y ser utilizados por las llaves / dongles del ÍTEM 1
- El soporte y actualización deberán ser compatibles con las herramientas InsEYEtS Pro UFED (UFED 4PC) y InsEYEtS Pro PA (UFED PHYSICAL ANALYZER / CLOUD), existentes en la institución.
- El soporte y actualización deberán incluir los Conectores y Adaptadores (Sin Costo para la Convocante), para los dispositivos conforme a los requerimientos del Software.
- El soporte y actualización deberán incluir las capacitaciones necesarias y el acompañamiento por parte del Fabricante y/o representante de la misma.
- La vigencia deberá ser de al menos 12 meses

-Propiedad intelectual y definición de licencias:

Todo código fuente del software o versión de software resultante del proceso licitatorio será de libre disposición por parte de la POLICÍA NACIONAL quien se constituye en propietario / titular del mismo. Quien establecerá el uso, distribución, reproducción, incluyendo además derechos como: extraer partes, copiar, modificar, fusionar y todo aquel uso lícito, a favor de todo o parte del sector público, constituyéndose en licencia de software libre con propiedad intelectual del Estado

Documentación del Proceso de Análisis.

Se requiere la presentación del Listado de casos de uso, descripción de casos de uso, diagrama de cada caso de uso, documento de especificación de requerimientos, documento de arquitectura, entre otros

El código fuente versionado deberá estar alojado en los repositorios oficiales de la Policía Nacional. Adicionalmente el oferente adjudicado deberá realizar una copia del código fuente versionado definido por la contratante en los repositorios de código fuente del MITIC

Informe de entrega y evidencias de control de calidad.

Corresponde a un documento donde el oferente declara haber realizado las pruebas necesarias y detalla las funcionalidades entregadas. Deberá estar firmado por el oferente adjudicado o coordinador del mismo e incluir evidencias de las pruebas realizadas.

Manuales:

Manual de instalación para ambiente en desarrollo: Paso a paso de la instalación del software en ambiente de desarrollo Manual de instalación para ambiente en producción: Paso a paso de la instalación del software en ambiente de producción. Manual del usuario

Otra documentación requerida y especificada por la Policía Nacional.

Instaladores:

En caso de que requiera software no contemplado en los manuales entregados

## De las MIPYMES

En procedimientos de Menor Cuantía, la aplicación de la preferencia reservada a las MIPYMES prevista en el artículo 34 inc b) de la Ley N° 7021/22 "De Suministro y Contrataciones Públicas" será de conformidad con las disposiciones que se emitan para el efecto. Son consideradas Mipymes las unidades económicas que, según la dimensión en que organicen el trabajo y el capital, se encuentren dentro de las categorías establecidas en el Artículo 4° de la Ley N° 7444/25 QUE MODIFICA LA LEY N° 4457/2012 "PARA LAS MICRO, PEQUEÑAS Y MEDIANAS EMPRESAS", y se ocupen del trabajo artesanal, industrial, agroindustrial, agropecuario, forestal, comercial o de servicio.

## Plan de entrega de los bienes

La entrega de los bienes se realizará de acuerdo al plan de entrega, indicado en el presente apartado. El proveedor se encuentra facultado a documentarse sobre cada entrega. Así mismo, de los documentos de embarque y otros que deberá suministrar el proveedor indicado a continuación:

No Aplica

## Plan de prestación de los servicios

La prestación de los servicios se realizará de acuerdo al plan de prestación, indicados en el presente apartado. El proveedor se encuentra facultado a documentarse sobre cada prestación.

LOTE N° 1 LICENCIA FORTINET- ACTIVIDAD 2

Ítem	Descripción del servicio	Cantidad	Unidad de medida de los servicios	Lugar donde los servicios serán prestados	Fecha(s) final(es) de ejecución de los servicios
1	Software de control de acceso a internet	1	unidad	Comandancia de la Policía Nacional - Paraguay Independiente N° 289 e/ Chile y N.S.A	3 (tres) días hábiles a partir de la recepción de Orden de Compra.

LOTE N° 2 ADQUISICIÓN DE SOFTWARE PARA EL DEPARTAMENTO ESPECIALIZADO EN EL CONTROL Y FISCALIZACIÓN DE EMPRESAS DE SEGURIDAD PRIVADA Y AFINES. ACTIVIDAD 5

Ítem	Descripción del servicio	Cantidad	Unidad de medida de los servicios	Lugar donde los servicios serán prestados	Fecha(s) final(es) de ejecución de los servicios
1	Licencia de Software de Bases de Datos	1	unidad	DEPARTAMENTO ESPECIALIZADO EN EL CONTROL Y FISCALIZACIÓN DE EMPRESAS DE SEGURIDAD PRIVADA Y AFINES	09 (nueve) semanas desde la recepción de la orden de servicio

LOTE N° 3 LICENCIA SOFTWARE- ACTIVIDAD 8

Ítem	Descripción del servicio	Cantidad	Unidad de medida de los servicios	Lugar donde los servicios serán prestados	Fecha(s) final(es) de ejecución de los servicios
1	Desarrollo de software a medida	1	unidad	Departamento de Identificaciones de la Policía Nacional Tesorería R I 2 Ytororo e/ Avd. Boggiani	El plazo máximo de entrega y funcionamiento es de 5 días hábiles posteriores a la recepción de la orden de compra/servicio

LOTE N° 4 ADQUISICIÓN DE SERVICIO DE AMPLIACIÓN Y ACTUALIZACIÓN DE SISTEMAS DE ADMISIÓN Y COBRANZAS - ISEPOL- ACTIVIDAD 6

Ítem	Descripción del servicio	Cantidad	Unidad de medida de los servicios	Lugar donde los servicios serán prestados	Fecha(s) final(es) de ejecución de los servicios
1	Mantenimiento y actualización de software	1	unidad	ACADEMIA NACIONAL DE POLICIA - Avda. del Cadete y Ofic. Insp. Leongino Santacruz	El plazo máximo de entrega será de 30 días hábiles a partir de la recepción de la orden de servicio

LOTE N° 5 DESARROLLO DEL SISTEMA DE GESTION DE CERTIFICADOS, ANTECEDENTES E INFORME DE HISTORIAL ACADEMICO Y MESA DE ENTRADAS - ISEPOL- ACTIVIDAD 6

Ítem	Descripción del servicio	Cantidad	Unidad de medida de los servicios	Lugar donde los servicios serán prestados	Fecha(s) final(es) de ejecución de los servicios
1	Software para desarrollo de programas	1	unidad	ACADEMIA NACIONAL DE POLICIA - Avda. del Cadete y Ofic. Insp. Leongino Santacruz	El plazo máximo de entrega será de 30 días hábiles, a partir de la recepción de la orden de servicio

LOTE N° 6 RENOVACION Y ACTUALIZACIÓN DE LICENCIA SOFTWARE- ACTIVIDAD 9

Ítem	Descripción del servicio	Cantidad	Unidad de medida de los servicios	Lugar donde los servicios serán prestados	Fecha(s) final(es) de ejecución de los servicios
1	Renovación, Actualización y Soporte Técnico de los Dispositivos con Software Forense UFED TOUCH (Inseyets Pro UFED) y PHYSICAL ANALYZER (InsEYets Pro PA), para Llave / Dongle Serie N° 218776161 (Departamento Contra el Crimen Organizado), Llave / Dongle 886021208 (Departamento Antisecuestro de Personas) y Llave / Dongle 7210903 (Departamento Antisecuestro de Personas)	2	unidad	(Departamento Contra el Crimen Organizado y Departamento Antisecuestro de Personas)	Hasta 15 (quince) días hábiles posteriores a la recepción de la orden de servicio
2	Soporte y Actualización InsEYets Online Limited Unlocks 120	1	unidad	Tesorería de la Actividad 09 - Servicio s Especiales y de Contención - Cnel. Pedro Gracia, 468, Asunción	Hasta 15 (quince) días hábiles posteriores a la recepción de la orden de servicio

Planos y diseños

Para la presente contratación se pone a disposición los siguientes planos o diseños:

No Aplica

Embalajes y documentos

El embalaje, la identificación y la documentación dentro y fuera de los paquetes serán como se indican a continuación:

No Aplica

## Inspecciones y pruebas

Las inspecciones y pruebas serán como se indica a continuación:

No Aplica

# CONDICIONES CONTRACTUALES

Esta sección constituye las condiciones contractuales a ser adoptadas por las partes para la ejecución del contrato.

## Interpretación

1. Si el contexto así lo requiere, el singular significa el plural y viceversa; y "día" significa día corrido, salvo que se haya indicado expresamente que se trata de días hábiles.
2. Condiciones prohibidas, inválidas o inejecutables. Si cualquier provisión o condición del contrato es prohibida o resultase inválida o inejecutable, dicha prohibición, invalidez o falta de ejecución no afectará la validez o el cumplimiento de las otras provisiones o condiciones del contrato.

## Documentación electrónica

Cuando las documentaciones se expidan de manera electrónica en cumplimiento de la Ley N° 6715 "DE PROCEDIMIENTOS ADMINISTRATIVOS" y la Ley N° 6822 "DE SERVICIOS DE CONFIANZAS PARA LAS TRANSACCIONES ELECTRÓNICAS, DEL DOCUMENTO ELECTRÓNICO Y LOS DOCUMENTOS TRANSMISIBLES ELECTRÓNICOS, las mismas se considerarán válidas a los efectos de dar cumplimiento a los requerimientos y obligaciones contractuales, salvo que las normativas exijan una forma determinada.

## Formalización de la contratación

Se formalizará esta contratación mediante:

Contrato

## Documentación requerida para la firma del contrato

Luego de la notificación de adjudicación, el proveedor deberá presentar en el plazo establecido en las reglamentaciones vigentes, los documentos indicados en el presente apartado.

### 1. Personas Físicas / Jurídicas

- Certificado de no encontrarse en quiebra o en convocatoria de acreedores expedido por la Dirección General de Registros Públicos;
- Certificado de no hallarse en interdicción judicial expedido por la Dirección General de Registros Públicos;
- Constancia de no adeudar aporte obrero patronal expedida por el Instituto de Previsión Social.
- Certificado laboral vigente expedido por la Dirección de Obrero Patronal dependiente del Viceministerio de Trabajo, siempre que el sujeto esté obligado a contar con el mismo, de conformidad a la reglamentación pertinente - CPS
- En el caso que suscriba el contrato otra persona en su representación, acompañar poder suficiente del apoderado para asumir todas las obligaciones emergentes del contrato hasta su terminación.
- Certificado de cumplimiento tributario vigente a la firma del contrato.
- Declaración jurada en el que se manifieste que las condiciones verificadas por el Comité respecto a los supuestos del Art. 21 de la Ley N° 7021/22, se mantienen vigentes a la firma del contrato.

### 2. Documentos. Consorcios

- Cada integrante del Consorcio que sea una persona física o jurídica deberá presentar los documentos requeridos para oferentes individuales especificados en los apartados precedentes.
- Original o fotocopia de la Escritura Pública de constitución del Consorcio constituido
- Documentos que acrediten las facultades del firmante del contrato para comprometer solidariamente al consorcio.
- En el caso que suscriba el contrato otra persona en su representación, acompañar poder suficiente del apoderado para asumir todas las obligaciones emergentes del contrato hasta su terminación.

La convocante deberá recurrir a fuentes oficiales para la verificación y comprobación del contenido declarado por el oferente que resultare adjudicado, con anterioridad a la firma del contrato. Si el oferente realizare una declaración jurada falsa, la adjudicación será revocada, la garantía de mantenimiento de oferta será ejecutada y los antecedentes serán remitidos a la Dirección Nacional de Contrataciones Públicas.

Indicadores de Cumplimiento de Contrato

El documento requerido para acreditar el cumplimiento contractual, será:

LOTE N° 1 LICENCIA FORTINET- ACTIVIDAD 2				
Ítem	Descripción del servicio	INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA
1	Software de control de acceso a internet	Nota de Remisión / CONTRATO	ORDEN DE SERVICIO /Nota de Remisión / Acta de recepción	3 (tres) días hábiles a partir de la recepción de Orden de Compra.
LOTE N° 2 ADQUISICIÓN DE SOFTWARE PARA EL DEPARTAMENTO ESPECIALIZADO EN EL CONTROL Y FISCALIZACIÓN DE EMPRESAS DE SEGURIDAD PRIVADA Y AFINES. ACTIVIDAD 5				
Ítem	Descripción del servicio	INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA
1	Licencia de Software de Bases de Datos	Nota de Remisión / CONTRATO	ORDEN DE SERVICIO /Nota de Remisión / Acta de recepción	09 (nueve) semanas desde la recepción de la orden de servicio
LOTE N° 3 LICENCIA SOFTWARE- ACTIVIDAD 8				
Ítem	Descripción del servicio	INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA
1	Desarrollo de software a medida	Nota de Remisión / CONTRATO	ORDEN DE SERVICIO /Nota de Remisión / Acta de recepción	El plazo máximo de entrega y funcionamiento es de 5 días hábiles posteriores a la recepción de la orden de compra/servicio
LOTE N° 4 ADQUISICIÓN DE SERVICIO DE AMPLIACIÓN Y ACTUALIZACIÓN DE SISTEMAS DE ADMISIÓN Y COBRANZAS - ISEPOL- ACTIVIDAD 6				
Ítem	Descripción del servicio	INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA
1	Mantenimiento y actualizacion de software	Nota de Remisión / CONTRATO	ORDEN DE SERVICIO /Nota de Remisión / Acta de recepción	El plazo máximo de entrega será de 30 días hábiles a partir de la recepción de la orden de servicio

LOTE N° 5 DESARROLLO DEL SISTEMA DE GESTION DE CERTIFICADOS, ANTECEDENTES E INFORME DE HISTORIAL ACADEMICO Y MESA DE ENTRADAS - ISEPOL- ACTIVIDAD 6

Ítem	Descripción del servicio	INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA
1	Software para desarrollo de programas	Nota de Remisión / CONTRATO	ORDEN DE SERVICIO /Nota de Remisión / Acta de recepción	El plazo máximo de entrega será de 30 días hábiles, a partir de la recepción de la orden de servicio

LOTE N° 6 RENOVACION Y ACTUALIZACIÓN DE LICENCIA SOFTWARE- ACTIVIDAD 9

Ítem	Descripción del servicio	INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA
1	Renovación, Actualización y Soporte Técnico de los Dispositivos con Software Forense UFED TOUCH (Inseyets Pro UFED) y PHYSICAL ANALYZER (Inseyets Pro PA), para Llave / Dongle Serie N° 218776161 (Departamento Contra el Crimen Organizado), Llave / Dongle 886021208 (Departamento Antisecuestro de Personas) y Llave / Dongle 7210903 (Departamento Antisecuestro de Personas)	Nota de Remisión / CONTRATO	ORDEN DE SERVICIO /Nota de Remisión / Acta de recepción	Hasta 15 (quince) días hábiles posteriores a la recepción de la orden de servicio
2	Soporte y Actualización Inseyets Online Limited Unlocks 120	Nota de Remisión / CONTRATO	ORDEN DE SERVICIO /Nota de Remisión / Acta de recepción	Hasta 15 (quince) días hábiles posteriores a la recepción de la orden de servicio

De manera a establecer indicadores de cumplimiento, a través del sistema de seguimiento de contratos, la convocante deberá determinar el tipo de documento que acredite el efectivo cumplimiento de la ejecución del contrato, así como planificar la cantidad de indicadores que deberán ser presentados durante la ejecución. Por lo tanto, la convocante en este apartado y de acuerdo al tipo de contratación de que se trate, deberá indicar el documento a ser comunicado a través del módulo de Seguimiento de Contratos y la cantidad de los mismos.

## Subcontratación

En caso de que aplique, la subcontratación del contrato deberá ser realizada conforme a las disposiciones contenidas en la Ley, el Decreto Reglamentario y la reglamentación que emita para el efecto la DNCP.

En caso de que la presentación del formulario de personas a subcontratar/subcontratadas, se realice en la etapa contractual, el Administrador del Contrato deberá evaluar el contenido del formulario a los efectos de constatar que el subcontratista no se encuentra comprendido en alguna de las causales de prohibición previstas en el Art. 21 de la Ley N° 7021/22, pudiendo requerir al proveedor o contratista, la información que sea necesaria.

## Derechos Intellectuales

1. Los derechos de propiedad intelectual de todos los planos, documentos y otros materiales conteniendo datos e información proporcionada a la contratante por el proveedor, seguirán siendo, salvo prueba en contrario, de propiedad del proveedor. Si esta información fue suministrada a la contratante directamente o a través del proveedor por terceros, incluyendo proveedores de materiales, los derechos de propiedad intelectual de dichos materiales seguirán siendo de propiedad de dichos terceros.

2. Sujeto al cumplimiento por parte de la contratante del párrafo siguiente, el proveedor indemnizará y liberará de toda responsabilidad a la contratante, sus empleados y funcionarios en caso de pleitos, acciones o procedimientos administrativos, reclamaciones, demandas, pérdidas, daños, costos y gastos de cualquier naturaleza, incluyendo gastos y honorarios por representación legal, que la contratante tenga que incurrir como resultado de la transgresión o supuesta transgresión de derechos de propiedad intelectual como patentes, dibujos y modelos industriales registrados, marcas registradas, derechos de autor u otro derecho de propiedad intelectual registrado o ya existente en la fecha del contrato debido a:

- La instalación de los bienes por el proveedor o el uso de los bienes en la República del Paraguay; y
- La venta de los productos producidos por los bienes en cualquier país.

Dicha indemnización no procederá si los bienes o una parte de ellos fuesen utilizados para fines no previstos en el contrato o para fines que no pudieran inferirse razonablemente del contrato. La indemnización tampoco cubrirá cualquier transgresión que resultará del uso de los bienes o parte de ellos, o de cualquier producto producido como resultado de asociación o combinación con otro equipo, planta o materiales no suministrados por el proveedor en virtud del contrato.



3. Si se entablara un proceso legal o una demanda contra la contratante como resultado de alguna de las situaciones indicadas en la cláusula anterior, la contratante notificará prontamente al proveedor y éste por su propia cuenta y en nombre de la contratante responderá a dicho proceso o demanda, y realizará las negociaciones necesarias para llegar a un acuerdo de dicho proceso o demanda.
4. Si el proveedor no notifica a la contratante dentro de treinta (30) días a partir del recibo de dicha comunicación de su intención de proceder con tales procesos o reclamos, la contratante tendrá derecho a emprender dichas acciones en su propio nombre.
5. La contratante se compromete, a solicitud del proveedor, a prestarle toda la asistencia posible para que el proveedor pueda contestar las citadas acciones legales o reclamaciones. La contratante será reembolsada por el proveedor por todos los gastos razonables en que hubiera incurrido.
6. La contratante deberá indemnizar y eximir de culpa al proveedor y a sus empleados, funcionarios y subcontratistas, por cualquier litigio, acción legal o procedimiento administrativo, reclamo, demanda, pérdida, daño, costo y gasto, de cualquier naturaleza, incluyendo honorarios y gastos de abogado, que pudieran afectar al proveedor como resultado de cualquier transgresión o supuesta transgresión de patentes, modelos de aparatos, diseños registrados, marcas registradas, derechos de autor, o cualquier otro derecho de propiedad intelectual registrado o ya existente a la fecha del contrato, que pudieran suscitarse con motivo de cualquier diseño, datos, planos, especificaciones, u otros documentos o materiales que hubieran sido suministrados o diseñados por la contratante o a nombre suyo.

## Transporte

La responsabilidad por el transporte de los bienes será según se establece en los Incoterms.

Si no está de acuerdo con los Incoterms, la responsabilidad por el transporte deberá ser como sigue:

No Aplica

## Confidencialidad en el procedimiento de contratación y el contrato

La contratante y el proveedor deberán mantener confidencialidad y en ningún momento divulgarán a terceros, sin el consentimiento de la otra parte, documentos, datos u otra información que hubiera sido directa o indirectamente proporcionada por la otra parte en conexión con el contrato, antes, durante o después de la ejecución del mismo. No obstante, el proveedor podrá proporcionar a sus subcontratistas los documentos, datos e información recibidos de la contratante para que puedan cumplir con su trabajo en virtud del contrato. En tal caso, el proveedor obtendrá de dichos subcontratistas un compromiso de confidencialidad similar al requerido al proveedor en la presente cláusula.

La contratante no utilizará dichos documentos, datos u otra información recibida del proveedor para ningún uso que no esté relacionado con el contrato. Así mismo el proveedor no utilizará los documentos, datos u otra información recibida de la contratante para ningún otro propósito diferente al de la ejecución del contrato.

La obligación de las partes arriba mencionadas, no aplicará a la información que:

1. La contratante o el proveedor requieran compartir con otras instituciones que participan en el financiamiento del contrato,
2. Actualmente o en el futuro se hace de dominio público sin culpa de ninguna de las partes,
3. Puede comprobarse que estaba en posesión de esa parte en el momento que fue divulgada y no fue previamente obtenida directa o indirectamente de la otra parte, o
4. Que de otra manera fue legalmente puesta a la disponibilidad de esa parte por un tercero que no tenía obligación de confidencialidad.

Las disposiciones precedentes no modificarán de ninguna manera ningún compromiso de confidencialidad otorgado por cualquiera de las partes a quien esto compete antes de la fecha del contrato con respecto a los suministros o cualquier parte de ellos.

Las disposiciones de esta cláusula permanecerán válidas después del cumplimiento o terminación del contrato por cualquier razón

## Obligatoriedad de declarar información del personal del proveedor, consultor o contratista en el SICP

1. El proveedor deberá proporcionar los datos de identificación de sus subproveedores, así como de las personas físicas por medio de las cuales propone cumplir con las obligaciones del contrato, dentro de los treinta días posteriores a la obtención del código de contratación, y con anterioridad al primer pago que vaya a percibir en el marco de dicho contrato, con las especificaciones respecto a cada una de ellas. A ese respecto, el contratista deberá consignar dichos datos en el Formulario de Identificación del Personal (FIP) y en el Formulario de Identificación de Servicios Personales (FIS), a través del Registro del Proveedor del Estado.
2. Cuando ocurra algún cambio en la nómina del personal o de los subcontratistas propuestos, el proveedor o contratista está obligado a actualizar el FIP.
3. Como requerimiento para efectuar los pagos a los proveedores o contratistas, la contratante, a través del procedimiento establecido para el efecto por la entidad previsional, verificará que el proveedor o contratista se encuentre al día en el cumplimiento con sus obligaciones para con el Instituto de Previsión Social (IPS).
4. La contratante podrá realizar las diligencias que considere necesarias para verificar que la totalidad de las personas que prestan servicios personales en relación de dependencia para la contratista y eventuales subcontratistas se encuentren debidamente individualizados en los listados recibidos.
5. El proveedor o contratista deberá permitir y facilitar los controles de cumplimiento de sus obligaciones de aporte obrero patronal, tanto los que fueran realizados por la contratante como los realizados por el IPS, y por funcionarios de la DNCP. La negativa expresa o tácita se considerará incumplimiento del contrato por causa imputable al proveedor o contratista.
6. En caso de detectarse que el proveedor o contratista o alguno de los subcontratistas, no se encontraran al día con el cumplimiento de sus obligaciones para con el IPS, deberán ser emplazados por la contratante para que en diez (10) días hábiles cumplan con sus obligaciones pendientes con la previsional. En el caso de que no lo hiciera, se considerará incumplimiento del contrato por causa imputable al proveedor o contratista.

## Porcentaje de Garantía de Fiel Cumplimiento de Contrato

El Porcentaje de Garantía de Fiel Cumplimiento de Contrato es de:

10,00 %

El proveedor debe presentar esta garantía dentro de los 10 días corridos siguientes a la fecha de suscripción del contrato.

## Forma de Instrumentación de Garantía de Fiel Cumplimiento de Contrato

La garantía de fiel cumplimiento de contrato adoptará alguna de las siguientes formas: Garantía bancaria o Póliza de Seguros.

## Periodo de validez de la Garantía de Cumplimiento de Contrato

El plazo de vigencia de la Garantía de Fiel Cumplimiento de Contrato será (en días corridos) de:

Desde la suscripción del contrato al 31 de enero de 2027.

Si la entrega de los bienes o la prestación de los servicios, se realizare en un plazo menor o igual a diez (10) días corridos posteriores a la firma del contrato, la garantía de fiel cumplimiento deberá ser entregada antes del cumplimiento de la prestación.

Una vez cumplidas las obligaciones por parte del proveedor o contratista, la Garantía de Fiel Cumplimiento de Contrato podrá ser liberada y devuelta al proveedor, a requerimiento de parte, dentro de los treinta (30) días contados a partir de la fecha de cumplimiento de las obligaciones, incluyendo cualquier obligación relativa a la garantía de los bienes y/o servicios.

## Formas y condiciones de pago

El adjudicado para solicitar el pago de las obligaciones deberá presentar la solicitud acompañada de los siguientes documentos:

### 1. Documentos Genéricos:

- Nota de remisión u orden de prestación de servicios según el objeto de la contratación;
- La factura de pago, con timbrado vigente, la cual deberán expresar claramente por separado el Impuesto al Valor Agregado (IVA) de conformidad con las disposiciones tributarias aplicables. En ningún caso el valor total facturado podrá exceder el valor adjudicado o las adendas aprobadas;
- REPSE (registro de prestadores de servicios) todos los que son prestadores de servicios;
- Certificado de Cumplimiento Tributario;
- Constancia de Cumplimiento con la Seguridad Social;
- Formulario de Identificación de Servicios Personales (FIS);
- Certificado laboral vigente expedido por la Dirección de Obrero Patronal dependiente del Viceministerio de Trabajo, siempre que el sujeto esté obligado a contar con el mismo, de conformidad a la reglamentación pertinente - CPS

Otras formas y condiciones de pago al proveedor en virtud del contrato serán las siguientes:

El pago por la entrega se hará en guaraníes, con fondos provenientes de la Ley del Presupuesto General de la Nación para el año 2025, con Fuente de Financiamiento 10 (FF 10) Recursos Ordinarios del Tesoro y con Fuente de Financiamiento 30 (FF 30) Recursos Institucionales, y sujeto a la aprobación de la partida presupuestaria para el Periodo 2026.

2. La Contratante efectuará los pagos, dentro del plazo establecido en este apartado, sin exceder sesenta (60) días después de la presentación de una factura por el proveedor. La contratante deberá expedirse respecto a la aceptación o rechazo de la factura, a más tardar en quince (15) días corridos posteriores a su presentación.

3. De conformidad a las disposiciones del Decreto N° 7781/2006, del 30 de junio de 2006 y modificatoria, en las contrataciones con Organismos de la Administración Central, el proveedor deberá habilitar su respectiva cuenta corriente o caja de ahorro en un Banco de plaza y comunicar a la Contratante para que ésta gestione ante la Dirección General del Tesoro Público, la habilitación en el Sistema de Tesorería (SITE).

El certificado previsto en el inciso g), se requerirá únicamente para el último pago.

## Solicitud de suspensión de la ejecución del contrato

Si la mora en el pago por parte de la contratante fuere superior a sesenta (60) días corridos, el proveedor, consultor o contratista, tendrá derecho a solicitar por escrito la suspensión de la ejecución del contrato por causas imputables a la contratante.

La solicitud deberá ser respondida por la contratante dentro de los 10 (diez) días hábiles de haber recibido por escrito el requerimiento. Pasado dicho plazo sin respuesta se considerará denegado el pedido, con lo que se agota la instancia administrativa quedando expedita la vía contencioso administrativa.

Si la demora en el pago fuese superior a ciento veinte (120) días corridos, el proveedor, consultor o contratista podrá proceder a la suspensión del cumplimiento del contrato, debiendo comunicar a la contratante con un mes de antelación tal circunstancia, a efectos del reconocimiento de los derechos que puedan derivarse de dicha suspensión, en los términos establecidos en la Ley. En este supuesto, el pago total de lo adeudado por la contratante determinará la continuidad del cumplimiento del contrato.

## Anticipo MIPYMES

Se otorgará Anticipo MIPYMES:

Si

## Solicitud de Pago de Anticipo

El plazo dentro del cual se solicitará el anticipo será (en días corridos) de:

Para todos los Lotes, se solicita la inclusión del Anticipo equivalente al 20% del monto total adjudicado, el pedido es a fin de que el adjudicado cuente con recursos para la ejecución inmediata del contrato y así contar con el bien en el menor plazo posible. Este pedido de Anticipo 20% es solo aplicable a las empresas MIPYMES (Micro, Pequeña y Mediana Empresa) en virtud a la Circular DNCP N° 02/2023.

1. El anticipo es la suma de dinero que se entrega al proveedor, consultor o contratista destinada al financiamiento de los costos en que éste debe incurrir para iniciar la ejecución del objeto contractual. El mismo no constituye un pago por adelantado; debe estar amparado con una garantía correspondiente al cien por ciento de su valor y deberá ser amortizado durante la ejecución del contrato y durante la ejecución de contrato demostrar el debido uso. La Garantía de Anticipo deberá mantener su vigencia hasta su total amortización.

Los recursos entregados en calidad de anticipo no podrán destinarse a fines distintos a los relacionados con el objeto del contrato.

El proveedor, consultor o contratista que reciba pagos en concepto de anticipo estará obligado a informar a la contratante sobre el destino y la forma de aplicación del mismo, que en todos los casos estará relacionado al efectivo cumplimiento del contrato.

En caso de extensión de la Garantía de Anticipo, la misma deberá cubrir el saldo pendiente de amortización.

2. Si se establece en el SICP el otorgamiento de anticipos, no podrá superar en ningún caso el porcentaje establecido en la legislación vigente.

3. La solicitud de pago del anticipo deberá ser presentada por escrito, con la factura, el plan de inversiones y la Garantía de Anticipo.

4. El proveedor podrá remitir una comunicación por escrito a la contratante, en la cual informe que rechaza el anticipo previsto en el PBC. La falta de solicitud de anticipo en el plazo previsto en el PBC será considerada como un rechazo del mismo. En estos casos podrá darse inicio al cómputo de la ejecución contractual en las condiciones establecidas en el pliego de bases y condiciones.

5. El Pago del Anticipo debe ser total. En el caso que se realice el pago de un porcentaje inferior al 100% del mismo, el proveedor podrá rechazarlo en el plazo de cinco (5) días hábiles mediante una nota de reclamo remitida a la Contratante. Transcurrido dicho plazo, se considerará que el Anticipo ha sido aceptado por el proveedor y podrá darse inicio al cronograma de ejecución contractual en las condiciones establecidas en el pliego de bases y condiciones.

6. En el caso de que el proveedor haya solicitado el anticipo en las condiciones establecidas en la presente cláusula y la convocante no ha procedido al pago, el oferente no está obligado a iniciar la ejecución del contrato hasta tanto el pago se haya efectuado de forma total o de acuerdo a lo dispuesto en el punto 5.

7. La amortización del anticipo se realizará de acuerdo con lo establecido en el contrato, en la proporción que éste indique.

8. Para la ejecución de esta garantía, especialmente cuando sea instrumentada a través de Póliza de Seguro de caución, será requisito que previamente el proveedor sea notificado del incumplimiento y la intimación de que se hará efectiva la ejecución del monto asegurado.

9. A menos que se indique otra cosa en este apartado, la Garantía de Anticipo será liberada por la contratante y devuelta al proveedor, a requerimiento de parte, a más tardar treinta (30) días contados a partir de la fecha de cumplimiento de las obligaciones del proveedor en virtud del contrato, pudiendo ajustarse por el saldo adeudado.

10. En el caso de rescisión o terminación anticipada del contrato, los proveedores o contratistas deberán reintegrar a la contratante el saldo por amortizar

## Forma de Instrumentación de Garantía de anticipo

La forma de instrumentación de la Garantía de Anticipo será:

Póliza de Seguro

## Reajuste

El precio del contrato estará sujeto a reajustes. La fórmula y el procedimiento para el reajuste serán los siguientes:

Los precios ofertados estarán sujetos a reajustes, siempre y cuando la variación del IPC publicado por el BCP haya sufrido una variación igual o mayor al quince por ciento (15%) referente a la fecha de apertura de ofertas. El reajuste de precio deberá ser solicitado por el Contratista y aprobado por el Contratante por medio de notas oficiales. Los precios reajustados, solo tendrán incidencia sobre los bienes y/o servicios aún no proveídos; y, no tendrán ningún efecto retroactivo respecto a los ya fueron proveídos antes de la verificación del reajuste. El Precio Reajustado del Contrato, estará determinado por la siguiente fórmula:

$$Pr = P \times IPC1$$

IPC0

Pr: Precio Reajustado

P: Precio adjudicado

IPC1: Índice de precios al Consumidor publicado por el Banco Central del Paraguay, correspondiente al mes de la entrega del suministro.

IPC0: Índice de precios al Consumidor publicado por el Banco Central del Paraguay, correspondiente al mes de la apertura de ofertas.

En caso de que el Proveedor se halle atrasado con respecto al plazo de entrega indicado en el contrato, no se reconocerá reajuste de precios por variaciones en el IPC con posterioridad a las fechas de entrega establecidas en dicho contrato.

La variación del valor del contrato por reajuste de precios, no constituye modificación del contrato en los términos de la Ley N° 7021/22 "De Suministro y Contrataciones Públicas", sin embargo, deberá contar con un Código de Contratación, para cuya obtención se deberá cumplir con los requerimientos establecidos por la DNCP.

## Porcentaje de multas

El valor del porcentaje de multas que será aplicado por el atraso en la entrega de los bienes, prestación de servicios será de:

0,05 %

La contratante podrá deducir en concepto de multas una suma equivalente al porcentaje del precio de entrega de los bienes atrasados, por cada día de atraso indicado en este apartado.

La aplicación de multas no libera al proveedor del cumplimiento de sus obligaciones contractuales.

## Tasa de interés por Mora

En caso de que la contratante incurriera en mora en los pagos, se aplicará una tasa de interés por cada día de atraso, del:

0,02

En ningún caso el porcentaje podrá superar al tope máximo definido en la Resolución MEF N° 12/2025, en cuyo supuesto, se aplicará un ajuste automático al contrato con los topes respectivos, de conformidad a las reglas establecidas en la mencionada resolución, según se traten de contratos en guaraníes o en dólares estadounidenses.

La mora será computada a partir del día siguiente del vencimiento del pago y no incluye el día en el que la contratante realiza el pago.

Si la contratante no efectuara cualquiera de los pagos al proveedor en las fechas de vencimiento correspondiente, la contratante pagará al proveedor interés sobre los montos de los pagos morosos a la tasa establecida en este apartado, por el período de la demora hasta que haya efectuado el pago completo, ya sea antes o después de cualquier juicio.

Si la mora fuera superior a 60 días, el proveedor, consultor o contratista tendrá derecho a la suspensión del contrato, por motivos que no le serán imputables, previa comunicación a la contratante, de acuerdo a lo establecido en el artículo 66 de la Ley N° 7021/22.

## Impuestos y derechos

En el caso de bienes de origen extranjero, el proveedor será totalmente responsable del pago de todos los impuestos, derechos, gravámenes, timbres, comisiones por licencias y otros cargos similares que sean exigibles fuera y dentro de la República del Paraguay, hasta el momento en que los bienes contratados sean entregados al contratante.

En el caso de origen nacional, el proveedor será totalmente responsable por todos los impuestos, gravámenes, comisiones por licencias y otros cargos similares incurridos hasta el momento en que los bienes contratados sean entregados a la contratante.

El proveedor será responsable del pago de todos los impuestos y otros tributos o gravámenes con excepción de los siguientes:

No Aplica

## Convenios Modificatorios

La contratante podrá acordar modificaciones al contrato conforme al artículo N° 67 de la Ley N° 7021/22 "De Suministro y Contrataciones Públicas".

1. Cuando el sistema de adjudicación adoptado sea de abastecimiento simultáneo las ampliaciones de los contratos se regirán por las disposiciones contenidas en la Ley N° 7021/22, sus modificaciones y reglamentaciones, que para el efecto emita la DNCP.
2. Tratándose de contratos abiertos, las modificaciones a ser introducidas se regirán atendiendo a la reglamentación vigente.
3. La celebración de un convenio modificatorio conforme a las reglas establecidas en el artículo N° 67 de la Ley N° 7021/22, que constituyan condiciones de agravación del riesgo cuando la Garantía de Cumplimiento de Contrato sea formalizada a través de póliza de seguro, obliga al proveedor a informar a la compañía aseguradora sobre las modificaciones a ser realizadas y en su caso, presentar ante la contratante los endosos por ajustes que se realicen a la póliza original en razón al convenio celebrado con la contratante.

## Limitación de responsabilidad

Excepto en casos de negligencia grave o actuación de mala fe, el proveedor no tendrá ninguna responsabilidad contractual de agravio o de otra índole frente a la contratante por pérdidas o daños indirectos o consiguientes, pérdidas de utilización, pérdidas de producción, o pérdidas de ganancias o por costo de intereses, estipulándose que esta exclusión no se aplicará a ninguna de las obligaciones del proveedor de pagar a la contratante las multas previstas en el contrato.

## Responsabilidad del proveedor

El proveedor deberá suministrar todos los bienes o servicios de acuerdo con las condiciones establecidas en el pliego de bases y condiciones, sin perjuicio de las responsabilidades establecidas en la Ley N° 7021/22.

## Caso Fortuito o Fuerza Mayor

El proveedor no estará sujeto a la ejecución de su Garantía de Cumplimiento, liquidación por daños y perjuicios o terminación por incumplimiento en la medida en que la demora o el incumplimiento de sus obligaciones en virtud del contrato sea el resultado de un evento de Caso fortuito o Fuerza Mayor.

Para fines de esta cláusula, "Fuerza Mayor" significa un evento o situación fuera del control del proveedor que es imprevisible, inevitable y no se origina por descuido o negligencia del mismo. Tales eventos pueden incluir sin que éstos sean los únicos actos de la autoridad en su capacidad soberana, catástrofes naturales, incendios, inundaciones, epidemias, pandemias, restricciones de cuarentena, embargos de cargamentos, explosiones, guerras, insurrección, movilización, huelgas, temblores de tierras y decisiones gubernamentales.

Para fines de esta cláusula, "Caso Fortuito" significa es un evento extraordinario, imprevisto, inevitable, que imposibilita absolutamente el cumplimiento de la prestación y/u obligación.

El proveedor deberá demostrar el nexo existente entre el caso notorio y la obligación pendiente de cumplimiento. El caso fortuito o la fuerza mayor solamente podrá afectar a la parte del contrato cuyo cumplimiento imposible fue demostrado.

Por consiguiente, no se considerarán como casos fortuitos o de Fuerza Mayor los actos o acontecimientos cuya ocurrencia podría preverse y cuyas consecuencias podrían evitarse actuando con diligencia razonable. De la misma manera, no se considerarán caso fortuito o fuerza mayor los actos o acontecimientos que hagan el cumplimiento de una obligación únicamente más difícil o más onerosa para la parte correspondiente.

Si se produjera un acontecimiento de Caso fortuito o fuerza mayor, el contratista tendrá derecho a una prórroga razonable de los plazos de ejecución.

Si se presentara un evento de Caso Fortuito o de Fuerza Mayor, el proveedor notificará por escrito a la contratante sobre dicha condición y causa, en el plazo de siete (7) días calendario a partir del día siguiente en que el proveedor haya tenido conocimiento del evento o debiera haber tenido conocimiento del evento. Transcurrido el mencionado plazo, sin que el proveedor o contratista haya notificado a la convocante la situación que le impide cumplir con las condiciones contractuales, no podrá invocar caso fortuito o fuerza mayor. Excepcionalmente, la convocante bajo su responsabilidad, podrá aceptar la notificación del evento de caso fortuito o de fuerza mayor en un plazo mayor, debiendo acreditar el interés público comprometido.

El caso fortuito o de fuerza mayor debe ser invocado con posterioridad a la suscripción del contrato y durante la vigencia del contrato, siempre y cuando el hecho haya ocurrido dentro del plazo de ejecución contractual.

A menos que la contratante disponga otra cosa por escrito, el proveedor continuará cumpliendo con sus obligaciones en virtud del contrato en la medida que sea razonablemente práctico, y buscará todos los medios alternativos de cumplimiento que no estuviesen afectados por la situación de caso fortuito o fuerza mayor existente

## Causales de terminación del contrato

### 1. Terminación por Incumplimiento

a) La contratante, sin perjuicio de otros recursos a su disposición en caso de incumplimiento del contrato, podrá terminar el contrato, en cualquiera de las siguientes circunstancias:

- i. Si el proveedor no entrega parte o ninguno de los bienes dentro del período establecido en el contrato, o dentro de alguna prórroga otorgada por la contratante; o
- ii. Si el proveedor no cumple con cualquier otra obligación en virtud del contrato; o
- iii. Si el proveedor, a juicio de la contratante, durante el proceso de licitación o de ejecución del contrato, ha participado en actos de fraude y corrupción;
- iv. Cuando las multas por atraso superen el monto de la Garantía de Cumplimiento de Contrato;
- v. Por suspensión de los trabajos, imputable al proveedor o al contratista, por más de sesenta días calendarios, sin que medie fuerza mayor o caso fortuito;
- vi. En los demás casos previstos en este apartado.

### 2. Terminación por insolvencia o quiebra

La contratante podrá terminar el contrato mediante comunicación por escrito al proveedor si éste se declarase en quiebra o en estado de insolvencia.

### 3. Terminación por conveniencia

a) La contratante podrá en cualquier momento terminar total o parcialmente el contrato por razones de interés público debidamente justificada, mediante notificación escrita al proveedor. La notificación indicará la razón de la terminación, así como el alcance de la terminación con respecto a las obligaciones del proveedor, y la fecha en que se hace efectiva dicha terminación.

b) Los bienes que ya estén fabricados y estuviesen listos para ser enviados a la contratante dentro de los treinta (30) días siguientes a la fecha de recibo de la notificación de terminación del contrato deberán ser aceptados por la contratante de acuerdo con los términos y precios establecidos en el contrato. En cuanto al resto de los bienes la contratante podrá elegir entre las siguientes opciones:

-Que se complete alguna porción y se entregue de acuerdo con las condiciones y precios del contrato; y/o

-Que se cancele la entrega restante y se pague al proveedor una suma convenida por aquellos bienes que hubiesen sido parcialmente completados y por los materiales y repuestos adquiridos previamente por el proveedor.

Se podrán establecer otras causales de terminación de contrato, de acuerdo a su naturaleza, y se deberán tener en cuenta además, las previstas en el artículo 72 y concordantes de la Ley N° 7021/22.

## Otras causales de terminación del contrato

Además de las ya indicadas en la cláusula anterior, otras causales de terminación de contrato son:

No Aplica

## Medio alternativo de Resolución de Conflictos a través del Avenimiento.

“Los contratistas, proveedores, consultores y contratantes, podrán solicitar la intervención de la Dirección Nacional de Contrataciones Públicas alegando el incumplimiento de los términos y condiciones pactados en los contratos regidos por la Ley N° 7021/22. Una vez recibida la solicitud respectiva, dentro de los 15 (quince) días hábiles siguientes a la fecha de su recepción, la Dirección Nacional de Contrataciones Públicas señalará día y hora para audiencia de avenimiento a la que serán citadas las partes. Los requisitos y formalidades para admitir o rechazar la solicitud de intervención, así como los demás trámites del procedimiento de avenimiento serán dispuestos en la reglamentación. Serán aplicables al procedimiento de Avenimiento las disposiciones contenidas en la sección I del Capítulo XVI “PROCEDIMIENTOS JURIDICOS SUSTANCIADOS ANTE LA DIRECCIÓN NACIONAL DE CONTRATACIONES PÚBLICAS” de la Ley N° 7021/22.

## Medio Alternativo de Resolución de Conflictos a través de la Mediación

El procedimiento de Mediación se podrá llevar a cabo ante:

No Aplica

El mediador deberá pertenecer a las Listas del Poder Judicial o del CAMP, según la selección de sede establecida.

## Medio alternativo de Resolución de Conflictos a través del Arbitraje

El procedimiento arbitral se podrá llevar a cabo ante las sedes del Centro de Arbitraje y Mediación del Paraguay (en adelante, "CAMP"). El tribunal será conformado por:

No Aplica

El o los árbitros designados deberán pertenecer a la lista del cuerpo arbitral del CAMP, que decidirá conforme a derecho, siendo el laudo definitivo y vinculante para las partes.

---

## MODELO DE CONTRATO

Este modelo de contrato, constituye la proforma del contrato a ser utilizado una vez adjudicado al proveedor y en los plazos dispuestos para el efecto por la normativa vigente.

EL MODELO DE CONTRATO SE ENCUENTRA EN UN ARCHIVO ANEXO A ESTE DOCUMENTO.



## FORMULARIOS

Los formularios dispuestos en esta sección son los estándar a ser utilizados por los potenciales oferentes para la preparación de sus ofertas.

ESTA SECCIÓN DE FORMULARIOS SE ENCUENTRA EN UN ARCHIVO ANEXO A ESTE DOCUMENTO, DEBIENDO LA CONVOCANTE MANTENERLO EN FORMATO EDITABLE A FIN DE QUE EL OFERENTE LO PUEDA UTILIZAR EN LA PREPARACION DE SU OFERTA.

