
PLIEGO DE BASES Y CONDICIONES

Convocante:

Banco Nacional de Fomento (BNF)
Uoc Bnf

Nombre de la Licitación:

SERVICIO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC)
(versión 2)

ID de Licitación:

485892



Modalidad:

Licitación Pública Nacional

Publicado el:

05/10/2026

"Pliego para la Adquisición de Bienes y/o Servicios - CONVENCIONAL - Ley N° 7021/22."
Versión 4

RESUMEN DEL LLAMADO

Datos de la Convocatoria

ID de Licitación:	485892	Nombre de la Licitación:	SERVICIO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC)
Convocante:	Banco Nacional de Fomento (BNF)	Categoría:	81000000 - Servicios basados en ingeniería investigación y tecnología
Unidad de Contratación:	Uoc Bnf	Tipo de Procedimiento:	LPN - Licitación Pública Nacional

Etapas y Plazos

Lugar para Realizar Consultas:	Sistema DNCP	Fecha Límite de Consultas:	12/10/2026 12:00
Lugar de Entrega de Ofertas:	En las oficinas de la GDOC - Casa Matriz del BNF (25 de Mayo casi Yegros)	Fecha de Entrega de Ofertas:	16/10/2026 09:00
Lugar de Apertura de Ofertas:	En las oficinas de la GDOC - Casa Matriz del BNF (25 de Mayo casi Yegros).	Fecha de Apertura de Ofertas:	16/10/2026 09:15

Adjudicación y Contrato

Sistema de Adjudicación:	Total	Anticipo:	No se otorgará anticipo
Vigencia del Contrato:	Hasta cumplimiento total de obligaciones		

Datos del Contacto

Nombre:	Silvio Eduardo Estigarribia Quiñones.	Cargo:	Gerente de la Gerencia Departamental Operativa de Contrataciones
Teléfono:	021 4191496	Correo Electrónico:	contrataciones@bnf.gov.py

ADENDA

Adenda

Las modificaciones al presente procedimiento de contratación son los indicados a continuación:

ADENDA N° 1

Señores

Presente:

Tenemos el agrado de dirigirnos a ustedes, con relación a la LICITACIÓN PÚBLICA NACIONAL BNF LPN N.º 13/2026 para el SERVICIO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC) ID N.º 485.892.

Conforme a la Providencia DNCP con fecha de emisión 21 de septiembre de 2026, cumplimos en informar la modificación de **las etapas y plazos**, quedando conforme a lo establecido en el Sistema de Información de Contrataciones Públicas (SICP).

Asimismo, se informa que el Pliego de Bases y Condiciones **quedará modificado específicamente en los siguientes puntos:**

REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN

EXPERIENCIA REQUERIDA

Demostrar la experiencia en la provisión del Servicio de Centro de Operaciones de Seguridad SOC con facturaciones de venta, contratos y/o recepciones finales, por un monto equivalente al 40% como mínimo del monto total ofertado en el presente procedimiento de contratación, de los últimos 5 (cinco) años (2021, 2022, 2023, 2024 y 2025). Las sumatorias de las facturaciones deben alcanzar el porcentaje indicado, no será necesaria la presentación del porcentaje del monto establecido por cada año.

CAPACIDAD TÉCNICA

g. 1 (un) Analista de Seguridad SOC, in-situ:

- El personal debe contar con al menos 3 certificaciones y/o cursos de ciberseguridad de organizaciones reconocidas internacionalmente, tales como ISC2, ISACA, EC-Council, ISO, Fortinet, Cisco, Microsoft, Certiprot, Hack The Box, PortSwigger Academy y TryHackMe

REQUISITOS DOCUMENTALES PARA EVALUAR EL CRITERIO DE CAPACIDAD TÉCNICA

a. 1 (un) Director General del Servicio de Ciberseguridad:

- Presentación de Curriculum Vitae, adjuntando copias de las certificaciones correspondientes y/o certificaciones que se encuentren en proceso de renovación con constancia de vigencia, títulos universitarios, conforme a lo solicitado en el apartado de capacidad técnica
- El director debe encontrarse inscripto en la Planilla de IPS del oferente y contar con una antigüedad mínima comprobable de 6 (seis) meses de vínculo laboral con la empresa oferente.

b. 1 (un) Coordinador de SOC / Líder Operativo:

- Presentación de Curriculum Vitae, adjuntando copias de las certificaciones correspondientes y/o certificaciones que se encuentren en proceso de renovación con constancia de vigencia, títulos universitarios, conforme a lo solicitado en el apartado de capacidad técnica.
- El coordinador debe encontrarse inscripto en la Planilla de IPS del oferente y contar con una antigüedad mínima comprobable de 6 (seis) meses de vínculo laboral con la empresa oferente.

c. 3 (tres) Analistas de Seguridad SOC:

- Presentación de Curriculum Vitae, adjuntando copias de las certificaciones correspondientes y/o certificaciones que se encuentren en proceso de renovación con constancia de vigencia, constancia de estudiante de carreras informáticas o afines, con independencia del año en curso, acreditable mediante historial académico y/o constancia o proforma de inscripción universitaria vigente, y/o título, conforme a lo solicitado en el apartado de capacidad técnica.

d. 1 (un) Especialista en Cacería de Amenazas (Threat Hunting):

- Presentación de Curriculum Vitae, adjuntando copias de las certificaciones correspondientes, y/o certificaciones que se encuentren en proceso de renovación con constancia de vigencia constancia de estudiante de carreras informáticas o afines, con independencia del año en curso, acreditable mediante historial académico y/o constancia o proforma de inscripción universitaria vigente, y/o título, conforme a lo solicitado en el apartado de capacidad técnica.

e. 1 (un) Arquitecto de Ciberseguridad:

- Presentación de Curriculum Vitae, adjuntando copias de las certificaciones correspondientes, y/o certificaciones que se encuentren en proceso de renovación con constancia de vigencia, constancia de estudiante de carreras informáticas o afines, con independencia del año en curso, acreditable mediante historial académico y/o constancia o proforma de inscripción universitaria vigente, y/o título, conforme a lo solicitado en el apartado de capacidad técnica.

f. 2 (dos) Analistas de Ciberseguridad:

- Presentación de Curriculum Vitae, adjuntando copias de las certificaciones correspondientes, y/o certificaciones que se encuentren en proceso de renovación con constancia de vigencia, constancia de estudiante de carreras informáticas o afines, con independencia del año en curso, acreditable mediante historial académico y/o constancia o proforma de inscripción universitaria vigente, y/o título, conforme a lo solicitado en el apartado de capacidad técnica.

SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS

DETALLE DE LOS BIENES Y/O SERVICIOS

EL OFERENTE DEBERÁ CONTAR CON LOS SIGUIENTES PERFILES TÉCNICOS:

7. Analista de Seguridad SOC, in-situ (Cantidad: 1 (uno)), quien será responsable de las tareas operativas y de seguimiento, y nexo de las tareas de remediación, además de las tareas operativas de gestión de eventos e incidentes de seguridad, modalidad presencial in situ, de lunes a viernes, horario de 08:00 a 16:00 horas, conforme al numeral 1.3 «Modalidad de atención remota y presencial» (Sección 1 Generalidades del Servicio) de las EETT.

1. GENERALIDADES DEL SERVICIO

CARACTERÍSTICA	DESCRIPCIÓN TÉCNICA	MÍNIMO REQUERIDO
1.2. Continuidad operativa del servicio	El servicio deberá garantizar la continuidad operativa permanente de las capacidades de monitoreo, detección, análisis y gestión de incidentes, sin interrupciones que afecten la capacidad de respuesta ante eventos de ciberseguridad.	Exigido

CARACTERÍSTICA	DESCRIPCIÓN TÉCNICA	MÍNIMO REQUERIDO
	El oferente deberá disponer de un Centro de Operaciones de Seguridad (SOC) principal en la República del Paraguay y un centro secundario —ya sea propio, de un tercero o mediante un servicio de nube pública—; se exigirá una distancia lineal mínima de 50 kilómetros entre ambos centros únicamente cuando el sitio secundario corresponda a una infraestructura física, quedando exceptuado dicho requisito de distancia en caso de optar por una solución en la nube pública, debiendo el proponente acreditar fehacientemente en cualquier modalidad la alta disponibilidad, la resiliencia y la continuidad operativa del servicio.	Exigido
	El servicio deberá apoyarse en plataformas con alta disponibilidad, tolerancia a fallos y mecanismos de redundancia acordes a entornos de misión crítica.	Exigido
	El servicio deberá contar con cobertura operativa continua (24x7) para la atención de eventos e incidentes de ciberseguridad durante toda la vigencia del contrato, basado en un esquema de turnos, roles definidos y mecanismos de escalamiento técnico funcional en base a la criticidad de los incidentes.	Exigido
	La convocante podrá requerir la documentación y/o verificaciones que considere pertinentes para acreditar el carácter operativo de ambos Centros de Operaciones de Seguridad, tanto durante la evaluación de las ofertas como durante la ejecución del contrato.	Exigido
	El segundo Centro de Operaciones de Seguridad deberá contar con capacidad operativa para sostener la continuidad de las capacidades críticas del servicio (monitoreo, detección y respuesta) ante la indisponibilidad total o parcial del centro principal, no admitiéndose su mera existencia física.	Exigido
	Ambos Centros de Operaciones de Seguridad deberán permanecer operativos durante toda la vigencia del contrato. La convocante se reserva la facultad de verificar el cumplimiento de esta condición durante la ejecución por los medios que estime pertinentes.	Exigido

2. ARQUITECTURA DEL SERVICIO Y MODELO OPERATIVO DEL SOC Y CSIRT

CARACTERÍSTICA	DESCRIPCIÓN TÉCNICA	MÍNIMO REQUERIDO
2.2. Modelo de Operación	El modelo operativo deberá permitir la ejecución de actividades de análisis y respuesta de forma distribuida entre equipos especializados, manteniendo una coordinación centralizada del incidente. Serán aceptadas arquitecturas basadas en software libre, plataformas open source o soluciones híbridas, siempre que cumplan con los niveles de servicio requeridos.	Exigido

9. INVESTIGACIÓN Y ANÁLISIS FORENSE

CARACTERÍSTICA	DESCRIPCIÓN TÉCNICA	MÍNIMO REQUERIDO
9.12 Prohibición de investigación puramente manual	No se aceptarán ofertas donde las capacidades de investigación y análisis forense dependan exclusivamente de actividades manuales, herramientas aisladas o servicios profesionales no integrados al SOC. El servicio deberá contar con capacidades de análisis forense con validez probatoria, conforme a las buenas prácticas internacionales de identificación, recolección, adquisición y preservación de evidencia digital (ISO/IEC 27037). A tal efecto, la adquisición y el tratamiento de la evidencia deberán realizarse con herramientas forenses reconocidas y validadas en la industria que garanticen la no alteración de la evidencia original —incluyendo mecanismos de bloqueo de escritura (write-blocking)—, la integridad mediante funciones criptográficas de hash, la trazabilidad y la cadena de custodia.	Exigido

Los demás requisitos no mencionados expresamente en la presente Adenda permanecen sin variación.

Se detectaron modificaciones en las siguientes cláusulas:

Sección: Requisitos de participación y criterios de evaluación

- Experiencia requerida
- Capacidad Técnica
- Requisitos documentales para evaluar el criterio de capacidad técnica

Sección: Suministros requeridos - especificaciones técnicas

- Detalle de los bienes y/o servicios

Se puede realizar una comparación de esta versión del pliego con la versión anterior en el siguiente enlace: <https://www.contrataciones.gov.py/licitaciones/convocatoria/1f131b63-38b7-6ec4-8454-2d5ff024094f/pliego/2/diferencias/1.html?seccion=adenda>

La adenda es el documento emitido por la convocante, mediante la cual se modifican aspectos establecidos en las bases de la contratación. A los efectos legales, la adenda será considerada parte integrante del documento cuyo contenido modifique.

La convocante podrá introducir modificaciones cuando se ajuste a los parámetros establecidos en la Ley.

Las adendas serán difundidas en el SICP respetando los plazos establecidos en la resolución por la cual se Reglamentan los Procedimientos de Contratación regidos por la Ley N° 7021/22.

Obs: Cuando la convocante requiera prorrogar la fecha tope de presentación y apertura de ofertas, sin modificar los demás datos e información de las bases de la contratación, será difundida automáticamente a través del SICP y no se instrumentará a través de adenda.

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 SICP. Es responsabilidad del oferente examinar todos los documentos y la información de la convocatoria que obren en el mismo.

Contratación Pública Sostenible - 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, por medio de prácticas como la modificación de los procesos de producción, manutención y mantenimiento de equipos y gestión de las instalaciones, así como 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 por las convocantes 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.

Formato y firma de la oferta

1. El formulario de oferta y la lista de precios serán firmados, física o electrónicamente, según corresponda 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. Los textos entre líneas, tachaduras o palabras superpuestas serán válidos solamente si llevan la firma de la persona que firma la oferta.
4. La falta de foliatura no podrá ser considerada como motivo de descalificación de las ofertas.
5. Cuando la Garantía de Mantenimiento de Ofertas sea instrumentada a través de Declaración Jurada, deberá estar firmada en todas sus páginas.

Plazo para presentar las ofertas

Las ofertas deberán ser presentadas en la fecha y hora que se indican 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 apertura de ofertas.

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.

Cuando la presentación de oferta sea electrónica la misma deberá sujetarse a la reglamentación vigente.

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

Cuando la presentación de la oferta se realice a través del módulo de oferta electrónica, se considerará que el listado de ítems forma parte del formulario de oferta electrónico, y deberá sujetarse en todo lo demás a la reglamentación vigente.

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

- a) El precio cotizado deberá ser el mejor precio posible, considerando que en la oferta no se aceptará la inclusión de descuentos de ningún tipo.
- b) 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.
- c) 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 a la planilla de precios.
- d) 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 a la planilla de precios.
- e) En todos los casos, independientemente 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. Los precios indicados en la lista de precios serán consignados separadamente, de acuerdo a lo previsto en el SICP y según se detalla a continuación:

- 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 ensamble de los bienes;
- b) Todo impuesto al valor agregado u otro tipo de impuesto que obligue 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 multiplicando 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. 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 simultáneo, en este apartado se deberá indicar la manera de distribución de los mismos:

No Aplica

Supuesto de abastecimiento simultáneo

El abastecimiento se registrará por el supuesto de:

No Aplica

Moneda de la oferta y pago

La moneda de la oferta y pago será:

Moneda Nacional

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 decimos y céntimos.

Moneda extranjera

La moneda extranjera para la oferta y pago, será:

No Aplica

Copias de la oferta - CPS

El oferente presentará su oferta original. Adicionalmente, la convocante podrá requerir copias de las ofertas en la cantidad indicada en este apartado, las copias deberán estar indicadas como tales.

Cuando la presentación de las ofertas se realice a través del módulo de Oferta Electrónica, la convocante no requerirá de copias.

Cantidad de copias requeridas:

Ninguna Copia

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 del Perfil del proveedor.**
 - 1.1. Ofertas físicas

Los oferentes inscriptos en el Registro de Proveedores del Estado, podrán presentar con su oferta, la Constancia del Perfil del Proveedor que contiene el reporte de los documentos obrantes en el Registro.

Con su presentación en la oferta, dicha constancia reemplazará a los documentos solicitados por la convocante en el presente pliego.
Será considerada válida la Constancia que se presente con firma manuscrita o electrónica cualificada por él o los representantes legales.

1.2.Ofertas electrónicas

Cuando la presentación de oferta sea electrónica, 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.

Ofertas Alternativas

Se permitirá la presentación de oferta alternativa, según los siguientes criterios a ser considerados para la evaluación de la misma:

No Aplica

Una oferta alternativa se configura necesariamente con la presentación de la oferta principal, que se ajuste a las condiciones previstas en las bases y condiciones; y, de manera separada e independiente una propuesta alternativa, que implique alternativas técnicas a los requerimientos de la licitación y cuya consideración estaría sujeta a que dicha alternativa reúna mejores condiciones de oportunidad, calidad y costo.

Periodo de validez de las ofertas

Las ofertas deberán mantenerse válidas por:

90

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 a los oferentes la extensión del periodo de validez de la oferta. En caso de aceptar dicha solicitud, el oferente deberá manifestar su consentimiento de forma expresa, y, en consecuencia, prorrogar igualmente la Garantía de Mantenimiento de la Oferta.

El oferente podrá rechazar la solicitud de prórroga sin que ello implique la ejecución de su Garantía de Mantenimiento de la Oferta. En caso de aceptar la extensión solicitada, no se le pedirá ni se le permitirá modificar su oferta.

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:
 - a. Garantía bancaria emitida por un banco establecido en la República del Paraguay, la que deberá ajustarse a las condiciones establecidas por la DNCP.
 - b. 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.
 - c. En los procedimientos, cuyo monto de estimación de la contratación sea inferior a los dos mil (2.000) jornales mínimos, se admitirá la instrumentación de las garantías de mantenimiento de ofertas a través de Declaraciones Juradas con certificación de firma por Escribano Público. La certificación de firma podrá corresponder a la misma fecha del documento certificado o a una fecha posterior, siempre y cuando sea de fecha previa a la presentación y apertura de sobres.
 - d. En caso de utilizarse el Módulo de Ofertas Electrónicas, las declaraciones juradas serán generadas y firmadas a través del módulo y no requerirán certificación de firmas.
- 1.2. En los contratos abiertos, el porcentaje de las garantías a ser presentado por los oferentes que participen, deberá ser aplicado sobre el monto máximo total del llamado; si la adjudicación fuese por lote o ítem ofertado, deberán sumarse los valores máximos de cada lote o ítem ofertado, o de la suma de los valores máximos obtenidos por la multiplicación de los precios unitarios ofertados con las cantidades máximas, a fin de obtener el monto sobre el cual se aplicará el porcentaje de la citada garantía.
- 1.3. En caso de instrumentarse las garantías a través de Garantía Bancaria o Declaración jurada, 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:

- a. Consorcio 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.
- b. Consorcio 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:

- a. Si el oferente altera las condiciones de su oferta,
- b. Si el oferente retira su oferta durante el período de validez de ofertas,
- c. Si no acepta la corrección aritmética del precio de su oferta, en caso de existir, o
- d. Si el adjudicatario no procede, por causa imputable al mismo a:
 - d.1 Firmar el contrato,
 - d.2 Suministrar los documentos indicados en las bases de la contratación para la firma del contrato,
 - d.3 Suministrar en tiempo y forma la garantía de cumplimiento de contrato,
- e. Cuando se comprobare que las declaraciones juradas presentadas por el oferente adjudicado con su oferta sean falsas,
- f. No se formaliza el consorcio por escritura pública antes de la firma del contrato.
- g. Si el adjudicatario no presentare las legalizaciones correspondientes para la firma del contrato, cuando éstas sean requeridas.

La Garantía de Mantenimiento de Oferta, sea cual fuere la forma de instrumentación adoptada, cuando se tenga acreditada una de las causales de ejecución de la garantía deberá ser pagadera según el tipo de garantía que haya sido solicitada.

Periodo de Validez de la Garantía de Mantenimiento de Oferta

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

120

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.

El plazo mínimo de validez será de al menos 30 días posteriores al plazo de validez establecido para las ofertas.

Condiciones especiales de la Garantía de Mantenimiento de Oferta

Las condiciones especiales de la Garantía de Mantenimiento de Oferta serán:

No Aplica

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 de ofertas

El método de presentación de ofertas para esta convocatoria será:

Un sobre

En caso de presentación física, los sobres deberán:

1. Indicar el nombre, RUC y la dirección del oferente;
2. Estar dirigidos a la convocante;
3. Llevar la identificación específica del proceso de contratación indicado en el SICP; y
4. Llevar una advertencia de no abrir antes de la hora y fecha de apertura de ofertas.
5. Identificar si se trata de un sobre técnico o económico.

Para los casos de consorcios con acuerdo de intención, los sobres deberán contemplar el RUC provisorio generado en el Registro de Proveedores.

La convocante podrá determinar el método de presentación de ofertas en un sobre o en doble sobre. En este último caso, el primer sobre contendrá la oferta técnica, incluyendo los documentos que acrediten la personería del oferente y el segundo sobre, contendrá la oferta económica. En caso de presentación de ofertas físicas, las mismas deberán ser entregadas a la convocante en sobres cerrados. Cuando las mismas deban ser presentadas en doble sobre, la convocante deberá resguardar las ofertas técnicas y económicas hasta su apertura.

En caso de la utilización del módulo de ofertas electrónicas, la misma se registrará por las disposiciones establecidas en la normativa vigente y la guía de ofertas electrónicas.

Cuando el sobre no cuente con el RUC, se podrá subsanar dicha omisión al momento de la presentación.

Retiro, sustitución y modificación de las ofertas

1. Ofertas físicas.

1.1 Un oferente podrá retirar, sustituir o modificar su oferta después de presentada mediante el envío de una comunicación por escrito, debidamente firmada por el representante autorizado. La sustitución o modificación correspondiente de la oferta deberá acompañar dicha comunicación por escrito.

1.2. Todas las comunicaciones deberán ser:

- a) Presentadas conforme a la forma de presentación e identificación de las ofertas y además los respectivos sobres deberán estar marcados "RETIRO", "SUSTITUCION" o "MODIFICACION";
- b) Realizadas antes del plazo límite establecido para el acto de apertura de ofertas cuando las ofertas sean identificadas con "RETIRO", y;
- c) Realizadas antes del plazo límite establecido para la presentación de ofertas cuando las ofertas sean identificadas con "SUSTITUCIÓN" o "MODIFICACIÓN".

Las ofertas cuyo retiro, sustitución o modificación fuere solicitada serán devueltas sin abrir a los oferentes remitentes, durante el acto de apertura de ofertas.

1.3. Ninguna oferta podrá ser retirada durante el intervalo comprendido entre la fecha límite para el acto de apertura y la expiración del período de validez de las ofertas indicado en el Formulario de Oferta o cualquier extensión si la hubiere, caso contrario, se hará efectiva la Garantía de Mantenimiento de Oferta.

1.4. Ninguna oferta podrá ser sustituida o modificada durante el intervalo comprendido entre la fecha límite para presentar ofertas y la expiración del período de validez de las ofertas indicado en el Formulario de Oferta o cualquier extensión si la hubiere, caso contrario, se hará efectiva la Garantía de Mantenimiento de Oferta.

2. Ofertas electrónicas.

2.1. Un oferente podrá retirar, sustituir o modificar su oferta después de presentada, hasta antes de la fecha límite de presentación y apertura de ofertas, para ello deberá sujetarse a la reglamentación pertinente.

Apertura de ofertas

1. Desarrollo del acto de apertura de ofertas.

1.1. La entidad convocante procederá a la apertura de las ofertas en acto público en presencia de los oferentes o sus representantes según la hora, fecha y lugar previamente establecidos en el SICP.

1.2. Cuando la presentación de la oferta sea electrónica, el acto de apertura deberá sujetarse a la reglamentación vigente, en la hora y fecha establecida en el SICP.

1.3. Primero la convocante deberá verificar que los oferentes se encuentren inscritos en el Registro de Proveedores del Estado conforme con los datos previstos en el sobre, en caso de que, no sea posible identificar al oferente mediante el sobre presentado, la UOC procederá a abrirlo con el fin de verificar el número de RUC incluido entre los documentos de la oferta, para constatar si el oferente se encuentra inscripto en el Registro de Proveedores del Estado. En caso de que el oferente no inscripto en el Registro haya presentado la oferta, la convocante deberá dejar constancia en el acta de apertura electrónica.

La oferta del oferente no inscripto que cuente con la identificación de RUC en el sobre, no será abierta sino devuelto al oferente remitente. La oferta del oferente que no cuente con la identificación de RUC en el sobre será abierta y remitida al órgano evaluador de la convocante, para la evaluación de la oferta o su rechazo, según corresponda.

La presente disposición será aplicable en los procedimientos de doble sobre en los que será abierta la oferta técnica para la verificación respectiva, siempre y cuando la misma esté debidamente identificada como sobre técnico.

Esta disposición no será aplicable a los procedimientos que utilicen el módulo de ofertas electrónicas y a aquellos procedimientos especiales que, por su naturaleza, expresamente no requieran de la inscripción en el Registro de Proveedores del Estado como condición de participación.

1.4. Luego se procederá a verificar los sobres de las ofertas recibidas, marcados como:

a) "RETIRO": Se leerán en voz alta y el sobre con la oferta correspondiente no será abierto sino devuelto al oferente remitente. No se permitirá el retiro de ninguna oferta a menos que la comunicación de retiro contenga una autorización válida y sea leída en voz alta en el acto de apertura de las ofertas.

b) "SUSTITUCION": Se leerán en voz alta y se intercambiará con la oferta correspondiente que está siendo sustituida; la oferta sustituida no se abrirá y se devolverá al oferente remitente. No se permitirá la sustitución de ninguna oferta a menos que la comunicación de sustitución contenga una autorización válida y sea leída en voz alta en el acto de apertura de las ofertas.

c) "MODIFICACION": Se abrirán y leerán en voz alta con la oferta correspondiente. No se permitirá ninguna modificación a las ofertas a menos que la comunicación de modificación contenga una autorización válida y sea leída en voz alta en el acto de apertura de las ofertas.

Solamente se considerarán en la evaluación los sobres que se abren y leen en voz alta durante el Acto de Apertura de las Ofertas.

1.5. Los representantes de los oferentes que participen en la apertura de las ofertas deberán contar con autorización suficiente para suscribir el acta y para revisar los documentos de los demás oferentes, bastando para ello la presentación de una autorización escrita del firmante de la oferta, esta autorización podrá ser incluida en el sobre oferta o ser portada por el representante.

1.6. Se solicitará a los representantes de los oferentes presentes que firmen el acta. La omisión de la firma por parte de un oferente no invalida el contenido y efecto del acta. El acta se difundirá a través del SICP.

1.7. Las ofertas sustituidas y modificadas, que no sean abiertas y leídas en voz alta durante el acto de apertura no podrán ser consideradas para la evaluación sin importar las circunstancias y serán devueltas sin abrir a los remitentes.

1.8. Si los sobres no están cerrados e identificados como se requiere, la convocante deberá dejar constancia de ello en el acto de apertura y no se responsabilizará en caso de que la oferta se extravíe o sea abierta prematuramente.

1.9. La falta de firma en un documento sustancial, es considerada una omisión sustancial que no podrá ser subsanada en ninguna oportunidad una vez abiertas las ofertas. En cuanto a la garantía de mantenimiento de oferta deberá estar debidamente extendida.

2. Comunicación del acta de apertura.

2.1. En el sistema de un solo sobre el acta de apertura deberá ser comunicada a través del SICP para su difusión, dentro de los dos (02) días hábiles de la realización del acto de apertura.

2.2. En el sistema de doble sobre, el acta de apertura técnica deberá ser comunicada a través del SICP, para su difusión, dentro de los dos (02) días hábiles de la realización del acto de apertura, se procederá de igual manera una vez finalizado el acto de apertura económico.

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:

No 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. Las mismas deberán ser presentadas en el momento determinado en este apartado. La falta de presentación de las muestras en tiempo y condiciones 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:

NO APLICA

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:

No Aplica

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.

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.

Confidencialidad de la Información

Reserva de información en respuestas a 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".

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 los Arts. 17 y 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 la empresa, 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, pudiendo 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

Basado únicamente en precio

En caso de optar por el método de multiplicidad de criterios deberá estar supeditado a los lineamientos emitidos por el MEF y la DNCP.

Análisis de 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, cuando los montos cotizados se aparten de los parámetros o rangos establecidos en la normativa aplicable.

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.

Para la evaluación de ofertas basada en la multiplicidad de criterios.

En cuanto al análisis del precio se podrá considerar el parámetro dispuesto en el presente apartado.

Composición de Precios

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

1	COSTO DE PRODUCTO Y/O MANO DE OBRA
2	IMPUESTOS
3	GASTOS OPERACIONALES
4	GASTOS ADMINISTRATIVOS
5	UTILIDAD
6	PRECIO TOTAL

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 normativa aplicable.

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, el oferente podrá complementar 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.

b) Oferentes en Consorcio:

b.1. Provisión de Bienes. El CPEN debe ser expedido a nombre del miembro, o los miembros, que fabrique o produzca los bienes objeto de la contratación. En el caso que ninguno de los integrantes del consorcio 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 constituido o en formación, o a nombre de cualquiera de los integrantes del mismo.

b.2. Provisión de Servicios. Todos los integrantes del consorcio deben contar con el CPEN. (Se entenderá por el término "servicio" aquello que comprende a los servicios en general, las consultorías, obras públicas y servicios relacionados a obras públicas).

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 específico certificado.

Para los casos de prestación de servicios, el CPEN será intransferible. Se permite el uso del CPEN por terceros exclusivamente en caso de productos y bajo autorización expresa del titular del certificado, éste podrá ser utilizado por terceros para la presentación de ofertas en el marco de un procedimiento de contratación, de acuerdo con lo establecido en la reglamentación respectiva.

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

Margen de preferencia en procedimientos de contratación de carácter internacional

No Aplica

Requisitos documentales para la evaluación de las condiciones de participación.

1. Formulario de Oferta (*)

[El formulario de oferta y lista de precios, generados electrónicamente a través del SICP, deben ser completados y firmados por el oferente. En caso de que se emplee el módulo de oferta electrónica 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.]

2. Garantía de Mantenimiento de Oferta (*)

[La garantía de mantenimiento de oferta debe ser extendida, bajo la forma establecida en el SICP.

3. Certificado de Cumplimiento con la Seguridad Social ()**

4. Declaración jurada de conocimiento de la existencia de un conflicto de intereses respecto a los funcionarios públicos intervinientes en el procedimiento. ()**

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 profesional, comercial y/o industrial del municipio en donde esté asentado el establecimiento del oferente. ()**

8. Documentos legales. Oferentes

8.1. Personas Físicas.

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. (*)

8.2. Personas Jurídicas.

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. (*)
8.3. Oferentes en Consorcio en formación.
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).
c. 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) (*).
8.4. 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).

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

En caso de que los procedimientos no sean por el módulo de oferta electrónica, el oferente deberá presentar el Formulario de Oferta y la Planilla de precio. Para los casos en que se utilice el Módulo de Oferta Electrónica los datos se deberán cargar en el Formulario de oferta electrónica de conformidad a la normativa vigente.

Los documentos indicados con asterisco (*) son considerados documentos sustanciales a ser presentados con la oferta de conformidad al Decreto Reglamentario, y deberán estar vigente a la fecha y hora tope de presentación de oferta.

Los documentos indicados con doble asterisco (**) son considerados documentos formales y deben estar vigentes a la fecha y hora tope de presentación de ofertas. 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 o cuando el titular de una empresa no sea empleador, 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 RG.**
Deberán cumplir el siguiente parámetro:
a. Ratio de Liquidez: activo corriente / pasivo corriente
Deberá ser igual o mayor que 1, en promedio, en los años (2022, 2023 y 2024)
b. Endeudamiento: pasivo total / activo total
No deberá ser mayor a 0,80 en promedio, en los años (2022, 2023 y 2024)
c. Rentabilidad: Porcentaje de utilidad después de impuestos o pérdida con respecto al Capital
El promedio de los años (2022, 2023 y 2024) no deberá ser negativo
- b. **Para contribuyente de IRPC/IRE SIMPLE o IRACIS/IRE SIMPLE**
Deberán cumplir el siguiente parámetro:
Eficiencia: (Ingreso/Egreso)
Deberá ser igual o mayor que 1, en promedio, en los años (2022, 2023 y 2024)
- c. **Para contribuyente de IRP/IRP-RSP**
Deberán cumplir el siguiente parámetro:
Eficiencia: (Ingreso/Egreso)
Deberá ser igual o mayor que 1, en promedio, en los años (2022, 2023 y 2024)
- d. **Para contribuyentes de exclusivamente IVA General**
Deberán cumplir el siguiente parámetro:
Eficiencia: (Ingreso/Egreso)
Deberá ser igual o mayor que 1, en promedio, en los años (2022, 2023 y 2024)
Los oferentes al efecto de lo anteriormente señalado, deberán presentar los documentos que se indican en los requisitos documentales.

Observación: Si en alguno de los tres años, o los tres años presentados por la Empresa, su pasivo es igual a 0, se considerará el Ratio de Liquidez igual a 1 y se dará por cumplido el Ratio de Endeudamiento.
Esta salvedad en el PBC hace posible calcular el promedio del índice de liquidez de los 3 (tres) ejercicios analizados, debido a que se otorga un valor que puede ser promediado.

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 Cuadro de Estado de Resultados de los tres años (2022, 2023 y 2024) para contribuyente de IRACIS/IRE RG. |
| b. IVA General de 36 (treinta y seis) meses (2022, 2023 y 2024) para contribuyentes sólo del IVA General. |
| c. Formulario 106 IRPC, Formulario 501 IRE Simple de los 3 (tres) años (2022, 2023 y 2024) para contribuyentes del IRPC/IRE SIMPLE o IRACIS/IRE SIMPLE. |
| d. Formulario 104 IRP, Formulario 515 IRP-RSP de los 3 (tres) años (2022, 2023 y 2024) para contribuyentes de IRP/IRP-RSP |

Experiencia requerida

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

Demostrar la experiencia en la provisión del Servicio de Centro de Operaciones de Seguridad SOC con facturaciones de venta, contratos y/o recepciones finales, por un monto equivalente al 40% como mínimo del monto total ofertado en el presente procedimiento de contratación, **de los últimos 5 (cinco) años (2021, 2022, 2023, 2024 y 2025)**. Las sumatorias de las facturaciones deben alcanzar el porcentaje indicado, no será necesaria la presentación del porcentaje del monto establecido por cada año.

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

1. Copia de facturaciones, contratos y/o recepciones finales que avalen la experiencia requerida.

Copia de contratos, facturaciones y/o recepciones finales que avalen la experiencia requerida.

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:

1. El oferente deberá poseer certificados vigentes de Gestión de Calidad (CSG) según la norma ISO 9001 y/o de Gestión de Servicios de TI (ITSM) según la norma 20000, para garantizar estándares internacionales de calidad para el cumplimiento de los servicios. Se debe evidenciar que el alcance de la certificación corresponde o supera a los servicios requeridos en el presente llamado.
2. El oferente deberá poseer certificación de Calidad ISO 27001 vigente, con el objetivo de cumplir con los más altos estándares de seguridad de la información, preservando la confidencialidad, integridad y disponibilidad de la información relacionada con la convocante. Se debe evidenciar que el alcance de la certificación corresponde o supera a los servicios requeridos en el presente llamado.
3. El oferente debe contar como mínimo con los siguientes perfiles técnicos:
 - a. **1 (un) Director General del Servicio de Ciberseguridad:**
 - Deberá contar con experiencia comprobable en ciberseguridad, gestión de riesgos, respuesta a incidentes y prestación de servicios de seguridad gestionados en entornos complejos. La experiencia será acreditada mediante certificados de trabajo y/o documentos de nómina y/o constancias laborales y/o designaciones emitidas por el empleador.
 - Debe ser parte del staff del oferente y de residencia permanente en Paraguay.
 - Debe ser un profesional egresado de carreras informáticas o afines.
 - Debe contar con al menos una maestría en ciberseguridad o seguridad de la información.
 - Debe contar con al menos 1 (una) de las siguientes certificaciones vigentes de gestión de ciberseguridad: ISACA CISM, ECCouncil CCISO.
 - Debe contar con al menos 1 (una) de las siguientes certificaciones vigentes de ciberseguridad: ISC2 CISSP, PECB ISO 27032 Senior Lead Cybersecurity Manager, PECB ISO 27035 Senior Lead Incident Manager.
 - Debe contar con al menos 5 (cinco) años de experiencia en roles de Director/Gerente de Ciberseguridad o Seguridad de la Información en empresas públicas y/o privadas, nacionales o internacionales. La experiencia será acreditada mediante certificados de trabajo y/o documentos de nómina y/o constancias laborales y/o designaciones emitidas por el empleador.
 - b. **1 (un) Coordinador de SOC / Líder Operativo:**
 - Debe ser parte del Staff del oferente y de residencia permanente en Paraguay.
 - Debe ser un profesional egresado de carreras informáticas o afines.
 - Debe contar con al menos un diplomado en ciberseguridad o seguridad de la información.
 - Debe contar con al menos 2 (dos) capacitaciones y/o certificaciones en seguridad o ciberseguridad, de organizaciones reconocidas internacionalmente como: ISC2, ISACA, ECCouncil, PECB, Certiprof.
 - Debe contar con al menos 1 (una) certificación específicamente relacionada a seguridad ofensiva y/o defensiva (RedTeam / BlueTeam).
 - Debe contar con al menos 5 años de experiencia comprobables en roles específicos de TI, ciberseguridad o seguridad de la información. La experiencia será acreditada mediante certificados de trabajo y/o documentos de nómina y/o constancias laborales y/o designaciones emitidas por el empleador.
 - c. **3 (tres) Analistas de Seguridad SOC:**
 - Debe ser parte del staff del oferente y de residencia permanente en Paraguay.
 - Debe ser estudiante o egresado de carreras informáticas o afines.
 - Debe contar con al menos 2 (dos) capacitaciones y/o certificaciones en seguridad o ciberseguridad, de organizaciones reconocidas internacionalmente como: ISC2, ISACA, ECCouncil, PECB, Certiprof, Hack The Box, PortSwigger Academy, TryHackMe.
 - Debe contar con al menos 2 años de experiencia comprobables en roles específicos de TI, ciberseguridad o seguridad de la información. La experiencia será acreditada mediante certificados de trabajo y/o documentos de nómina y/o constancias laborales y/o designaciones emitidas por el empleador.
 - d. **1 (un) Especialista en Cacería de Amenazas (Threat Hunting):**
 - Debe ser parte del staff del oferente y de residencia permanente en Paraguay.
 - Debe ser estudiante o egresado de carreras informáticas o afines.
 - Debe contar con al menos un diplomado en ciberseguridad o seguridad de la información.
 - Debe contar con al menos 4 (cuatro) capacitaciones y/o certificaciones específicamente relacionadas a seguridad defensiva (BlueTeam / Threat Hunting).
 - Debe contar con al menos 4 años de experiencia específica en SOC y/o Cacería de amenazas. La experiencia será acreditada mediante certificados de trabajo y/o documentos de nómina y/o constancias laborales y/o designaciones emitidas por el empleador.
 - e. **1 (un) Arquitecto de Ciberseguridad:**
 - Debe ser parte del staff del oferente y de residencia permanente en Paraguay.
 - Debe ser estudiante o egresado de carreras informáticas o afines.
 - Debe contar con al menos un diplomado en ciberseguridad o seguridad de la información.
 - Debe contar con al menos 1 (una) de las siguientes certificaciones vigentes de seguridad o seguridad de la información: CEH, CISSP, CISM. Debe contar con certificaciones en productos o soluciones de ciberseguridad.
 - Debe contar con al menos 5 años de experiencia comprobables en roles asociados a seguridad de la información o ciberseguridad. La experiencia será acreditada mediante certificados de trabajo y/o documentos de nómina y/o constancias laborales y/o designaciones emitidas por el empleador.
 - f. **2 (dos) Analistas de Ciberseguridad:**
 - Deben ser del staff del oferente y de residencia permanente en Paraguay.
 - Deben ser estudiantes o egresados de carreras informáticas o afines, o en su defecto contar con al menos un diplomado en ciberseguridad o seguridad de la información.
 - Deben contar con al menos 2 (dos) de las siguientes certificaciones: ISO 27001 Lead Auditor, CEH, Security+.
 - Debe contar con al menos 1 año de experiencia comprobable en roles asociados a seguridad de la información o ciberseguridad. La experiencia será acreditada mediante certificados de trabajo y/o documentos de nómina y/o constancias laborales y/o designaciones emitidas por el empleador.
 - g. **1 (un) Analista de Seguridad SOC, in-situ:**
 - Debe ser del staff del oferente y de residencia permanente en Paraguay. comprobable mediante la presentación de Certificado de Vida y Residencia.
 - El personal debe contar con al menos 3 certificaciones y/o cursos de ciberseguridad de organizaciones reconocidas internacionalmente, tales como ISC2, ISACA, EC-Council, ISO, Fortinet, Cisco, Microsoft, Certiprof, Hack The Box, PortSwigger Academy y TryHackMe
4. El oferente debe presentar una descripción técnica de toda la arquitectura del servicio gestionado del oferente. Se debe especificar de manera explícita todas las tecnologías que serán utilizadas en el proyecto, indicando **marca, modelo y procedencia** de las mismas.
5. El oferente se compromete a cumplir con las especificaciones técnicas y plazos de entrega del servicio solicitado.

Requisitos documentales para evaluar el criterio de capacidad técnica

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

1. Copia de la Certificación ISO 9001:2015 vigente.
2. Copia de la Certificación ISO 27001 vigente.
3. El oferente debe contar como mínimo con los siguientes perfiles técnicos:

a. 1 (un) Director General del Servicio de Ciberseguridad,

- Presentación de Curriculum Vitae, adjuntando copias de las certificaciones correspondientes y/o certificaciones que se encuentren en proceso de renovación con constancia de vigencia, títulos

universitarios, conforme a lo solicitado en el apartado de capacidad técnica

- El director debe encontrarse inscripto en la Planilla de IPS del oferente y contar con una antigüedad mínima comprobable de 6 (seis) meses de vínculo laboral con la empresa oferente.
- Se debe presentar Vida y Residencia para avalar lo solicitado.

b. 1 (un) Coordinador de SOC / Líder Operativo:

- Presentación de Curriculum Vitae, adjuntando copias de las certificaciones correspondientes y/o certificaciones que se encuentren en proceso de renovación con constancia de vigencia, títulos universitarios, conforme a lo solicitado en el apartado de capacidad técnica.
- El coordinador debe encontrarse inscripto en la Planilla de IPS del oferente y contar con una antigüedad mínima comprobable de 6 (seis) meses de vínculo laboral con la empresa oferente.
- Se debe presentar Vida y Residencia para avalar lo solicitado.

c. 3 (tres) Analistas de Seguridad SOC:

- Presentación de Curriculum Vitae, adjuntando copias de las certificaciones correspondientes y/o certificaciones que se encuentren en proceso de renovación con constancia de vigencia, constancia de estudiante de carreras informáticas o afines, con independencia del año en curso, acreditable mediante historial académico y/o constancia o proforma de inscripción universitaria vigente, y/o título, conforme a lo solicitado en el apartado de capacidad técnica.
- Los analistas deben encontrarse inscriptos en la Planilla de IPS del oferente y contar con una antigüedad mínima comprobable de 1 (un) año de vínculo laboral con la empresa oferente.
- Se debe presentar Vida y Residencia para avalar lo solicitado.

d. 1 (un) Especialista en Cacería de Amenazas (Threat Hunting):

- Presentación de Curriculum Vitae, adjuntando copias de las certificaciones correspondientes, y/o certificaciones que se encuentren en proceso de renovación con constancia de vigencia constancia de estudiante de carreras informáticas o afines, con independencia del año en curso, acreditable mediante historial académico y/o constancia o proforma de inscripción universitaria vigente, y/o título, conforme a lo solicitado en el apartado de capacidad técnica.
- El especialista debe encontrarse inscripto en la Planilla de IPS del oferente y contar con una antigüedad mínima comprobable de 1 (un) año de vínculo laboral con la empresa oferente.
- Se debe presentar Vida y Residencia para avalar lo solicitado.

e. 1 (un) Arquitecto de Ciberseguridad:

- Presentación de Curriculum Vitae, adjuntando copias de las certificaciones correspondientes, y/o certificaciones que se encuentren en proceso de renovación con constancia de vigencia, constancia de estudiante de carreras informáticas o afines, con independencia del año en curso, acreditable mediante historial académico y/o constancia o proforma de inscripción universitaria vigente, y/o título, conforme a lo solicitado en el apartado de capacidad técnica.
- El arquitecto debe encontrarse inscripto en la Planilla de IPS del oferente y contar con una antigüedad mínima comprobable de 1 (un) año de vínculo laboral con la empresa oferente.
- Se debe presentar Vida y Residencia para avalar lo solicitado

f.2 (dos) Analistas de Ciberseguridad:

- Presentación de Curriculum Vitae, adjuntando copias de las certificaciones correspondientes, y/o certificaciones que se encuentren en proceso de renovación con constancia de vigencia, constancia de estudiante de carreras informáticas o afines, con independencia del año en curso, acreditable mediante historial académico y/o constancia o proforma de inscripción universitaria vigente, y/o título, conforme a lo solicitado en el apartado de capacidad técnica.
- Los analistas deberán encontrarse inscriptos en la Planilla de IPS del oferente y contar con una antigüedad mínima comprobable de 1 (un) año de vínculo laboral con la empresa oferente.
- Se debe presentar Vida y Residencia para avalar lo solicitado.

g. 1 (un) Analista de Seguridad SOC, in-situ:

- Presentación de Curriculum Vitae, adjuntando copias de las certificaciones correspondientes.
- El analista debe encontrarse inscripto en la Planilla de IPS del oferente y contar con una antigüedad mínima comprobable de 1 (un) año de vínculo laboral con la empresa oferente.

4. El oferente debe presentar una Declaración Jurada en la cual detalle la descripción técnica de toda la arquitectura del servicio gestionado del oferente, En dicho documento, el oferente deberá especificar de manera explícita todas las tecnologías que serán utilizadas en el proyecto, indicando **marca, modelo y procedencia** de las mismas.

5. El oferente debe presentar una Declaración Jurada en la cual se compromete a cumplir con las especificaciones técnicas y plazos de entrega del servicio solicitado.

Justificación Certificación ISO 27001

1. Especificar cuál es el objeto de la certificación, qué es lo certificado (la producción, el producto, la distribución, otros)
 - El objeto de la certificación es la EMPRESA
 2. Explicar cómo incide dicha certificación en la ejecución del contrato;
 - La certificación ISO 27001 se enfoca en certificar el sistema de gestión de la seguridad de la información (SGSI) de una organización. Esto implica que lo que se certifica es la capacidad de la empresa para proteger la confidencialidad, integridad y disponibilidad de la información. La certificación ISO 27001 garantiza que la empresa tiene procesos y procedimientos establecidos para gestionar y proteger la información contra amenazas y vulnerabilidades.
 3. Especificar las empresas en el mercado que cuentan con la certificación indicada (mencionar tres Empresas por lo menos):
 - Netlogic
 - Olam
 - ITCS
 - ISS
4. Si se han previsto en el pliego de bases y condiciones otras certificaciones equivalentes definidas como tales para satisfacer el requerimiento establecido.
- No se han previsto otras certificaciones equivalentes

Justificación Certificación ISO 9001

1. Especificar cuál es el objeto de la certificación, qué es lo certificado (la producción, el producto, la distribución, otros)
 - El objeto de la certificación es la EMPRESA
 2. Explicar cómo incide dicha certificación en la ejecución del contrato;
 - La certificación ISO 9001 se enfoca en certificar el sistema de gestión de la calidad (SGC) de una organización. Esto implica que lo que se certifica es la capacidad de la empresa para diseñar, producir y entregar productos o servicios que cumplan con los requisitos de los clientes y las regulaciones aplicables. En otras palabras, la certificación ISO 9001 garantiza que la empresa tiene procesos y procedimientos establecidos para asegurar la calidad en todas las etapas, desde la planificación hasta la entrega del producto o servicio.
 3. Especificar las empresas en el mercado que cuentan con la certificación indicada (mencionar tres Empresas por lo menos)
 - Netlogic
 - Olam
 - ITCS
 - ISS
4. Si se han previsto en el pliego de bases y condiciones otras certificaciones equivalentes definidas como tales para satisfacer el requerimiento establecido.
- No se han previsto otras certificaciones equivalente

Otros criterios que la convocante requiera

Otros criterios para la evaluación de las ofertas a ser considerados en ésta contratación serán:

Para Personas Jurídicas u Oferentes en Consorcio.

Copias simples de las Constancias del Registro de Personas y Estructuras Jurídicas, y las Constancias del Registro de Beneficiarios Finales, dispuestas por la Ley N° 6446/2019, Decreto Reglamentario N°

Para los oferentes consorciados:

1. CAPACIDAD FINANCIERA	Los índices financieros deberán ser cumplidos el 100% por cada uno de los integrantes.
2. EXPERIENCIA Y CAPACIDAD TÉCNICA	Todas las partes combinadas deberán cumplir con el 100% de los requisitos solicitados.
3. CALIFICACIÓN LEGAL	El socio líder y cada socio deberá cumplir con el 100% de lo exigido

OTROS DOCUMENTOS A PRESENTAR PARA LA FIRMA DEL CONTRATO:

- De conformidad al Art. 33 de la Resolución N° 70 de la SEPRELAD, el oferente adjudicado deberá proveer los datos y documentos respaldatorios solicitado en la misma

Evaluación basada en multiplicidad de criterios

Se deben establecer los criterios de evaluación que serán aplicados al principio de valor por dinero, indicando por cada criterio la siguiente información:

No Aplica

En caso de optar por el método de multiplicidad de criterios deberá estar sujeto a los lineamientos emitidos por el MEF y la DNCP.

Ponderación de criterios de evaluación - Multiplicidad de criterios

La ponderación de cada criterio de evaluación especificado en la cláusula anterior será el siguiente:

No Aplica

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 aritmético.

El comité de evaluación deberá 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.

Disconformidades, 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.

Con la condición de que la oferta cumpla sustancialmente con los Documentos de la Licitación, la convocante corregirá errores aritméticos de la siguiente manera y notificará al oferente para su aceptación:

- Si hay una discrepancia entre un precio unitario y el precio total obtenido al multiplicar ese precio unitario por las cantidades correspondientes, prevalecerá el precio unitario y el precio total será corregido.
- Si hay un error en un total que corresponde a la suma o resta de subtotales, los subtotales prevalecerán y se corregirá el total.
- En caso que el oferente haya cotizado su precio en moneda extranjera con décimos y céntimos la convocante procederá a realizar el redondeo hacia abajo.
- Si hay una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras a menos que la cantidad expresada en palabras corresponda a un error aritmético, en cuyo caso prevalecerán las cantidades en cifras de conformidad con los párrafos (a) y (b) mencionados.

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 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.

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.

En los procedimientos de contratación en los cuales se aplique la combinación de criterios, la evaluación de las ofertas se llevará a cabo con base a la metodología, criterios y parámetros establecidos en los pliegos de bases y condiciones que permitan establecer cuál es aquella que ofrece mayor valor por dinero.

En los demás casos, 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.

Notificación del resultado

La notificación del resultado se realizará a través del SICP de manera automática, desde la comunicación 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 comunicación de los documentos en el SICP, comprenderá la Resolución del resultado y el informe de evaluación respectivo. La fecha de esta notificación se considera válida a todos los efectos, siempre que se cumplan con las formalidades previstas en el Art. 52 y 55 de la Ley N.º 7021/22 y, lo previsto en el Título V, Capítulo VI, Sección IV y V del Decreto Reglamentario N.º 2264/24.

En casos excepcionales, 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 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 comunicación 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 fecha prevista en 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.

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 respecto al análisis de su oferta.

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 y/o servicios 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 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.** Diego Popoff, Gerente. Gerencia Departamental de Seguridad Lógica, dependiente de la Gerencia de Área de Seguridad. Miguel Acevedo, Gerente. Gerencia de Área de Seguridad.
- **Justificación de la necesidad que se pretende satisfacer mediante la contratación a ser realizada:** La contratación del Servicio de Centro de Operaciones de Seguridad (SOC) se fundamenta en la necesidad de fortalecer la gestión de la seguridad de la información de la organización, considerando el incremento sostenido de las amenazas cibernéticas, la criticidad de los activos digitales y la dependencia de los sistemas de información para la continuidad del negocio.

El SOC proporciona monitoreo continuo (24/7) de la infraestructura tecnológica, permitiendo la detección temprana, análisis y respuesta oportuna ante incidentes de seguridad, lo cual reduce significativamente el impacto operativo, financiero y reputacional que podrían generar ataques cibernéticos, accesos no autorizados, fuga de información o interrupciones del servicio.

Asimismo, la contratación de este servicio responde a la limitación de recursos internos especializados, ya que la operación de un SOC propio implica altos costos asociados a la contratación de personal altamente calificado, implementación de herramientas tecnológicas especializadas y cobertura permanente. El servicio externalizado permite acceder a capacidades técnicas avanzadas y experiencia especializada, optimizando los costos y garantizando un nivel adecuado de protección.

Desde el punto de vista normativo, el SOC contribuye al cumplimiento de estándares y marcos de referencia de seguridad de la información, tales como ISO/IEC 27001, NIST,

PCI DSS y normativas de protección de datos personales, al asegurar la trazabilidad de eventos, la gestión de incidentes y la generación de reportes para auditorías y organismos de control.

En consecuencia, la contratación del Servicio de Centro de Operaciones de Seguridad se justifica como una medida estratégica y preventiva, orientada a proteger los activos de información, asegurar la continuidad operativa, mejorar la postura de seguridad institucional y permitir que la organización concentre sus esfuerzos en el cumplimiento de sus objetivos principales.

- **Justificación de la planificación:** La planificación de esta contratación es sucesiva ya que dicho servicio es requerido de manera constante.

Las especificaciones técnicas deberán estar sustentadas en el dictamen técnico, requerido al momento de la comunicación de la convocatoria.

Especificaciones Técnicas "CPS"

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

El propósito de las 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. Siempre que sea posible deberán especificarse normas de calidad internacionales. 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 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 oferta), donde el oferente proporcionará la información detallada de dichas características técnicas o de funcionamiento con relación a los valores aceptables o garantizados.

Cuando 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:

Objeto del Servicio

El presente Pliego de Bases y Condiciones tiene por finalidad la contratación de un Servicio de Centro de Operaciones de Seguridad (SOC), destinado a resguardar los sistemas de información, las infraestructuras tecnológicas y los canales digitales del Banco Nacional de Fomento - BNF, atendiendo a la criticidad de la información administrada y al impacto que un incidente de ciberseguridad podría generar sobre la operación institucional y la prestación de servicios públicos.

En el contexto actual, las amenazas cibernéticas han evolucionado tanto en volumen como en complejidad, afectando de manera directa a organismos del sector público. A nivel nacional, se han registrado incidentes que incluyen, entre otros, ataques de ransomware, campañas de phishing, infecciones por malware y accesos no autorizados a sistemas institucionales, evidenciando un escenario de riesgo que requiere capacidades técnicas especializadas y un enfoque de gestión permanente.

En respuesta a esta realidad, el BNF considera necesaria la contratación de un Servicio de Centro de Operaciones de Seguridad (SOC), con un enfoque continuo y preventivo, que permita fortalecer las capacidades institucionales para la prevención, detección, análisis, respuesta y mitigación de incidentes de ciberseguridad, así como para la reducción progresiva de la superficie de ataque y la mejora sostenida de la postura de seguridad.

Las especificaciones técnicas establecidas en el presente documento definen los **requisitos mínimos obligatorios** que deberá cumplir el oferente para la correcta prestación del servicio. Dichos requisitos deberán ser verificados bajo un esquema de cumple / no cumple y su cumplimiento debe estar plenamente justificado y documentado, además de que se encuentran alineados a buenas prácticas y estándares internacionales reconocidos en materia de ciberseguridad, gestión de incidentes y continuidad operativa.

El servicio deberá prestarse bajo un modelo de servicio gestionado, siendo responsabilidad exclusiva del proveedor la provisión, operación, administración y mantenimiento de cualquier plataforma tecnológica, herramienta y capacidades necesarias para la ejecución del servicio durante toda la vigencia del contrato. En ningún caso estas soluciones implicarán la adquisición o el licenciamiento de software por parte del BNF.

La prestación del servicio deberá garantizar la continuidad operativa y resiliencia, acordes a la criticidad de los activos y servicios protegidos, asegurando una capacidad efectiva de respuesta ante incidentes de ciberseguridad de distinta naturaleza y severidad.

Impacto Esperado

Como resultado de la contratación del servicio de ciberseguridad gestionado, el BNF espera alcanzar, entre otros, los siguientes resultados:

- Disminución de los tiempos de detección, análisis y contención de incidentes de alta criticidad.
- Reducción progresiva de la superficie de ataque mediante acciones preventivas y correctivas continuas.
- Mejora de la capacidad de respuesta y recuperación ante incidentes de ciberseguridad.

EL OFERENTE DEBERÁ CONTAR CON LOS SIGUIENTES PERFILES TÉCNICOS:

1. **Director General del Servicio de Ciberseguridad (Cantidad: 1 (uno))**, quien será Responsable de la supervisión integral, dirección técnica y responsabilidad global del servicio.
2. **Coordinador de SOC / Líder Operativo (Cantidad: 1 (uno))**, quien será Responsable de la coordinación diaria del servicio, gestión de incidentes, escalamiento técnico y enlace operativo con la convocante.
3. **Analistas de Seguridad SOC (Cantidad: 3 (tres))**, quienes serán Responsables del monitoreo, detección, análisis y gestión de eventos e incidentes de ciberseguridad, incluyendo análisis avanzado, correlación de eventos y respuesta inicial ante incidentes.
4. **Especialista en Cacería de Amenazas (Threat Hunting) (Cantidad: 1 (uno))**, quien será Responsable de la identificación proactiva de amenazas avanzadas que no hayan sido detectadas automáticamente por las herramientas de seguridad, mediante el análisis de comportamiento, correlación avanzada de eventos, análisis de telemetría y validación de hipótesis de ataque.
5. **Arquitecto de Ciberseguridad (Cantidad: 1 (uno))**, quien será responsable del diseño, acompañamiento y soporte de arquitecturas de seguridad, y de liderar iniciativas de la remediación técnica de vulnerabilidades, hardening de sistemas y apoyo técnico durante y post-incidentes.
6. **Analistas de Ciberseguridad (Cantidad: 2 (dos))**, quienes serán responsables de la evaluación, acompañamiento y apoyo a las tareas de remediación de vulnerabilidades detectadas, en coordinación con el SOC y el equipo técnico del BNF.
7. **Analista de Seguridad SOC, in-situ (Cantidad: 1 (uno))**, quien será responsable de las tareas operativas y de seguimiento, y nexa de las tareas de remediación, además de las tareas operativas de gestión de eventos e incidentes de seguridad, modalidad presencial in situ, de lunes a viernes, horario de 08:00 a 16:00 horas, conforme al numeral 1.3 «Modalidad de atención remota y presencial» (Sección 1 Generalidades del Servicio) de las EETT.

CARACTERÍSTICAS	DESCRIPCIÓN TÉCNICA	MÍNIMO REQUERIDO
1. GENERALIDADES DEL SERVICIO		
1.1. Objetivo y alcance del servicio	El servicio deberá establecer un modelo integral de ciberseguridad gestionado, con operación continua (24x7) durante un período de 24 (veinte y cuatro) meses, orientado a la prevención, detección, análisis, contención y respuesta ante incidentes de ciberseguridad. El alcance deberá cubrir de forma explícita los sistemas, redes, infraestructuras, dispositivos tecnológicos, servicios digitales y activos de información de la Entidad, incluyendo entornos on-premise, cloud e híbridos cuando correspondan.	Exigido
	El servicio deberá operar como un conjunto integrado de capacidades, asegurando que monitoreo, detección, correlación, respuesta, investigación, gestión de vulnerabilidades, que funcionen de forma coordinada.	Exigido
1.2. Continuidad operativa del servicio	El servicio deberá garantizar la continuidad operativa permanente de las capacidades de monitoreo, detección, análisis y gestión de incidentes, sin interrupciones que afecten la capacidad de respuesta ante eventos de ciberseguridad.	Exigido
	El oferente deberá disponer de un Centro de Operaciones de Seguridad (SOC) principal en la República del Paraguay y un centro secundario —ya sea propio, de un tercero o mediante un servicio de nube pública—; se exigirá una distancia lineal mínima de 50 kilómetros entre ambos centros únicamente cuando el sitio secundario corresponda a una infraestructura física, quedando exceptuado dicho requisito de distancia en caso de optar por una solución en la nube pública, debiendo el proponente acreditar fehacientemente en cualquier modalidad la alta disponibilidad, la resiliencia y la continuidad operativa del servicio.	Exigido
	El servicio deberá apoyarse en plataformas con alta disponibilidad, tolerancia a fallos y mecanismos de redundancia acordes a entornos de misión crítica.	Exigido
	El servicio deberá contar con cobertura operativa continua (24x7) para la atención de eventos e incidentes de ciberseguridad durante toda la vigencia del contrato, basado en un esquema de turnos, roles definidos y mecanismos de escalamiento técnico funcional en base a la criticidad de los incidentes.	Exigido

	La convocante podrá requerir la documentación y/o verificaciones que considere pertinentes para acreditar el carácter operativo de ambos Centros de Operaciones de Seguridad, tanto durante la evaluación de las ofertas como durante la ejecución del contrato.	Exigido	
	El segundo Centro de Operaciones de Seguridad deberá contar con capacidad operativa para sostener la continuidad de las capacidades críticas del servicio (monitoreo, detección y respuesta) ante la indisponibilidad total o parcial del centro principal, no admitiéndose su mera existencia física.	Exigido	
	Ambos Centros de Operaciones de Seguridad deberán permanecer operativos durante toda la vigencia del contrato. La convocante se reserva la facultad de verificar el cumplimiento de esta condición durante la ejecución por los medios que estime pertinentes.	Exigido	
1.3. Modalidad de atención remota y presencial	El servicio de SOC deberá ser de forma híbrida 24x7 de los cuales en la modalidad presencial In-Situ deberá ser presentada de lunes a viernes de 08:00 a 16:00 horas con todas las capacidades técnicas, tecnológicas y operativas para que el servicio pueda prestarse y de forma remota, mediante canales seguros, controlados y auditables, fuera del horario mencionado sábados, domingos y feriados.	Exigido	
1.5. Escalabilidad del servicio	El servicio deberá ser escalable, permitiendo la incorporación de nuevos activos, fuentes de eventos o volúmenes de información sin afectar la continuidad operativa ni requerir rediseños estructurales ni la interrupción del servicio.	Exigido	
	El servicio no deberá imponer límites contractuales artificiales en cuanto a cantidad de eventos, alertas, incidentes gestionados u horas de análisis, especialmente en escenarios de alta actividad o crisis de ciberseguridad.	Exigido	
2. ARQUITECTURA DEL SERVICIO Y MODELO OPERATIVO DEL SOC Y CSIRT			
2.1. Arquitectura general del servicio	El servicio deberá basarse en una arquitectura integrada de ciberseguridad, en la cual las capacidades de monitoreo, detección, correlación, respuesta, investigación y gestión de vulnerabilidades operen de forma coordinada como un único servicio lógico.	Exigido	
	El servicio deberá contar con un plano centralizado de monitoreo y análisis de seguridad, capaz de recibir, normalizar y procesar telemetría proveniente de múltiples fuentes tecnológicas de la Entidad.	Exigido	
	La arquitectura del servicio deberá contemplar la separación lógica entre los planos de recolección de telemetría, análisis/correlación, respuesta operativa y gestión de incidentes, evitando dependencias rígidas entre componentes.	Exigido	
	El modelo operativo deberá estar diseñado de forma independiente a marcas o fabricantes específicos, priorizando capacidades técnicas y procesos operativos sobre dependencias tecnológicas rígidas.	Exigido	
2.2. Modelo de Operación	El Centro de Operaciones de Seguridad (SOC) deberá constituir el núcleo operativo del servicio, siendo responsable del monitoreo continuo, análisis de eventos, detección de amenazas y activación de procesos de respuesta.	Exigido	
	El modelo operativo deberá garantizar la integración funcional entre el SOC y el CSIRT, permitiendo el traspaso fluido de incidentes, escalamiento técnico y coordinación durante la respuesta a incidentes de distinta criticidad.	Exigido	
	El servicio deberá operar bajo un esquema de niveles de atención diferenciados, permitiendo escalar incidentes según su complejidad técnica, impacto y criticidad, sin interrupciones en la gestión del incidente.	Exigido	
	El modelo operativo deberá permitir la ejecución de actividades de análisis y respuesta de forma distribuida entre equipos especializados, manteniendo una coordinación centralizada del incidente. Serán aceptadas arquitecturas basadas en software libre, plataformas open source o soluciones híbridas, siempre que cumplan con los niveles de servicio requeridos.	Exigido	
2.3. Integración de capacidades de automatización	La arquitectura del servicio deberá contar con capacidades avanzadas sólidas de automatización y orquestación de respuestas, reduciendo tiempos de reacción y estandarizando acciones ante incidentes recurrentes. No serán aceptados capacidades de automatización basadas únicamente en el uso de scripts desarrollados manualmente o ejecutadas de manera no integradas.	Exigido	
	El servicio deberá soportar la ejecución de flujos de respuesta automatizados y asistidos, coordinando acciones entre herramientas de detección, plataformas de análisis y equipos operativos.	Exigido	
2.4. Gestión unificada del incidente	El modelo operativo deberá asegurar que cada incidente sea gestionado como una única entidad lógica, independientemente de la cantidad de alertas, activos o fuentes involucradas.	Exigido	
3. GESTIÓN DE ACTIVOS, CONTEXTO Y PROTECCIÓN BASE			
3.1. Clasificación y contexto operacional	El servicio deberá permitir clasificar activos por criticidad (crítico/no crítico) y por función (servidor, endpoint usuario, red, seguridad, aplicación), y mantener dicha clasificación como metadato disponible para SOC/CSIRT.	Exigido	
	El servicio deberá mantener estado operativo de seguridad del activo (p.ej., agente instalado, política aplicada, última comunicación, cobertura activa), visible para SOC y auditable.	Exigido	
3.2. Agente unificado de gestión y telemetría	Todos los activos bajo alcance deberán contar con un agente unificado para recolección de telemetría y aplicación de políticas, gestionado centralmente (alta/baja, políticas, estado).	Exigido	
	La gestión del agente deberá contemplar operación continua aun ante interrupciones temporales de conectividad con el plano de control, manteniendo configuraciones de forma segura.	Exigido	

3.3. Protección base en endpoints	El servicio deberá incluir una capa de protección preventiva base en endpoints, operando localmente en el activo, orientada a bloquear amenazas comunes y conocidas antes de su ejecución, como condición mínima de cobertura.	Exigido
	La protección base deberá incluir prevención de malware mediante mecanismos automatizados, habilitados por defecto en los endpoints protegidos.	Exigido
	La protección base deberá incluir una capa dedicada de protección contra ransomware con capacidad de prevención basada en comportamiento (no solo firmas), como mínimo.	Exigido
	La protección base deberá incluir protección contra amenazas en memoria (in-memory), orientada a técnicas que evitan escribir payloads en disco, con capacidad de prevención.	Exigido
	La protección base deberá incluir prevención de comportamiento malicioso (malicious behavior), con generación de eventos para análisis posterior por SOC.	Exigido
4. TELEMETRÍA Y VISIBILIDAD		
4.1. Recolección centralizada de telemetría	El servicio deberá garantizar la recolección centralizada y continua de telemetría de seguridad proveniente de los activos tecnológicos de la Entidad, permitiendo su análisis unificado como parte del servicio SOC.	Exigido
4.2. Fuentes de telemetría soportadas	El servicio deberá permitir la recolección de telemetría de seguridad mediante agentes instalados en los activos, incluyendo como mínimo: - eventos del sistema operativo (Windows y Linux), - actividad de procesos y subprocesos, - ejecución de comandos e intérpretes, - actividad de archivos y artefactos, - telemetría de red originada en el endpoint, - contexto de usuario y privilegios.	Exigido
	El servicio deberá permitir la recolección de telemetría de seguridad mediante integraciones nativas y/o APIs desde fuentes externas, incluyendo como mínimo: - dispositivos de red y seguridad, - servicios de directorio e identidad, - plataformas cloud e infraestructura, - aplicaciones y servicios web, - servicios de correo y colaboración, sin requerir desarrollos personalizados para cada fuente. Como mínimo deben ser soportadas las siguientes tecnologías: -eventos del WAF F5 -eventos del Fortigate central y periféricos (todas las Sucursales) -eventos del Checkpoint -eventos del NAC -eventos del AD -eventos de AV -eventos del PAM	Exigido
4.3. Capacidades de recolección de telemetría	La telemetría recolectada deberá incluir información de procesos, tipo como creación, terminación, jerarquía de procesos, comandos ejecutados y relaciones padrehijo, tales como: - argumentos y parámetros de ejecución, - relaciones entre procesos y subprocesos, - uso de intérpretes de comandos y scripting, - ejecución desde rutas no convencionales, - procesos iniciados por servicios o tareas programadas.	Exigido
	La telemetría recolectada deberá incluir información sobre archivos y artefactos, incluyendo creación, modificación, ejecución, hashes, ubicación y mecanismos de persistencia, sin depender exclusivamente de firmas estáticas. Debe ser posible igualmente identificar: - cambios en atributos y permisos, - creación de archivos ejecutables en ubicaciones temporales, - uso de técnicas de persistencia basadas en archivos, - ejecución de binarios no firmados o con firmas inválidas.	Exigido
	El servicio deberá recolectar telemetría asociada a actividades en memoria, permitiendo identificar ejecuciones sin archivo, inyecciones de código, cargas dinámicas, uso anómalo de bibliotecas del sistema y técnicas de evasión basadas en memoria.	Exigido
	La telemetría recolectada deberá incluir conexiones de red iniciadas desde los endpoints, incluyendo direcciones IP, dominios, puertos, protocolos y su relación con procesos.	Exigido
	El servicio deberá recolectar telemetría asociada a actividades de usuarios, incluyendo autenticaciones, uso de credenciales, elevaciones de privilegios y cambios de contexto de seguridad.	Exigido

4.4. Normalización de eventos	El servicio deberá normalizar la telemetría recolectada, permitiendo su análisis y correlación de forma consistente, independientemente de la fuente de origen.	Exigido
4.5. Integridad de la telemetría	El servicio deberá garantizar la integridad de la telemetría durante su transmisión y almacenamiento, incluyendo como mínimo: - uso de canales cifrados para la transmisión de eventos, - mecanismos que eviten la alteración o eliminación no autorizada de registros, - preservación de la secuencia temporal de los eventos y detección de lagunas o pérdidas de eventos durante la ingestión, - control de acceso a la información recolectada.	Exigido
4.6. Baja latencia en la ingestión	El servicio deberá garantizar que la telemetría recolectada esté disponible para análisis operativo en el SOC en un plazo compatible con la detección y respuesta temprana a incidentes, evitando arquitecturas basadas en procesamiento diferido o cargas por lotes.	Exigido
4.7. Visibilidad unificada de activos	El servicio deberá proporcionar visibilidad unificada y en tiempo casi real de la actividad de los activos monitoreados, permitiendo comprender su comportamiento normal y anómalo.	Exigido
4.8. Acceso del SOC a telemetría cruda	El servicio deberá permitir al SOC acceder a la telemetría cruda y enriquecida para actividades de análisis avanzado, investigación y cacería de amenazas.	Exigido
4.9. Soporte a consultas avanzadas	El servicio deberá soportar capacidades avanzadas de consulta y análisis sobre la telemetría recolectada, incluyendo: - búsquedas complejas multi-campo, - correlación temporal entre eventos, - consultas basadas en comportamiento, - análisis exploratorio para cacería de amenazas, sin depender exclusivamente de reglas predefinidas o dashboards estáticos.	Exigido
4.10. Escalabilidad de ingestión	El servicio deberá soportar incrementos inmediatos de al menos un cincuenta por ciento (50%) sobre el volumen de telemetría procesado en cualquier momento, sin degradar la capacidad de análisis, detección ni la continuidad operativa del servicio, ni que implique costos adicionales a la contratante.	Exigido
4.11. Diferenciación por criticidad	El servicio deberá permitir diferenciar lógicamente la telemetría proveniente de activos críticos respecto de activos no críticos, habilitando análisis y tratamiento diferenciado cuando corresponda.	Exigido
5. INTELIGENCIA DE AMENAZAS Y GESTIÓN DE LA EXPOSICIÓN		
5.1. Integración de inteligencia de amenazas externa	El servicio deberá incorporar capacidades de inteligencia de amenazas avanzadas, integradas de forma nativa a los procesos de detección, correlación y respuesta del SOC, permitiendo enriquecer eventos e incidentes con contexto táctico, técnico y operacional.	Exigido
	El servicio deberá incorporar inteligencia de amenazas externa proveniente de múltiples fuentes especializadas, integrada de forma operativa al SOC para enriquecer detecciones, investigaciones y actividades de cacería de amenazas.	Exigido
	La inteligencia de amenazas deberá incluir indicadores de compromiso, tácticas, técnicas y procedimientos (TTPs), infraestructura maliciosa, campañas activas y actores de amenaza, con actualización continua y sin intervención manual del analista. No se aceptará que el servicio cuente con fuentes de inteligencia únicamente de origen open source.	Exigido
	La inteligencia utilizada deberá actualizarse de forma continua y automática, sin depender exclusivamente de cargas manuales o procesos ad-hoc por parte de analistas.	Exigido
	El servicio deberá enriquecer automáticamente eventos e incidentes de seguridad con información de inteligencia de amenazas, incluyendo reputación de IPs, dominios, URLs, hashes y contexto de campañas activas.	Exigido
	El enriquecimiento deberá ejecutarse de forma nativa dentro del flujo de análisis del SOC, impactando directamente la priorización, clasificación y respuesta a incidentes.	Exigido
5.2. Monitoreo de exposición digital	El servicio deberá incluir capacidades de monitoreo continuo de la exposición digital de la Entidad, permitiendo identificar activos, servicios, aplicaciones y vectores de ataque expuestos desde el exterior que incrementen la superficie de ataque, incluyendo como mínimo activos expuestos, dominios, subdominios, servicios accesibles públicamente y configuraciones inseguras visibles desde Internet.	Exigido
	El monitoreo deberá realizarse desde una perspectiva externa (attacker view), considerando infraestructura, aplicaciones, servicios web, dominios, subdominios y otros elementos públicamente accesibles.	Exigido
	El monitoreo de exposición digital deberá ejecutarse de forma recurrente y automatizada, permitiendo detectar cambios en la superficie de ataque sin ejecuciones manuales puntuales.	Exigido
	El servicio deberá incluir monitoreo continuo de fuentes abiertas, cerradas y Dark Web para identificar filtraciones, credenciales comprometidas, accesos ofrecidos a la venta o información sensible asociada a la Entidad.	Exigido
	Los hallazgos de inteligencia en Dark Web deberán integrarse al SOC como eventos de seguridad, permitiendo su correlación con telemetría interna y procesos de respuesta.	Exigido

	El servicio deberá incluir capacidades de detección de abuso de marca, incluyendo dominios similares (typosquatting), campañas de phishing, suplantación y uso indebido de nombres institucionales.	Exigido
	La inteligencia de amenazas y los hallazgos de exposición digital deberán alimentar directamente actividades de cacería de amenazas, análisis proactivo y ajuste de detecciones.	Exigido
5.3. Validación continua de postura de seguridad multivector	El servicio deberá ejecutar actividades continuas de validación técnica de la postura de seguridad, orientadas a identificar debilidades reales explotables mediante simulación controlada de técnicas utilizadas por actores de amenaza.	Exigido
	La validación deberá contemplar múltiples vectores de ataque, incluyendo como mínimo: infraestructura, aplicaciones, configuraciones expuestas, controles de seguridad y superficie de ataque digital.	Exigido
	El servicio deberá incluir ejercicios técnicos de simulación controlada de ataques, combinando técnicas automatizadas y manuales, con el objetivo de validar la efectividad real de los controles de seguridad desplegados.	Exigido
	Las simulaciones deberán ejecutarse de forma coordinada con el SOC, garantizando que los eventos generados puedan ser detectados, correlacionados y analizados como parte de la operación normal del servicio.	Exigido
	El servicio deberá incluir capacidades para evaluar la postura de seguridad asociada al factor humano, mediante la validación técnica de comportamientos de riesgo, uso indebido de credenciales y exposición a vectores de ingeniería social.	Exigido
	El servicio de identificación y gestión de los hallazgos de seguridad deberá ser provisto a través de herramientas tecnológicas especializadas para dicho fin, permitiendo el registro, seguimiento y control de los hallazgos desde su identificación hasta su remediación.	Exigido
	Las herramientas utilizadas deberán permitir la colaboración en tiempo real entre el equipo técnico de la Entidad, el SOC y el CSIRT, facilitando la coordinación de acciones de análisis, validación y remediación.	Exigido
	El servicio deberá garantizar que los hallazgos se encuentren disponibles en tiempo casi real, en un entorno seguro, auditable y trazable, preservando la integridad y el historial de cada hallazgo.	Exigido
	Las herramientas tecnológicas utilizadas para la gestión de hallazgos deberán contar con mecanismos de control de acceso granular basados en roles, así como con trazabilidad completa de acciones, cambios de estado, evidencias y comentarios asociados.	Exigido
	No se aceptarán soluciones basadas en repositorios genéricos de documentos, herramientas ofimáticas colaborativas o medios no diseñados específicamente para la gestión técnica de hallazgos de ciberseguridad.	Exigido
5.4. Integración con procesos de detección y respuesta	Los hallazgos identificados deberán integrarse con los procesos de detección, correlación, cacería de amenazas y respuesta a incidentes, permitiendo su uso directo para el ajuste de detecciones, validación de controles y mejora continua de la postura de seguridad.	Exigido
6. CAPACIDADES DE DETECCIÓN Y CORRELACIÓN		
6.1. Capacidades avanzadas de detección automática	El servicio deberá incorporar capacidades de detección de amenazas que no dependan exclusivamente de firmas estáticas o listas de indicadores, permitiendo identificar actividades maliciosas conocidas y desconocidas mediante el análisis avanzado de la telemetría recolectada.	Exigido
	El servicio deberá realizar análisis de comportamiento sobre usuarios, cuentas, endpoints y entidades tecnológicas, permitiendo identificar desviaciones significativas respecto a patrones normales de actividad.	Exigido
	El servicio deberá detectar el uso indebido de credenciales legítimas, incluyendo accesos fuera de patrón, autenticaciones anómalas, elevaciones irregulares de privilegios y reutilización sospechosa de credenciales.	Exigido
	El servicio deberá detectar técnicas de movimiento lateral, incluyendo uso indebido de herramientas administrativas, protocolos internos y acceso entre activos sin relación operativa legítima.	Exigido
	El servicio deberá detectar ataques sin archivo, incluyendo ejecución desde memoria, abuso de intérpretes de comandos, scripting y cargas dinámicas, sin depender de artefactos persistentes en disco.	Exigido
	El servicio deberá detectar mecanismos de persistencia utilizados por actores maliciosos, incluyendo tareas programadas, servicios, claves de inicio, modificaciones de configuración y otros métodos de permanencia.	Exigido
	El servicio deberá detectar comportamientos asociados a ransomware, incluyendo cifrado masivo, manipulación de copias de seguridad, deshabilitación de controles de seguridad y técnicas orientadas al impacto sobre la disponibilidad.	Exigido
	El servicio deberá detectar malware desconocido y variantes polimórficas mediante análisis heurístico, correlación de comportamiento y detección basada en técnicas, sin depender exclusivamente de firmas.	Exigido
	El servicio deberá detectar técnicas de evasión y anti-análisis, incluyendo desactivación de defensas, ocultamiento de procesos, ofuscación, bypass de controles y técnicas de living-off-the-land.	Exigido

6.2. Correlación automática avanzada multi-evento y análisis contextual	El servicio deberá correlacionar múltiples eventos relacionados en el tiempo para identificar secuencias completas de ataque, sin depender exclusivamente de reglas estáticas o correlaciones manuales.	Exigido
	El servicio deberá correlacionar telemetría proveniente de endpoints, red, identidad, aplicaciones e infraestructura dentro de un único motor analítico.	Exigido
	El servicio deberá permitir la correlación de eventos no necesariamente consecutivos ni inmediatos, habilitando la detección de ataques persistentes, de baja frecuencia o de múltiples etapas.	Exigido
	El servicio deberá soportar correlaciones basadas en patrones de comportamiento y contexto operativo, y no exclusivamente en coincidencias de indicadores o firmas.	Exigido
	El servicio deberá enriquecer automáticamente las detecciones con contexto adicional, incluyendo información del activo, criticidad, rol del usuario, historial de actividad y relación con otros eventos.	Exigido
	El servicio deberá permitir la priorización de detecciones considerando el contexto del activo afectado, la etapa del ataque y el impacto potencial, evitando el tratamiento homogéneo de eventos.	Exigido
6.3. Detección por etapas del ataque	El servicio deberá incorporar capacidades automáticas para detectar y correlacionar actividades asociadas a distintas etapas del ataque, incluyendo reconocimiento, acceso inicial, ejecución, persistencia, escalamiento de privilegios, movimiento lateral y acciones sobre el objetivo.	Exigido
6.4. Cobertura de técnicas de ataque	El servicio deberá incorporar capacidades automáticas para identificar actividades alineadas a marcos reconocidos de técnicas de ataque, permitiendo mapear detecciones a tácticas y técnicas utilizadas por actores maliciosos.	Exigido
6.5. Capacidades técnicas para cacería de amenazas	El servicio deberá contar con capacidades técnicas específicas para la ejecución de cacería de amenazas, incluyendo como mínimo acceso directo a telemetría cruda y enriquecida, ejecución de consultas complejas multi-evento y multi-fuente, correlación temporal flexible sin ventanas rígidas y análisis exploratorio sin depender de detecciones o alertas preexistentes.	Exigido
6.6. Cacería de amenazas basada en hipótesis	El servicio deberá permitir la ejecución de actividades de cacería de amenazas basadas en hipótesis, donde los analistas puedan formular, validar y refinar escenarios de ataque utilizando telemetría histórica y en tiempo casi real, sin requerir el desarrollo de reglas o detecciones permanentes.	Exigido
6.7. Ciclo de vida gestionado de detecciones	El servicio deberá contar con un ciclo de vida gestionado de detecciones que permita la creación, modificación, validación y despliegue centralizado de nuevas detecciones de forma controlada y consistente en toda la plataforma de monitoreo.	Exigido
6.8. Actualización estructurada de capacidades de detección	El servicio deberá permitir la incorporación de nuevas capacidades de detección mediante mecanismos estructurados y reutilizables, evitando depender exclusivamente de ajustes manuales caso por caso realizados por analistas.	Exigido
7. RESPUESTA, CONTENCIÓN Y AUTOMATIZACIÓN		
7.1. Capacidades avanzadas y automatizadas de respuesta	El servicio deberá incluir capacidades avanzadas y automatizadas de respuesta a incidentes de ciberseguridad, integradas de forma operativa con las plataformas de detección y análisis, permitiendo ejecutar acciones técnicas de contención y mitigación sin depender de ejecución manual caso por caso.	Exigido
7.2. Orquestación de respuesta multi-herramienta	El servicio deberá incluir capacidades de orquestación que permitan coordinar acciones de respuesta entre múltiples herramientas y dominios de seguridad, incluyendo detección en endpoints, SIEM, controles de red, seguridad perimetral y servicios externos, desde un único plano de control.	Exigido
7.3. Orquestación basada en flujos visuales	El servicio deberá incluir un motor de orquestación basado en flujos lógicos visuales, que permita diseñar, modificar y ejecutar respuestas de forma ágil, estructurada y reutilizable, sin requerir desarrollo de scripts personalizados para cada escenario.	Exigido
7.4. Ejecución controlada de flujos de respuesta	El servicio deberá permitir la ejecución de flujos de respuesta de manera automática o asistida, bajo condiciones claramente definidas, incorporando validaciones, controles y puntos de decisión según la criticidad del incidente.	Exigido
7.5. Playbooks operativos de respuesta	El servicio deberá incluir playbooks operativos de respuesta a incidentes, implementados de forma funcional dentro de la plataforma de orquestación, y no únicamente como procedimientos documentales o manuales.	Exigido
7.6. Reutilización y parametrización de playbooks	Los playbooks deberán ser reutilizables y parametrizables, permitiendo su aplicación a distintos incidentes y entornos sin necesidad de rediseñar el flujo para cada caso.	Exigido
7.7. Playbooks mínimos preexistentes de respuesta	El servicio deberá incluir experiencia comprobable en la implementación y operación de playbooks de respuesta automatizada, ya implementados y utilizados en entornos productivos, que cubran como mínimo los siguientes escenarios: detección y contención de malware, ransomware, compromiso de credenciales, accesos no autorizados, movimiento lateral, comunicaciones de comando y control, explotación de vulnerabilidades críticas y ataques a servicios expuestos.	Exigido

7.8. Demostrabilidad de playbooks	El servicio deberá permitir la demostración funcional de los playbooks de respuesta incluidos, en un entorno controlado, a solicitud de la Entidad durante la fase de evaluación técnica.	Exigido
7.9. Acciones de contención remota	El servicio deberá incluir capacidades de contención remota ejecutables desde la plataforma de respuesta, sin intervención manual directa sobre el activo, incluyendo como mínimo aislamiento lógico, bloqueo de comunicaciones y mitigación inmediata de amenazas.	Exigido
7.10. Integración tecnológica SOCSOAR	Las capacidades de respuesta y automatización deberán estar integradas tecnológicamente con el SOC, permitiendo que los incidentes gestionados activen flujos de respuesta directamente desde la plataforma de operación, sin dependencia de herramientas externas o procesos manuales.	Exigido
7.11. Gestión técnica del ciclo de vida del incidente	El servicio deberá incluir capacidades técnicas para la gestión del ciclo de vida del incidente dentro de la plataforma de respuesta, incluyendo estados, transiciones, acciones ejecutadas y trazabilidad operativa.	Exigido
7.12. Trazabilidad y auditoría de respuestas	El servicio deberá garantizar la trazabilidad completa y auditable de todas las acciones de respuesta ejecutadas, incluyendo acciones automáticas y asistidas, con registro de tiempo, responsable y resultado de cada acción.	Exigido
7.13. Escalamiento automático de incidentes	El servicio deberá incluir mecanismos técnicos de escalamiento automático de incidentes, activando flujos de respuesta más avanzados cuando el incidente evolucione en criticidad, alcance o impacto.	Exigido
7.14. Integración funcional con cacería de amenazas	Las capacidades de respuesta deberán integrarse funcionalmente con actividades de cacería de amenazas, permitiendo ejecutar acciones de validación, contención o mitigación directamente desde investigaciones activas.	Exigido
7.15. Evolución y adaptación de flujos	El servicio deberá permitir la modificación, versionado y mejora continua de los flujos de respuesta dentro de la plataforma de orquestación, sin requerir rediseños estructurales ni desarrollos externos.	Exigido
8. CAPACIDADES DEL EQUIPO DE RESPUESTA A INCIDENTES (CSIRT)		
8.1. Capacidades técnicas del CSIRT	El servicio deberá incluir una capacidad CSIRT integrada técnica y operativamente al SOC, al SIEM y a las capacidades de automatización, no aceptándose modelos donde el CSIRT opere de forma aislada o únicamente reactiva.	Exigido
	El CSIRT deberá gestionar los incidentes desde una plataforma centralizada, permitiendo el seguimiento técnico, correlación de eventos, acciones ejecutadas y evolución del incidente en un único sistema.	Exigido
	El CSIRT deberá contar con capacidad técnica y operativa para gestionar múltiples incidentes simultáneos, sin degradar la calidad del análisis ni la capacidad de respuesta ante incidentes de alta criticidad.	Exigido
	El CSIRT deberá gestionar incidentes que involucren múltiples activos, fases del ataque y vectores combinados, permitiendo el análisis de campañas o intrusiones prolongadas.	Exigido
	El CSIRT deberá realizar análisis técnico profundo de los incidentes, incluyendo reconstrucción de la secuencia de ataque, identificación de técnicas utilizadas y determinación del alcance real del compromiso.	Exigido
	Las actividades del CSIRT deberán basarse en el uso directo de la telemetría recolectada por el servicio, no aceptándose modelos que dependan exclusivamente de información resumida, alertas o reportes del SOC.	Exigido
	El CSIRT deberá ejecutar acciones de validación, contención y mitigación apoyándose en las capacidades de automatización y orquestación del servicio, no aceptándose una gestión exclusivamente manual del incidente.	Exigido
	El CSIRT deberá gestionar técnicamente el ciclo de vida completo del incidente dentro de la plataforma del servicio, incluyendo estados, transiciones, acciones ejecutadas y cierre técnico validado.	Exigido
	El CSIRT deberá demostrar capacidad para escalar y gestionar incidentes de muy alta criticidad, incluyendo ransomware activo, intrusión persistente, compromiso de identidad y afectación de servicios críticos.	Exigido
	El CSIRT deberá coordinar acciones técnicas entre múltiples dominios de seguridad (endpoint, red, identidad, perímetro, vulnerabilidades) como parte de un mismo incidente.	Exigido
	El CSIRT deberá producir análisis técnicos post-incidente que incluyan causa raíz, debilidades explotadas y recomendaciones técnicas accionables para prevenir recurrencias.	Exigido
	El CSIRT deberá retroalimentar activamente las capacidades de detección, correlación y automatización del servicio en función de los incidentes gestionados.	Exigido

	El CSIRT deberá operar como parte del servicio gestionado continuo, alineado a la cobertura 24x7 del SOC, no aceptándose esquemas de atención bajo demanda o solo en horario laboral.	Exigido
9. INVESTIGACIÓN Y ANÁLISIS FORENSE		
9.1 Capacidades técnicas preexistentes de investigación	El servicio deberá contar desde el inicio del contrato con capacidades técnicas operativas para la investigación de incidentes, integradas al SOC y disponibles de forma permanente, sin depender de la incorporación posterior de herramientas, desarrollos ad-hoc o servicios profesionales puntuales.	Exigido
	Las capacidades de investigación deberán estar soportadas por funcionalidades técnicas ya implementadas en la plataforma de monitoreo y análisis, y no basarse exclusivamente en procedimientos manuales ejecutados por analistas.	Exigido
9.2 Investigación basada en telemetría completa	El servicio deberá permitir investigaciones técnicas basadas en telemetría histórica y en tiempo casi real, sin requerir que el incidente haya sido previamente detectado por una alerta específica.	Exigido
	La investigación deberá permitir correlacionar procesos, archivos, memoria, red, identidades y actividades del sistema dentro de un mismo flujo analítico.	Exigido
9.3 Reconstrucción técnica de la cadena de ataque	El servicio deberá permitir reconstruir técnicamente la cadena completa del ataque, incluyendo acceso inicial, ejecución, persistencia, escalamiento, movimiento lateral y acciones sobre el objetivo.	Exigido
	La reconstrucción deberá generarse mediante correlación automática y análisis contextual, no exclusivamente mediante análisis manual de eventos aislados.	Exigido
9.4 Líneas de tiempo forenses operativas	El servicio deberá generar líneas de tiempo técnicas del incidente de forma estructurada, permitiendo visualizar eventos, relaciones y evolución del ataque en orden temporal.	Exigido
	Las líneas de tiempo deberán ser navegables, reutilizables y exportables como parte del proceso de investigación y documentación del incidente.	Exigido
9.5 Análisis forense lógico integrado al SOC	El servicio deberá permitir análisis forense lógico a partir de la telemetría recolectada, sin requerir obligatoriamente adquisición física de discos o memoria para cada investigación.	Exigido
	El análisis forense deberá permitir identificar mecanismos de persistencia, evasión, abuso de credenciales y técnicas de living-off-the-land.	Exigido
9.6 Investigación de incidentes complejos y persistentes	El servicio deberá soportar la investigación de incidentes de múltiples etapas, baja frecuencia o larga duración, incluyendo ataques persistentes avanzados.	Exigido
	La investigación no deberá limitarse a ventanas temporales rígidas ni a correlaciones inmediatas.	Exigido
9.7 Integración obligatoria con respuesta y contención	Las capacidades de investigación deberán integrarse de forma directa con los procesos de respuesta y contención, permitiendo ejecutar acciones técnicas basadas en los hallazgos de la investigación.	Exigido
	El servicio deberá permitir que los resultados de la investigación alimenten flujos automáticos o asistidos de respuesta, sin reprocesos manuales.	Exigido
9.8 Análisis post-incidente estructurado	El servicio deberá incluir un proceso técnico estructurado de análisis post-incidente, soportado por evidencias técnicas generadas durante la investigación.	Exigido
	El análisis post-incidente deberá derivar en ajustes verificables de detecciones, correlaciones, playbooks o controles preventivos.	Exigido
9.9 Documentación técnica basada en evidencias	El servicio deberá generar documentación técnica del incidente basada en evidencias objetivas recolectadas durante la investigación, evitando informes meramente descriptivos o narrativos.	Exigido
9.10 Soporte a requerimientos regulatorios y legales	El servicio deberá permitir la preservación, exportación y entrega controlada de evidencias técnicas para auditorías, investigaciones administrativas o procesos legales.	Exigido
9.11 Integración con cacería de amenazas	Los resultados de investigaciones y análisis post-incidente deberán integrarse directamente a las actividades de cacería de amenazas, permitiendo identificar patrones recurrentes y compromisos adicionales.	Exigido
9.12 Prohibición de investigación puramente manual	No se aceptarán ofertas donde las capacidades de investigación y análisis forense dependan exclusivamente de actividades manuales, herramientas aisladas o servicios profesionales no integrados al SOC. El servicio deberá contar con capacidades de análisis forense con validez probatoria, conforme a las buenas prácticas internacionales de identificación, recolección, adquisición y preservación de evidencia digital (ISO/IEC 27037). A tal efecto, la adquisición y el tratamiento de la evidencia deberán realizarse con herramientas forenses reconocidas y validadas en la industria que garanticen la no alteración de la evidencia original —incluyendo mecanismos de bloqueo de escritura (write-blocking)—, la integridad mediante funciones criptográficas de hash, la trazabilidad y la cadena de custodia. Asimismo, el servicio deberá contar con una capacidad forense acreditada.	Exigido
10. RETENCIÓN, DISPONIBILIDAD Y CONTINUIDAD DEL SERVICIO		

10.1. Disponibilidad continua del servicio	El servicio deberá garantizar la disponibilidad continua de las capacidades de recolección, análisis, correlación, investigación y respuesta ante incidentes, sin interrupciones operativas durante la vigencia del contrato.	Exigido
	El servicio deberá operar sobre una arquitectura tolerante a fallos, eliminando puntos únicos de falla en los planos de ingestión, análisis y almacenamiento de información de seguridad.	Exigido
10.2. Capacidad de Retención	El servicio deberá garantizar una capacidad mínima de 2 TB (dos terabytes) de almacenamiento disponible para análisis operativo inmediato, sin degradación de capacidades de detección, correlación, cacería e investigación.	Exigido
	El servicio deberá soportar una ingestión sostenida mínima de 300 GB (trescientos gigabytes) diarios de telemetría de seguridad, sin pérdida de eventos ni degradación del servicio.	Exigido
	El servicio deberá garantizar una capacidad total de retención mínima de ciento diez terabytes (110 TB) de información de seguridad durante los 24 (veinticuatro) meses de vigencia del contrato.	Exigido
	La capacidad de retención histórica no deberá afectar negativamente el rendimiento del análisis operativo ni limitar la detección durante picos de actividad o incidentes masivos.	Exigido
10.3. Accesibilidad a datos históricos	El servicio deberá permitir el acceso técnico a la información histórica para fines de investigación, auditoría y análisis forense, sin requerir restauraciones manuales desde respaldos.	Exigido
10.4. Integridad y trazabilidad de los datos	El servicio deberá preservar la integridad, secuencia temporal y trazabilidad de los datos durante todo su ciclo de vida, desde la ingestión hasta la conservación histórica.	Exigido
10.5. Continuidad durante incidentes de alta carga	El servicio deberá garantizar continuidad operativa durante escenarios de alta carga, incluyendo incidentes masivos, campañas activas o generación anómala de eventos.	Exigido
10.6. Escalamiento inmediato de capacidad	El servicio deberá permitir el escalamiento inmediato de capacidad de ingestión, análisis y almacenamiento ante incrementos súbitos de volumen, sin intervención manual.	Exigido
10.7. Independencia de infraestructura del cliente	La retención, disponibilidad y continuidad del servicio no deberán depender de la infraestructura tecnológica propia de la Entidad.	Exigido
10.8. Prohibición de retención basada en backups	No se aceptarán esquemas donde la retención de información dependa exclusivamente de copias de seguridad no indexadas o inaccesibles para análisis.	Exigido
11. CUADROS DE MANDO Y CONTROL (DASHBOARDS), MÉTRICAS Y REPORTERIA		
11.1. Cuadros de mando y control (Dashboards)	El servicio deberá proporcionar dashboards operativos que reflejen en tiempo real el estado de la seguridad, eventos relevantes, alertas activas e incidentes en curso, alimentados directamente desde la telemetría y procesos del SOC.	Exigido
	Los dashboards deberán actualizarse de forma automática y continua, sin depender de cargas manuales ni generación periódica de reportes.	Exigido
	El servicio deberá incluir dashboards orientados a la supervisión del servicio, permitiendo visualizar volumen de eventos, incidentes gestionados, estados, tendencias y carga operativa del SOC.	Exigido
	Los dashboards deberán permitir segmentación por criticidad de activos, tipo de amenaza, origen del evento y estado del incidente.	Exigido
	El servicio deberá proporcionar dashboards de nivel ejecutivo, orientados a la visualización del nivel de riesgo, evolución de amenazas, incidentes relevantes y métricas clave del servicio.	Exigido
	Los dashboards ejecutivos deberán derivarse directamente de la operación real del SOC, sin reinterpretaciones manuales de la información.	Exigido
	El servicio deberá permitir acceso controlado a dashboards por parte de la Entidad, con perfiles diferenciados según rol, garantizando confidencialidad y segregación de información.	Exigido
11.2. Métricas	El servicio deberá generar métricas operativas automáticas del SOC, incluyendo como mínimo: volumen de eventos procesados, alertas generadas, incidentes abiertos/cerrados y tiempos de atención.	Exigido
	El servicio deberá generar métricas técnicas asociadas a la detección y respuesta, incluyendo tiempos de detección, tiempos de análisis y tiempos de contención, basadas en datos reales de operación.	Exigido

	El servicio deberá permitir el acceso histórico a métricas y reportes para análisis de tendencias, auditorías y evaluaciones posteriores.	Exigido
	El servicio deberá permitir visualizar tendencias y evolución de amenazas en el tiempo, incluyendo tipos de ataque, vectores predominantes y activos más afectados.	Exigido
11.3. Reportería	El servicio deberá incluir la generación de reportes periódicos que reflejen de forma objetiva la operación del SOC, incidentes gestionados, hallazgos relevantes y evolución de la postura de seguridad.	Exigido
	Los reportes deberán generarse a partir de la información real del SOC y no podrán consistir únicamente en resúmenes narrativos sin respaldo técnico.	Exigido
	El servicio deberá permitir trazar cualquier métrica o conclusión incluida en los reportes hacia eventos, incidentes o datos operativos reales del SOC.	Exigido
	No se aceptarán servicios donde los dashboards o reportes dependan exclusivamente de procesos manuales, planillas, presentaciones o documentos generados fuera de la plataforma operativa del SOC.	Exigido
11.4. Personalización de vistas y reportes	El servicio deberá permitir la personalización de dashboards y reportes según necesidades operativas y de gestión de la Entidad, sin desarrollo a medida ni dependencia del proveedor.	Exigido
12. SERVICIOS DE PREVENCIÓN Y PROTECCIÓN PARA ACTIVOS CRITICOS		
12.1. Generales	Las capacidades definidas en este apartado aplicarán exclusivamente a activos críticos definidos por la Entidad, hasta un máximo de 800 (ochocientos), incluyendo servidores Windows y Linux, sistemas críticos y otros activos tecnológicos compatibles.	Exigido
	Las capacidades deberán aplicarse sobre activos donde la tecnología utilizada sea compatible, sin requerir desarrollos ad-hoc, adaptaciones manuales o degradar la seguridad del activo.	Exigido
	El servicio deberá incluir todo el equipamiento a ser utilizado en las instalaciones del Banco para la prestación del servicio in situ (Monitores, Computadoras, Notebooks, etc). La conectividad será proporcionada por el Banco.	Exigido
	Todas las capacidades aplicadas a activos críticos deberán integrarse operativamente con el SOC y CSIRT según se detalla en los apartados anteriores	Exigido
12.2. Bloqueo de infraestructura maliciosa	El servicio deberá incluir protección DNS avanzada gestionada como parte integral del servicio de ciberseguridad, orientada a prevenir comunicaciones maliciosas desde y hacia activos críticos, incluso antes de que se establezcan conexiones a nivel de red o aplicación.	Exigido
	La protección DNS deberá permitir la aplicación de políticas diferenciadas basadas en tipo de activo, rol operativo y criticidad, y no únicamente en direcciones IP o rangos de red.	Exigido
	El servicio deberá asociar las consultas DNS a activos específicos y su contexto operativo, permitiendo trazabilidad y control granular de decisiones de bloqueo o permisividad.	Exigido
	El servicio deberá detectar y bloquear dominios maliciosos emergentes, incluyendo dominios generados algorítmicamente (DGA), dominios recién registrados y nueva infraestructura C2, sin depender exclusivamente de listas estáticas.	Exigido
	La protección DNS deberá integrarse con fuentes avanzadas de inteligencia de amenazas para bloquear infraestructura asociada a campañas activas, malware, ransomware y actores maliciosos.	Exigido
	El servicio deberá generar registros auditables de consultas DNS, bloqueos y decisiones de seguridad, integrables con el SOC y el SIEM para análisis, correlación e investigación.	Exigido
	La seguridad DNS deberá operar como una capa preventiva independiente de los controles del endpoint, permitiendo bloquear comunicaciones maliciosas aun cuando otros controles hayan sido evadidos.	Exigido
	No se aceptarán soluciones basadas en servicios de resolución DNS públicos o gratuitos, ni configuraciones sin control por políticas, identidad, auditoría e integración al SOC.	Exigido

De las MIPYMES

En los 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.

Ítem	Descripción del servicio	Unidad de medida	Lugar de entrega de los Servicios	Plazo de inicio de los servicios
1	Servicio de Centro de Operaciones de Seguridad (SOC)	Mes	Banco Nacional de Fomento - Casa Matriz	20 días corridos posteriores a la firma del c

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

1. El Proveedor embalará los bienes en la forma necesaria para impedir que se dañen o deterioren durante el transporte al lugar de destino final indicado en el contrato. El embalaje deberá ser adecuado para resistir, sin limitaciones, su manipulación brusca y descuidada, su exposición a temperaturas extremas, la sal y las precipitaciones, y su almacenamiento en espacios abiertos. En el tamaño y peso de los embalajes se tendrá en cuenta, cuando corresponda, la lejanía del lugar de destino final de los bienes y la carencia de equipo pesado de carga y descarga en todos los puntos en que los bienes deban transbordarse.

2. El embalaje, las identificaciones y los documentos que se coloquen dentro y fuera de los bultos deberán cumplir estrictamente con los requisitos especiales que se hayan estipulado expresamente en el contrato y cualquier otro requisito si lo hubiere, especificado en las condiciones contractuales.

Inspecciones y pruebas

Las inspecciones y pruebas serán como se indica a continuación:

No Aplica

1. El proveedor realizará todas las pruebas y/o inspecciones de los Bienes, por su cuenta y sin costo alguno para la contratante.

2. Las inspecciones y pruebas podrán realizarse en las instalaciones del Proveedor o de sus subcontratistas, en el lugar de entrega y/o en el lugar de destino final de entrega de los bienes, o en otro lugar indicado en este apartado.

Cuando dichas inspecciones o pruebas sean realizadas en recintos del Proveedor o de sus subcontratistas se le proporcionarán a los inspectores todas las facilidades y asistencia razonables, incluso el acceso a los planos y datos sobre producción, sin cargo alguno para la Contratante.

3. La Contratante o su representante designado tendrá derecho a presenciar las pruebas y/o inspecciones mencionadas en la cláusula anterior, siempre y cuando éste asuma todos los costos y gastos que ocasione su participación, incluyendo gastos de viaje, alojamiento y alimentación.

4. Cuando el proveedor esté listo para realizar dichas pruebas e inspecciones, notificará oportunamente a la contratante indicándole el lugar y la hora. El proveedor obtendrá de una tercera parte, si corresponde, o del fabricante cualquier permiso o consentimiento necesario para permitir a la contratante o a su representante designado presenciar las pruebas o inspecciones.

5. La Contratante podrá requerirle al proveedor que realice algunas pruebas y/o inspecciones que no están requeridas en el contrato, pero que considere necesarias para verificar que las características y funcionamiento de los bienes cumplan con los códigos de las especificaciones técnicas y normas establecidas en el contrato. Los costos adicionales razonables que incurra el Proveedor por dichas pruebas e inspecciones serán sumados al precio del contrato, en cuyo caso la contratante deberá justificar a través de un dictamen fundado en el interés público comprometido. Asimismo, si dichas pruebas y/o inspecciones impidieran el avance de la fabricación y/o el desempeño de otras obligaciones del proveedor bajo el Contrato, deberán realizarse los ajustes correspondientes a las Fechas de Entrega y de Cumplimiento y de las otras obligaciones afectadas.

6. El proveedor presentará a la contratante un informe de los resultados de dichas pruebas y/o inspecciones.

7. La contratante podrá rechazar algunos de los bienes o componentes de ellos que no pasen las pruebas o inspecciones o que no se ajusten a las especificaciones. El proveedor tendrá que rectificar o reemplazar dichos bienes o componentes rechazados o hacer las modificaciones necesarias para cumplir con las especificaciones sin ningún costo para la contratante. Asimismo, tendrá que repetir las pruebas o inspecciones, sin ningún costo para la contratante, una vez que notifique a la contratante.

8. El proveedor acepta que ni la realización de pruebas o inspecciones de los bienes o de parte de ellos, ni la presencia de la contratante o de su representante, ni la emisión de informes, lo eximirán de las garantías u otras obligaciones en virtud del contrato.

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 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.

Formalización de la Contratación

La convocante formalizará la contratación mediante: 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.

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 especificados en el apartado precedente.
- 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.

En caso de consorcio en formación, el mismo deberá actualizar el RUC definitivo del consorcio constituido a través del Registro de Proveedores del Estado, previo a la comunicación del contrato y emisión del código de contratación.

Derechos Intelectuales

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:

- a. La instalación de los bienes por el proveedor o el uso de los bienes en la República del Paraguay; y
- b. 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

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.

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.

Cuando dicha información incluya datos personales de personas físicas, las partes se obligan a realizar su tratamiento en estricto cumplimiento de la Ley N° 7593/2025 "De Protección de Datos Personales", su reglamentación y demás normas aplicables, respetando en particular los principios de licitud, finalidad, minimización, confidencialidad, seguridad y diligencia debida, y limitando el tratamiento exclusivamente a los fines vinculados con la ejecución del contrato.

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.

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.

Condiciones especiales de la Garantía de Fiel Cumplimiento de Contrato

Las condiciones especiales de la Garantía de Fiel Cumplimiento de Contrato serán:

No Aplica

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:

La Garantía de Fiel Cumplimiento de Contrato deberá extenderse por todo el periodo de ejecución del Contrato: *Plazo de ejecución del servicio: 24 meses contados desde la suscripción más 1* (un) mes de plazo de liberación de la Garantía de Fiel Cumplimiento de Contrato.

La Garantía de Fiel Cumplimiento de Contrato deberá ser presentada en las oficinas de la GDOC - Casa Matriz del BNF (25 de Mayo casi Yegros).

En circunstancias motivadas, la Contratante solicitará al Proveedor que presente prórrogas extendiendo el periodo de validez de la Garantía de Cumplimiento de Contrato, la cual deberá ser presentada antes del vencimiento. La falta de constitución y entrega oportuna de la prórroga de la garantía podrá ser causal de la Ejecución de la Garantía de Cumplimiento de Contrato, y posterior Rescisión del Contrato por hecho imputable al Proveedor y comunicado a la Dirección de Contrataciones Públicas

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 corridos contados a partir de la fecha de cumplimiento de las obligaciones, incluyendo cualquier obligación relativa a la garantía de los bienes y/o servicios.

Solicitud de Pago de Anticipo

El plazo dentro del cual se solicitará el anticipo será (en días corridos) de:

No Aplica

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 estar vigente desde la solicitud de pago del anticipo, y 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 SIPC 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. El proveedor deberá usar el anticipo únicamente para pagar costos que se requieran específicamente para la ejecución del contrato respectivo. El proveedor deberá informar a la contratante sobre el destino y la forma de aplicación del mismo y demostrar que ha utilizado el anticipo para gastos relacionados al efectivo cumplimiento del contrato mediante la presentación de copias de las facturas u otros documentos al administrador del contrato, quien junto con la contratante realizará el seguimiento y control de los recursos entregados. El proveedor estará obligado a proporcionar a la contratante los comprobantes y cualquier otra información que le fuera requerida con el objeto de comprobar el cumplimiento del plan de inversión del anticipo.

8. La amortización del anticipo se realizará de acuerdo con lo establecido en el contrato, en la proporción que éste indique.

9. 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.

10. 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.

11. 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

Indicar en este apartado la forma de instrumentar la garantía de anticipo.

No Aplica

Disponibilidad de créditos presupuestarios

El alcance de los compromisos asumidos, así como la provisión de los bienes y servicios acordados, quedarán supeditados durante su ejecución, a la efectiva disponibilidad de los créditos presupuestarios y de los planes financieros aprobados para el Ejercicio Fiscal vigente y en los ejercicios fiscales siguientes.

La Entidad contratante debe comunicar formalmente al proveedor la existencia del CDP correspondiente al ejercicio fiscal vigente.

En ausencia del CDP y de su comunicación expresa al proveedor, este quedará eximido de realizar la provisión de bienes y/o servicios, sin que dicha abstención genere responsabilidad alguna ni constituya causal de incumplimiento contractual, aun cuando se hubiera emitido la orden de ejecución.

En ningún caso serán admitidas como deudas del ejercicio fiscal vigente ni dará derecho a reclamación de pago alguno, la provisión de bienes o prestaciones de servicios que se efectúen sin contar con la disponibilidad de los créditos presupuestarios correspondientes.

Indicadores de Cumplimiento de Contrato

El documento requerido para acreditar el cumplimiento contractual, será:

- Planificación de indicadores de cumplimiento:
- **Para bienes y Servicios:** Acta de conformidad.
 - **Serán presentados:** 24 (veinticuatro) Actas de conformidad.
 - **Frecuencia:** Mensual

Planificación de indicadores de cumplimiento:

INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA
• Acta 1	• Acta de conformidad.	Conforme al Plan de Entregas
• Acta 2	• Acta de conformidad.	
• Acta 3	• Acta de conformidad.	
• Acta 4	• Acta de conformidad.	
• Acta 5	• Acta de conformidad.	
• Acta 6	• Acta de conformidad.	
• Acta 7	• Acta de conformidad.	
• Acta 8	• Acta de conformidad.	
• Acta 9	• Acta de conformidad.	
• Acta 10	• Acta de conformidad.	
• Acta 11	• Acta de conformidad.	
• Acta 12	• Acta de conformidad.	
• Acta 13	• Acta de conformidad.	
• Acta 14	• Acta de conformidad.	
• Acta 15	• Acta de conformidad.	

• Acta 16	• Acta de conformidad.
• Acta 17	• Acta de conformidad.
• Acta 18	• Acta de conformidad.
• Acta 19	• Acta de conformidad.
• Acta 20	• Acta de conformidad.
• Acta 21	• Acta de conformidad.
• Acta 22	• Acta de conformidad.
• Acta 23	• Acta de conformidad.
• Acta 24	• Acta de conformidad.

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

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.

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:

- a. Nota de remisión u orden de prestación de servicios según el objeto de la contratación;
- b. 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;
- c. REPSE (registro de prestadores de servicios) todos los que son prestadores de servicios;
- d. Certificado de Cumplimiento Tributario;
- e. Constancia de Cumplimiento con la Seguridad Social;

- f. Formulario de Identificación de Servicios Personales (FIS);
- g. 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

2.Documentos Específicos a la presente convocatoria:

- El reporte de la carga de la nómina del personal en el FIP, asignado a los servicios contratados o la actualización en su caso;
- La Declaración Jurada del Salario expedida por el Instituto de Previsión Social a fin de corroborar el cumplimiento efectivo de las cargas sociales;
- El extracto de las acreditaciones de pago de salarios al personal asignado, realizadas a través de Red Bancaria;
- Planilla de marcación de entrada y salida de los empleados de la empresa a la institución contratante.

Otras formas y condiciones de pago al proveedor en virtud del contrato serán las siguientes: Los proveedores adjudicados deberán presentar documentos requeridos por la SEPRELAD según el Artículo 33 de la Resolución 70/2019 política de Conozca a su proveedor formulario Anexo 2 Perfil del cliente. Así mismo, se deberá adjuntar al legajo documentario copia de la nota de notificación de adjudicación emitida por la Gerencia Departamental Operativa de Contrataciones.

Conforme al Artículo 63 de la Ley N° 7021/22 De Contrataciones Públicas, se retendrá el 0,4% (cero puntos cuatro por ciento) sobre el importe de cada factura, deducido los impuestos correspondientes, al momento de su cobro.

Teniendo en cuenta que el llamado es Plurianual, la validez o continuidad de la contratación quedará supeditada a la disponibilidad de créditos presupuestarios aprobados y asignación del Plan Financiero en los Ejercicios Fiscales siguientes, de acuerdo a lo previsto en la legislación vigente.

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.

Anticipo MIPYMES

Se otorgará Anticipo MIPYMES:

No Aplica

Reajuste

El precio del contrato estará sujeto a reajustes. La fórmula y el procedimiento para el reajuste serán los siguientes:

El precio del contrato estará sujeto a reajustes. EL **PROVEEDOR** solicitará por escrito a **La contratante** el reajuste de precios exponiendo la causa del mismo.

La contratante reconocerá un reajuste en los costos de los servicios, en la medida en que durante su vigencia, exista una variación sustancial de precios en la economía nacional y ésta se vea reflejada en el índice de los precios de consumo, publicado por el Banco Central del Paraguay, en un valor igual o mayor al 15% (quince) por ciento, sobre la inflación oficial esperada para el mismo periodo. Los reajustes se aplicarán de la siguiente manera:

V1=	P x I.I.BCP
	15%

V1=Reajuste de la Oferta

P= Precio del Servicio

I.I. BCP= Índice de Inflación emitido por el Banco Central del Paraguay

15%= Mínimo necesario para reajuste del precio

Los precios reajustados, solo tendrán incidencia sobre los servicios aún no ejecutados; y, no tendrán ningún efecto retroactivo respecto a los servicios que fueron ejecutados antes de la verificación del reajuste.

Para tal efecto, **EL PROVEEDOR** deberá solicitar por escrito a **LA CONTRATANTE**.

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, cuando la variación sea positiva, para cuya obtención se deberá cumplir con los requerimientos establecidos por la DNCP.

La aplicación de la fórmula deberá prever la deducción del anticipo financiero, en caso de haber sido otorgado. En caso que los índices oficiales que se deben utilizar en el cálculo no estén disponibles, se podrán efectuar ajustes provisionales utilizando los últimos índices conocidos. Los ajustes se corregirán cuando se conozcan los valores relativos a los meses en cuestión.

El coeficiente de ajuste se redondea a la millonésima superior.

El pago del reajuste se efectuará únicamente después de la emisión del acto administrativo que autoriza el precio reajustado y del correspondiente código de contratación.

Los reajustes de precios se aplicarán bajo solicitud expresa por parte del proveedor, conforme a la forma y plazo establecida en la normativa. El Administrador del Contrato es responsable de velar por la aplicación del reajuste de precios en caso de ser favorable a la Contratante.

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:

0,50 %

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:

0,08

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 plazo de 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 correspondientes, 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 solicitar la suspensión del contrato, por motivos que no le serán imputables, de acuerdo a lo establecido en el artículo 66 de la Ley N° 7021/22.

La contratante, en virtud de causas establecidas en el contrato, está facultada para suspender la tramitación de un pago, en tal caso, las sumas correspondientes durante los atrasos resultantes no devengarán intereses por mora.

Pago de interés por mora.

Procedimiento para el pago de interés por mora:

En caso de que la contratante incurriera en mora en el pago de las obligaciones derivadas del presente contrato, se aplicará el siguiente procedimiento:

- Configuración de la mora: La mora se configura de pleno derecho al vencimiento del plazo contractual de pago, en concordancia con lo dispuesto en la Ley N° 7021/2022 y el Código Civil (Ley N° 1183/1985).
- Devengamiento de intereses: Los intereses moratorios se devengarán desde el día siguiente al vencimiento del plazo de pago hasta la fecha del pago total e íntegro del capital adeudado.
- Tasa aplicable: Los intereses moratorios se calcularán conforme a la fórmula: $\text{Capital} \times (\text{tasa anual} / 365) \times \text{días de mora efectivos}$, aplicando como tasa máxima la establecida por Resolución M.E.F. N° 12/2025, a saber: (i) para contratos en guaraníes (G), la Tasa de Política Monetaria (TPM) del Banco Central del Paraguay vigente el mes anterior a la constitución de la obligación; (ii) para contratos en dólares americanos (USD), la tasa SOFR a 6 meses del mes anterior, publicada por el BCP. En ningún caso los intereses moratorios podrán capitalizarse.
- Pago conjunto: La contratante abonará el monto principal adeudado junto con los intereses moratorios devengados hasta la fecha del pago total, de forma conjunta y en un solo acto, salvo acuerdo expreso en contrario.
- Suspensión del cómputo: No se generarán intereses por mora durante el período en que la contratante, por causas debidamente fundadas y documentadas, suspenda la tramitación del pago, conforme a las causales admisibles establecidas en el contrato y en el Decreto N° 2264/2024. Cesada la causa de suspensión, el cómputo de intereses se reanudará automáticamente.
- Regularización: Efectuado el pago íntegro del capital e intereses, la obligación quedará regularizada, dejándose constancia en el expediente contractual, en el Sistema de Información de las Contrataciones Públicas (SICP) y en los registros administrativos internos, con indicación del capital, intereses liquidados, fecha de pago y documento de respaldo.

Refs.: Ley N° 7021/2022; Decreto N° 2264/2024; Resolución M.E.F. N° 12/2025; Ley N° 1535/1999; Código Civil (Ley N° 1183/1985); instrucciones DNCP.

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, guerras o revoluciones, 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 un evento extraordinario, imprevisto, inevitable, que imposibilita absolutamente el cumplimiento de la prestación y/u obligación. Cuando la previsión humana pueda anticipar el caso fortuito, el proveedor deberá acreditar haber empleado todos los recursos a su alcance para evitarlo y no se debe atribuir a la culpa o negligencia del mismo. Se debe tratar de un hecho externo al proveedor.
- 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 proveedor tendrá derecho a una prórroga razonable de los plazos de ejecución.
- La parte que invoque fuerza mayor o caso fortuito deberá enviar una notificación sobre el caso a la otra parte, inmediatamente después que el acontecimiento sucedió y dentro del plazo máximo de siete (7) días calendarios a partir del día siguiente en que haya tenido conocimiento del evento o debiera haber tenido conocimiento del evento.
- La notificación se enviará por nota o correo electrónico, estableciendo los elementos constitutivos del caso fortuito o la fuerza mayor y sus consecuencias probables para la ejecución del contrato, adjuntando toda la documentación comprobatoria. En todo caso, la parte afectada deberá tomar todas las medidas necesarias para conseguir, en el menor plazo posible, la reanudación normal de la ejecución de las obligaciones afectadas por el caso fortuito o fuerza mayor.
- Cuando la parte que invoque el caso fortuito o la fuerza mayor sea el contratista, y esta no 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 cuando el atraso de la comunicación se deba a causas no imputables al proveedor, debiendo el administrador del contrato emitir un dictamen fundado aceptando o rechazando la notificación fuera del plazo máximo establecido.
- El caso fortuito o de fuerza mayor debe ser invocada 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.

Cuando una situación de fuerza mayor o caso fortuito ha existido durante un período de más de seis (6) meses, podrá ser causal de rescisión o terminación anticipada del contrato.

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.

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.

Si no fuere posible acordar los términos del convenio modificatorio, la contratante podrá ejercer sus derechos establecidos en el artículo 65 de la Ley N° 7021 de Suministro y de Contrataciones Públicas.

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

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:

- 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
- Si el proveedor no cumple con cualquier otra obligación en virtud del contrato; o
- 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;
- Cuando las multas por atraso superen el monto de la Garantía de Cumplimiento de Contrato;
- 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;
- Si el proveedor no cumple con las obligaciones laborales, de seguridad social y/o de salud y seguridad ocupacional.
- 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

Las controversias, diferencias o reclamos que se susciten entre las partes con motivo del presente contrato, su interpretación, ejecución, cumplimiento, resolución o terminación, y que sean susceptibles de transacción, conciliación o mediación, podrán ser sometidas de manera voluntaria a un procedimiento de mediación, conforme a lo dispuesto en la Ley N° 1879/2002 "De Mediación", en la Ley N° 7021/2022 "De Suministro y Contrataciones Públicas", y a las condiciones establecidas en el presente contrato.

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 y actuará como tercero neutral e imparcial, de conformidad con la normativa aplicable.

El procedimiento de mediación se iniciará mediante solicitud de cualquiera de las partes y se sustanciará conforme al reglamento vigente de la sede seleccionada, el cual las partes declaran conocer y aceptar, incluyendo las disposiciones relativas a honorarios, gastos y costas, que se considerarán parte integrante de esta cláusula.

La mediación deberá concluir en un plazo máximo de treinta (30) días hábiles, contados a partir de la primera audiencia de mediación, plazo que podrá ser prorrogado por única vez, hasta por un período adicional de quince (15) días, únicamente mediante acuerdo expreso y escrito de las partes.

La mediación concluirá con la suscripción del acta de acuerdo, con la constancia de imposibilidad de acuerdo, o con la certificación correspondiente emitida por la sede de mediación. Vencido el plazo máximo sin haberse alcanzado un acuerdo, o concluido el procedimiento sin solución de consensuada, las partes quedarán habilitadas para recurrir a las instancias correspondientes. Para la homologación y ejecución del acta de mediación, así como para el conocimiento de las controversias no resueltas mediante este mecanismo, las partes se someten a la jurisdicción de los tribunales competentes de la ciudad de Asunción, República del Paraguay.

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.

Todas las controversias que deriven del presente contrato o que guarden relación con éste serán resueltas definitivamente por arbitraje, conforme con las disposiciones de la Ley N° 7021/22 "De Suministro y Contrataciones Públicas", de la Ley N° 7.561 "De Arbitraje" y las condiciones del Contrato. Se aplicará el reglamento respectivo y demás disposiciones que regule dicho procedimiento al momento de ser requerido, declarando las partes conocer y aceptar los vigentes, incluso en orden a su régimen de gastos y costas, considerándolos parte integrante del presente contrato. Para la ejecución del laudo arbitral, o para dirimir cuestiones que no sean arbitrables, las partes se someterán a la jurisdicción de los tribunales de la ciudad de Asunción, República del Paraguay".

MODELO DE CONTRATO

Este modelo de contrato, constituye la proforma del contrato a ser utilizada de manera obligatoria, una vez adjudicado al proveedor y en los plazos dispuestos para el efecto por la normativa vigente, teniendo en cuenta que en los procedimientos de contratación cuyo objeto sea obras, locaciones o consultorías, deberán ser instrumentados mediante contratos y necesariamente deberán contar con una orden de inicio.

Así también, cuando en el procedimiento sea de menor cuantía y se deban emitir más de una orden de ejecución, independientemente al sistema de adjudicación, se deberá formalizar a través de un contrato, salvo aquellos casos previstos en el artículo 37 Inc. e) de la Ley N° 7021/22 "De Suministro y Contrataciones Públicas"

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.

