DICTAMEN TÉCNICO EN EL CUAL SE SUSTENTAN LAS ESPECIFICACIONES TÉCNICAS REQUERIDAS EN EL PROCEDIMIENTO DE CONTRATACIÓN

En cumplimiento del artículo 12 de la Resolución DNCP N° 453/24, en virtud del cual se solicita la emisión de dictamen técnico en el cual se sustenten las especificaciones técnicas requeridas en el procedimiento de contratación, refrendado por el responsable del área requirente o del técnico que las recomendó; se emite el siguiente dictamen en los siguientes términos:

INFORMACIÓN BÁSICA DE LA CONVOCATORIA(*).

A. **DENOMINACIÓN DE LA CONVOCATORIA:** LICITACIÓN PÚBLICA NACIONAL N° 38/24 SERVICIO DE ALINEACIÓN DE CONTROLES DE CIBERSEGURIDAD A ESTÁNDARES INTERNACIONALES – ID 443965.-
B. **MONTO TOTAL DEL PAC:** Gs. 840.000.000.
C. **ÁREA TÉCNICA REQUIRENTE DEL PROCESO:** Departamento de Ciberseguridad.
D. **FUNCIONARIO/S RESPONSABLE/S DESIGNADO/S PARA LA ADMINISTRACION DEL CONTRATO, ENCARGADO/S DE LA CARGA EN EL SISTEMA DE INFORMACIÓN DE CONTRATACIONES PÚBLICAS DE LOS DOCUMENTOS CONTRACTUALES Y DE LOS INDICADORES DE CUMPLIMIENTO:**
   TITULAR:
   - Nombre y apellido: Aditardo Vazquez
   - Cédula de Identidad: 1.624.369
   - Fecha de nacimiento: 7/06/1983
   - Número telefónico de contacto: (595 21) 619 2696
   - Cargo en el área requirente: Director

   AUXILIAR:
   - Nombre y apellido: Freddy Barreto Villar
   - Cédula de Identidad: 3.812.186
   - Fecha de nacimiento: 28/04/1985
   - Número telefónico de contacto: (59521) 619 2722
   - Cargo en el área requirente: Jefe de Sección Políticas y Riesgos de Ciberseguridad
E. **MODALIDAD DE LA CONTRATACIÓN**
   …X… CONTRATO CERRADO

SECCIÓN I - DATOS DE LA CONVOCATORIA

- **Idioma de la oferta:**
  La oferta deberá ser presentada en idioma castellano o en su defecto acompañado de su traducción oficial, realizada por un traductor público matriculado en la República del Paraguay.
  …X… APLICA
  ……. NO APLICA
  …….. SÍ, la convocante aceptará la presentación de catálogos, anexos técnicos, folletos, certificaciones y otros textos complementarios en idioma inglés, los cuales no requerirán traducción fidedigna al idioma castellano. Los documentos citados presentados en otros idiomas distintos al castellano y al inglés deberán estar traducidos al castellano por un traductor público matriculado en la República del Paraguay.

- **Visita al sitio de ejecución del contrato:**
  …X… NO APLICA

- **Autorización del Fabricante:**
  Los ítems a los cuales se le requerirá Autorización del Fabricante son los indicados a continuación:
  …X… APLICA
  REQUISITO: El oferente deberá presentar fotocopia simple del documento vigente que acredite fehacientemente que el mismo es Fabricante y/o Representante Oficial y/o Distribuidor y/o Sub-Distribuidor y/o Partner Autorizado para el Paraguay de la herramienta objeto del servicio; ya sea mediante documento emitido por la firma autorizante o mediante la presentación del Formulario correspondiente incluido en la Sección Formularios debidamente suscripto por la firma autorizante.

- **Muestras:**
  …X… NO APLICA

- **Periodo de validez de la Garantía de los bienes:**
  …X… APLICA El periodo de validez de la Garantía de los bienes/servicios será el siguiente:
  El proveedor deberá emitir una Garantía de Buen Servicio y Calidad, mediante una nota en carácter de declaración jurada a nombre del Banco Central del Paraguay, en virtud de la cual garantice, por todo el plazo de prestación del servicio contratado, que correrá a su cargo, por cuenta propia y sin costo para la Convocante, las reposiciones, sustituciones, reparaciones y/o modificaciones que correspondan, cuando se observasen fallas y/o deficiencias, por causas que le fueran imputables.
  En caso de que dicha Nota de Garantía haya sido presentada por el Proveedor al momento de la presentación de su oferta, la misma será válida durante la ejecución contractual, no siendo necesaria la presentación de la misma nuevamente.

SECCIÓN II - REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN

- **Experiencia requerida**

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

a. Demostrar una antigüedad mínima de 5 (cinco) años de existencia legal (inclusive para las firmas unipersonales).
b. Demostrar experiencia en la prestación de servicios de soporte de gestión de seguridad de la información o en soluciones integrales para la gestión de riesgos, cumplimiento normativo y gobernanza de ciberseguridad, dentro del periodo comprendido entre los años 2021 a 2024, con la documentación requerida en los inc. b) y c) del siguiente apartado "Requisitos documentales para la evaluación de la experiencia".
En caso de Consorcios el Socio Líder deberá cumplir con los requisitos establecidos en los ítems a) y c), así como el 60% del requisito mínimo establecido en el ítem b). Los Socios restantes combinados deben cumplir con el 40% del requisito mínimo establecido en el ítem b).

- **Requisitos documentales para la evaluación de la experiencia**

a). Fotocopia simple de Estatuto de Constitución y/o Constancia de RUC que demuestren una antigüedad mínima de 5 (cinco) años de existencia legal (inclusive para las firmas unipersonales).
b). Fotocopia/s simple/s de contrato/s finalizado/s, y/o facturas, y/o recepciones finales de prestación de servicios de soporte de gestión de seguridad de la información o en soluciones integrales para la gestión de riesgos, cumplimiento normativo y gobernanza de ciberseguridad, a Instituciones Públicas y/o Privadas, dentro del periodo comprendido entre los años 2021 a 2024, cuyos montos sumados representen un monto igual o superior al 30% del monto total ofertado en la presente licitación. Podrán presentarse la cantidad de fotocopia/s de contrato/s finalizado/s, y/o factura/s y/o recepciones finales que fueren necesarias

para acreditar el monto solicitado, siempre y cuando dichas prestaciones hayan sido realizadas dentro del periodo mencionado.
c). Fotocopia simple de referencias satisfactorias de clientes finales, como mínimo 3 (tres), formalizadas por documentos que contengan la debida identificación y suscripción del emisor, de haber prestado servicios de soporte de gestión de seguridad de la información o en soluciones integrales para la gestión de riesgos, cumplimiento normativo y gobernanza de ciberseguridad, dentro del periodo comprendido entre los años 2021 al 2024, expedidas por Instituciones Públicas y/o Privadas con quienes mantiene y/o mantuvo relaciones comerciales.

- **Capacidad Técnica**

El oferente deberá proporcionar evidencia documentada que demuestre su cumplimiento con los siguientes requisitos de capacidad técnica relacionada con soporte de gestión de seguridad de la información o en soluciones integrales para la gestión de riesgos, cumplimiento normativo y gobernanza de ciberseguridad:

- Las especificaciones técnicas completadas y firmadas conforme al detalle y requisitos establecido en la Sección "Suministros requeridos - especificaciones técnicas" de la herramienta objeto del servicio, con las respectivas documentaciones como ser: catálogos o impresos descriptivos de la herramienta objeto del servicio con los vínculos (links/URL) oficiales del fabricante.
- Contar con un Equipo Técnico capacitado, compuesto como mínimo por 3 miembros de acuerdo con lo establecido en el apartado 4. “Capacidad del Equipo Técnico” en las especificaciones técnicas.
- Contar dentro del equipo técnico con al menos uno (1) miembro con una certificación/especialización de nivel Profesional o equivalente del fabricante de la herramienta objeto del servicio
- Garantía de Buen Servicio y Calidad por todo el plazo de la prestación.
- Garantizar la actualización y la garantía del fabricante de la herramienta objeto del servicio durante todo el plazo de vigencia del contrato.
- Garantizar el soporte y mantenimiento local (proveedor) y del fabricante durante todo el plazo de vigencia del contrato.
- Ser Fabricante y/o Representante Oficial y/o Distribuidor Oficial y/o Partner Autorizado por el mismo para el Paraguay de la herramienta objeto del servicio.

- **Requisito documental para evaluar la capacidad técnica**

a)	Nota en carácter de Declaración Jurada en la cual el Oferente manifieste que cuenta con el personal técnico capacitado de acuerdo con lo establecido en el apartado 4. “Capacidad del Equipo Técnico” en las especificaciones técnicas, a efectos de la instalación, configuración y actualización de la herramienta objeto del servicio. Se deberá detallar el nombre de los mismos y los roles asignados al servicio.
b)	Currículum Vitae actualizado de los profesionales que conforman el equipo técnico para el cumplimiento de los servicios, con los documentos acreditantes de lo exigido en el apartado 4. “Capacidad del Equipo Técnico” en las especificaciones técnicas. El BCP se reserva el derecho a verificar la información y para el efecto se deberá incluir una lista de los clientes (Empresa, contacto, teléfono, correo) en los cuales los miembros del equipo técnico han prestado sus servicios.
c)	Fotocopia simple de documento emitido por el fabricante que acredite que al menos uno (1) de los miembros del equipo técnico posee una certificación/especialización de nivel Profesional o equivalente, de la herramienta objeto del servicio.
d)	Nota en carácter de declaración jurada en la cual se detallen las especificaciones técnicas de la herramienta objeto del servicio, con la inclusión de las descripciones y demás requisitos exigidos en la sección de especificaciones Técnicas.
e)	Catálogos o impresos descriptivos de la herramienta objeto del servicio, incluyendo el modelo exacto a ser ofertado con los vínculos (links/URL) oficiales del fabricante, en los cuales se puedan corroborar las especificaciones técnicas de esta.

f)	Garantía de Buen Servicio y Calidad, mediante una nota en carácter de declaración jurada a nombre de la Convocante, en virtud de la cual el Oferente manifieste que correrán a su cargo, por cuenta propia y sin costo para el BCP, las reposiciones, sustituciones, reparaciones y/o modificaciones que correspondan, cuando se observasen fallas y/o deficiencias en el servicio, por causas que le fueran imputables, durante todo el plazo de la prestación del servicio.
g)	Nota en carácter de Declaración jurada, por la cual el Oferente manifieste que se compromete a brindar la actualización y la garantía del fabricante de la herramienta objeto del servicio durante todo el plazo de vigencia del contrato.
h)	Nota en carácter de Declaración jurada, por la cual el Oferente se compromete a asegurar el soporte y mantenimiento local (proveedor) y del fabricante durante todo el plazo de vigencia del contrato.
i)	Documento vigente que acredite fehacientemente que el Oferente es Fabricante y/o Representante Oficial y/o Distribuidor Oficial y/o Partner Autorizado por el mismo para el Paraguay de la herramienta objeto del servicio, ya sea mediante documento emitido y debidamente suscripto por la firma autorizante.

- **Otros criterios que la convocante requiera**

…X… NO APLICA

SECCIÓN III- SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS

- **Identificación de la unidad solicitante y justificaciones**

- El presente llamado para publicar ha sido solicitado por el Departamento de Ciberseguridad del Banco Central del Paraguay, de acuerdo con las necesidades de la Institución y con aprobación de la máxima autoridad. Los nombres de las personas requirentes de la contratación obran en los registros del BCP y en el Dictamen Técnico publicado en el SICP.

- **Justificar la necesidad que se pretende satisfacer mediante la contratación a ser realizada(*).:**
  Este servicio se enmarca en lo establecido en el Plan Director de Ciberseguridad aprobado por el Directorio del Banco Central del Paraguay (BCP) y que además forma parte del PEI (PE19), en la Actividad 10: "Alineación a controles de ciberseguridad".
  La alineación estratégica a estándares internacionales de ciberseguridad (ISO 27001/27002, NIST Cybersecurity Framework, CIS Controls, COBIT, entre otros) puede ayudar a establecer una base sólida para la gestión de ciberseguridad y a mejorar la eficiencia y eficacia de la ejecución del Plan Director de Ciberseguridad del BCP.

- **Justificar la planificación:**
  Con relación a la planificación, se indica que: se trata de una necesidad temporal.

- **Justificar las especificaciones técnicas establecidas(*).:**
  Las especificaciones técnicas establecidas se justifican en las necesidades actuales de la Institución, en su infraestructura. Las especificaciones técnicas están diseñadas, para cubrir necesidades relacionadas con el cumplimiento desde este departamento DCS con los estándares de ciberseguridad reconocidos internacionalmente.

- **Especificaciones técnicas**

MODALIDAD DE CONTRATACIÓN
Contrato Cerrado.

ESPECIFICACIONES TÉCNICAS

Requisito	Detalle y definiciones	Exigido	Ofrecido (Campo a ser completado por el oferente)
1 ÍTEM – SERVICIO DE ALINEACIÓN DE CONTROLES DE CIBERSEGURIDAD A ESTÁNDARES INTERNACIONALES			
1. Generalidades, descripción y alcance del servicio			
1.1	El servicio debe proporcionar una solución integral para la gestión de riesgos, cumplimiento normativo y gobernanza	SI	
1.2	El servicio debe identificar el marco normativo existente (políticas, normas, procedimientos, instructivos, estándares, etc.) y generar un análisis de brechas. En el marco de este servicio, se deben identificar los procesos de seguridad existentes (brecha entre procesos existentes y procedimientos documentados o formalizados) y realizar una identificación de controles existentes y faltantes	SI	
1.3	El servicio debe alinearse con las versiones más actualizadas de tres estándares: ISO 27000, CIS Controls y NIST, que deberá incluir: 1. Análisis de brechas: Identificar las diferencias entre las prácticas actuales y los requisitos de los estándares 2. Implementación de mejoras: Desarrollar e implementar acciones correctivas para cumplir con los estándares. 3. Pre-auditoría: Realizar pre-auditorías para asegurar que, al finalizar el servicio, los resultados sean conformes con los estándares implementados	SI	
1.4	El servicio debe proporcionar una herramienta que tenga funcionalidades que permitan a la institución identificar, evaluar, gestionar y proponer un plan de acción para mitigar riesgos, así como asegurar el cumplimiento de las normativas aplicables y mejorar la gobernanza interna	SI	
1.5	En relación con la gestión y mitigación de riesgos de ciberseguridad, el servicio debe incluir la identificación, evaluación y generación de un plan de mitigación	SI	
1.6	El servicio debe contemplar el desarrollo de políticas, normas, procedimientos, guías, directrices y recomendaciones, basadas en estándares y mejores prácticas de seguridad de la información, tales como el conjunto de normas: La familia ISO 27.000, ISO 22.300, NIST, MGCTI, entre otros.	SI	
1.7	El servicio debe contemplar la evaluación del cumplimiento del marco normativo de seguridad del BCP versus normativas locales e internacionales aplicables a la industria. Ejemplo: SOC 2, ISO 27001, NIST CSF, CIS Controls	SI	
1.8	En relación con Gobierno de ciberseguridad, el servicio debe contemplar la definición y monitoreo de cumplimiento de políticas, procedimientos y controles internos	SI	
1.9	El servicio debe conseguir la alineación de la gestión de Incidentes a los estándares actualizados: contemplando la detección, respuesta, resolución y documentación de incidentes de seguridad y cumplimiento	SI	
1.10	En relación con las auditorías y reportes, el servicio debe incluir la generación de informes y documentación para auditorías internas y externas	SI	

1.11	El servicio debe incluir la alineación de programas de formación y concienciación de ciberseguridad y cumplimiento para el personal de la institución existentes, de acuerdo con los estándares internacionales vigentes.	SI	
1.12	El servicio debe incluir la provisión de una herramienta para la gestión de riesgos, cumplimiento normativo y gobernanza de ciberseguridad, con licenciamiento y soporte del fabricante, en modalidad de suscripción en la nube por 12 meses computados a partir de la emisión de la orden de inicio emitida por el área administradora del contrato.	SI	
1.13	El servicio debe incluir la provisión de un **Equipo Técnico** dedicado, compuesto como mínimo por 3 miembros, el cual será responsable de la solución integral para la gestión de riesgos, cumplimiento normativo y gobernanza de ciberseguridad.	SI	
1.14	El servicio debe incluir la provisión de un miembro del **Equipo Técnico** dedicado, on-site (8*5), el cual será responsable de la operativa y administración de la herramienta objeto del servicio.	SI	
1.15	El servicio debe incluir la provisión de por lo menos 40 horas mensuales acumulables y bajo demanda de un especialista en la solución, para el desarrollo y optimización de todos los procesos, procedimientos e integraciones que formen parte de la herramienta objeto del servicio	SI	
2. Descripción de la herramienta			
2.1	Indicar Marca	SI	
2.2	Indicar Solución / Modelo	SI	
2.3	La herramienta debe ser capaz de evaluar de manera periódica el nivel de madurez de los procesos, procedimientos y controles implementados de manera automatizada y con mínimo input manual	SI	
2.4	La herramienta debe ser capaz de generar informes del cumplimiento o nivel de madurez, la postura de seguridad de la institución, identificado incluyendo las oportunidades de mejora o no cumplimientos identificados	SI	
3. Características técnicas de la herramienta			
3.1	El nivel de disponibilidad que el proveedor de servicios en la nube se compromete a ofrecer para sus servicios debe ser del 99,9%. - Debe cumplir con los estándares: SOC 1, SOC 2, SOC 3 e ISO 27018. - Debe cubrir los estándares ISO 27001, ISO 9001	SI	
3.2	Debe cumplir con los requerimientos de seguridad indicados en la RESOLUCIÓN N° 10, Acta N° 43 de fecha 28 de julio de 2022 - REGLAMENTO DE USO DE SERVICIOS PARA COMPUTACIÓN EN LA NUBE	SI	
3.3	Debe ser compatible y automatizar la gestión de controles y procesos de cumplimiento con normativas como: SOC 2, ISO 27001, NIST CSF, CIS Controls	SI	
3.4	Debe ser capaz de integrarse otros sistemas y herramientas existentes como: gestión de identidades y acceso, herramientas de gestión de vulnerabilidades, herramientas de desarrollo y CI/CD, herramientas SIEM, herramientas de ITSM, herramientas de gestión de proyectos,	SI	

	herramientas de backup y recuperación, herramientas de protección de endpoints, entre otros.		
3.5	Debe ser capaz de monitorizar y evaluar riesgos de manera continua mediante integraciones y flujos de trabajo automatizados	SI	
3.6	Debe ser capaz proporcionar paneles de control que puedan ser personalizados para mostrar métricas clave y el estado de cumplimiento en tiempo real	SI	
3.7	Debe ser capaz envía alertas y notificaciones automáticas sobre eventos críticos, vencimientos de auditorías, y cambios en el estado de cumplimiento	SI	
3.8	Debe ser capaz de la creación, revisión, aprobación y distribución de políticas de seguridad y cumplimiento	SI	
3.9	Debe ofrecer capacidades para generar informes de cumplimiento, auditoría, evaluación de riesgos, incidentes de seguridad, estado de políticas, y simulaciones de controles, todos personalizables según las necesidades del usuario	SI	
3.10	Debe tener la capacidad de tener el acceso basado en roles y responsabilidades, asegurando que solo el personal autorizado pueda acceder a ciertos datos y funciones	SI	
3.11	Debe tener la capacidad de proporcionar un repositorio seguro y centralizado para almacenar documentos de cumplimiento, auditoría, y políticas	SI	
3.12	Debe tener la capacidad para soportar la realización de auditorías automatizadas y la generación de informes de auditoría detallados	SI	
3.13	Debe permitir realizar simulaciones y pruebas de controles para asegurar la efectividad y preparar la organización para auditorías externas	SI	
3.14	Debe tener la capacidad del registro y seguimiento de incidentes de seguridad y cumplimiento, con flujos de trabajo para la resolución de incidentes	SI	
3.15	Debe tener la capacidad de mantener las normativas y regulaciones aplicables actualizadas, facilitando el cumplimiento continuo con múltiples estándares	SI	
3.16	Debe tener la capacidad de análisis de datos mediante herramientas nativas que permitan generar reportes detallados sobre el estado de riesgos y cumplimiento	SI	
3.17	Debe contar con cifrado de datos en tránsito y en reposo, así como otras medidas avanzadas de seguridad para proteger la información sensible	SI	
3.18	Debe permitir diseñar y gestionar flujos de trabajo personalizados para distintos procesos de cumplimiento y gestión de riesgos.	SI	
4. Capacidad del Equipo Técnico			
Preparación del Equipo Técnico:			
4.1	Se requiere un plantel técnico que esté conformado por 3 (tres) o más profesionales con grado académico universitario en las áreas de Informática, Ciberseguridad o Telecomunicaciones. El "Equipo técnico" presentado deberá estar conformado como mínimo por: ✓ 1 (un) soporte técnico dedicado on site (8*5) ✓ 1 (un) consultor senior con Certificación en ISO 27001 ("Líder técnico")	SI	

	✓ 1 (un) especialista en la solución (certificado en la herramienta objeto del servicio)		
Experiencia especifica del Líder Técnico:			
4.3	Debe contar por lo menos con 3 (tres) de las siguientes certificaciones: ✓ CCISO Certified Chief Information Security Offic. ✓ CDPSE Certified Data Privacy Solutions Engineer ✓ CISA Certified Information Systems Auditor ✓ GISP Geographic information systems (GIS) professional ✓ CSF LI Certified NIST Cybersecurity Framework Lead Implementer ✓ ISO 27001 Senior Lead Implementer ✓ ISO 27001 Senior Lead Auditor ✓ CISM - Certified Information Security Manager ✓ CISSP - Certified Information Systems Security Professional ✓ ISO 27032 - Senior Lead Cybersecurity Manager ✓ ISO 31000 - Lead Risk Manager ✓ CGEIT - Certified in Governance of Enterprise IT ✓ CRISC - Certified in Risk and Information Systems Control ✓ LCSPC - Lead Cybersecurity Professional Certificate ✓ CCSP Certified Cloud Security Professional ✓ CompTIA Cloud+ Debe contar con experiencia demostrable igual o mayor a 5 años en soporte de gestión de seguridad de la información.	SI	
Certificaciones del Equipo técnico:			
4.4	Exceptuando las certificaciones del líder técnico, los demás miembros del equipo técnico deben contar con al menos dos (2) certificaciones en marcos de trabajo de gestión y soporte de seguridad de la información, así como en soluciones integrales para la gestión de riesgos, cumplimiento normativo y gobernanza de ciberseguridad. Las certificaciones aceptadas son: ✓ ISO 27001 Lead Implementer ✓ ISO 27001 Lead Auditor ✓ CISM - Certified Information Security Manager ✓ CISSP - Certified Information Systems Security Professional ✓ ISO 27032 - Senior Lead Cybersecurity Manager ✓ ISO 31000 - Lead Risk Manager ✓ CGEIT - Certified in Governance of Enterprise IT ✓ CRISC - Certified in Risk and Information Systems Control ✓ LCSPC - Lead Cybersecurity Professional Certificate ✓ CEH / CEH Master ✓ CCSP Certified Cloud Security Professional ✓ CompTIA Cloud+	SI	
Experiencia del Equipo técnico:			
4.5	Se requiere que el “Equipo técnico” presentado (cualquiera de sus miembros o en sumatoria) cuente con una experiencia específica demostrable en soporte de gestión de seguridad de la información o en soluciones integrales para	SI	

	la gestión de riesgos, cumplimiento normativo y gobernanza de ciberseguridad igual o mayor a 10 (diez) años.		
4.6	Se requiere que la suma de experiencia comprobable de los miembros del plantel presentado sea al menos de 500 (quinientas) horas de servicio exitoso ejecutado, realizados a entidades nacionales y/o internacionales, durante el periodo comprendido en los años 2021 a 2024. Solo se podrán contabilizar servicios de soporte de gestión de seguridad de la información o soluciones integrales para la gestión de riesgos, cumplimiento normativo y gobernanza de ciberseguridad que hayan requerido como mínimo 20 horas de servicio, y para todos los casos se deberá indicar la cantidad de horas efectivamente ejecutadas por el profesional para ese proyecto en concreto. En caso de que esta información se encuentre en periodo de tiempo diferentes, tales como días, semanas o meses, se contabilizará a razón de 8 horas por día, 40 horas por semana, 120 horas por mes.	SI	
5. Garantías de seguridad			
5.1	Los centros de datos que almacenan la información personal deben de estar certificadas con SOC 2 Type II, ISO 27001.	SI	
6. Soporte			
6.1	Debe incluir el soporte técnico del tipo 8*5 tanto por parte del fabricante como por parte del Proveedor durante 12 meses.	SI	
6.2	Debe incluir soporte telefónico para casos de Emergencia	SI	
6.3	Debe cumplir con SLA de respuesta técnica: - Urgente: El soporte debe asistir al cliente en un tiempo menor a 2 horas ya sea de forma presencial o remota de acuerdo con la necesidad de la contratante. - Alta: El soporte debe asistir al cliente en un tiempo menor a 4 horas ya sea de forma presencial o remota de acuerdo a la necesidad de la contratante. La definición respecto al nivel de criticidad será determinada exclusivamente por el BCP en la solicitud de soporte. El Proveedor facilitará el nombre, número telefónico y correo electrónico del contacto para gestionar los incidentes críticos y no críticos.	SI	
6.4	En cuanto a los acuerdos de nivel de servicio (ANSs) se deberá tener una disponibilidad del servicio del 100%.	SI	
6.5	Debe garantizar el servicio en un 99.999% de disponibilidad mensual mientras dure el contrato.	SI	
6.6	Debe incluir el acceso a las documentaciones, configuración y mejores prácticas.	SI	
6.7	Debe incluir soporte por parte del fabricante en un tiempo no mayor a 120 minutos	SI	
7. Licenciamiento			
7.1	Se debe incluir las licencias y/o suscripciones necesarias para la inclusión de 3 estándares de control y para 5 usuarios de acceso, por una duración de 12 meses.	SI	
8. Implementación y capacitación			
8.1	En los procesos de implementación/mantenimiento, los miembros del plantel técnico que requieran acceso remoto, debe solicitarlo a través del correo dcs@bcp.gov.py para la	SI	

	activación de usuario y la correspondiente concesión de permisos de acceso. La solicitud debe contemplar los siguiente datos: Nombre y apellido del técnico, fecha y hora de inicio y culminación de trabajos, análisis de riesgo/impacto de la tarea a ser desempeñada.		
8.1	Se debe incluir la implementación, configuración y monitoreo del software; así como la capacitación al personal designado por el área técnica administradora del Contrato del BCP para la gestión de la herramienta.	SI	

CONDICIONES GENERALES:

SERVICIO SOLICITADO: el Proveedor deberá proponer, definir, describir y desarrollar todas las acciones y entregables necesarios relacionados a este servicio, incluyendo previsiones a futuro y acorde a los objetivos estratégicos del BCP.

A continuación, se definen las fases, los entregables, el plazo y el porcentaje de pago:

Fase nro. 1			
Ítem	**Descripción del entregable**	**Plazo de entrega**	**Porcentaje de pago**
1	Incorporación de Recursos On-site	Dentro de los 90 días posteriores a la fecha de orden de inicio de servicios	20 % del monto total contratado
Fase nro. 2			
Ítem	**Descripción del entregable**	**Plazo de entrega**	**Porcentaje de pago**
	El informe del relevamiento realizado que debe contener los siguientes ítems:	Entre los 90 y 180 días posteriores a la fecha de orden de inicio de servicios	20 % del monto total contratado
1	El análisis de brecha		
2	La medición con relación al cumplimiento basado en las mejores prácticas del sector		
3	La metodología que implementar para el desarrollo de las actividades		
4	Los requerimientos, restricciones, supuestos, riesgos y propuesta del "Equipo técnico" involucrado (plan de acción), tanto por parte del proveedor como el que éste requiera del BCP		
5	Propuesta de Estrategia de Implementación		
Fase nro. 3			
Ítem	**Descripción del entregable**	**Plazo de entrega**	**Porcentaje de pago**

1	Implementación de herramienta GRC	Entre los 181 y 270 días posteriores a la fecha de orden de inicio de servicios	30 % del monto total contratado
2	Inclusión del estándar de control de Normas ISO 27001 a la herramienta		
3	Inclusión del estándar de control de NIST Cybersecurity Framework a la herramienta		
4	Inclusión del estándar de control CIS Controls a la herramienta		
Fase nro. 4			
Ítem	**Descripción del entregable**	**Plazo de entrega**	**Porcentaje de pago**
1	Entrega de normas nuevas recomendadas y la pre-auditoría	Entre los 271 y 365 días posteriores a la fecha de orden de inicio de servicios	30 % del monto total contratado
2	Entrega de procesos mapeados a los nuevos controles		
3	Entrega de materiales de capacitación y sistemas instalados relacionados con el servicio para todo el personal afectado, consistente en materiales de difusión masiva (flyers), presentaciones en power point o similar, desarrollo de talleres y jornadas de capacitación que a criterio del DCS sean necesarios.		

Compromiso de Confidencialidad: el personal contratado interviniente del proveedor deberá firmar un Compromiso de Confidencialidad de la Información, dado que podría acceder a información confidencial de la Contratante en los términos del Formulario de la Sección Formularios Adicionales. La firma del Compromiso de Confidencialidad se realizará al momento de la suscripción del Contrato. El Departamento de Ciberseguridad será el responsable de gestionar la firma de dicha documentación. En caso de que se incorpore nuevo personal del Proveedor se deberá gestionar la firma del Compromiso de Confidencialidad por parte de los mismos.

Soporte Técnico: El Proveedor deberá disponer de los canales de solicitud habilitados para el soporte, consistentes en dos números de contacto y cuentas de correo electrónico para la gestión de los reclamos o cambios requeridos. En ese sentido, el Proveedor una vez adjudicado, deberá detallar los siguientes datos: Nombres y apellidos, cargos, correos corporativos y números de teléfono de línea fija y móvil de los responsables del servicio de soporte técnico incluyendo una matriz de escalamiento. El BCP designará el equipo de trabajo que acompañará la implementación y/o soporte de la herramienta.

Ante cada notificación por parte de la contratante, el Proveedor deberá realizar y presentar al BCP un informe que contendrá como mínimo la siguiente información: descripción detallada del problema, su causa y solución propuesta,

personal que se asignó a la resolución de éste, problemas que se presentaron durante la resolución, documentación de los cambios realizados, recomendaciones, fecha y hora de resolución. El proveedor deberá garantizar durante la vigencia del contrato, que la herramienta se encuentre actualizada en su última versión estable y con los últimos parches de seguridad aplicados correctamente.

Planificación y documentación del servicio: el Proveedor deberá presentar una documentación con diagramas, configuraciones necesarias y otros detalles relevantes, además de un cronograma de trabajo para su implementación de acuerdo con los plazos definidos en el apartado CONDICIONES GENERALES, del "SERVICIO SOLICITADO". Una vez finalizada la implementación, el proveedor deberá presentar un documento en el cual se detalle todos los datos necesarios como diagrama de implementación, URLs, direcciones IP, credenciales de usuario y de sistema, configuraciones y otros.

Informes: El Proveedor deberá elaborar de manera trimestral un informe técnico de cumplimiento que contemple las actividades desarrolladas respecto al servicio que fuera adjudicado (deberá contener como mínimo fecha de la actividad, tareas realizadas, participantes, entre otros datos relacionados).

Área Técnica Administradora del Contrato: la administración del contrato estará a cargo del Departamento de Ciberseguridad.

Lugar y horario de la prestación de los servicios y/o soportes: se podrá realizar de forma remota, a través de herramientas tecnológicas tales como Microsoft Teams, o similares; o de forma presencial en el Edificio BCP, sito en la Av. Federación Rusa y Av. Augusto Roa Bastos, cuando el área administradora del contrato (Departamento de Ciberseguridad del BCP) lo requiera; preferentemente en el horario de lunes a viernes de 08:00 a 16:00 horas. En caso de necesidad la convocante podrá solicitar asistencia fuera del horario ordinario de trabajo o en días no laborables.

- **Plan de entrega de los bienes: NO APLICA**

- **Plan de entrega de los servicios:**

Ítems	Descripción del servicio	Cantidad	Unidad de medida	Lugar y horario de prestación de los servicios	Plazo de prestación/ejecución de los servicios	Plazo de vigencia del Contrato
De acuerdo a la Lista de Precios publicada en el SICP	De acuerdo a la Lista de Precios publicada en el SICP	De acuerdo a la Lista de Precios publicada en el SICP	De acuerdo a la Lista de Precios publicada en el SICP	La prestación de los servicios y/o soportes se podrá realizar de forma remota, a través de herramientas tecnológicas tales como Microsoft Teams, o similares; o de forma presencial en el Edificio BCP, sito en la Av. Federación Rusa y Av. Augusto Roa Bastos, cuando el área administradora del contrato (Departamento de Ciberseguridad del BCP) lo requiera; preferentemente en el horario de lunes a viernes de 08:00 a 16:00 horas. En caso de necesidad la convocante podrá solicitar asistencia fuera del horario ordinario de trabajo o en días no laborables.	El plazo total de prestación del servicio será de 12 meses, contados a partir de la fecha a ser consignada al efecto en la Orden de Inicio de Servicio, que será emitida por el área administradora dentro de los 10 (diez) días hábiles siguientes a la suscripción del Contrato.	El plazo de vigencia del Contrato será a partir de la fecha a ser consignada en la Orden de Inicio de Servicio que será emitida por el área administradora dentro de los 10 (diez) días hábiles siguientes a la suscripción del Contrato hasta el cumplimiento total de las obligaciones contractuales.

- **Otras aclaraciones:**

a) FORMA DE PAGO ESPECÍFICA.

…X… APLICA. **Detallar:** de acuerdo a lo establecido en el apartado **CONDICIONES GENERALES**, del "**SERVICIO SOLICITADO**".

Los pagos se realizarán de la siguiente forma:

20 % del monto total contratado luego de la entrega total de la Fase N° 1.

20% del monto total contratado luego de la entrega total de la Fase N° 2.

30% del monto total contratado luego de la entrega total de la Fase N° 3.

30% del monto total contratado luego de la entrega total de la Fase N° 4.

b) ANTICIPO.

…… APLICA.

…X….NO APLICA.

c) COMPROMISO DE CONFIDENCIALIDAD:

…X… APLICA.

…….NO APLICA.

- **Identificar y justificar de forma expresa si algún requerimiento podría limitar la participación de potenciales oferentes(*).**

  …… APLICA.

  …X….NO APLICA.

- **Si en las bases licitatorias se indica una marca específica u otro derecho intelectual exclusivo, mencionar la justificación que respalda lo solicitado o que no existe otro modo de identificarlo. Se aclara que, en caso de incluirlos, los mismos tendrán carácter referencial(*).**

  …… APLICA.

  …X….NO APLICA.

FIRMA DEL RESPONSABLE DEL ÁREA REQUIRENTE (*):

ADITARDO VAZQUEZ ROJAS

Firmado digitalmente por ADITARDO VAZQUEZ ROJAS
Fecha: 2024.07.25 15:55:15 -04'00'

FIRMA DEL RESPONSABLE DE LA UOC (*):

MARIA LORENA MEZA ARIAS

Firmado digitalmente por MARIA LORENA MEZA ARIAS
Fecha: 2024.07.26 09:52:57 -04'00'

(*) Datos obligatorios solicitados en Circular DNCP N° 27/24.