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 DE MENOR CUANTÍA NACIONAL (MCN) N° 51/2024 – SERVICIO DE MEJORA EN LA GESTIÓN DE CRISIS ANTE CIBERATAQUES – ID N° 444066.

B. MONTO TOTAL DEL PAC: G. 350.000.000.-

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: 07/06/1983
- Número telefónico de contacto: (595 21) 619 2696
- Cargo en el área requirente: Director del Departamento de Ciberseguridad

AUXILIAR:

- Nombre y apellido: Miguel Toffoletti
- Cédula de Identidad: 4.293.038.
- Fecha de nacimiento: 16/07/1987
- Número telefónico de contacto: (595 21) 619 2294.
- Cargo en el área requirente: Jefe de la División Operaciones de Ciberseguridad

E. MODALIDAD DE LA CONTRATACIÓN

...X... CONTRATO CERRADO
..... CONTRATO ABIERTO

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.
..... APLICA
...X... NO APLICA

La convocante permitirá con la oferta, la presentación de catálogos, anexos técnicos o folletos en idioma distinto al castellano y sin traducción:
..... SI
...X.... NO

- **Visita al sitio de ejecución del contrato:**

..... APLICA
...X... NO APLICA

- **Autorización del Fabricante:**

Los ítems a los cuales se le requerirá Autorización del Fabricante son los indicados a continuación:
..... APLICA
...X... NO APLICA

- **Muestras:**

..... APLICA
...X... NO APLICA

- **Periodo de validez de la Garantía de los bienes/servicios:**

...X... APLICA

El periodo de validez de la Garantía de los bienes/servicios será el siguiente:

El Proveedor deberá presentar una Nota de Compromiso de Buen Servicio y Calidad, 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 en el servicio prestado, por causas que le fueran imputables.

En caso de que dicha Nota de Compromiso 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 a la gestión de crisis ante ciberataques, en instituciones públicas y/o privadas dentro del periodo comprendido entre los años 2021 al 2024.

En caso de Consorcios el Socio Líder deberá cumplir con el requisito establecido en los inc. a) y c), así como el 60% del requisito mínimo establecido en el inc. b). Los Socios restantes combinados deben cumplir con el 40% del requisito mínimo establecido en el inc. 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 factura/s, y/o recepción/es final/es, y/o conformidad/es de haber prestado servicios de soporte a la gestión de crisis ante ciberataques a Instituciones Públicas y/o Privadas, dentro del periodo comprendido entre los años 2021 al 2024, cuyos montos sumados representen un monto igual o superior al 25% del monto total ofertado en la presente licitación. Podrán presentarse la cantidad de documentaciones indicadas 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 a la gestión de crisis ante ciberataques, 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:

Los requisitos de capacidad técnica a ser evaluados se detallan en el siguiente punto "Requisitos documentales para evaluar el criterio de capacidad técnica".

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

a)	Nota de Compromiso de Buen Servicio y Calidad, a nombre del Banco Central del Paraguay, en virtud de la cual el Oferente 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 en el servicio prestado, por causas que le fueran imputables.
b)	Nota en la cual se detallen las especificaciones técnicas del soporte ofrecido, con la inclusión de las descripciones y demás requisitos exigidos en la Sección "Suministros Requeridos – Especificaciones Técnicas".
c)	Nota en la cual el Oferente manifieste que cuenta con el personal técnico capacitado de acuerdo a lo exigido en la Sección "Suministros Requeridos – Especificaciones Técnicas".
d)	Fotocopia simple del título o certificado de estudios con grado académico universitario en las áreas de Informática, Ciberseguridad o Telecomunicaciones del equipo de trabajo propuesto, a fin de verificar lo requerido en el numeral 2.1 incluido en el apartado 2. "Capacidad Técnica" de las Especificaciones técnicas.
e)	Fotocopia simple de las certificaciones del personal solicitado, a fin de verificar lo requerido en los numerales 2.2 y 2.3 incluidos en el apartado 2. "Capacidad Técnica" de las Especificaciones técnicas.
f)	Currículum de la empresa donde se debe plasmar en el organigrama organizacional la presencia de la división responsable de los servicios de gestión de crisis ante ciberataques.

- **Otros criterios que la convocante requiera**

...X... APLICA

1. La convocante se reserva el derecho a requerir la información y/o documentación adicional que estime pertinente a fin de acreditar la veracidad de la información contenida en la documentación presentada por el oferente.

SECCIÓN III - SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS

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

- Identificar el nombre, cargo y la dependencia de la Institución de quien solicita el llamado a ser publicado:

El presente llamado a ser publicado ha sido solicitado por: el Departamento de Ciberseguridad del Banco Central del Paraguay, de acuerdo con las necesidades de la Institución y con la aprobación correspondiente.

El funcionario responsable del área requirente según Dictamen Técnico: Aditardo Vazquez (en carácter de Director del Departamento de Ciberseguridad).

- Justificar la necesidad que se pretende satisfacer mediante la contratación a ser realizada:

La necesidad que se pretende satisfacer mediante la contratación realizada radica en: Este servicio se enmarca en lo establecido en el Plan Director de Ciberseguridad aprobado por el Directorio del BCP y que además forma parte del PEI (PE19), en la Actividad 16: "Mejora en la Gestión de Crisis ante Ciberataques al Sistema Financiero".

La gestión de incidentes de ciberseguridad es esencial para proteger los datos de una organización contra las amenazas cibernéticas. Una parte muy importante de la gestión de incidentes de ciberseguridad es testear que los procesos y procedimientos documentados sean completos y útiles en casos de incidentes reales que puedan afectar a la institución.

Para llevar a cabo pruebas de seguridad exhaustivas, se requiere contratar un servicio especializado que cuente con un equipo de expertos en ciberseguridad capaces de simular uno o varios ataques cibernéticos realistas contra la organización de manera segura y controlada, evitando cualquier impacto negativo no deseado. Estas pruebas, conocidas como "Table Top", permiten identificar debilidades en los sistemas y procesos de la institución y ajustar los procesos de gestión de incidentes para responder de forma efectiva ante situaciones de crisis reales. Los ejercicios de crisis de ciberseguridad son cruciales para que la institución pueda mejorar su infraestructura y procesos de seguridad y estar preparada para enfrentar posibles amenazas.

Además, estos servicios pueden ayudar a identificar áreas en las que el personal requiere capacitación adicional en temas de ciberseguridad. Por ejemplo, si los empleados caen fácilmente en trampas de phishing, el equipo de expertos en ciberseguridad puede identificar la necesidad de mayor capacitación en ciberseguridad para el personal, incluyendo a aquellos que forman parte del equipo de respuesta ante incidentes.

- Justificar la planificación:

Con relación a la planificación, se indica que: se trata de un llamado eventual (nuevo), ya que se realiza de acuerdo a la necesidad.

- Justificar las especificaciones técnicas establecidas:

Las especificaciones técnicas establecidas se justifican en: las especificaciones técnicas establecidas se justifican en las necesidades actuales de la Institución, en su infraestructura y en el conocimiento del área técnica.

- **Especificaciones técnicas**

ESPECIFICACIONES TECNICAS

Requisito	Detalle y definiciones	Exigido	Ofrecido (Campo a ser completado por el oferente)
SERVICIO DE MEJORA EN LA GESTIÓN DE CRISIS ANTE CIBERATAQUES			
1. GENERALIDADES			
1.1	Debe proponer, definir, describir y desarrollar todas las documentaciones necesarias relacionadas a la gestión de crisis ante ciberataques, incluyendo previsiones a futuro y acorde a los objetivos estratégicos del BCP.	SI	
1.2	Debe redactar en forma detallada todo tipo de documentaciones asociadas al proceso de gestión de crisis ante ciberataques, ya sean políticas, normas, procedimientos, guías, entre otros.	SI	
1.3	Debe desarrollar las políticas, normas, procedimientos, guías, directrices y recomendaciones, basadas en los estándares y mejores prácticas de seguridad de la información, tales como el conjunto de normas ISO 27.000, ISO 22.300, NIST, MGCTI entre otros.	SI	
1.4	Debe definir y realizar planes de capacitación sobre el marco normativo y los procesos de gestión de crisis ante ciberataques en base a las necesidades, y llevarlas a cabo dentro del BCP o la ubicación que la contratante lo designe. Esta capacitación podrá ser implementada a través de talleres, charlas, documentos para distribución masiva a través de medios electrónicos, o cualquier otro mecanismo que a criterio del DCS sea necesario.	SI	
1.5	Debe ejecutar, en conjunto con el DCS, otras áreas que formen parte del proceso y actores del sistema financiero, ejercicios de simulaciones y pruebas de los procedimientos de gestión de crisis ante ciberataques, con el fin de identificar oportunidades de mejora en los planes desarrollados e implementar dichas mejoras como parte del servicio.	SI	

2. CAPACIDAD TÉCNICA			
2.1	**Cantidad de personal presentado en el equipo de trabajo propuesto:** Se requiere un plantel técnico que como mínimo esté conformado por 3 (tres) o más profesionales con grado académico universitario en las áreas de Informática, Ciberseguridad o Telecomunicaciones. El plantel técnico presentado deberá estar conformado por un "Líder técnico" y un "Equipo del Proyecto".	SI	
2.2	**Certificaciones del personal solicitado: Líder técnico:** Se requiere 1 (un) Líder del Proyecto que cuente con la certificación PMP - Project Management Professional y adicionalmente, al menos 2 (dos) de las certificaciones listadas a continuación: 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	SI	
2.3	**Certificaciones del personal solicitado: Equipo del Proyecto:** Se requiere de un equipo de trabajo compuesto por al menos 2 (dos) personas, cada una con al menos 3 (tres) de las certificaciones listadas a continuación: 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 CEH / CEH Master	SI	

CONDICIONES GENERALES:

SERVICIO SOLICITADO:

Mejora en la Gestión de Crisis ante Ciberataques: El Proveedor deberá proponer, definir, describir y desarrollar todas las documentaciones necesarias relacionadas a la gestión de crisis ante ciberataques, incluyendo previsiones a futuro y acorde a los objetivos estratégicos del BCP.

A continuación, se definen los documentos a ser entregados por el proveedor, así como el plazo para la entrega de estos:

1. Dentro de los 15 días calendario desde la fecha establecida en la Orden de Inicio del Servicio:
   - **Plan del proyecto:** que incluya un cronograma de trabajo, metodología a implementar para el desarrollo de las actividades, requerimientos, restricciones, supuestos, riesgos y propuesta de equipo de trabajo involucrado, tanto por parte del proveedor como el que éste requiera del BCP.
2. Dentro de los 60 días calendario desde la fecha establecida en la Orden de Inicio del Servicio:
   - **Informe del Diagnóstico realizado (Análisis de Brecha)**: que describa el análisis realizado sobre el marco normativo de los procesos de gestión de crisis ante ciberataques incluyendo un plan de acción para la implementación de las adecuaciones/mejoras sobre los procesos de gestión de crisis ante ciberataques, acorde con buenas prácticas definidas.
   - **Plan de Acción:** el plan deberá incluir el listado de documentos que forman parte del marco normativo y que requieren actualización o el listado de documentos que deben ser desarrollados.
3. Dentro de los 300 días calendario desde la fecha establecida en la Orden de Inicio del Servicio:
   - **Documentos actualizados y/o desarrollados por el proveedor:** Entrega de políticas, normas, procedimientos, estándares, guías, playbooks o cualquier otro tipo de documento que, como parte del análisis de brecha realizado, haya sido identificado, incluido en el plan de acción y desarrollado por el proveedor.
   - **Materiales de capacitación y ejercicios de simulación:** materiales de capacitación y ejercicios de simulación sobre el proceso de gestión de crisis para todo el personal afectado por dicho proceso, tanto dentro del BCP como aquellos que se realicen en conjunto con otros actores del sistema financiero, 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 del PBC. La firma del Compromiso de Confidencialidad se realizará posterior a

la suscripción de la Orden de Compra. El Departamento de Ciberseguridad será el responsable de gestionar la firma de dicha documentación. En caso de que se incorpore nuevo personal del Oferente se deberá gestionar la firma del Compromiso de Confidencialidad por parte de estos.

Informes: El Proveedor deberá presentar de manera periódica, según lo defina el área técnica administradora del contrato, un informe de cumplimiento del proyecto indicando las actividades realizadas y su grado de avance en relación con el plan de trabajo definido.

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:** APLICA

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 (doce) 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 del contrato dentro de los 10 (diez) días hábiles siguientes a la suscripción de la Orden de Compra.	El plazo de vigencia será a partir de la fecha a ser consignada al efecto en la Orden de Inicio de Servicio, que será emitida por el área administradora del contrato dentro de los 10 (diez) días hábiles siguientes a la suscripción de la Orden de Compra, hasta el cumplimiento total de las obligaciones contractuales.

- **Otras aclaraciones:**

a) FORMA DE PAGO ESPECÍFICA.
Los pagos se realizarán de la siguiente forma:
...X... APLICA. Detallar.

Los pagos se realizarán de la siguiente forma:

- 10% del monto total contratado luego de la entrega del Plan del Proyecto.
- 15% del monto total contratado luego de la entrega del Informe del Diagnóstico realizado (Análisis de Brecha).
- 15% del monto total contratado luego de la entrega del Plan de Acción.

- 30% del monto total contratado luego de la entrega de los Documentos actualizados y/o desarrollados por el proveedor.
- 30% del monto total contratado luego de la entrega de los Materiales de Capacitación y Ejercicios de simulación.

.....NO APLICA.

b) ANTICIPO:
..... APLICA. Detallar porcentaje y justificación: .....
...X....NO APLICA.

c) COMPROMISO DE CONFIDENCIALIDAD:
...X... APLICA.
.....NO APLICA.

FIRMA DEL RESPONSABLE DEL ÁREA REQUIRENTE (*):	ADITARDO VAZQUEZ ROJAS Firmado digitalmente por ADITARDO VAZQUEZ ROJAS Fecha: 2024.07.24 13:35:57 -04'00'
FIRMA DEL RESPONSABLE DE LA UOC (*):	MARIA LORENA MEZA ARIAS Firmado digitalmente por MARIA LORENA MEZA ARIAS Fecha: 2024.07.24 14:18:11 -04'00'

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