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° 33/24 SERVICIO PARA LA TRANSFORMACIÓN DE LA ESTRATEGIA DE CIBERSEGURIDAD ALINEADAS AL NEGOCIO – ID 443931.-
B. **MONTO TOTAL DEL PAC:** Gs. 1.000.000.000.
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
  La convocante permitirá con la oferta, la presentación de catálogos, anexos técnicos o folletos en idioma distinto al castellano y sin traducción:
  …X… SI
  ……. NO
  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:
  …… APLICA
  …X… NO APLICA

- **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:

- Demostrar una antigüedad mínima de 5 (cinco) años de existencia legal (inclusive para las firmas unipersonales).
- Demostrar experiencia en la prestación y/o provisión servicios 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 y/o provisión de servicios 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 50% 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 provisiones / 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 brindado la prestación y/o provisión de servicios 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:

- Contar con un Equipo de Trabajo, compuesto como mínimo por 4 miembros de acuerdo con lo establecido en el apartado 3. "Equipo de Trabajo" de las especificaciones técnicas.
- Garantía de Buen Servicio y Calidad por todo el plazo de la prestación del servicio.
- Las especificaciones técnicas completadas y firmadas con la inclusión de las descripciones y demás requisitos exigidos en la SECCIÓN III- SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS.
- Garantizar que el servicio suministrado se alinea con las mejores prácticas y/o estándares en materia de estrategia de ciberseguridad que sean aplicables en el Banco Central del Paraguay como la ISO, NIST, entre otros.

- **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 3. "Equipo de Trabajo" de las especificaciones técnicas, a efectos de la realización del servicio. Se deberá detallar el nombre de estos 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 conforme a lo exigido para cada perfil en el apartado 3. "Equipo de Trabajo" de 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 de trabajo han prestado sus servicios.
c) 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 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 contratado, por causas que le fueran imputables, durante el plazo de prestación del servicio contratado.
d) Nota en carácter de declaración jurada en la cual se detallen las especificaciones técnicas del servicio, con la inclusión de las descripciones y demás requisitos exigidos en la SECCIÓN III- SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS
e) Nota en carácter de declaración jurada en la cual se garantice que el servicio suministrado se alinea con las mejores prácticas y/o estándares en materia de estrategia de ciberseguridad que sean aplicables en el Banco Central del Paraguay como la ISO, NIST, entre otros.

- **Otros criterios que la convocante requiera**

… … APLICA
…X… NO APLICA

SECCIÓN III- SUMINISTROS REQUERIDOS – ESPECIFICACIONES TÉCNICAS

- **Identificación de la unidad solicitante y justificaciones:** 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 aprobación de la máxima autoridad. Los nombres de las personas requirentes: Aditardo Vazquez – Director, Freddy Barreto Villar - Jefe de Sección Políticas y Riesgos de Ciberseguridad.
- **Justificar la necesidad que se pretende satisfacer mediante la contratación a ser realizada(*)**:
  Como parte del Plan Director de Ciberseguridad aprobado por el Directorio del BCP y que además forma parte del PEI aprobado, en su PE19, se ha establecido la actividad Nº 4 "Transformaciones de las Operaciones de Ciberseguridad orientadas al Negocio".
  El servicio denominado "Transformación de la estrategia de ciberseguridad alineadas al negocio" consiste en un conjunto de servicios profesionales que tienen como objetivo mejorar la estrategia de ciberseguridad de una organización, asegurando que esté alineada con los objetivos del negocio. Este servicio es de suma importancia para el Banco Central, ya que la ciberseguridad hoy en día es considerada como parte de la estrategia general del Banco, para el logro de sus objetivos estratégicos y la protección de la información.
  La alineación de una estrategia de ciberseguridad con los objetivos del negocio se considera una buena práctica internacional, ya que ayuda a una organización a priorizar sus esfuerzos y recursos en las áreas más críticas y alineadas con los objetivos del negocio. El principal objetivo de este servicio es lograr mapear la seguridad de la información y la protección de los activos de información con los objetivos estratégicos institucionales. La importancia de que la ciberseguridad esté alineada a los objetivos radica en el aseguramiento de los procesos para el logro de resultados, minimizando la probabilidad de materialización de riesgos o disrupciones, lo que a su vez garantiza la confidencialidad, integridad y disponibilidad de los activos de información del banco.
  A su vez, este servicio permitirá identificar de manera más precisa el retorno de la inversión en ciberseguridad, ya que se identifican y priorizan los procesos que requieren del acompañamiento de iniciativas o proyectos de ciberseguridad, con el fin de implementar soluciones efectivas para proteger la información de estos.
  Además, en general, pretende mejorar los procesos de gestión de incidentes, gestión de usuarios, gestión de riesgos de ciberseguridad, gestión de indicadores y métricas de ciberseguridad.
  Este servicio se ejecutará a lo largo de 12 (doce) meses y los entregables se constituirán en una serie de informes y documentos normativos que deben ser entregados a lo largo de la prestación del servicio. Los resultados finales serán plasmados en un informe final, detallando las mejoras realizadas y recomendaciones para continuar mejorando la estrategia de ciberseguridad del banco.
  Este servicio será brindado por un grupo de profesionales con certificación internacional y con una alta experiencia en materia de ciberseguridad / seguridad de la información.
- **Justificar la planificación:** Con relación a la planificación: 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 el conocimiento del área técnica.

- **Especificaciones técnicas**

GENERALIDADES:
MODALIDAD DE CONTRATACIÓN
Contrato Cerrado.

ESPECIFICACIONES TÉCNICAS			
Requisito	**Detalle y definiciones**	**Exigido**	**Ofrecido (Campo a ser completado por el oferente)**
ÍTEM N° 1 – SERVICIO DE TRANSFORMACIÓN DE LA ESTRATEGIA DE CIBERSEGURIDAD ALINEADAS AL NEGOCIO			
1. Generalidades			
1.1	Se solicita la provisión de un servicio profesional de 12 (doce) meses para la transformación de las estrategias de ciberseguridad alineándolas con los objetivos institucionales. Este servicio debe permitir establecer las actividades a desarrollar en los próximos años, basándose en estándares, buenas prácticas o frameworks reconocidos internacionalmente, y contando con el aporte de profesionales certificados, altamente capacitados y con vasta experiencia en ciberseguridad.	SI	
1.2	**Diagnóstico y Evaluación.** El servicio debe realizar un análisis del panorama de ciberseguridad actual del BCP, identificando las amenazas, vulnerabilidades y riesgos, así como la madurez actual de las estrategias de ciberseguridad existentes.	SI	
1.3	**Desarrollo de una Estrategia.** El servicio debe diseñar una estrategia de ciberseguridad personalizada y alineada con los objetivos estratégicos institucionales, incorporando las mejores prácticas de la industria y elementos que aprovechen las tecnologías más recientes en ciberseguridad.	SI	
1.4	**Metodología para la aplicación de la transformación.** El servicio debe desarrollar guías y prácticas basadas en metodologías ágiles cuando sean aplicables a fin de adoptar las estrategias identificadas.	SI	
1.5	**Guía para adopción de la nueva estrategia.** El servicio elaborará guías tendientes a la adopción de la nueva estrategia de ciberseguridad enfocadas a todos los niveles de la institución, que tendrán como objetivos evitar las posibles resistencias al cambio y el fomento de cultura de ciberseguridad sólida.	SI	
1.6	**Capacitación.** El servicio debe desarrollar y ejecutar programas de capacitación estratégicos para el personal del departamento de Ciberseguridad y a otras áreas previamente identificadas con el objetivo de fortalecer las capacidades necesarias para la adopción efectiva de la nueva estrategia de ciberseguridad orientada al negocio.	SI	
1.7	**Monitoreo y Evaluación Continua.** El servicio debe entregar métricas y KPIs (Tableros) para medir el éxito de la implementación de la estrategia.	SI	
2. Alcance del Servicio			

2.1	El servicio debe realizar un análisis exhaustivo del estado actual de la ciberseguridad del BCP, incluyendo la evaluación de la infraestructura tecnológica, los procesos, las políticas y procedimientos de ciberseguridad, el alcance, efectividad y eficiencia de los controles de ciberseguridad implementados y en progreso, y el nivel de cumplimiento de las normativas y estándares relevantes, con el objetivo de determinar oportunidades de mejora, de conformidad a los objetivos estratégicos institucionales.	SI	
2.2	El servicio debe proponer y desarrollar el plan de acción detallado para alinear la estrategia de ciberseguridad con los objetivos estratégicos institucionales, incluyendo recomendaciones específicas para la implementación de controles de ciberseguridad.	SI	
2.3	El servicio debe desarrollar y/o actualizar las guías, marcos y procedimientos para la adecuada implementación de un gobierno de ciberseguridad alineado a los estándares y políticas de ciberseguridad del BCP y las buenas prácticas internacionales, definiendo aspectos claves como: mecanismos de control, cumplimiento y monitoreo. Definición de roles y responsabilidades, de procesos de aprobación y supervisión, entre otros.	SI	
2.4	El servicio debe realizar la evaluación de madurez de la estrategia de ciberseguridad actual del BCP utilizando marcos de referencia reconocidos internacionalmente, como el NIST Cybersecurity Framework y/o el COBIT, entre otros, asegurando la alineación de la estrategia de ciberseguridad a la necesidad del negocio. El ejercicio de evaluación debe ofrecer un tablero interactivo compatible con herramientas del paquete MS Office (Excel, Power BI), que muestre el progreso y avance conforme se van implementando las medidas de ciberseguridad en base a la estrategia definida.	SI	
2.5	El servicio debe evaluar la ejecución del plan estratégico de ciberseguridad 2020 - 2024 aprobado, identificando los factores de éxito y/o las barreras que impidieron su completa implementación y entregar un análisis de la ejecución y recomendaciones para superar las barreras identificadas.	SI	
2.6	El servicio debe realizar un ejercicio de evaluación del impacto potencial de los riesgos cibernéticos, cuantificando el posible daño financiero, operativo, reputacional u otros.	SI	
2.7	El servicio debe proponer los procesos de intercambio de información sobre ciberseguridad entre el BCP y otros actores relevantes, mediante el desarrollo de guías técnicas, evaluación de documentos técnicos de integración, propuesta y definición de iniciativas y protocolos de colaboración, entre otros.	SI	

2.8	El servicio debe establecer un programa de monitoreo de la ciberseguridad del BCP, que permita detectar y responder a amenazas de manera efectiva y eficiente, utilizando herramientas de análisis de seguridad e inteligencia de amenazas, de manera a identificar oportunidades de mejora en los procesos operativos del SOC del BCP.	SI	
2.9	El servicio debe informar sobre el estado de la ciberseguridad del BCP, incluyendo el análisis de incidentes, el seguimiento de riesgos y el cumplimiento de normativas, con recomendaciones para la mejora continua.	SI	
2.10	El servicio debe entregar un informe final que documente todo el proceso de transformación de la estrategia de ciberseguridad del BCP, incluyendo los resultados obtenidos, las lecciones aprendidas y las recomendaciones para el futuro.	SI	
3. Equipo de trabajo			
3.1	Se requiere un Equipo de trabajo que esté conformado por 4 (cuatro) o más profesionales. El "Equipo de trabajo" presentado deberá estar conformado como mínimo por: - **1 (un) Máster en Ciberseguridad:** Liderará el diseño y el desarrollo de la estrategia de ciberseguridad, asegurando su alineación con los objetivos de negocio y las mejores prácticas. - **1 (un) Experto en Riesgo:** Realizará análisis continuos de riesgos para identificar y evaluar las amenazas emergentes, proporcionando información clave para la toma de decisiones. - **1 (un) Especialista en Ciberseguridad:** Encargado de investigar, identificar e implementar soluciones y tecnologías de ciberseguridad emergentes y disruptivas, con el objetivo de mejorar la postura de seguridad del BCP y anticiparse a las amenazas futuras. - **1 (un) Gerente de Servicio con Experiencia en Transformación y Gestión del Cambio Organizacional:** Desarrollará la guía de adopción de la estrategia, asegurando que se cumplan los plazos y el presupuesto, y que la transformación sea adoptada de manera sostenible. Su enfoque en la gestión del cambio garantizará que la organización esté preparada para aprovechar las nuevas tecnologías y procesos.	SI	
Formación y Experiencia del Equipo			
3.2	**Máster en Ciberseguridad:** El profesional propuesto debe contar con: -Título de grado (Ingeniero o Analista en Sistemas) -Título de Máster en Ciberseguridad -Al menos 2 (dos) de las siguientes certificaciones: - CISSP - ISO 27001 Senior Lead Implementer	SI	

	- ISO 27032 Lead Cybersecurity Manager -Una certificación CISM, que demuestre su conocimiento y experiencia en la supervisión de programas de ciberseguridad en las empresas. -Con al menos 10 años de experiencia en roles de ciberseguridad estratégica. -Experiencia previa en instituciones financieras.		
3.3	**Experto en Riesgo:** El profesional propuesto debe contar con: -Título de grado (Ingeniero o Analista en Sistemas). -Al menos 3 de las siguientes certificaciones: - ISO 22301 Lead Implementer - ISO 22301 Lead Auditor - ISO 27031 Lead Implementer - ISO 27032 Cybersecurity Manager - Certified ISO 27001 Lead Implementer - Certified ISO 27002 Lead Implementer - Certified ISO 27035 Lead Incident Manager - Certified ISO 20000 Lead Auditor - Certified Business Continuity Maturity Model (BCMM) Professional	SI	
3.4	**Especialista en Innovación en Ciberseguridad:** El profesional propuesto debe contar con: -Título de grado (Ingeniero o Analista en Sistemas). -Las siguientes certificaciones: -CISSP (Certified Information Systems Security Professional). -CISM (Certified Information Security Manager).	SI	
3.5	**Gerente de Servicio con Experiencia en Transformación y Gestión del Cambio Organizacional** El profesional propuesto debe contar con: -Título de grado (Ingeniero o Analista en Sistemas). -Con una certificación en metodología de gestión de proyecto. -Con experiencia comprobada en participación de proyectos, en la prestación de servicios de mejora continua relacionadas con Ciberseguridad. -Al menos una de las siguientes certificaciones: - PMP (Project Management Professional) - PRINCE2 Foundation - PRINCE2 Practitioner - PRINCE2 Agile - AgilePM Practitioner - Certified ScrumMaster	SI	
4. Capacitación			
4.1	Se debe incluir capacitación a todo el personal del área administradora del contrato y a otras áreas previamente identificadas, 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.	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	Diagnóstico y Planificación de la ejecución del servicio.	Dentro de los 90 días posteriores a la fecha de orden de inicio de servicios.	20 % del monto total de la contratación.
Fase nro. 2			
Ítem	**Descripción del entregable**	**Plazo de entrega**	**Porcentaje de pago**
1	Estrategia de ciberseguridad personalizada alineada a la estrategia institucional.	Entre los 91 y 180 días posteriores a la fecha de orden de inicio de servicios.	30 % del monto total de la contratación.
2	Guías, marcos, procesos y procedimientos de gobierno de ciberseguridad.		
3	Metodología para la aplicación de la estrategia		
Fase nro. 3			
Ítem	**Descripción del entregable**	**Plazo de entrega**	**Porcentaje de pago**
1	Desarrollo de KPIs y métricas de ciberseguridad con visualización en tablero interactivo de los avances	Entre los 181 y 270 días posteriores a la fecha de orden de inicio de servicios.	30 % del monto total de la contratación..
2	Guía de adopción de la estrategia		
3	Programa de monitoreo de la ciberseguridad del BCP		
4	Guías técnicas y definición de iniciativas para el intercambio de información sobre ciberseguridad.		
Fase nro. 4			
Ítem	**Descripción del entregable**	**Plazo de entrega**	**Porcentaje de pago**
1	Desarrollo y ejecución de programas de capacitación estratégicos	Entre los 271 y 365 días posteriores a la fecha de orden de inicio de servicios.	20 % del monto total de la contratación.
2	Informe final del servicio con resultados, lecciones aprendidas y recomendaciones.		

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 incluyendo una matriz de escalamiento. El BCP designará el equipo de trabajo que acompañará el desarrollo del servicio solicitado.

Informes y actas: El Proveedor deberá elaborar de manera mensual 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).
Al final de cada fase, se deberá elaborar un acta de conformidad por los trabajos que será suscrito en conjunto con el área administradora del contrato. En el acta, el proveedor deberá consignar los puntos entregados de los requerimientos indicados en el cuadro "ESPECIFICACIONES TÉCNICAS".

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

Lugar y Horario de Trabajo: Se podrá realizar de forma remota, a través de herramientas tecnológicas tales como Microsoft Teams, o similares; y de forma presencial cuando el área administradora del contrato (Departamento de Ciberseguridad del BCP) lo requiera en el Edificio BCP, sito en la Av. Federación Rusa y Av. Augusto Roa Bastos, 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 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. de acuerdo con lo establecido en el apartado **CONDICIONES GENERALES** de las especificaciones técnicas.
Los pagos se realizarán de la siguiente forma:
20 % del monto total contratado luego de la entrega total de la Fase N° 1.
30% 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.
20% 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: 2024.08.14 14:10:39 -04'00'

FIRMA DEL RESPONSABLE DE LA UOC (*):

MARIA LORENA MEZA ARIAS
Firmado digitalmente por MARIA LORENA MEZA ARIAS
Fecha: 2024.08.14 14:57:46 -04'00'

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