Contratación de Servicios de Consultoría

P.A.C. PRIORITARIO Nº 01/2024

"CONSULTORIA DE SEGURIDAD INFORMATICA - AD REFERENDUM"

ID Nº 436.577

	PERFIL Y REQUISITOS DOCUMENTALES PARA EVALUAR EL PLANTEL TECNICO

GERENTE DEL PROYECTO

- Deberá participar activamente en todas las etapas y fases comprendidas en esta consultoría de evaluación y ajustes de cumplimiento en Ciberseguridad para el PJ, trabajando de cerca con el equipo técnico de la DGTIC, redactando los documentos a ser presentados durante el avance del proyecto. Estas funciones tienen un carácter enunciativo y no delimitante.
  - Cantidad: 1

Perfil Técnico mínimo	Puntaje	Puntaje Total
1. Graduado universitario de las carreras de Ingeniería en Informática, Licenciatura en Análisis de Sistemas, Ingeniería en Sistemas o relacionada a las Ciencias de la Computación o Tecnologías de la Información y Comunicación. ***Sírvase remitir el Título correspondiente acompañando el formulario (TEC – 3.1), que forma parte del presente llamado.***	**EXC.**	**8**
2. Experiencia mínima de 3 (tres) años en gerenciamiento o liderazgo de equipos de trabajo para el desarrollo e implementación de proyectos tecnológicos, lo que valdrá 2 puntos. ***Por cada año adicional al mínimo requerido se le otorgará 1 punto hasta un máximo de 4 puntos.***	**4**	
3. Curso de Postgrado en Gestión de Proyectos y/o certificación PMP, PRINCE2 o similar. ***Para la asignación de los puntos, el postulante debe declarar contar con alguno/s de los postgrados/certificaciones mencionados y presentar la documentación respaldatoria correspondiente.***	**2**	
4. Experiencia comprobable en gerenciamiento o liderazgo de equipos de trabajo para el desarrollo e implementación de proyectos de Ciberseguridad y Protección de la Información.	**2**	

Requisito Documental

1. Curriculum Vitae conforme al modelo expuesto en el anexo (TEC – 3.1) donde manifiesta en carácter de declaración jurada que se compromete a trabajar con el oferente, conforme a lo dispuesto en el pliego de bases y condiciones, en caso de ser adjudicado y que toda la información proporcionada detallada en el historial laboral es veraz y demuestra la experiencia solicitada. Asimismo, deberá indicar el contacto de la empresa donde prestó servicios, número de teléfono y correo electrónico. **Observación**: No se podrá presentar el mismo candidato para más de un perfil.
2. Copia de cédula de identidad.
3. Copias autenticadas del título universitario, certificados de Cursos o Estudios oficiales para ser considerados como información válida.
4. La experiencia será demostrable con copia de contratos, facturas o documento que la certifique, con su respectiva conformidad de prestación servicios.

JEFE CONSULTOR/EVALUADOR DE SEGURIDAD		
➢ Su función principal será llevar a cabo la consultoría de evaluación y ajustes de cumplimiento en Ciberseguridad para el PJ, liderando el equipo técnico del oferente y trabajando de manera coordinada con la DCPI y la DGTIC, elaborando los documentos e insumos a ser entregados en las diferentes etapas e hitos de control previstas en esta consultoría. Estas funciones tienen un carácter enunciativo y no delimitante. • Cantidad: 1		
Perfil Técnico mínimo	**Puntaje**	**Puntaje Total**
1. Graduado universitario de las carreras de Ingeniería en Informática, Licenciatura en Análisis de Sistemas, Ingeniería en Sistemas o relacionada a las Ciencias de la Computación o Tecnologías de la Información y Comunicación. ***Sírvase remitir el Título correspondiente acompañando el formulario (TEC – 3.1), que forma parte del presente llamado.***	EXC.	12
1. Experiencia mínima de 3 años de trabajo como Jefe de Consultores y Evaluadores de seguridad, lo que valdrá 2 puntos. ***Por cada año adicional al mínimo requerido se le otorgará 1 punto hasta un máximo de 4 puntos.***	4	
2. Conocimientos comprobables en marcos de seguridad tales como las normas **ISO/IEC 27001/2, ISO/IEC 27035, NIST, ITIL, COBIT**. Los puntos serán otorgados de acuerdo a la siguiente escala de proporcionalidad: • Certificación en más de una de las mencionadas: 4 puntos • Certificación en una de ellas: 3 puntos • Certificación no vigente en alguna de las mencionadas: 2 puntos • Cursos y/o capacitaciones de preparación para certificación: 1 punto ***Para la asignación de los puntos, el postulante debe declarar contar con alguna/s de las certificaciones mencionadas y presentar la documentación respaldatoria correspondiente.***	4	
3. Conocimientos comprobables en seguridad de la información y/o ciberseguridad: **CISSP, ECSS, ECSA, CISM, CISA, CCISO** o equivalente. Los puntos serán otorgados de acuerdo a la siguiente escala de proporcionalidad: • Certificación vigente en más de una de las mencionadas: 4 puntos • Certificación vigente en alguna de las mencionadas: 3 puntos • Certificación no vigente en alguna de las mencionadas: 2 puntos • Cursos y/o capacitaciones de preparación para certificación: 1 punto. ***Para la asignación de los puntos, el postulante debe declarar contar con alguna/s de las certificaciones mencionadas y presentar la documentación respaldatoria correspondiente.***	4	
Requisito Documental		

1. Curriculum Vitae conforme al modelo expuesto en el anexo (TEC – 3.1) donde manifiesta en carácter de declaración jurada que se compromete a trabajar con el oferente, conforme a lo dispuesto en el pliego de bases y condiciones, en caso de ser adjudicado y que toda la información proporcionada detallada en el historial laboral es veraz y demuestra la experiencia solicitada. Asimismo, deberá indicar el contacto de la empresa donde prestó servicios, número de teléfono y correo electrónico. **Observación**: No se podrá presentar el mismo candidato para más de un perfil.
2. Copia de cédula de identidad.
3. Copias autenticadas del título universitario, certificados de Cursos o Estudios oficiales para ser consideradas como información válida.
4. La experiencia será demostrable con copia de contratos, facturas o documento que la certifique, con su respectiva conformidad de prestación servicios.

EQUIPO DE TRABAJO (EVALUADOR, ANALISTA, AUDITOR DE SEGURIDAD)

- Su función principal será llevar a cabo las tareas específicas determinadas para la consultoría de evaluación y ajustes de cumplimiento en Ciberseguridad para el PJ, reportando al Jefe Consultor/Evaluador de Seguridad y trabajando de manera coordinada con los equipos internos de la DGTIC que deben ser involucrados.
  - Le corresponderá (las siguientes funciones tienen un carácter enunciativo y no delimitante):
    - Realizar análisis exhaustivos de los sistemas y plataformas informáticas, así como de las redes de la institución, de tal manera a identificar vulnerabilidades y puntos débiles en su seguridad.
    - Realizar las pruebas de intrusión y penetración para detectar posibles brechas y riesgos, que servirán de insumo para la elaboración de recomendaciones y medidas correctivas a ser realizadas para mitigarlas o erradicarlas.
    - Realizar una revisión exhaustiva de los controles y medidas de seguridad implementadas por la institución.
    - Evaluar el cumplimiento de las políticas y estándares de seguridad, identificar posibles brechas y riesgos, y colaborar con propuestas y recomendaciones para mejorar la postura de seguridad institucional, así como el establecimiento de buenas prácticas que rigen la materia tanto a nivel nacional como internacional.
  - Cantidad: mínimo 2

Perfil Técnico mínimo	Puntaje	Puntaje Total
1. Al menos uno de los expertos deberá tener experiencia mínima de 4 años de trabajo como Evaluador, Analista, Auditor de seguridad de la información y/o ciberseguridad.	EXC.	30
2. Graduado universitario de las carreras de Ingeniería en Informática, Licenciatura en Análisis de Sistemas, Ingeniería en Sistemas o relacionada a las Ciencias de la Computación o Tecnologías de la Información y Comunicación. ***Sírvase remitir el Título correspondiente acompañando el formulario (TEC – 3.1), que forma parte del presente llamado.*** • ***Se otorgarán 2 (dos) puntos por cada profesional del equipo de trabajo con título, hasta un máximo de 4 (cuatro) puntos.***	4	
3. Experiencia comprobable de al menos 2 años en seguridad de la información y/o ciberseguridad: SIEM, Forensica digital (Forensic Tools), Respuesta a Incidentes (Incident Response Tools), Inteligencia de amenazas,	20	

orquestación y automatización de respuesta, auditoría de vulnerabilidades, administración de logs (Log Management tools), Virtualización, Gestión de Identidad y Accesos, Emulación de adversarios, SOAR, UTM, Firewalls, Vulnerability Management tools, Cyberthreat Intelligence Platform, Security by Deception tools, Traffic Capture & Flow Analyses, Adversary Emulation/Simulation tools, DFIR stacks/tools, SASE, plataformas o herramientas de Zero Trust, IAM, CASB, Native Virtualization Platforms, Switching/Routing Intermediate, etc. u otros tipos de herramientas/tecnologías asociados. Por cada persona del equipo: • Más 2 y menos de 3 años de experiencia laboral (conforme al criterio anterior) **puntuará 3 puntos**. • Más de 3 y menos de 5 años **puntuará 5 puntos**. • Más de 5 años **puntuará 10 puntos**. Hasta un máximo de 20 (veinte) puntos. • ***Para la asignación de los puntos, el postulante debe declarar contar con alguna/s de las certificaciones mencionadas y presentar la documentación respaldatoria correspondiente.***		
4. Conocimientos comprobables en seguridad de la información y/o ciberseguridad: **CISSP, ECSS, ECSA, CISM, CISA, CCISO, CCIE, CCNP, CND, ECIH, CEH, CSA, CPENT, CTIA, eJPT** o equivalente. Por cada persona del equipo, los puntos serán otorgados de acuerdo a la siguiente escala de proporcionalidad: • Certificación vigente en alguna de las mencionadas: 2 puntos • Certificación no vigente en alguna de las mencionadas: 1 puntos • Cursos y/o capacitaciones de preparación para certificación: 0.5 puntos Hasta un máximo de 6 (seis) puntos. • ***Para la asignación de los puntos, el postulante debe declarar contar con alguna/s de las certificaciones mencionadas y presentar la documentación respaldatoria correspondiente***	**6**	
Requisito Documental		
1. Curriculum Vitae conforme al modelo expuesto en el anexo (TEC – 3.1) donde manifiesta en carácter de declaración jurada que se compromete a trabajar con el oferente, conforme a lo dispuesto en el pliego de bases y condiciones, en caso de ser adjudicado y que toda la información proporcionada detallada en el historial laboral es veraz y demuestra la experiencia solicitada. Asimismo, deberá indicar el contacto de la empresa donde prestó servicios, número de teléfono y correo electrónico. **Observación**: No se podrá presentar el mismo candidato para más de un perfil. **2.** Copia de cédula de identidad. **3.** Copias autenticadas del título universitario, certificados de Cursos o Estudios oficiales para ser consideradas como información válida. **4.** La experiencia será demostrable con copia de contratos, facturas o documento que la certifique, con su respectiva conformidad de prestación servicios.		

OBSERVACIONES:

- Para comprobar la experiencia requerida de todos los profesionales y aval de la misma se deberá acompañar al FORMULARIO TEC 3-1 un documento donde esté detallado el nombre y teléfono del contacto de la empresa y/o institución donde haya prestado servicios.
- Se deberá declarar en el Formulario TEC 3-1 de Formato de Currículum Vitae (CV) todo lo relacionado a la experiencia tanto general como específica.
- Toda la documentación relacionada a la formación profesional deberá ser correctamente documentada mediante copia autenticada de Títulos Profesionales, Certificados de Cursos o Estudios oficiales para ser considerada como información válida.
- La formación académica (Grado, Postgrado) deberá ser avalada con copia autenticada de título habilitante.
- Para los cursos se deberá presentar copia de las constancias y/o diplomas obtenidos.

(Sobre N. º 1)

SECCIÓN 5

ALCANCES y TÉRMINOS DE REFERENCIA (TDR)

1. ANTECEDENTES

El Poder Judicial de la República del Paraguay, en cumplimiento de las normativas y leyes vigentes en la República, incluyendo la Resolución MITIC Nro. 277/2020, el Manual de Gobierno y Control de las Tecnologías de la Información (MGCTI) del Banco Central del Paraguay, y las recomendaciones de los estándares internacionales ISO/IEC 27001, CIS Controls, NIST SP 800-53, CSF, COBIT y ITIL, busca contratar los servicios de una empresa especializada en seguridad de la información y ciberseguridad para realizar una evaluación exhaustiva de su infraestructura, sistemas, procesos, servicios y prácticas de seguridad de la información, contemplando la planificación de acciones correctivas para mitigar las debilidades encontradas y la ejecución tutelada de las mismas por parte del socio tecnológico contratado, constituyendo un trabajo integral de mejora de las capacidades institucionales en seguridad de la información y ciberseguridad.

2. ALCANCE DEL PROYECTO

La consultoría de evaluación de seguridad de la información y ciberseguridad debe abarcar, pero no limitarse, a los siguientes aspectos:

- Análisis de Riesgos y Amenazas:
  - Identificación y evaluación de todos los activos de información y su valoración.
  - Identificación y evaluación de amenazas y vulnerabilidades.
  - Análisis de riesgos y determinación de su impacto.

- Evaluación de Controles de Seguridad:
  - Revisión de las políticas, normas y procedimientos de seguridad existentes.
  - Evaluación de la gestión de accesos y permisos.
  - Análisis de la gestión de parches y actualizaciones.
  - Revisión de los controles de seguridad física y lógica.
  - Evaluación de la robustez en seguridad y resiliencia de los sistemas, aplicaciones y servicios informáticos institucionales, teniendo presente las recomendaciones de la organización internacional OWASP (Open Web Application Security Project® - https://owasp.org/) expuestas en su WSTG (Web Security Testing Guide - https://owasp.org/www-project-web-security-testing-

guide/) para aplicaciones web, la norma ISO/IEC 22301 y la NIST SP 800-34 acerca de la continuidad del negocio y planes de contingencia, así como otras iniciativas aplicables.
  - Matriz de controles CIS (última versión), evaluada completamente y teniendo presente la situación institucional.
  - Análisis de las brechas existentes ("Gap Analysis") entre los procesos ejecutados actualmente por la DGTIC versus los principales estándares nacionales e internacionales, así como las buenas prácticas y recomendaciones que rigen la materia.

- Pruebas de Intrusión y Penetración:
  - Realización de pruebas de penetración en la infraestructura y sistemas institucionales.
  - Identificación de posibles brechas de seguridad y vulnerabilidades.

- Evaluación de la Gestión de Incidentes y Respuesta a Emergencias:
  - Análisis de los planes y protocolos de respuesta a incidentes existentes.
  - Evaluación de la capacidad de detección y respuesta a amenazas cibernéticas.
  - Revisión de los mecanismos de notificación y comunicación interna y externa en caso de incidentes de seguridad.

- Análisis de Cumplimiento Normativo:
  - Verificación del cumplimiento de las normativas y leyes aplicables.
  - Evaluación de las políticas de privacidad y protección de datos.

- Planificación y previsión de las acciones correctivas necesarias en base al análisis previo:
  - Identificación, previsión, involucrados y asignación de responsabilidades.

- Implantación de las acciones y medidas identificadas, correctivas o de mitigación:
  - Ejecución de las tareas definidas en base a la planificación previa, con las acciones correctivas tendientes a mejorar las capacidades en ciberseguridad de la institución.

- Programa de entrenamiento y capacitación continua:
  - Diseño del programa de capacitación continua de desarrollo de competencias en el área de seguridad de la información y ciberseguridad para los funcionarios de la institución.

3. ENTREGABLES ESPERADOS.

La empresa de consultoría deberá entregar los siguientes documentos, sujetos a aprobación de la DCPI-DGTIC, enmarcados en las siguientes Etapas de la consultoría:

- **Etapa 1: Planeación y cronograma de ejecución de cada ítem de trabajo especificado en el alcance de esta consultoría.**

- **Plazo**: a los 30 días de la firma de contrato.

  a) Documento con la especificación de los trabajos a ser realizados en cada ítem incluyendo: lugar de trabajo, horario en (caso de ser necesario), forma de registro de actividades, de registro de actualizaciones, de reportes de trabajo, de horas utilizadas y otros relevantes para

lograr el adecuado registro de los indicadores de éxito de cada ítem. Este documento deberá incluir el relevamiento de información necesario para la planificación de todas las actividades, incluyendo las documentaciones de las reuniones, visitas in situ a la institución, revisiones con los diferentes equipos internos para avanzar en los entregables.

b) Formulario de relevamiento de los componentes de infraestructura, herramientas, sistemas y plataformas tecnológicas internas que posee la institución y que puedan ser de utilidad al prestador para lograr los objetivos propuestos en el alcance de esta consultoría. El resultado de la validación deberá presentarse al contratante con el plan de mitigación en caso de presentarse observaciones o requisitos adicionales. De existir componentes faltantes de infraestructura, herramientas, sistemas o plataformas, estos no deberán ser causales de interrupción en el avance de la consultoría.

c) Documento con los requerimientos de acceso a las herramientas, componentes o dispositivos de infraestructura, plataformas, servicios internos, sistemas informáticos, bases de datos y otros que requieran para realizar su trabajo.

d) Documento con el plan de cumplimiento mínimo de niveles de servicio especificados (SLA) y la definición de los indicadores clave de rendimiento (KPI) y métricas de adopción o uso de los ítems respectivos, para poder evaluar el éxito de este proyecto de evaluación y fortalecimiento institucional en ciberseguridad. Estos pueden incluir el porcentaje de reducción de incidentes de seguridad, tiempo de respuesta ante incidentes, cumplimiento de políticas de seguridad, etc.

e) Documento con el programa de entrenamiento y plan de capacitación a funcionarios judiciales, así como la transferencia tecnológica y cognitiva a todos los funcionarios institucionales de los equipos internos directamente involucrados en las tareas de la consultoría.

f) Documento con Matriz de responsabilidades del proveedor y el Poder Judicial.

g) Documento con el cronograma de trabajo, especificando fechas, responsables y entregables concretos.

- **<u>Etapa 2</u>**: **Evaluación de la ciberseguridad institucional actual**.

- **<u>Plazo</u>**: a los 180 días de la firma de contrato.

a) Informe de Evaluación de Ciberseguridad:

i) Datos, análisis y conclusiones sobre las pruebas de intrusión y penetración.
ii) Resumen ejecutivo de los hallazgos, incluyendo una evaluación del nivel de riesgo.
iii) Detalles de las brechas de seguridad y vulnerabilidades identificadas, así como de las recomendaciones de mitigación para cada una de ellas.

b) Reporte de análisis de las brechas existentes (“Gap Analysis”) entre los procesos ejecutados actualmente por la DGTIC versus los principales estándares nacionales e internacionales, así como las buenas prácticas y recomendaciones que rigen la materia:

i) ISO/IEC 27001: “Information Security Management System”.
ii) CIS Controls: “Center for Internet Security – Critical Security Controls”.
iii) ISO/IEC 27035-1:2023 “Information security incident management”
iv) ISO/IEC 22301: “Security and resilience”.

c) Planilla de evaluación de los controles de seguridad existentes y recomendaciones de mejora, teniendo presente las siguientes guías:

i) Matriz de controles CIS (última versión) completa con la situación institucional.
ii) Resolución MITIC Nro. 277/2020.

d) Informe con el análisis de la conformidad normativa y recomendaciones para el cumplimiento.
e) Documento de evaluación de la madurez de la gestión de incidentes y respuesta a emergencias.

- **Etapa 3**: **Plan de acciones correctivas y mitigación de riesgos**.

- **Plazo**: a los 210 días de la firma de contrato.

a) Propuesta estratégica de las acciones a seguir a corto, mediano y/o largo plazo, con base a los hallazgos encontrados para la elaboración de un plan de ciber resiliencia.
b) Descripción detallada de las medidas correctivas propuestas.
c) Estimación de costos y recursos necesarios para implementar las recomendaciones.
d) Cronograma de implementación, incluyendo hitos y responsabilidades.

- **Etapa 4**: **Implantación de acciones correctivas y mitigación de riesgos**.

- **Plazo**: a los 365 días de la firma de contrato.

a) Ejecución de las medidas y acciones correctivas.
b) Elaboración de manuales, procedimientos, disposiciones, normativas, mecanismos e instructivos específicos que formalicen los procesos críticos involucrados en las contramedidas ejecutadas y que congreguen las buenas prácticas/recomendaciones del sector que rigen en la materia.
c) Transferencia tecnológica y cognitiva a todos los funcionarios institucionales y equipos involucrados.

4. REQUISITOS DE LA EMPRESA CONSULTORA

La empresa interesada en participar en esta licitación debe cumplir con los siguientes requisitos:

1) Experiencia:
   a) Demostrar experiencia comprobable en la realización de las actividades mencionadas en el alcance de esta consultoría en ciberseguridad.
   b) Contar con personal especializado y certificado en ciberseguridad y protección de la información.

2) Referencias:
   a) Presentar referencias de clientes anteriores que puedan dar testimonio de la calidad y profesionalismo de los servicios prestados.

3) Cumplimiento Normativo:
   a) Cumplir con las leyes y regulaciones aplicables en materia de protección de datos y privacidad.

5. PROCESO DE EVALUACIÓN DE LAS PROPUESTAS.

Las propuestas serán evaluadas con base en los siguientes criterios:

- Experiencia del oferente en evaluaciones de seguridad de la información, ciberseguridad, planificación e implementación de medidas correctivas y de cumplimiento.
- Calidad y detalle del enfoque metodológico propuesto.
- Claridad y exhaustividad de los entregables propuestos.
- Experiencia y certificaciones del personal clave asignado al proyecto.

Para la calificación de los aspectos técnicos de la propuesta se tendrá en cuenta el sistema de puntuaciones detallado seguidamente. El puntaje técnico máximo es de 100 puntos y el mínimo requerido para calificar es de 70 (setenta) puntos.

Al efecto, se establecen los factores a evaluar, la importancia de cada factor (ponderación del factor), y los puntajes a utilizar para calificar cada factor (puntaje de calificación).

La calificación final de cada firma se obtendrá de la suma ponderada de los puntajes logrados en cada factor de evaluación.

6. REEMPLAZO DE PROFESIONALES.

Se aclara que la Corte Suprema de Justicia se reserva el derecho de solicitar el reemplazo de profesionales durante la ejecución del contrato, si los mismos no cumplen con el desempeño esperado. El nuevo profesional propuesto deberá contar con la aprobación de la Corte Suprema de Justicia, estando obligado a cumplir con el mismo perfil original solicitado o superior.

Una vez recibida la solicitud de reemplazo de personal por parte de la Corte Suprema de Justicia, el oferente adjudicado deberá considerar hasta un máximo de ***45 (cuarenta y cinco) días calendario***, para la incorporación de este profesional, sin afectar la continuidad del servicio, salvo orden expresa de la institución en la solicitud de reemplazo.

7. PRESTACIÓN DEL SERVICIO.

El personal técnico de la empresa contratada podrá realizar sus trabajos en su local propio, debiendo asistir a las oficinas de la DGTIC y/o al Palacio de Justicia cuando así le sea requerido para el cumplimiento de las tareas establecidas por la Convocante o necesarias para el correcto y completo cumplimiento del alcance de esta consultoría.

En caso de necesidad, el administrador del contrato podrá solicitar la presencia de los Técnicos fuera del horario mencionado. Los trabajos relativos a la ejecución de pruebas de intrusión y penetración (PENTESTING), y todos aquellos previstos en las diferentes etapas de esta consultoría a ser llevados por la empresa contratada, así como toda la infraestructura y elementos requeridos para el efecto (mobiliario, equipos informáticos, útiles de oficina, etc.), contemplando los horarios, tiempos de respuesta ante las solicitudes y demás condiciones de trabajo, quedan bajo exclusiva responsabilidad y administración de la firma contratada.

El lugar de prestación de los servicios será en la Corte Suprema De Justicia, Mariano Roque Alonso y Testanova, en la Dirección General de Tecnología de la Información y las Comunicaciones (DGTIC), el Lugar de la Consultoría es en las Oficinas habilitadas para el efecto por la Dirección General de Administración y Finanzas.

8. GARANTÍA DE LOS SERVICIOS

El Consultor deberá ofrecer una garantía en relación a los productos contratados y los entregables suministrados, por un plazo de 6 (seis) meses una vez terminada la consultoría, plazo en el cual deberá dar asistencia y solución a los inconvenientes que se presenten en relación a los entregables y servicios provistos durante esta consultoría.

Esta garantía no cubre la elaboración de nuevos entregables ni de prestaciones de servicios no especificados en el alcance de esta consultoría y en el entregable de la "Etapa 1: Planeación y cronograma de ejecución de cada ítem de trabajo especificado en el alcance de esta consultoría".