Corte Suprema de Justicia

ADENDA 5

LICITACIÓN POR CONCURSO DE OFERTAS PAC PRIORITARIO N° 01/2024 "CONSULTORIA DE SEGURIDAD INFORMATICA - AD REFERENDUM" I.D. N° 436.577.

Por la que se introducen modificaciones o enmiendas a los plazos del llamado correspondiente a la Contratación de referencia los cuales quedan redactados de la siguiente forma:

Se modifican los siguientes eventos:

***FECHA TOPE DE CONSULTAS**
***FECHA DE ENTREGA FÍSICA**
***FECHA DE APERTURA FÍSICA**

**** Se aclara que las fechas se encuentran en el Sistema de Información de las Contrataciones Públicas.**

DATOS DE LA CONTRATACIÓN
INSTRUCCIONES PARA LOS CONSULTORES
HOJA DE DATOS

Visita al sitio de ejecución del contrato.

- **Fecha:** Las visitas podrán ser realizadas hasta 1 (un) día hábil antes de la fecha tope de consultas.
- **Lugar:** Las visitas se realizarán en el Palacio de Justicia de Asunción sito en las calles Mariano Roque Alonso y Pedro Blasio Testanova.
- **Hora:** Las visitas se realizarán de lunes a viernes de 08:00 a 12:00 hs.
- **Procedimiento:** Los Oferentes que realizarán la visita, deberán presentarse en la Dirección General de Tecnología de la Información y las Comunicaciones, ubicada en el 8vo piso de la torre sur del Palacio de Justicia de Asunción, con una nota con membrete de la empresa, en la cual mencionan NOMBRE y NÚMERO DE CEDULA de la persona que realizará la visita y firmar el acuerdo de confidencialidad respectivo. Al término de cada visita se emitirá una constancia.
- **Nombre del funcionario responsable de guiar la visita:** Francisco Zacarias y/o Manuel Torres y/o Mauricio Coronel y/o Rubén Portillo y/o Marcelo Demestri.
- **Participación obligatoria:** No. Se podrá presentar Declaración Jurada de conocer las instalaciones.

Al culminar la visita, se labrará acta en la cual conste, la fecha, lugar y hora de realización, en la cual se identifique el nombre de las personas que asistieron en calidad de potenciales oferentes, así como del funcionario encargado de dicho acto.

Los gastos relacionados con dicha visita correrán por cuenta del oferente.

DOCUMENTOS ADICIONALES: (SOBRE 1)

- Formulario TEC-2: Organización experiencia y del consultor.
  - Organización del consultor
  - Experiencia del consultor

  - Experiencia General de la firma
  - Experiencia Específica de la firma
- Formulario TEC-3: Plantel de Profesionales
  - Formulario TEC 3.1 Formación Profesional - Currículo del personal profesional propuesto (Títulos, Certificados, Constancias, etc.).
- Formulario TEC-4: Descripción del enfoque, la metodología y el plan de actividades para la ejecución del trabajo.
- Formulario TEC-5: Composición del equipo y asignación de responsabilidades
- Formulario TEC-6: Calendario de actividades del Personal.
- Formulario TEC-7: Plan de Trabajo.
- Balance General y Estados de Resultados (comparativo) de los años 2020, 2021, 2022, firmados por el contador, propietario y/o representante legal si correspondiere, acorde a las normas contables y a los modelos establecidos en las Normativas Vigentes de la Dirección Nacional de Ingresos Tributarios, que se encuentran en la página web www.set.gov.py.
- Formulario 500 para los años 2020, 2021 y 2022 correspondientes a la Declaración Jurada del Impuesto a la Renta.
- Formulario 120 para contribuyentes del IVA General de los últimos 36 (TREINTA Y SEIS) meses, correspondiente a los años 2020,2021 y 2022.
- Formulario 501 para los años 2020, 2021 y 2022 correspondientes a contribuyentes del IRE SIMPLE.
- Formulario 515 solo para contribuyentes de Renta Personal y Formulario 516 IRP RGC para los años 2020, 2021 y 2022.
- Declaración Jurada de que el consultor se compromete a la realización total de la Consultoría.
- Fotocopia simple de la cédula tributaria (Constancia de inscripción en el Registro Único de Contribuyentes - RUC).
- Listado detallado de los integrantes de la sociedad en el cual detallan el NOMBRE, APELLIDO Y NUMERO DE CEDULA DE IDENTIDAD, de cada uno, a fin de dar cumplimiento a la CALIFICACIÓN LEGAL. PROHIBICIONES DE LOS INCS. "A" Y "B" DEL ARTÍCULO 40, conforme a lo establecido en la Resolución DNCP N° 849/2015.
- Declaración Jurada en la cual el oferente se compromete a que serán de su entera responsabilidad, todos aquellos daños a los bienes, infraestructura o sistemas de la convocante, resultantes de hechos voluntarios e involuntarios, causados por la negligencia o impericia de sus empleados, sin cargo alguno para la institución.
- Declaración Jurada en la cual el oferente se compromete a no utilizar, disponer, divulgar, difundir a ninguna otra institución o persona, ni antes ni durante ni después de la prestación de servicios, información alguna a la que haya podido tener acceso mediante esta contratación, debiendo ser considerada toda esta información como de estricta y absoluta confidencialidad sobre los datos almacenados y la arquitectura tecnológica de Corte Suprema de Justicia.
- **Constancia de Visita e Inspección emitida por la Dirección General de Tecnología de la Información y las Comunicaciones (DGTIC) de la Corte Suprema de Justicia o en su defecto deberá presentar una Declaración Jurada en la cual manifieste que conoce las instalaciones.**

(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 27001:2015, 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.

- **Se establece el siguiente cuadro con información referencial:**

Equipos	Descripción	Cantidad	Físico	Virtual
Hipervisores		10	10	0
Servidores	Windows + Linux	106	29	77
Storage + Expansion		10		
San Switch		5		
Servicios	DB	22		
	Correo	2		
	AntiSpam	1		
	Antivirus	1		
	Controladores de dominio	12		
	Servidor de Aplicaciones	14		
Router/Firewall		20		
Switch		6		
Proxy		3		
		212		

- 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:

- **<u>Etapa 1</u>: 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 a la 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.

- **Etapa 2**: **Evaluación de la ciberseguridad institucional actual**.

- **Plazo**: 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) Matriz de Riesgos Tecnológicos y Riesgos Cibernéticos.
f) 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. 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 el oferente 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.

5. 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).

6. 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.

- **<u>OBSERVACIÓN</u>: solo se modifican los puntos citados en la presente adenda, quedando invariables los demás puntos del pliego de bases y condiciones.**

ABG. OSCAR E. SANABRIA P.
Jefe - Dpto. de Licitación
UOC - Corte Suprema de Justicia