URUGUAY

Proyecto URU/21/009 "Apoyo a la implementación del Programa para el Fortalecimiento de la Ciberseguridad en Uruguay".

CONTRATACIÓN CONSULTOR/A DE OBRA
ESPECIALISTA EN CIBERSEGURIDAD PARA TELECOMUNICACIONES

I. ANTECEDENTES

1.1. Uruguay se ha posicionado como líder en la región y referente internacional en el desarrollo de Gobierno Digital a partir de una estrategia digital reflejada actualmente en la Agenda Digital Uruguay 2025.

1.2. El Objetivo Estratégico X de la Agenda Digital Uruguay 2025, expresa la necesidad de incrementar la ciberseguridad para prevenir y mitigar riesgos en el ciberespacio y avanzar en el cumplimiento del marco nacional de ciberseguridad, basado en la cooperación público y privada, garantizando la disponibilidad de los activos críticos de información.

1.3. La Ley N° 19.924 de 18/12/2020 artículo 84, dio nueva redacción a : Ley 18.719 de 27/12/2010 artículo 149: mediante el cual encomienda a la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), a dirigir las políticas, metodologías y mejores prácticas, y regular en materia de seguridad de la información y ciberseguridad a nivel nacional, así como fiscalizar, auditar su cumplimiento y brindar apoyo en las etapas de implementación de las mismas en todas las entidades públicas, y además, en las entidades privadas vinculadas a servicios o sectores críticos del país. Dichos cometidos serán ejercidos a través de la Dirección de Seguridad de la Información.

II. OBJETIVOS

2.1 Una línea de acción de la Agencia es fortalecer el ecosistema nacional de ciberseguridad, desarrollando un Marco de Ciberseguridad en las verticales de gobierno, salud, telecomunicaciones y financiero, en colaboración y acuerdo con los reguladores de cada sector.

2.2 El objetivo de la contratación de esta consultoría es desarrollar una nueva versión del Marco de Ciberseguridad y su guía de implementación en la vertical telecomunicaciones en colaboración y acuerdo con reguladores y principales actores del sector.

III. ACTIVIDADES

Las actividades a realizar para el cumplimiento de los objetivos son las siguientes, sin perjuicio de otras que se puedan proponer en el desarrollo de los trabajos:

a) Mantener reuniones con los principales actores y reguladores de las telecomunicaciones en Uruguay.

b) Investigar a nivel internacional, estándares, marcos, normas y reglamentaciones en ciberseguridad vigentes y que apliquen a las telecomunicaciones.

c) Presentar un informe detallando la documentación analizada, con los principales hallazgos y conclusiones sobre el estudio; y realizar análisis comparativo con la normativa vigente a nivel nacional.

d) Elaborar una propuesta de requisitos que resulten en una nueva versión del MCU para aplicarse en el sector de las telecomunicaciones, contemplando el punto de vista de los principales actores a través de continuos intercambios con los mismos.

e) Identificar la madurez de los principales actores identificados para la implementación de cada requisito; así como potenciales desafíos futuros.

f) Proponer una guía de implementación del Marco de ciberseguridad, contemplando también la visión de los principales actores.

g) Deberá colaborar con la adecuación de la herramienta de evaluación de ciberseguridad provista por el BID, para el sector de telecomunicaciones.

h) Toda otra tarea similar o afín a las ya mencionadas en el marco del trabajo a implementar que sean necesarias para cumplir con el objetivo.

IV. PRODUCTOS DE LA CONSULTORÍA

PRODUCTO 1: Estado del arte y plan de trabajo. Relevamiento de estándares, marcos y requisitos existentes vinculados a seguridad de la información en telecomunicaciones, a nivel nacional e internacional. Deberá presentarse:

- Informe técnico con presentación del estado del arte, estándares utilizados, y detalle de legislación y normativa referentes a su implementación.
- Un plan de trabajo que contenga entre otros aspectos:
  - Detalle las instituciones o perfiles necesarios para la realización del mismo.
  - Estimación de esfuerzo, y cronograma de reuniones.

(A entregar en un plazo máximo de 30 días a partir de la firma del contrato).

PRODUCTO 2: Documento técnico que detalle los principales hallazgos sobre la documentación analizada, describiendo un análisis comparativo con la normativa vigente a nivel internacional y nacional. Se deberán identificar los principales requisitos vinculados a seguridad de la información en sector de telecomunicaciones de Uruguay.
(A entregar en un plazo máximo de 60 días a partir de la validación del producto 1).

PRODUCTO 3: Primera versión del documento técnico que establezca los requisitos mapeados al marco de ciberseguridad de Uruguay en su versión vigente, para incluir en una nueva guía de implementación del Marco de Ciberseguridad para el sector de telecomunicaciones de Uruguay.
(A entregar en un plazo máximo de 120 días a partir de la validación del producto 2).

PRODUCTO 4: Documento que identifique la madurez del de los principales actores identificados para la implementación de los requisitos identificados en producto 3; así como potenciales desafíos futuros.
(A entregar en un plazo máximo de 60 días a partir de la validación del producto 3).

PRODUCTO 5: Documento técnico final basado en el producto 3, teniendo en cuentas los aspectos identificados en el producto 4.
(A entregar en un plazo máximo de 60 días a partir de la validación del producto 4).

La aprobación de cada uno de los entregables deberá estar validado con las partes involucradas y aprobado por AGESIC, lo que se será requisito necesario para la liberación de los pagos establecidos en el numeral 7.2.

V. PERFIL DEL CONSULTOR

La persona a contratar deberá demostrar haber obtenido título de grado de 4 años o superior, Certificación o Posgrado técnicos de relevancia para el proyecto:

1. Formación en TIC. (Ejemplo: Titulación en Ingeniería en Telecomunicaciones, Informática, Sistemas o Electrónica).

2. Especialidad en seguridad de la información y/o ciberseguridad. (Al menos una certificación vigente CISSP, CCIE, CCNP, ECIH, CISM).

Contar con Experiencia en el Sector de las Telecomunicaciones. Se podrá solicitar referencias de las experiencias mencionadas.

Se valorará antecedentes específicos y experiencia laboral, trabajos académicos y cursos o especialización referidos a ciberseguridad aplicados a telecomunicaciones.

Se valorará también la capacidad de trabajar en equipos interdisciplinarios y contar con buena capacidad de relacionamiento interpersonal. Quien se postule deberá tener adaptabilidad y flexibilidad, ser proactivo, orientado a los resultados.

VI. SUPERVISIÓN

El Consultor será supervisado directamente por la división Gestión y Auditoría del área de Seguridad de la Información de AGESIC.

VII. PLAZOS, CRONOGRAMA Y COSTOS

7.1 El cronograma de pagos de la Consultoría será por producto, verificándose la aprobación de cada uno de los entregables con las partes involucradas y por AGESIC, lo que se será requisito necesario para la liberación de los pagos establecidos en el numeral 7.2.

7.2 El contrato será de obra por un período de 12 meses con el siguiente esquema de pagos:

10% contra entrega y conformidad del Producto 1
25% contra entrega y conformidad del Producto 2
30% contra entrega y conformidad del Producto 3
25% contra entrega y conformidad del Producto 4
10% contra entrega y conformidad del Producto 5

VIII. CONDICIONES DEL CONTRATO

8 .1 El consultor deberá tener disponibilidad para participar a todas las actividades de coordinación que sean necesarias tener con los técnicos de referencia de cada una de las organizaciones involucradas.

8 .2 El consultor no debe ser funcionario del Estado, Gobiernos Departamentales, Entes y Servicios Descentralizados, cualquiera sea la naturaleza del vínculo.

8 .3 La modalidad del contrato será contrato de obra.