

TERMINOS DE REFERENCIA

Proyecto URU/20/002 “Apoyo a la implementación de la Transformación digital del Estado”.

Posición: Técnico Senior para el CERT
Lugar de destino: Montevideo, Uruguay
Contrato/nivel: Técnico Profesional
Carga horaria: 40 horas semanales

1. Antecedentes generales del proyecto/asignación

El objetivo del Proyecto es apoyar a AGESIC en la implementación de la etapa final del Programa “Mejora de los Servicios Públicos y de la Interacción Estado-Ciudadano” financiada por el préstamo BID 3625/OC-UR y acompañar en la implementación del Programa “Apoyo a la Estrategia de Gobierno Digital”, financiado por el préstamo BID 4867/OC-UR (los “Programas BID”), realizando la gestión administrativa que se le encomiende de los mismos para la identificación y/o contratación de consultorías, la identificación y facilitación de actividades de capacitación, la adquisición de bienes y servicios y la gestión financiera¹ asociada a estas contrataciones, permitiendo así que AGESIC centre sus esfuerzos en la mejora de los servicios públicos en Uruguay. Este proyecto contribuirá a la transformación digital del Estado, con el objetivo de desarrollar e implantar plataformas, soluciones y servicios digitales que promuevan el ahorro y la eficiencia, la calidad de los servicios públicos y la transparencia. El proyecto comprende, simplificación de procesos administrativos sustantivos, ciencia de datos para la toma de decisiones, optimización de servicios públicos y desarrollo de servicios digitales para el ciudadano, soluciones de apoyo para actividades de monitoreo, gestión de recursos humanos y compras públicas, todo con foco en la reducción de los costos transaccionales de los organismos estatales.

Los productos que se esperan alcanzar son los siguientes:

- 1) Fortalecimiento transversal del Estado para la transformación digital;
- 2) Trámites simplificados a nivel sectorial;
- 3) Instrumentos para una mayor adopción del canal digital;
- 4) Estrategia de comunicación y posicionamiento de AGESIC en el entorno regional e internacional;
- 5) Coordinación, administración y supervisión del Proyecto.

La presente consultoría se enmarca en el segundo producto: Trámites simplificados a nivel

¹ Refiere a la gestión de pagos por servicios contratados y/o bienes adquiridos

sectorial.

2. Propósito y alcance de la asignación

El objetivo general de la consultoría es participar activamente en la gestión de incidentes del Centro Nacional de Respuesta a incidentes de seguridad informática, así como, liderar las iniciativas de investigación y gestionar soluciones de Seguridad de la información.

3. Actividades

- Participar en la gestión de incidentes informáticos.
- Realizar análisis forense.
- Realizar análisis de vulnerabilidades y otras actividades relacionadas.
- Realizar análisis de malware.
- Participar en la definición de servicios de ciberseguridad.
- Investigar nuevas soluciones en el área de seguridad de la información.
- Asistir en la generación de inteligencia de amenazas.
- Liderar la implementación de soluciones de ciberseguridad.
- Operar dispositivos de seguridad.
- Participar en procedimientos de adquisición de tecnologías de seguridad de la información.
- Liderar los procesos licitatorios necesarios para cumplir con la evolución de los productos.
- Contribuir en la definición de políticas de seguridad de la información genéricas.
- Trabajar activamente a nivel de las Instituciones Públicas en temas relacionados con su especialidad.
- Toda otra tarea que requiera el Área de Seguridad de la Información en función de sus competencias profesionales y/o personales.

4. Calificaciones y experiencia

a. Educación

Requisitos excluyentes

Se requieren conocimientos técnicos en:

- Redes de datos.
- Seguridad de la Información.
- Administración de Servidores Linux y/o Windows.

- Hacking ético y/o análisis de vulnerabilidades

Se valorará:

- Conocimientos en administración de Infraestructura TI en ambientes de alta criticidad.
- Certificaciones y/o cursos en Redes, Infraestructura o virtualización.
- Certificaciones y/o cursos en Seguridad de la Información
- Conocimientos en administración de WAF.
- Idioma inglés.

b. Experiencia laboral

Requisitos excluyentes

- Experiencia mínima de 5 años de trabajo en Tecnologías de la Información.
- Experiencia mínima de 3 años de trabajo en tareas directamente relacionadas con Ciberseguridad.

A valorar:

- Experiencia en gestión de proyectos y proveedores de Tecnologías de la Información.
- Experiencia en gestión de incidentes.
- Experiencia en análisis forense.
- Experiencia en diseño de arquitecturas seguras.

c. Competencias clave

- Orientación a resultados.
- Adaptabilidad y capacidad de manejo de la incertidumbre.
- Capacidad de análisis y resolución de problemas.
- Capacidad de autogestión.
- Capacidad de trabajo en equipo.
- Capacidad de comunicación y relacionamiento interpersonal.
- Capacidad de trabajo bajo presión.
- Proactividad.

