



Anexo A

Términos de referencia

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

Posición: Líder Técnico.

Lugar de destino: Montevideo, Uruguay

Contrato/nivel: Técnico /Profesional

Carga horaria: 40 horas semanales

Antecedentes generales del proyecto/asignación

El objetivo del Proyecto es apoyar a AGESIC en la implementación del Programa para el Fortalecimiento de la Ciberseguridad en Uruguay (UR-L1152) financiado por el Contrato de Préstamo BID N° 4843/OC-UR, realizando la gestión administrativa que se le encomiende del mismo 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 financiera asociada a estas contrataciones, permitiendo así que AGESIC centre sus esfuerzos en la mejora de la gestión la seguridad de la información de los servicios públicos en Uruguay. El Proyecto contribuirá a una mejora de la gestión en la seguridad de la información a nivel nacional, en particular en aspectos de prevención y respuesta a incidentes informáticos y la ampliación de las capacidades de ciberseguridad en el sector público y privado junto a la academia, a través de los siguientes objetivos específicos: i) mejorar las capacidades operativas y las herramientas del CERT.uy; ii) potenciar el uso de la tecnología avanzada para la formación de recursos humanos y; iii) fortalecer el ecosistema de ciberseguridad a nivel nacional.

Los productos que se esperan alcanzar son los siguientes:
1. Mejoramiento de las capacidades operativas y herramientas del CERT.uy



2. Fortalecimiento de capacidades, potenciación del uso de la tecnología, relacionamiento y cooperación internacional.

La presente consultoría se enmarca en el primer producto: Mejoramiento de las capacidades operativas y herramientas del CERT.uy

Propósito y alcance de la asignación

El objetivo general de la consultoría es el de desarrollar las iniciativas de investigación y gestionar soluciones de ciberseguridad, aportando al equipo del CERTuy mayores herramientas para el desarrollo de sus propósitos.

Actividades

- Investigar nuevas soluciones en el área de seguridad de la información.
- Participar en la realización de análisis de malware.
- Asistir en la generación de inteligencias y amenazas.
- Integrar fuentes de datos con soluciones SIEM y SOAR.
- Contribuir en la mejora de la detección de amenazas.
- Liderar la implementación de soluciones de ciberseguridad.
- Participar activamente en las tareas de análisis desarrolladas por el equipo del SOC.
- Operar dispositivos de seguridad.
- Administrar y generar herramientas de monitoreo.
- Colaborar en el armado de reglas, playbooks y capacitaciones para los analistas.
- Participar en la definición de nuevos servicios de ciberseguridad.
- Participar en procedimientos 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 del Área de Seguridad de la Información en función de sus competencias profesionales y/o personales.



Requisitos

Excluyentes:

- Formación:
 - Se requieren conocimientos técnicos en:
 - Redes de datos.
 - Seguridad de la información.
 - Administración de Servidores Linux y/o Windows.
- Se valorará:
 - Conocimientos en administración Infraestructura de TI en ambientes de alta criticidad.
 - Gestión de trazas de auditorías y eventos de sistemas (syslog/SIEM)
 - Hacking ético y/o análisis de vulnerabilidad.
 - Certificaciones y/o cursos en Redes, Infraestructura o virtualización.
 - Certificaciones y/o cursos en Seguridad de la Información.
 - Administración de plataformas virtualizadas.
 - Administración de WAF.
 - Dominio de Idioma inglés.



- Experiencia:
 - 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.
- Se valorará:
 - Experiencia en gestión de proyectos y proveedores de Tecnologías de la Información.
 - Experiencia en investigación con fuentes de datos abiertas (OSINT).
 - Experiencia en diseño de arquitecturas seguras.

Competencias claves

- 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.