Términos de referencia (TDR)

Profesional de Asistencia Técnica DTIC para Infraestructura y Seguridad TIC

A- Informaciones básicas del puesto

Identificación del puesto	Profesional de Asistencia Técnica DTIC para Infraestructura y Seguridad TIC
Vacancias	1 (una)
Dependencia en la cual prestará servicios	Programa PROCIENCIA
Ubicación física del puesto	Dr. Justo Prieto N°223 entre Teófilo del Puerto y Nicolás Billof, Villa Aurelia, Asunción
Modalidad de vinculación	Contratación temporal
Honorario Total	₲ 128.700.000, IVA INCLUIDO
Plazo de vigencia del contrato	Desde la firma del contrato hasta el 31/12/2022 el cual podrá ser renovado previa evaluación del desempeño y necesidades del programa.
Importe del contrato y forma de pago	El importe total del contrato será de ₲ 128.700.000[1], el cual será financiado de la siguiente manera: a la firma del contrato ₲ 9.900.000; contra presentación y aprobación de 10 informes de avance (cada informe tendrá un valor de ₲ 9.900.000); contra presentación y aprobación de informe final ₲ 19.800.000. El cronograma de presentación de informe será definido en el contrato de prestación de servicio. El contratado/a deberá emitir factura legal y certificado de cumplimiento tributario para el cobro de sus honorarios.

B- Informaciones generales del puesto

Objetivo general	Adoptar e implementar un marco de ciberseguridad estándar para asegurar la disponibilidad e integridad de los servicios de infraestructura, sistemas informáticos y bases de datos.
Objetivos específicos	Administrar servidores, bases de datos e infraestructura TIC. Implementar controles críticos de ciberseguridad CIS. Asegurar la disponibilidad del servicio de correo electrónico. Establecer niveles mínimos de disponibilidad de los servicios de infraestructura para la adecuada operación de los sistemas informáticos. Prevenir ciberataques. Identificar ciberincidentes y ciberataques. Planificar la respuesta en casos de desastre.

[1] El monto total del contrato podrá variar conforme a la fecha de firma del contrato. Este cálculo está basado considerando que el inicio de los servicios será en enero del año 2022.

	Identificar y evaluar vulnerabilidades en la infraestructura y los sistemas. Implementar las contramedidas de ciberseguridad resueltas en el Comité de Seguridad de la Información.
Alcance del trabajo	El trabajo será realizado en el marco del programa PROCIENCIA, ejecutado por el CONACYT
Descripción de actividades, según objetivos específicos	**Implementar controles críticos de ciberseguridad CIS.** Evaluar e implementar software de automatización que ejecute las acciones para la implementación efectiva de cada sub control. Monitorear la actividad del software implementado para automatización de sub controles. **Asegurar la disponibilidad del servicio de correo electrónico.** Identificar y controlar los factores que influyen en la operación de los servidores y software para correo electrónico. Implementar y mantener software de monitoreo de contenido malicioso. **Establecer niveles mínimos de disponibilidad de los servicios de infraestructura para la adecuada operación de los sistemas informáticos.** Construir indicadores para la medición de la disponibilidad de cada servicio. Monitoreo de forma continua los indicadores y registrar los datos generadores para construir estadísticas. **Prevenir ciberataques.** Establecer mecanismos y métodos para evitar el movimiento lateral, escalada de privilegios administrativos y ataques remotos. Verificar continuamente la efectividad de los mecanismos y métodos de prevención. **Identificar ciberincidentes y ciberataques.** Caracterizar los eventos de ciberseguridad para clasificarlos en ciberincidentes y ciberataques mediante el monitoreo continuo y la administración de eventos utilizando software especializado. **Planificar la respuesta en casos de desastre.** Formular y actualizar políticas de respuestas en casos de desastre y técnicas de equipo rojo. Evaluar la implementación del plan después de un desastre y presentar informes que incluyan parámetros como RTO y RPO. **Identificar y evaluar vulnerabilidades en la infraestructura y los sistemas.** Realizar cada año una evaluación de vulnerabilidades (GAP Analysis). Realizar por lo menos dos pen testing con objetivos específicos por año. **Implementar las contramedidas de ciberseguridad resueltas en el Comité de Seguridad de la Información.** Utilizar el estándar NIST para la implementación de las contramedidas a nivel operacional.
Resultados esperados	Implementar controles críticos de ciberseguridad CIS. **Resultado**: *Informe semestral calificado del 1 al 4 sobre el nivel de implementación de cada control*.

	Asegurar la disponibilidad del servicio de correo electrónico. **Resultado**: *informe anual de disponibilidad del servicio mayor al 99%.* Establecer niveles mínimos de disponibilidad de los servicios de infraestructura para la adecuada operación de los sistemas informáticos. **Resultado**: Niveles mínimos de disponibilidad establecidos en una política aprobada por resolución. Identificar ciberincidentes y ciberataques. **Resultado**: Informe anual sobre ciberincidentes y ciberataques detectados y respondidos, aunque estos no hayan escalado. Planificar la respuesta en casos de desastre. **Resultado**: Diseñar y actualizar anualmente una política de respuesta en casos de desastre que debe ser aprobada por resolución. Identificar y evaluar vulnerabilidades en la infraestructura y los sistemas. **Resultado**: informes anuales al Comité de Seguridad de la Información sobre el resultado del GAP Analysis y recomendaciones para la mitigación de vulnerabilidades. Implementar las contramedidas de ciberseguridad resueltas en el Comité de Seguridad de la Información. **Resultado**: Informe semestral de implementación y sus resultados presentado al Comité de Seguridad de la Información.
Supervisión e informes	El contratado/a trabajará bajo la supervisión de la DTIC y esta instancia verificará los informes del contratado.
Otras observaciones	El contratado/a podrá desarrollar sus actividades en las oficinas que el CONACYT establezca como sede, el CONACYT proporcionará todas las facilidades que sean necesarias para la buena ejecución de los servicios prestados tales como: espacio de trabajo, muebles y equipos de oficina, material y equipos de escritorio todo dentro de las normas vigentes para la utilización de los bienes del estado. Se tendrá en cuenta los antecedentes y referencias de los postulantes con relación a contratos previos con el CONACYT y con otras instituciones públicas y/o privadas. Si el postulante es actualmente beneficiario de los programas y/o proyectos ejecutados por el CONACYT (como ser PROCIENCIA, PROINNOVA, entre otros) deberá renunciar a su calidad de beneficiario en caso de resultar ganador del puesto.

C- Perfil requerido

Componente	Requisitos mínimos (excluyente)	Requisitos ideales
Experiencia laboral general	4 años en instituciones públicas o privadas.	5 años en instituciones públicas o privadas.

Componente	Requisitos mínimos (excluyente)	Requisitos ideales
Experiencia profesional específica	2 años en instituciones públicas y/o privadas en el área de infraestructura y/o ciberseguridad, específicamente: -Administración de Hypervisor (VmWare) para la gestión de máquinas virtuales. -Administración de Servidores y Servicios (Apache2, Tomcat, DNS, Proxy, Fail2ban (iptables), Jasperserver, Correo, Mail Gateway, Alient Vault, SVN, LDAP) -Administración de Servicios de Gestores CMS (Drupal, Alfresco, Wordpress, Moodle, Vufind, Dspace) -Administración de Base de Datos (Mysql, Postgres) -Administración de Firewall de Borde Fortigate -Administración de consola de Antivirus -Gestión de Software de Backup Veeam	4 años en instituciones públicas y/o privadas en el área de infraestructura y/o ciberseguridad: específicamente: -Administración de Hypervisor (VmWare) para la gestión de máquinas virtuales. -Administración de Servidores y Servicios (Apache2, Tomcat, DNS, Proxy, Fail2ban (iptables), Jasperserver, Correo, Mail Gateway, Alient Vault, SVN, LDAP) -Administración de Servicios de Gestores CMS (Drupal, Alfresco, Wordpress, Moodle, Vufind, Dspace) -Administración de Base de Datos (Mysql, Postgres) -Administración de Firewall de Borde Fortigate -Administración de consola de Antivirus -Gestión de Software de Backup Veeam -Implementación de SIEM (*Security Information and Event Manager*.
Formación académica	Profesional Universitario de las carreras en el área de las Tecnologías de la Información y Comunicación (TIC).	Maestría/Especialización en seguridad de la información, ciberseguridad o similares.
Eventos de capacitación	Se valorarán los cursos y/o diplomados realizados en los últimos 5 (cinco) años y con una carga horaria mínima de 40 (cuarenta) horas, en: Herramientas de ciberseguridad, IPS/IDS., dispositivos de seguridad de redes, seguridad en bases de datos, Certificaciones en TIC, Cursos o talleres prácticos de ciberseguridad, Hackatones y afines.	
Principales competencias	**Competencias técnicas y habilidades** Orientación específica hacia el área de ciberseguridad con habilidades para la implementación de medidas y contramedidas, manejo de ciberincidentes y ciberataques y capacidad de identificación y valoración de riesgos. Capacidad de comunicar los eventos y las cuestiones relacionadas a infraestructura en lenguaje no técnico. **Competencias cardinales** Capacidad de relacionamiento interpersonal; capacidad de liderazgo; capacidad de trabajo bajo presión; trabajo de equipos multidisciplinario; compromiso con la calidad de trabajo; iniciativa; integridad; flexibilidad; autocontrol; responsabilidad.	

Matriz de evaluación

Identificación del convocante: Consejo Nacional de Ciencia y Tecnología (CONACYT)
Identificación del programa: Programa PROCIENCIA
Identificación del puesto en evaluación: Profesional de Asistencia Técnica DTIC para Infraestructura y Seguridad TIC

Código del Postulante	Formación académica			TOTAL	Experiencia laboral general		Experiencia profesional específica		**TOTAL**	**Entrevista**	TOTAL GENERAL
	Requisito excluyente (cumple/no cumple)	Posgrados (hasta 20 puntos)	Cursos de capacitación (hasta 10 puntos)	Hasta 30 puntos	Requisito excluyente **(15 puntos)**	Experiencia laboral general (hasta 20 puntos)	Requisito excluyente (25 puntos)	Experiencia profesional específica (hasta 35 puntos)	Hasta 55 puntos	Hasta 15 puntos	Hasta 100 puntos
Postulante 1											
Postulante 2											
Postulante 3											

1- Formación académica

1.1 Grado

Título académico de grado según lo establecido en los términos de referencia (excluyente)

1.2 Posgrados

Para la asignación de los puntos el postulante deberá adjuntar la documentación respaldatoria de su formación académica. La puntuación de la formación académica no es acumulable, se otorga el puntaje equivalente a la última formación académica declarada conforme a los requerimientos del perfil. Se tomará el mayor de los puntajes entre (a) (b) (c)

(a) Maestría con énfasis en áreas solicitadas en los términos de referencia (finalizado) (20 puntos)
(b) Maestría con énfasis en áreas solicitadas en los términos de referencia (en curso) (18 puntos)
(c) Especialización con énfasis en áreas solicitadas en los términos de referencia (15 puntos)

En el caso de que el postulante disponga otros títulos de posgrado superiores a la maestría (por ejemplo doctorado) en las áreas requeridas en los términos de referencia se asignará el total de puntos para este criterio (20 puntos)

1.3 Cursos de capacitación

Los cursos de capacitación tendrán una puntuación máxima de 10 puntos. Serán consideradas aquellas capacitaciones realizadas en los ultimos 5 años y con una carga horaria mínima de 40 horas, en las áreas establecidas en los términos de referencia. No se realizará asignación proporcional de puntaje según las cargas horarias de las capacitaciones presentadas.
Para la asignación de los puntos el postulante deberá adjuntar los certificados de las capacitaciones. Se otorgará 2 (dos) puntos por cada curso y/o diplomado en áreas establecidas en los términos de referencia (hasta 10 puntos)

2- Experiencia laboral general/Experiencia profesional específica

2.1 Experiencia laboral general

Se aplica a las demás experiencias no consideradas como específicas. No se admitirá duplicación de puntuación, la Comisión de Selección deberá iniciar el análisis por la experiencia específica, en caso de que el postulante supere los años solicitados, el excedente deberá puntuar como experiencia general. Para situaciones inversas, no aplica. Para la asignación de los puntos el postulante debe declarar y adjuntar certificados y/o constancias de las experiencias laborales.

(a) Para la experiencia laboral excluyente establecida en los términos de referencia, se otorgará 15 puntos. (b) Para el requisito ideal se otorgará 20 puntos. Se tomará el mayor de los puntajes entre (a) y (b).

2.2 Experiencia profesional específica

Se aplica a la experiencia de los postulantes en funciones o naturalezas de trabajos relacionados directamente con las actividades que se describen en los términos de referencia, esta experiencia se considerará desde la obtención del título de grado. Para la asignación de los puntos, el postulante debe declarar y adjuntar certificados y/o constancias de las experiencias laborales.

(a) Para la experiencia profesional específica excluyente establecida en los términos de referencia, se otorgará 25 puntos

(b) Experiencia profesional específica de 3 (tres) años en cargos descritos en los términos de referencia, se otorgará 30 puntos

(c) Experiencia profesional específica de 4 (cuatro) años o más en cargos descritos en los términos de referencia, se otorgará 35 puntos

3- Entrevista

Será aplicada por la Comisión de Selección y estará basada en las competencias solicitadas en el perfil.

Otras Observaciones:

Documentación requerida a los postulantes para evaluarlos:

Documentos Excluyentes:

-Fotocopia de Cedula de Identidad Vigente (ambos lados)
-Fotocopia del Título Universitario Legalizado en el Rectorado de la Universidad e Inscripto y Legalizado en el MEC
-Constancia de trabajo, certificado y/o contrato en el que avale la experiencia laboral

Documentos No Excluyentes

Fotocopia simple de Constancia de eventos de capacitación
Fotocopia del Título de Posgrado Legalizado en el Rectorado de la Universidad e Inscripto y Legalizado en el MEC
Fotocopia de certificados o constancias de estudios de posgrados

Documentos No Excluyentes

Documentos para Adjudicación del Puesto

-Certificado de Antecedentes Policiales vigente
-Certificado de Antecedentes Judiciales vigente

Criterios De Desempate:

1. Formación Académica: Quien posea mayor puntaje en Formación Académica
2. Experiencia Específica: Quien posea mayor puntaje en experiencia específica.
3. Eventos De Capacitación: Quien posea mayor puntaje en eventos de capacitación relacionados al puesto, en caso de igualdad de puntaje se corroborará la cantidad de carga horaria total declarada.
4. Si persiste la paridad, se verificará la Experiencia Laboral, a favor del postulante con más años de Experiencia Laboral total declarada.
5. Si persiste la paridad, la Comisión de Selección definirá el indicador de desempate a ser aplicado.

Información Complementaria

La no presentación de alguno de los documentos excluyentes será de descalificación automática.
Para las constancias laborales presentar con las siguientes características (con membretes, números telefónicos para la reverificación, periodo de tiempo trabajado con fecha de inicio y finalización del mismo, cargo y/o función desempeñado y firma del anterior empleador). Los documentos de adjudicación serán requeridos al concursante seleccionado al cargo luego de todo el proceso de evaluación.
Los documentos no excluyentes no eliminarán al concursante del proceso, pero la no presentación implicará la no puntuación en la matriz de evaluación.

Puntuación mínima

El postulante deberá obtener por lo menos el 60% del puntaje total establecido en la evaluación curricular para pasar a la siguiente evaluación (entrevistas)