Ministerio de Economía y Finanzas

INVITACION A PRESENTAR EXPRESIONES DE INTERES (SERVICIOS DE CONSULTORIA-SELECCIÓN DE FIRMAS)

REPUBLICA ORIENTAL DEL URUGUAY
PROYECTO MEJORA DE SERVICIOS DE GOBIERNO ELECTRONICO A CIUDADANOS Y EMPRESAS (PROMESeG)

PRESTAMO BANCO MUNDIAL Nº 8778-UY

Llamado a Firmas Consultoras a presentar Expresiones de Interés para integrar la Lista Corta para la Consultoría para el DESARROLLO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) en Centro Ceibal

Referencia No.: 1-2-2-4 CF SBCC

El Gobierno de la República Oriental del Uruguay ha recibido un financiamiento del Banco Mundial a través del "Proyecto de Mejora de Servicios de Gobierno Electrónico para Ciudadanos y Empresas" (PROMESeG) y prevé utilizar parte de los fondos del Préstamo Nº 8778-UY para la contratación de servicios de consultoría.

El Proyecto se articula en cuatro componentes: 1) Mejora de la Prestación de los Servicios de Gobierno Electrónico a los Ciudadanos; 2) Mejora de la Prestación de Servicios de Gobierno Electrónico a las Empresas; 3) Mejora de la Prestación de los Servicios de Gobierno Electrónico a Organismos Públicos y 4) Diagnósticos Estratégicos, Intercambio de Actividades y Conocimiento, y Coordinación de Proyecto.

Los servicios de consultoría ("los servicios") comprenden la contratación de una firma consultora para apoyar al Centro Ceibal en su proceso de fortalecimiento institucional y profesionalización de la gestión, colaborando en la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), basado en los requisitos de la Norma Internacional ISO-27001:2013 y en la mejora del proceso de Gestión de la Continuidad del Negocio.

El Ministerio de Economía y Finanzas (MEF) invita a las firmas consultoras elegibles a expresar su interés en prestar los servicios solicitados. Los consultores interesados deberán proporcionar información que indique que tienen una experiencia relevante y están calificados para suministrar los servicios.

Los Términos de Referencia (TDR) detallados para esta consultoría se encuentran publicados como un adjunto a este Llamado a Expresiones de Interés.

A efectos de la decisión de manifestar interés, y de un eventual contrato, las firmas consultoras interesadas deberán tener en cuenta las causales de conflicto de interés y elegibilidad establecidas en las "Regulaciones de Adquisiciones para Prestatarios en Proyectos de Inversión del Banco Mundial" de Julio de 2016 revisada en noviembre 2017 y agosto 2018, parágrafos 3.14, 3.16 y 3.17. Asimismo, el Banco Mundial exige que se apliquen y se observen sus normas de lucha contra la corrupción, que incluyen, entre otras cosas, el derecho del Banco a sancionar, inspeccionar y realizar auditorías (Anexo IV, Fraude y Corrupción). https://projects.worldbank.org/en/projects-operations/products-and-services/brief/procurement-new-framework#framework
http://www.worldbank.org/en/projects-operations/products-and-services/brief/procurement-new-framework

OBJETIVO DE LA CONSULTORÍA:

Asistir al Centro Ceibal en la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), a través de la mejora del proceso de Gestión de la Continuidad del Negocio, y la preparación y capacitación necesarias para una certificación en el marco de la Norma Internacional ISO-27001:2013.

El monto estimado para la consultoría asciende a USD 91.000.- (dólares estadounidenses noventa y un mil), impuestos incluidos.

LOS CRITERIOS PARA LA SELECCIÓN DE LA LISTA CORTA SON LOS SIGUIENTES:

Antecedentes y experiencia de las empresas oferentes:

- Actividad principal: Consultoría - Consultoría en tecnología, ciberseguridad y continuidad del negocio.

- Antigüedad de la firma: Mínimo para ser considerado 2 años.

- Proyectos de consultoría relativos a la Seguridad de la Información y la Continuidad del Negocio implementados en empresas uruguayas de mediano o gran porte, detallando cantidad, duración y montos en dólares aproximados de los proyectos: **mínimo para ser considerado 3 proyectos en los últimos 5 años.**

- Capacidad técnica relativa a la Seguridad de la información y la Continuidad del Negocio, detallando si existen departamentos o secciones específicas dedicadas a estos temas, certificaciones que se posean a nivel corporativo y a nivel de los recursos humanos (no se evaluarán los antecedentes del personal clave en esta etapa): Mínimo 1 persona con certificaciones relativas a Seguridad de la Información y/o Continuidad del Negocio.

- Auditorías realizadas en el marco de la norma ISO 27001:2013 en empresas uruguayas de mediano o gran porte, detallando cantidad, duración y monto en dólares aproximado de las mismas (**mínimo 3 auditorías**).

Asimismo, deberán presentar una nota declarando ser sujeto de derecho habilitado a ejercer el comercio, con la siguiente información:

a) nacionalidad (en el caso de ser nacional deberá ser sociedad comercial constituida en el territorio nacional, según alguno de los tipos societarios establecidos en el Código de Comercio, en la Ley 16.060 del 5 de setiembre de 1989 y demás normas legales concordantes),

b) dirección,

c) número de teléfono, fax y dirección de correo electrónico y

d) razón social y RUT ("Registro Único Tributario" para firmas nacionales o su equivalente para firmas extranjeras).

Este llamado se orienta a la contratación de una firma consultora, utilizando el procedimiento **de Selección Basada en Calidad y Costo (SBCC)**, de acuerdo con las Regulaciones de Adquisiciones para Prestatarios en Proyectos de Inversión del Banco Mundial de julio de 2016 Revisadas en noviembre 2017 y agosto 2018. Para ello se requiere precalificar a una lista corta de entre 5 y 8 proponentes interesados en la presentación de las respectivas ofertas.
https://projects.worldbank.org/en/projects-operations/products-and-services/brief/procurement-new-framework#framework

Las firmas consultoras que resulten seleccionadas para integrar la Lista Corta deberán estar en **Estado: En Ingreso**, en el Registro Único de Proveedores del Estado (RUPE) **(***Estado: Activo ,en el momento de la Adjudicación, a los efectos de estar en condiciones de poder contratar con el organismo*[1]**)**.

En esta instancia del proceso no se requiere la presentación de información relacionada con los recursos humanos de las firmas consultoras. **La información presentada en referencia al equipo de trabajo propuesto no será tenida en consideración**

Las empresas consultoras que resulten seleccionadas para integrar la Lista Corta serán convocadas a una reunión informativa (presencial o virtual, dependiendo de las condiciones sanitarias), en donde se realizará una presentación del Centro Ceibal y los servicios de consultoría en cuestión. Esto permitirá evacuar dudas y establecer mejor el alcance de la consultoría, en beneficio de la calidad de las propuestas a presentar.

Las empresas que participan en contratos financiados por el Banco pueden conformar Asociaciones Temporales con empresas nacionales o extranjeras para mejorar sus calificaciones y capacidades. Las asociaciones temporales pueden ser de largo plazo (independientes de un proceso de adquisición en particular) o conformarse para participar en un proceso de adquisición específico. Todos los miembros de la asociación temporal serán conjunta y solidariamente responsables por la totalidad del contrato.

En caso de optar por la subcontratación o un acuerdo de sub-consultoría, llegado el momento de la evaluación de las propuestas de las firmas que finalmente conformen la "lista corta", solamente se evaluarán a los subcontratistas y subconsultores en los criterios "Enfoque Técnico", "Enfoque Metodológico" y "Calificaciones del personal profesional clave y competencia para el trabajo".

Será responsabilidad de la firma garantizar que sus expertos, subcontratistas, los integrantes de Asociaciones Temporales, cumplan con los requisitos de elegibilidad, según lo dispuesto en los párrafos 3.21, 3.22 y 3.23 del capítulo de Elegibilidad de las Regulaciones de Adquisiciones para Prestatarios en Proyectos de Inversión del Banco Mundial de julio de 2016.

Las firmas consultoras que resulten seleccionadas para conformar la lista corta no podrán consorciarse entre sí para presentar propuesta (técnica y financiera).

Las expresiones de interés deberán ser entregadas en:

- **Dirección:** Colonia 1089 Planta Baja (personalmente o por correo postal) **Unidad Coordinadora de Proyectos**, **Sector**: Adquisiciones, o
- Correo electrónico a ucp.llamados@mef.gub.uy ,

Plazo: a más tardar el **23 de mayo de 2022 a las 12 horas**.

En caso de presentarlas personalmente o por correo postal se requiere **original y copia impresos** (foliados) y una **copia del original firmado en formato "pdf" en medio magnético** (en DVD, CD, pendrive o vía email). En caso de discrepancias entre ambas versiones, primará la versión impresa.

[1] Para obtener más información sobre la inscripción visitar el portal de la Agencia de Compras y Contrataciones del Estado (ACCE), responsable del funcionamiento del RUPE. Link directo a las guías de inscripción: http://www.comprasestatales.red.uy/inicio/proveedores/rupe/como-inscribirse/ . Tener en cuenta que todos los proveedores que se encontraban registrados en la Tabla de beneficiarios de SIIF, automáticamente estarán en el RUPE, en estado "en ingreso", pero deberán completar la inscripción y quedar "activos" en el sistema. Será necesario encontrarse al menos en estado "en ingreso" para poder ofertar y en estado "activo" para poder resultar adjudicado en procedimientos de compra.

Los correos electrónicos deberán estar identificados en el Asunto: "**PROMESEG - Expresión de Interés Consultoría DESARROLLO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) en Centro Ceibal.**

"*Para la correcta recepción de los e-mails con dirección ucp.llamados@mef.gub.uy, los proveedores de servicios de correo (Gmail, Hotmail y eventualmente otros) requieren que nuestra dirección esté ingresada en la lista de contactos de su correo electrónico, de lo contrario nuestras comunicaciones le podrían llegar como SPAM o no ser le entregadas* ".

Los sobres (en caso de entrega personal o por correo postal) deberán estar identificados en el exterior con la siguiente leyenda:

Nombre de la oficina: UNIDAD COORDINADORA DE PROYECTOS - MEF
Atn: PROYECTO MEJORA DE SERVICIOS DE GOBIERNO ELECTRONICO A CIUDADANOS Y EMPRESAS (PROMESEG)
Dirección: COLONIA 1089 PLANTA BAJA – CP 11.100 - MONTEVIDEO –URUGUAY
Proceso: "**Consultoría DESARROLLO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) en Centro Ceibal". - *Expresión de Interés***.

CONSULTAS o ACLARACIONES: serán recibidas únicamente vía correo electrónico, a la siguiente dirección de e-mail: ucp.llamados@mef.gub.uy , hasta 5 días hábiles antes de la fecha prevista para la recepción de expresiones de interés **(hasta el 13/05/2022)**.
Las respuestas a las consultas serán publicadas conjuntamente con la pregunta en las páginas web del Ministerio de Economía y Finanzas y del Centro Ceibal, así como en el portal de la Agencia de Compras Estatales (https://www.mef.gub.uy y https://www.comprasestatales.gub.uy).

Ministerio de Economía y Finanzas

PROYECTO DE MEJORA DE SERVICIOS DE GOBIERNO ELECTRÓNICO A CIUDADANOS Y EMPRESAS (PROMESEG)

PRÉSTAMO Nº 8778-UY (BANCO MUNDIAL)

TÉRMINOS DE REFERENCIA

CONSULTORÍA PARA EL DESARROLLO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

1. ANTECEDENTES

Con fecha 7 de noviembre de 2017 se suscribió el Convenio de Préstamo Nº 8778-UY, destinado a financiar el "Proyecto de Mejora de Servicios de Gobierno Electrónico a Ciudadanos y Empresas" (PROMESeG), entre la República Oriental del Uruguay y el Banco Internacional de Reconstrucción y Fomento (Banco Mundial).

El objetivo general del Proyecto consiste en la mejora de la calidad de servicios de gobierno electrónico para los ciudadanos, empresas y los organismos públicos del Prestatario, para lo cual se debe alcanzar un acceso a estos servicios más equitativo y eficiente y construir el entorno propicio para un Uruguay más competitivo e innovador.

El Proyecto se articula en torno a 4 componentes:

Componente 1. Mejora de la Prestación de los Servicios de Gobierno Electrónico a los Ciudadanos con dos subcomponentes. Este componente apunta a mejorar la calidad de servicios seleccionados de gobierno electrónico a ciudadanos y facilitar su acceso a través de actividades enfocadas principalmente en el soporte de las mejoras a los sistemas de prestaciones de los organismos, gestión de proveedores y compromiso del usuario dirigido por AGESIC y el Centro Ceibal.

Componente 2. Mejora de la Prestación de Servicios de Gobierno Electrónico a las Empresas. Este componente apunta a la mejora de la calidad de servicios seleccionados de gobierno electrónico y a facilitar el acceso a través de actividades que den soporte a las mejoras de los sistemas de prestaciones (incluyendo el alcance de los servicios), gestión de proveedores y colaboración entre entidades dentro de VUCE, DGI, y ANII.

Componente 3. Mejora de la Prestación de los Servicios de Gobierno Electrónico a Organismos del Estado. Este componente apunta a la mejora de la calidad de determinados servicios de gobierno electrónico a organismos públicos y facilitar su acceso a través de actividades de que apoyen mejoras para el monitoreo de los pagos a proveedores y gestión de proveedores, sistema de entrega del Estado y colaboración entre los organismos con CGN, MEF, y otros organismos con una vinculación directa a las prioridades del MEF.

Componente 4. Diagnósticos Estratégicos, Actividades Compartidas e Intercambio de conocimientos, y Coordinación del Proyecto. Este componente apunta a fortalecer la capacidad del Estado para dar apoyo a reformas estratégicas en áreas que son críticas para el logro del Objetivo de Desarrollo del Proyecto (ODP).

2. BREVE DESCRIPCIÓN DEL COMPONENTE

Componente 1. Mejora de la Prestación de los Servicios de Gobierno Electrónico a Ciudadanos, Subcomponente 1.2 Fortalecimiento de la capacidad del Centro Ceibal de gestionar sus programas de e-aprendizaje. 1.2.2. CSIRT - Centro de Respuesta a Incidentes de Seguridad Informática.

3. ANTECEDENTES DEL CENTRO CEIBAL

El centro Ceibal se encuentra en proceso de implementación de un SGSI (Sistema de Gestión de Seguridad de

la Información) alineado a las buenas prácticas internacionales y adoptando el MCA (Marco de Ciberseguridad de AGESIC) como marco de referencia. El mismo se implementa a través de una serie de iniciativas y proyectos que implican acciones de mejoras a nivel de procesos, concientización y capacitación del personal e implementación de controles tecnológicos. De acuerdo al plan de implementación actual se considera necesario y fundamental el implementar un Plan de Continuidad del Negocio (BCP) desarrollando el proceso transversal y la documentación pertinente.

Para la implementación del SGSI, Centro Ceibal ha mejorado su estructura organizacional adecuándose a las necesidades en materia de seguridad de la información, trabajando en la gobernanza de la misma. Es así que se ha creado un Comité de Seguridad de la Información (conformado por las principales gerencias del Centro), un Grupo de Trabajo de Seguridad de la Información (conformado por referentes operativos de los principales sectores del Centro) y un equipo de seguridad de la información que integra el CSIRT (Centro de Respuesta a Incidentes de Seguridad, conformado por personal técnico idóneo en ciberseguridad) con el cometido de mejorar el nivel de madurez relativo a seguridad de la información.

4. OBJETO DE LA CONTRATACIÓN

El objetivo general de esta consultoría es asistir al Centro Ceibal en su proceso de fortalecimiento institucional y profesionalización de la gestión, colaborando en la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en las buenas prácticas a nivel internacional, en la mejora del proceso de Gestión de la Continuidad del Negocio y en la preparación y capacitación necesarias para una certificación en el marco de la Norma Internacional ISO-27001:2013. En este sentido, se deberán cumplir los siguientes objetivos:

1. Apoyar y guiar al equipo de Seguridad de la Información de Centro Ceibal en la elaboración de la documentación necesaria (políticas, procedimientos y demás documentos) para el desarrollo del Sistema de Gestión de Seguridad de la Información.
2. Realizar el diseño e implementación del proceso formal de la Continuidad del Negocio integrándolo en un marco general de gestión de riesgos y en particular con el Sistema de Gestión de Seguridad de la Información (SGSI).
3. Capacitar al equipo de Seguridad de la Información y el equipo de referentes del Centro Ceibal para el desarrollo de los conocimientos y habilidades necesarias para la correcta implementación del proceso de continuidad del negocio y la implementación del SGSI.
4. Asistir al equipo de Seguridad de la Información de Centro Ceibal en la preparación para el proceso de certificación en ISO 27001: 2013.
5. Auditar el Sistema de Gestión de Seguridad de la Información como paso previo a la certificación en ISO 27001:2013.

Alcance de la consultoría

La consultoría se estructurará en dos fases:

Fase 1: Con el objetivo principal de elaborar un Plan de Continuidad del Negocio.
Fase 2: Con el objetivo principal de preparar la certificación en Seguridad de la Información del Centro Ceibal en el marco de la norma ISO 27001:2013.

FASE 1

A los efectos de acotar el alcance de la consultoría y generar resultados en el corto plazo, se delimitarán las actividades y procesos en los que se deberá generar un apoyo con entregables concretos de acuerdo a los siguientes objetivos:

1. Elaboración de un Plan de Continuidad del Negocio (BCP).

a. Elaboración de un Análisis de Impacto en el Negocio (BIA).
b. Elaboración de un Plan de Recuperación de Desastres (DRP).

2. Elaboración de la matriz de riesgos de activos de la información del Centro Ceibal.

FASE 2

1. Revisión de la documentación del proceso de Gestión de la Seguridad de la Información con el objetivo de lograr la certificación en ISO 27001:2013.
2. Capacitación del equipo de Seguridad de la Información y referentes del Centro Ceibal para el desarrollo de conocimientos y habilidades necesarias para la implementación de los procesos que componen el SGSI, y su posterior mantenimiento.
3. Realizar una auditoría de los procesos que componen el SGSI con el objetivo de lograr la certificación en ISO 27001:2013.

5. PROPUESTA

REQUERIMIENTOS

5.1 ACTIVIDADES

A partir de los objetivos previamente identificados, se espera que el equipo consultor desarrolle las siguientes actividades en coordinación con el equipo de Seguridad de la Información.

FASE 1

1. Elaborar el Análisis de Impacto en el Negocio (BIA).
2. Elaborar la matriz de riesgos de activos de información.
3. Elaborar el Plan de Continuidad del Negocio (BCP).
4. Elaborar el Plan de Recuperación de Desastres (DRP).
5. Colaborar en la ejecución del set de pruebas de verificación de los planes desarrollados.

FASE 2

1. Realizar capacitaciones al equipo de Seguridad de la Información y referentes del Centro Ceibal para desarrollar los conocimientos y habilidades necesarios para el desarrollo y posterior mantenimiento y evolución del Sistema de gestión de Seguridad de la Información.
2. Colaborar en desarrollar los procesos de implementación del SGSI, aportando metodología, buenas prácticas y documentación que permita mejorar el nivel de madurez del SGSI en un proceso de mejora continua.
3. Asistir al equipo de Seguridad de la Información en la implementación del Sistema de Gestión de Seguridad de la Información. Revisar la documentación elaborada por el equipo y dar “feedback” para su mejora.
4. Realizar una auditoría preparatoria para la certificación ISO 27001.
5. Generar una propuesta de mejora en base a los hallazgos encontrados en la auditoría.

5.2 PERSONAL CLAVE

Para el cumplimiento de las actividades se espera que el consultor presente un equipo de trabajo conformado como mínimo por tres integrantes con los siguientes perfiles, **el no cumplimiento supondrá que la propuesta no sea evaluada**:

1. Un Jefe de Proyecto: Responsable de la gestión del proyecto, principal contraparte para la planificación y seguimiento de actividades y coordinación del equipo de trabajo. Profesional universitario del área ingeniería, con experiencia comprobable mínima de 5 años en gestión de proyectos relacionados con los procesos de Seguridad de la Información y Continuidad del Negocio.

2. Dos Consultores: Responsables de la ejecución y coordinación de las actividades de relevamiento y diseño y elaboración de entregables. Profesionales universitarios del área de ingeniería con experiencia mínima de 5 años de consultoría en proyectos relacionados con los procesos de Seguridad de la Información y Continuidad del Negocio.

El equipo de trabajo de la FASE 1 deberá contar con experiencia en implementación de planes de continuidad del negocio. El equipo de trabajo de la FASE 2 deberá contar con experiencia en impartir capacitaciones y realizar auditorías. Los equipos de trabajo de la FASE 1 y la FASE 2 podrán ser los mismos.

Esto no implica que este sea el único personal clave a presentar en la propuesta, sino que es la definición mínima aceptable. En el proceso de selección solo se evaluará al personal clave presentado.

El oferente debe presentar un Organigrama del Proyecto a desarrollar, el cual deberá contener el equipo mínimo requerido detallando los roles, perfiles y dedicación horaria de sus integrantes (en el organismo y fuera del organismo), así como el personal adicional que éste asignará al proyecto. Se valorará la formación, especialización y experiencia específica en las áreas que desarrollarán actividades, así como el poseer certificaciones relacionadas a los procesos de Seguridad de la Información y Continuidad del Negocio, como por ej.: CISSP, CISA, CRISC, CISM, SSCP.

Las tareas de relevamiento, así como las reuniones de coordinación, presentación de informes y documentación y demás actividades a ser desarrolladas por el equipo de trabajo de los consultores podrán ser en modalidad presencial y/o virtual a través de herramientas de videoconferencia. Centro Ceibal se reserva el derecho a decidir la mejor modalidad de trabajo de acuerdo a las condiciones sanitarias vigentes al momento de realizar la consultoría.

Equipo de proyecto	**Lugar en la propuesta** (#página)
Organización propuesta para el desempeño de los servicios solicitados.	
Para cada recurso a afectar al proyecto, detallar la formación (*Completar formulario CV*), certificaciones, experiencia y el rol que desempeñará en el proyecto, la dedicación total que tendrán expresada en horas por consultor asignado y la distribución en el transcurso del proyecto.	

Equipo de contraparte de CEIBAL

Participaran en la implementación del SGSI el equipo de Seguridad de la Información conformado por el Jefe del sector y tres Analistas, así como referentes de distintos sectores del Centro Ceibal.

En particular, para la implementación del Plan de Continuidad del Negocio también se contará con la colaboración de funcionarios de los sectores relacionados a Calidad (Procesos), Telecomunicaciones y Tecnología de la Información. Para la fase 2 se contará con el equipo de Seguridad de la Información y el apoyo de un grupo de trabajo compuesto por distintos sectores del Centro Ceibal.

6. CONDICIONES DE SEGURIDAD DE LA INFORMACIÓN, PRIVACIDAD Y PROTECCIÓN DE DATOS

Se deberá cumplir con los requisitos de seguridad de la información, privacidad y protección de datos establecidos en el Anexo I

7. PRODUCTOS Y ENTREGABLES

Los entregables identificados para la FASE 1 de la consultoría son:

1. Documento Plan de Trabajo.
2. Documento de Análisis de Impacto en el Negocio (BIA).
3. Documento Matriz de Riesgos de Activos de Información.
4. Documento Plan de Continuidad del Negocio (BCP).
5. Documento Plan de Recuperación de Desastres (DRP).
6. Primer set de pruebas de la eficacia del BCP y el DRP auditado.
7. Informe final de la consultoría incluyendo las recomendaciones que surjan con el objetivo de lograr la certificación ISO 27001:2013.

Los entregables identificados para la FASE 2 de la consultoría son:

1. Plan de capacitación, con material incluido y constancia de dictado detallando cantidad de horas.
2. Constancia de relevamiento de los procesos del SGSI, incluyendo material de apoyo para la mejora de los procesos.
3. Informe de auditoría con el objetivo de la futura certificación en ISO 27001:2013, incluyendo detalles de las observaciones y demás hallazgos.
4. Plan de mejora con detalle de las actividades necesarias para una adecuada implementación del SGSI y la certificación ISO 27001:2013.

8. CRONOGRAMA DE ENTREGABLES Y PAGOS

Se propone el siguiente cronograma de trabajo tentativo, el cual podrá ser ajustado en conjunto al iniciar el proyecto.

CRONOGRAMA FASE 1

#	Entregable	Días corridos a partir de la firma del contrato	Pagos asociados
1	Documento - Plan de Trabajo	10	10%
2	Documento - Análisis de Impacto en el Negocio (BIA)	130	
3	Documento - Matriz de Riesgos de Activos de Información	160	30%
4	Documento - Plan de Continuidad del Negocio (BCP)	200	
5	Documento - Plan de Recuperación de Desastres (DRP)	240	30%
6	Set de pruebas de la eficacia del BCP y el DRP auditado	280	
7	Informe final de la consultoría incluyendo las recomendaciones que surjan con vistas al proceso de certificación en la ISO 27001:2013.	300	30%
	Duración estimada para la FASE 1 de la consultoría	**10 meses**	

CRONOGRAMA FASE 2

#	Entregable	Días corridos a partir de la firma del contrato	Pagos asociados
1	Documento - Plan de trabajo que incluya plan de capacitación	10	10%
2	Documento - Constancia de la capacitación al equipo de Seguridad de la Información y referentes del SGSI. Materiales de la capacitación	60	30%
3	Documento - Relevamiento de los procesos del SGSI, incluyendo sugerencias y mejoras prácticas para aumentar el nivel de madurez.	90	30%
4	Documento - Informe de auditoría diagnóstica con el objetivo de certificación futura en ISO 27001:2013. Hallazgos y plan de mejora a implementar.	150	30%
	Duración estimada para la FASE 2 de la consultoría	**5 meses**	

9. ANTECEDENTES DEL OFERENTE

La propuesta deberá incluir una relación de antecedentes de la empresa en consultorías similares a las del presente llamado, vinculados a: diseño de procesos de gestión de la seguridad de la información y gestión de la continuidad del negocio, implementación de ISO 27001 / 22301 y desarrollo de sistemas de gestión de la seguridad de la información.

Asimismo, deberá incluir personas de contacto en los clientes.

El contratante podrá contactar a las referencias a efectos de ampliar la información y corroborar los datos aportados.

Se deberán presentar los comprobantes que acrediten la antigüedad de la empresa e información sobre el inicio de las operaciones.

10. OTRAS CONSIDERACIONES

Centro Ceibal suministrará al consultor la siguiente documentación y procesos disponibles como insumos para la consultoría:

- Inventario de activos de información del Centro Ceibal
- Inventario de procesos y subprocesos del Centro Ceibal

El Centro Ceibal tiene implementado un Sistema de Gestión de Calidad (SGC) certificado en ISO 9001:2015. Como referencia del esfuerzo en la elaboración de los entregables se brinda el mapa de procesos del Centro Ceibal (Anexo II).

11. PROPUESTA ECONÓMICA

Se deberá presentar una Propuesta Financiera con el valor de la hora de la consultoría para cada uno de los perfiles clave.

Las propuestas deberán ser cotizadas en dólares de los Estados Unidos de América, detallando por separado todos los impuestos correspondientes, de acuerdo al siguiente cuadro:

Ítem	Descripción	Precio Unitario sin impuestos	Cantidad	Precio Total sin Impuestos	Impuestos	Precio Total Impuestos Incluidos
a	Horas de Jefe de Proyecto					
b	Horas del Consultor I					
c	Hora del Consultor II					
Suma Global				**a+b+c**		

12. FORMA DE PAGO

La forma de pago estará basada en el cumplimiento de hitos descritos en el cronograma de proyectos.

A los efectos de la comparación de las propuestas, los oferentes deberán completar los cuadros que se presentan en este pliego.

13. SISTEMA DE PUNTOS

CRITERIOS DE EVALUACIÓN TÉCNICA DE LA PROPUESTA

Los criterios y sub- criterios, y el sistema de puntos (máximos) que se asignará a la evaluación de la Propuesta Técnica son:

	Puntaje Máx
(i) Actividad principal de la firma	**10**
- Especializada en seguridad de la información y continuidad del negocio	10
- No especializada en seguridad de la información y continuidad del negocio pero que cuente con un departamento/sección especializado en seguridad de la información y continuidad del negocio	5
(ii) Antigüedad de la firma	**10**
(iii) Experiencia de la firma en Proyectos similares al objeto de la consultoría, vinculados a: **-**diseño de procesos de gestión de seguridad de la información y gestión de la continuidad del negocio. -implementación de ISO 27001 / 22301 y desarrollo de sistema de gestión de la seguridad de la información.	**25**
Se deben presentar hasta 5 (cinco) Proyectos relevantes para la evaluación de criterio en los últimos 5 años	
A cada Proyecto se le otorgará un puntaje máximo de 5 (cinco), tomando en cuenta la relevancia, similitud de los objetivos con la presente Consultoría, así como porte de los Proyectos (detallados en la Invitación de Expresiones de Interés) de acuerdo con los siguientes factores de ponderación:	
a. Similitud de los objetivos del Proyecto con las actividades previstas en los Términos de Referencia (TDR)	7,5
b. Desarrollo en organizaciones del ámbito público o público no estatal	7,5
c. Desarrollo para procesos de similares características, gestión de la seguridad de la información y gestión de la continuidad del negocio.	10
(iv) Personal Profesional Clave y Competencia para el trabajo	**25**
a. Jefe del Equipo	11
b. Consultor No 1	7
c. Consultor No 2	7
Los puntajes se otorgarán basados en los CVs del personal presentado evaluando los siguientes criterios: **-EXPERIENCIA** **-** En Proyectos de Consultoría de seguridad de la información y continuidad del negocio (hasta 3 puntos) Por proyecto: Entre 1 y 3 (1 punto) Más de 3 (3 puntos) Por años: Entre 1 y 2 años (1 punto) Más de 2 (3 puntos) **-FORMACIÓN** **-** Posgrados en especialización en seguridad de la información y/o continuidad del negocio (3 puntos por cada uno).	

- Certificaciones vigentes en seguridad de la información y/o continuidad del negocio (1 punto por cada uno)	
Los puntos se acumulan hasta llegar al máximo establecido de acuerdo al rol del personal (11 o 7 puntos)	
(v) Experiencia en impartir capacitaciones y auditorias	**10**
a.- Experiencia en capacitaciones -Entre 1 año y 2 años (2 puntos) -Más de 2 años (5 puntos)	**5**
b.- Experiencia en Auditorías -Entre 1 año y 2 años (2 puntos) -Más de 2 años (5 puntos)	**5**
(vi) Lógica de la metodología y plan de trabajo propuestos en respuesta a los términos de referencia	**20**
a.- Enfoque teórico y metodología	**10**
b.- Plan de Trabajo	**10**
Los puntajes se otorgarán de acuerdo al material presentado donde se ponderarán los siguientes factores: Enfoque teórico y metodología: uso de los estándares ISO 27001 y 22301, NIST CSF y el MCA (Marco de ciberseguridad de Agesic) Plan de trabajo: cronogramas, diagramas de Gantt, EDTs, hitos, entregables, esquemas de comunicación, reuniones y puestas a punto junto con los demás componentes que hacen a las buenas prácticas en la gestión de proyectos	
El mínimo puntaje técnico Pt requerido para calificar es de 65 Puntos	

La Propuesta financiera (Fm) evaluada como la más baja recibe el máximo puntaje financiero (Sf) de 100.

La fórmula para determinar el puntaje financiero (Fp) de todas las demás Propuestas es la siguiente:

Sf = 100 x Fm/ F, donde "Sf" es el puntaje financiero

- "Fm" es el precio más bajo, y
- "F" es el precio de la propuesta bajo consideración.

Las ponderaciones asignadas a las propuestas técnicas (T) y financiera (P) son:

T = 60 y P = 40

Las propuestas clasificadas de acuerdo con los puntajes combinados técnicos (St) y financieros (Sf) utilizando los pesos (T = el peso dado a la Propuesta Técnica; P = el peso dado a la Propuesta de Precio; T + P = 1) así:

S = St x T% + Sf x P%.

Ministerio de Economía y Finanzas

ANEXOS

ANEXO I

CONDICIONES DE SEGURIDAD DE LA INFORMACIÓN, PRIVACIDAD Y PROTECCIÓN DE DATOS

Confidencialidad y protección de datos

El oferente deberá informar junto con su oferta dónde estarán alojados los datos que procese en caso de resultar adjudicado, debiendo el servidor encontrarse en países considerados con niveles adecuados a los estándares europeos de protección de datos. Caso contrario, se compromete a contar con el consentimiento de los titulares de los datos; a que el importador se encuentre adherido al marco de Privacy Shield; haya suscrito cláusulas contractuales tipo con el exportador o posea un Código de Conducta inscripto, con la consecuente autorización de transferencia internacional de datos tramitada ante la Unidad Reguladora y de Control de Datos Personales, en los dos últimos supuestos.

El oferente que resulte adjudicado se obliga en forma expresa a conservar en la más estricta confidencialidad toda la información que procese o utilice durante su relación con Centro Ceibal. La Empresa se obliga a tratar los datos a los que tuviere acceso en virtud de este contrato, de conformidad con la Ley Nº 18.331, de 11 de agosto de 2008 y Decreto Nº 414/2009, de 31 de agosto de 2009, únicamente para la prestación y en el marco del servicio contratado, no pudiendo utilizarlos para otra finalidad, ni en beneficio propio ya sea gratuito u oneroso, ni cederlos, comunicarlos o transferirlos a terceros, salvo previa autorización de Centro Ceibal.

Centro Ceibal es responsable de la base de datos y del tratamiento, siendo el oferente adjudicado encargado de tratamiento, de acuerdo con lo dispuesto en los literales H) y K) del artículo 4 de la Ley Nº 18.331. Por tanto, en ningún caso el acceso a datos podrá entenderse como cesión o permiso para su libre utilización por parte de quien resulte adjudicado.

El oferente adjudicado se obliga a adoptar las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de los datos y evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información.

Al término del contrato el oferente deberá suprimir de todos sus sistemas y archivos físicos y lógicos, sean propios o contratados a terceros, los datos personales accedidos, obtenidos o tratados en virtud de la contratación con Ceibal, así como los metadatos asociados, en caso de corresponder.

Se considera dato personal la información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables, a modo enunciativo, cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo que refiera a ellas directa o indirectamente, conforme con lo dispuesto en el artículo 4 de la Ley Nº 18.331 y artículos 1 y 4 del Decreto Nº 414/009.

Políticas de Seguridad de la Información

El oferente deberá conocer y cumplir con lo estipulado en el Manual de Políticas de Seguridad de la Información del Centro Ceibal.

https://www.ceibal.edu.uy/storage/app/media/manual-de-politicas-de-seguridad-de-la-informacion-wiki-ceibal.pdf

Acuerdo de confidencialidad

Los oferentes que resulten seleccionados para integrar la Lista Corta deberán firmar un acuerdo de confidencialidad (NDA) de acuerdo a lo estipulado en el punto 4. Confidencialidad y protección de datos del presente llamado.

Acuerdo de nivel de servicio

El oferente que resulte adjudicado podría tener que firmar un acuerdo de nivel de servicio (SLA) de acuerdo a lo estipulado en las políticas y procedimientos del Centro Ceibal.

Uso de la infraestructura del Centro Ceibal

En caso que los servicios que el oferente que resulte adjudicado incluyan el uso, instalación, configuración y/o mantenimiento de infraestructura de Ceibal tanto lógica como física, se deberán estipular claramente las condiciones, responsabilidades y usos adecuados de la información afectada de manera de asegurar la confidencialidad, integridad y disponibilidad de la misma.

Protección de la información manejada

La información sobre el Centro Ceibal manejada por el oferente que resulte adjudicado deberá cumplir con los requisitos establecidos en el Manual de Políticas de Seguridad de la Información. Para ello deberá cumplir con las medidas de seguridad que garanticen una confidencialidad, integridad y disponibilidad de la información tanto en reposo como en tránsito y en uso. En el caso que la información sea almacenada en servidores del proveedor ya sea en modalidad onpremise o en nubes, se deberán extremar los cuidados.

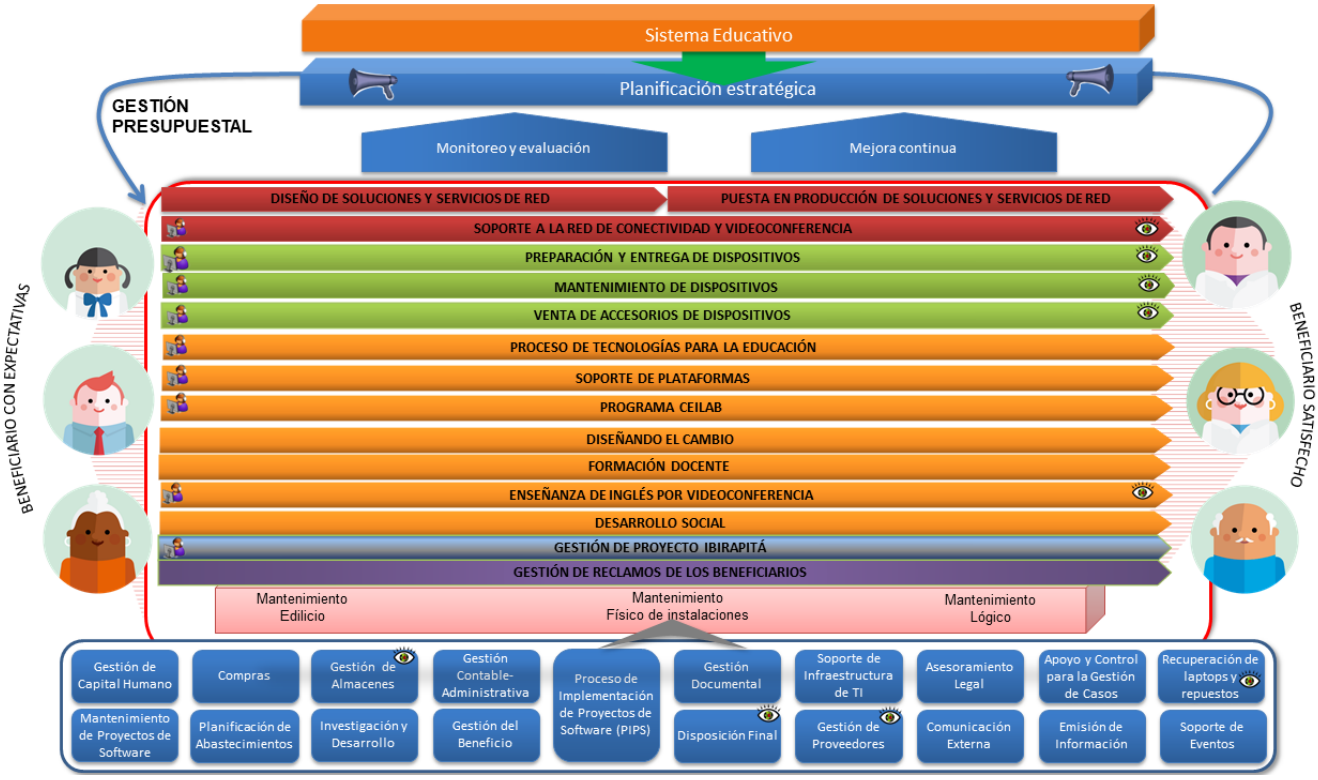
Concientización y capacitación del personal

El personal del oferente que resulta adjudicado deberá estar informado y concientizado con el objetivo de gestionar de manera segura la información que manejan del Centro Ceibal y dar un adecuado tratamiento a posibles incidentes de seguridad.

Trazabilidad y auditoría

Centro Ceibal se reserva el derecho de auditar los procesos relacionados a la seguridad de la información y la privacidad con el objetivo de verificar que se cumpla lo estipulado entre las partes. Para ello podrá solicitar al oferente que resulte adjudicado la documentación respaldante que corresponda en cada caso. A estos efectos deberá preverse tal facultad en el contrato.

ANEXO II


Sistema Educativo
Planificación estratégica
GESTIÓN PRESUPUESTAL
Monitoreo y evaluación
Mejora continua
DISEÑO DE SOLUCIONES Y SERVICIOS DE RED
PUESTA EN PRODUCCIÓN DE SOLUCIONES Y SERVICIOS DE RED
SOPORTE A LA RED DE CONECTIVIDAD Y VIDEOCONFERENCIA
PREPARACIÓN Y ENTREGA DE DISPOSITIVOS
MANTENIMIENTO DE DISPOSITIVOS
VENTA DE ACCESORIOS DE DISPOSITIVOS
PROCESO DE TECNOLOGÍAS PARA LA EDUCACIÓN
SOPORTE DE PLATAFORMAS
PROGRAMA CEILAB
DISEÑANDO EL CAMBIO
FORMACIÓN DOCENTE
ENSEÑANZA DE INGLÉS POR VIDEOCONFERENCIA
DESARROLLO SOCIAL
GESTIÓN DE PROYECTO IBIRAPITÁ
GESTIÓN DE RECLAMOS DE LOS BENEFICIARIOS
Mantenimiento Edilicio
Mantenimiento Físico de instalaciones
Mantenimiento Lógico
BENEFICIARIO CON EXPECTATIVAS
BENEFICIARIO SATISFECHO
Gestión de Capital Humano
Compras
Gestión de Almacenes
Gestión Contable-Administrativa
Proceso de Implementación de Proyectos de Software (PIPS)
Gestión Documental
Soporte de Infraestructura de TI
Asesoramiento Legal
Apoyo y Control para la Gestión de Casos
Recuperación de laptops y repuestos
Mantenimiento de Proyectos de Software
Planificación de Abastecimientos
Investigación y Desarrollo
Gestión del Beneficio
Disposición Final
Gestión de Proveedores
Comunicación Externa
Emisión de Información
Soporte de Eventos