

Consultas Realizadas

Licitación 417186 - CD N° 07/2022 CONTRACION DE SERVICIO DE CONSULTORIA PARA AUTODIAGNOSTICO DE CIBERSEGURIDAD

Consulta 1 - Solicitud de Prorroga

Consulta	Fecha de Consulta	22-09-2022
A efectos de posibilitar culminar favorablemente ciertos procedimientos requeridos por normas internas y de regulación (incluyendo aquellos relacionados con temas de independencia), solicitamos a la Convocante tenga a bien prorrogar 10 días la presentación prevista para el 29 de setiembre de 2022. Nuestra firma cuenta con la experiencia y capacidad necesarias para llevar a cabo el trabajo de manera exitosa.		

Respuesta	Fecha de Respuesta	28-09-2022
Saludos Cordiales. Favor ver adenda y fechas en el SICP. Se ha otorgado una prórroga a la apertura. No obstante, se menciona que, solo podrá ser prorrogado por dicho plazo y tomar en consideración que nos encontramos próximo al cierre de los plazos procesales por cierre del ejercicio. Atte.		

Consulta 2 - Solicitud de inclusión de otras certificaciones de Seguridad de la Información

Consulta	Fecha de Consulta	23-09-2022
De manera a dar mas apertura y posibilidades a más oferentes y profesionales de ciberseguridad, solicitamos puedan aceptar también otras certificaciones internacionales en seguridad, tales como CISM, ISO 27001 Lead Auditor, CEH, entre otros, para los siguientes Ítems del PBC: - Sección FACTOR B, b.1) Un Líder del proyecto, donde dice "- 10 (diez) puntos al profesional Líder del Proyecto que cuente con la Certificación de Alta Dirección en Ciberseguridad (al menos 2700 horas) o ITIL o Azure". - Sección FACTOR B, b.2) Equipo de Consultor/es Especialistas, donde dice "- 5 (cinco) puntos si al menos uno de los Consultores Especialistas cuente con alguna de las siguientes Certificaciones: Dirección de Ciberseguridad Avanzada y/o similar." - Sección FACTOR B, b.2) Equipo de Consultor/es Especialistas, donde dice "- 5 (cinco) puntos si al menos uno de los Consultores Especialistas cuente con las Certificaciones en Gestión de Políticas de Ciberseguridad y/o similar"		

Respuesta	Fecha de Respuesta	28-09-2022
Saludos Cordiales. Favor Ver Adenda. Atte.		

Consulta 3 - Solicitud de prorroga

Consulta	Fecha de Consulta	26-09-2022
<p>Se solicita amablemente a la convocante extender el periodo de consultas y así también la fecha de apertura de ofertas, para un análisis pormenorizado del pliego de bases y condiciones en atención a la envergadura del proyecto y su alcance para la institución, a fin de posibilitar la participación de una mayor cantidad de oferentes.</p> <p>Lo solicitado corresponde en consideración del plazo exiguo establecido inicialmente tomando en cuenta a partir desde la fecha de publicación del proceso y la fecha tope de consultas.</p>		

Respuesta	Fecha de Respuesta	28-09-2022
<p>Saludos Cordiales. Favor ver Adenda.</p> <p>Se prorroga el tiempo disponible para presentar oferta a fin de facilitar la participación. No obstante, se menciona que la capacidad de los potenciales oferentes para adaptarse a los requerimientos institucionales es parte de la capacidad técnica del mismo. Se recuerda que se encuentra vigente los plazos de cierre de procesos, por lo cual la prorroga no podrá extenderse demasiado.</p> <p>Atte.</p>		

Consulta 4 - Consultas

Consulta	Fecha de Consulta	26-09-2022
<p>En el Pliego de Bases y Condiciones, se menciona que uno de los requisitos para el profesional sea "que cuente con la Certificación de Alta Dirección en Ciberseguridad (al menos 2700 horas) o ITIL o Azure. "</p> <p>¿También se tendrá en cuenta como formación del profesional, las capacitaciones que no sean expedidas por ISACA?</p>		

Respuesta	Fecha de Respuesta	28-09-2022
<p>Saludos Cordiales. Favor ver Adenda.</p> <p>En la Carta Invitación no hemos encontrado referencia directa al ISACA, interpretando que el potencial oferente se refiere al " Information Systems Audit and Control Association".</p> <p>En tal sentido, se aceptarían formaciones y capacitaciones independientemente del órgano emisor, siempre y cuando el mismo cuente con algún tipo de reconocimiento nacional o internacional.</p> <p>Atte.</p>		

Consulta 5 - Solicitud de modificación Factor A

Consulta	Fecha de Consulta	26-09-2022
<p>Factor A: Se calificará hasta alcanzar los 20 (veinte) puntos todos aquellos trabajos vinculados: Con trabajos de proyectos relacionados a Ciberseguridad en Instituciones Financieras públicas o privadas: 5 puntos por cada trabajo realizado o en ejecución para el sector financiero, hasta un máximo de 20 puntos</p> <p>Solicitamos: el ajuste de instituciones financieras publicas a instituciones publicas o privadas teniendo en cuenta que el MTESS no es una institución financiera como así sería el caso de instituciones como el BNF.</p>		

Respuesta	Fecha de Respuesta	28-09-2022
<p>Saludos Cordiales.</p> <p>Favor ver adenda. Se aclara que se tomo en consideración la valoración dichas experiencias en consideración que en la institución se opera con el sistema de pago a través de instituciones de naturaleza financiera (venta de formularios, certificaciones, etc.).</p> <p>No obstante, a fin de permitir mayor participación, se ha procedido a efectuar la adenda.</p> <p>Atte.</p>		

Consulta 6 - Solicitud de modificación Líder del proyecto

Consulta	Fecha de Consulta	26-09-2022
<p>Un Líder del proyecto: Se requiere de un profesional universitario con título de grado. La calificación máxima será de 25 (veinticinco) puntos. Se valorará:</p> <ul style="list-style-type: none">- 10 (diez) puntos al profesional Líder del Proyecto que cuente con la Certificación de Alta Dirección en Ciberseguridad (al menos 2700 horas) o ITIL o Azure. <p>Solicitamos: el ajuste referente al punto al menos 2700 horas teniendo en cuenta que una certificación de tiempo prolongado incluso posgrados y maestrías tienen carga horaria inferior – solicitamos que sea válidas certificaciones comprobadas con título formal en alta dirección de ciberseguridad o ITIL o Azure.</p>		

Respuesta	Fecha de Respuesta	28-09-2022
<p>Saludos Cordiales. Favor ver Adenda. Se considerara certificación comprobada, siempre y cuando provenga de instituciones nacionales o internacionales reconocidas. Atte.</p>		

Consulta 7 - Solicitud de modificación Factor A

Consulta	Fecha de Consulta	26-09-2022
<p>Factor A: El oferente debe ser una empresa consultora con reconocida y comprobada experiencia en la elaboración, diseño y análisis en la Prevención y Control en Materia de Ciberseguridad, en el marco de lo establecido en la Ley N° 6207/2018 y su Decreto Reglamentario N° 2274/2019 vinculado a la Resolución MITIC N°346-2020 y/o Resolución 277/2020. Cumpliendo con este requisito el oferente podrá acceder a los puntos correspondientes a este factor.</p> <p>Aclaración: solicitamos este punto en específico pueda ser ajustado a empresas con experiencia comprobada en la elaboración, diseño y análisis en Prevención y Control en Materia de Ciberseguridad. Teniendo en cuenta que de la manera solicitada específica que la empresa tendría que haber realizado trabajos exclusivamente bajo esta ley sin embargo no difiere que la empresa tenga o no experiencia en la materia de ciberseguridad.</p>		

Respuesta	Fecha de Respuesta	28-09-2022
<p>Saludos Cordiales. Favor Ver Adenda al proceso. Atte.</p>		

Consulta 8 - Solicitud de prórroga

Consulta	Fecha de Consulta	26-09-2022
<p>Por la presente solicitamos una prórroga de una semana teniendo en cuenta que la licitación fue publicada en la fecha 22/09/2022 y la misma tiene fecha de entrega de oferta el 29/09/2022 siendo así 6 días hábiles siendo un plazo extremadamente corto para reunir la cantidad de información solicitada por el nivel de detalles específicos.</p>		

Respuesta	Fecha de Respuesta	28-09-2022
<p>Saludos Cordiales. Favor Ver Adenda. Se ha procedido a prorrogar el plazo. No obstante, se recuerda que se encuentra vigente el plazo de cierre de los procesos del presente ejercicio, por lo cual solo podrá efectuarse una prórroga al proceso a fin de facilitar la participación. Atte.</p>		

Consulta 9 - Consulta

Consulta	Fecha de Consulta	30-09-2022
<p>En el apartado Documentos de Planeación de cada Ítem y validación con el MTESS. A ser presentado a los 30 días de la firma del contrato.</p> <p>1. Documento con la especificación de los trabajos a ser realizados en cada Ítem incluyendo lugar de trabajo, horario en caso necesario, forma de registro de actividades, de registro de migraciones, de reportes de trabajo, de horas utilizadas y otros relevantes para lograr el adecuado registro de la volumetría y los Indicadores de éxito de cada ítem. Este documento deberá incluir el relevamiento de información sobre los sistemas a ser instalados incluyendo las documentaciones de las reuniones, visitas de campo, y documentos de los sistemas para avanzar en los entregables.</p> <p>2. Documento con el plan de capacitación a funcionarios usuarios del sistema una vez puesto en marcha el sistema.</p> <p>Al mencionar sistema, ¿a que se refiere la contratante? ¿Consideran la presentación de un sistema informático como parte integral de la propuesta?</p> <p>¿Nuestra propuesta debe incluir la provisión de un sistema informático? En caso de que sí, ¿Qué tipo de sistema?</p> <p>¿A que se refiere la contratante con "documentos de los sistemas para avanzar con los entregables"? ¿Requerimientos funcionales y no funcionales? ¿De que sistemas?</p> <p>¿La propuesta esperada debe considerar la ejecución del plan de capacitación que debe ser propuesto?</p> <p>¿Se considera como un requerimiento de la contratante la realización de análisis de vulnerabilidades como parte de nuestra propuesta?</p>		

Respuesta	Fecha de Respuesta	05-10-2022
<p>Saludos Cordiales.</p> <p>En relación a su consulta, se indica que la interpretación que se debe dar a "Sistemas" se refiere a las recomendaciones para las instalaciones de sistemas en el futuro, que faciliten la búsquedas de amenazas o consideración que deban tenerse en cuenta en el desarrollo de los mismos.</p> <p>Se menciona, que actualmente el MteSS se encuentra trabajando constantemente en la Sistematización de los Servicios tanto internos como externos, en donde se requiere asesoramiento sobre cuestiones de Cyberseguridad.</p> <p>No se requiere la entrega de ningún sistema, se busca obtener "Conocimiento del Como" para las políticas de Ciberseguridad institucional.</p> <p>Atte.</p>		

Consulta 10 - Consulta

Consulta	Fecha de Consulta	30-09-2022
<p>Según lo establecido en los TDR en el apartado Actividades Incluidas en los Ítems "La evaluación debe incluir a toda la organización: redes, sistemas, equipos, aplicaciones, procedimientos, datos y personas. Para poder realizar esta evaluación es necesario involucrar a todas las áreas involucradas, de modo a asegurar que las respuestas sean lo más certeras posibles." ¿Cuál es la cantidad de personas claves que deben ser consideradas? ¿Cuántas áreas debemos tener en cuenta como parte de nuestra metodología de trabajo? ¿De estas áreas, cuantas son críticas? ¿Cuántos equipos informáticos deben ser incluidos dentro de la propuesta? ¿Podríamos obtener la cuantificación de sistemas informáticos a incluir en la evaluación?</p>		

Respuesta	Fecha de Respuesta	05-10-2022
<p>Saludos, a modo de aclarar los alcances, se menciona: El acceso a los sistemas, todos los funcionarios de la Dirección de Tecnología de Información, Se debe tener en cuenta los departamentos de Secretaria General del Ministerio, de los Vice-Ministerio, Direcciones Generales y Departamentos abocados a la atención de funcionarios en las dependencias del MTESS sito en Herrera esq. Paraguari, como sus principales centros: Edificio DGE, sito en Avda. Peru esq. RIO de Janeiro, la Dirección General de Fiscalización sito en O'leary casi Jejuí. Todos en Asunción. Las áreas críticas son las Secretarías Generales y los Dpto. de Atienden a la ciudadanía, por su interacción con los recurrentes. Se dispone al menos 176 estaciones de trabajo en el edificio principal, 20 estaciones en la sede Fiscalización y al menos 100 estaciones de escritorio en el edificio Perú. Al menos 5 conexiones VPN 3 Servidores Físicos 2 Equipos de Borde Principal y 51 máquinas virtuales con sendos sistemas internos. Se reitera que no se requiere la entrega de ningún sistema o bien, se busca obtener "Conocimiento del Como" para las políticas de Ciberseguridad institucional. Atte.</p>		

Consulta 11 - Consulta

Consulta	Fecha de Consulta	30-09-2022
<p>¿El plazo solicitado para la ejecución de los trabajos puede ser ampliado?</p>		
Respuesta	Fecha de Respuesta	05-10-2022
<p>Saludos. Si se refiere al volumen de equipos para la formulación del plan o los locales para la evaluación y recomendaciones en Ciberseguridad, se indica que no seran ampliados. Si se refiere a algun espacio fisico requerido por el potencial consultor para prestar sus servicios, se indica que la misma podra ser solicitado al administrador de contrato al momento de la ejecución del contrato.</p>		