PREGÃO ELETRÔNICO BINACIONAL AF 1271-20
SUBASTA A LA BAJA ELECTRÓNICA BINACIONAL AF 1271-20

AQUISIÇÃO DE SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO EM TI

ADITAMENTO 4

I) Em conformidade com o disposto no subitem 2.6.1 do Caderno de Bases e Condições (CBC) do Pregão Eletrônico Binacional AF 1271-20, a ITAIPU responde perguntas realizadas por interessadas nesta licitação:

PERGUNTA 1
"Item 4.10 - É solicitado que a empresa vencedora ministre cursos oficiais da EXIN de forma presencial. Sugestão: Validar se isso é mandatório, pois foge do nosso escopo de atuação."

RESPOSTA
Conforme definido no "CAPÍTULO XIX - SUBCONTRATAÇÃO, CESSÃO, TRANSFERÊNCIA E DAÇÃO EM GARANTIA" da Minuta de Contrato este item é passível de subcontratação. O curso deverá em principio ser presencial, porém quando da realização dependerá da situação da pandemia de COVID-19 e poderá ser considerado outro método de aplicação. Gentileza reportar-se a resposta da Pergunta 14 em complementação a este entendimento.

PERGUNTA 2
"Item 5.1.12 - Considera varreduras não intrusivas de ambiente SCADA. Sugestão: Validar se podem ser consideradas outras abordagens como Cyber Security Design."

RESPOSTA
Não, pois esta é uma característica necessária ao software a ser fornecido.

PERGUNTA 3
"Item 5.1.17 - A solução de GV deve ser listada no quadrante Gartner ou no Forrester. Sugestão: Validar se podemos usar o Nessus como solução com o Íris apoiando e dando visão de inteligência do ciclo de vida das vulnerabilidades."

ADQUISICIÓN DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN TI

ADITIVO 4

I) De conformidad a lo dispuesto en el sub-ítem 2.6.1 del Pliego de Bases y Condiciones (PBC) de la Subasta a la Baja Electrónica Binacional AF 1271-20, la ITAIPU responde preguntas formuladas por empresas interesadas en esta licitación:

PREGUNTA 1
Ítem 4.10 – Se solicita que la empresa vencedora realice cursos oficiales de la EXIN de forma presencial. Sugerencia: Confirmar si eso es obligatorio, pues escapa de nuestro alcance de actuación.

RESPUESTA
Conforme definido en el CAPÍTULO XIX SUBCONTRATACIÓN, CESIÓN, TRANSFERENCIA Y DACIÓN EN GARANTÍA de la Minuta de Contrato, este ítem es pasible de subcontratación. El curso deberá en principio ser presencial, no obstante la realización dependerá de la situación de la pandemia de COVID-19 y podrá ser considerado otro método de aplicación. Favor remitirse a la respuesta de la Pregunta 14 en complemento a este entendimiento.

PREGUNTA 2
Ítem 5.1.12 – Considera exploraciones no intrusivas de ambiente SCADA. Sugerencia: Confirmar si pueden ser considerados otros enfoques como Cyber Security Design.

RESPUESTA
No, pues esta es una característica necesaria del software a ser suministrado.

PREGUNTA 3
Ítem 5.1.17 - La solución de GV debe estar listada en el cuadrante Gartner o en el Forrester. Sugerencia: Confirmar si podemos usar el Nessus como solución con el Íris apoyando y dando visión de inteligencia del ciclo de vida de las vulnerabilidades.

RESPOSTA
O software e demais componentes devem estar no quadrante Gartner ou no Forrester, como líderes.

RESPUESTA
El software y demás componentes deben estar en el cuadrante Gartner o en Forrester, como líderes.

PERGUNTA 4
"Item 6.2 - São considerados profissionais para regime de suporte remoto e local e uso sob demanda (Banco de horas). Sugestão: Validar se podemos atuar somente de forma remota ou se teremos a necessidade de contratação de um profissional localizado na cidade da companhia."

RESPOSTA
A ITAIPU pode solicitar o suporte técnico local, contudo não necessita que o técnico esteja residente na área de execução dos serviços, desde que se cumpra os níveis de serviço especificados.

PREGUNTA 4
Ítem 6.2 – Son considerados profesionales para el régimen de soporte remoto y local y uso sobre demanda (Banco de horas). Sugerencia: Confirmar si podemos actuar solo de forma remota o si tendremos la necesidad de contratación de un profesional localizado en la ciudad de la compañía.

RESPUESTA
La ITAIPU puede solicitar el soporte técnico local, sin embargo no necesita que el técnico esté residente en el área de ejecución de los servicios contratados, siempre que se cumplan los niveles de servicios especificados.

PERGUNTA 5
Pelo presente consorcio formado por XXXXXXX e XXXXXXX, por este meio solicitamos, se factível uma prorrogação para a data da sessão do dia 23 de novembro, já que tivemos problemas para o registro de fornecedores.

RESPOSTA
Pedido indeferido, não obstante ressaltamos que o certame já foi prorrogado uma vez, conforme Aditamento 1, publicado em 18.11.20.

PREGUNTA 5
"Por la presente el consorcio formado por XXXXXXX y XXXXXXX, por este medio solicitamos a ustedes por favor, si es factible de una prórroga para la fecha de apertura del día 23 de noviembre, ya que hemos tenido inconvenientes para el registro como proveedores."

RESPUESTA
Pedido denegado, no obstante resaltamos que el certamen ya fue prorrogado una vez, conforme Aditivo 1, publicado el 18.11.20.

PERGUNTA 6
As licenças de uso do software de gestão de vulnerabilidades que serão fornecidas a ITAIPU, poderiam estar no nome de um dos sócios do consórcio ou devem estar em nome da ITAIPU?

RESPOSTA
As licenças devem obrigatoriamente estar em nome da ITAIPU.

PERGUNTA 6
Las licencias de uso del software de Gestión de Vulnerabilidades que serán proveídas a Itaipu, podrían estar a nombre de uno de los socios del consorcio? O deben estar a nombre de Itaipu?

RESPUESTA
Las licencias deben estar obligatoriamente a nombre de la ITAIPU.

PERGUNTA 7
No ponto 5.1.5 estabelece que os colaboradores da ITAIPU devem ter acesso à base de conhecimento e fóruns de soluções no site do fabricante. Isso se refere ao fórum público do provedor ou alguma assinatura de suporte especial?

PREGUNTA 7
En el punto 5.1.5 establece que los colaboradores de la ITAIPU deberán tener acceso a la base de conocimiento y a foros de la solución en el sitio del fabricante. Esto se refiere al foro público del proveedor o a alguna suscripción especial de soporte?

RESPOSTA
A ITAIPU deverá ter acesso a todas as bases de conhecimento da solução ofertada.

PERGUNTA 8
A ferramenta de gerenciamento de vulnerabilidade deve incluir verificação de aplicativo? Se a resposta for sim, quantas aplicações no total devem ser consideradas? Quantos aplicativos internos e quantos externos?

RESPOSTA
Sim, deve incluir a verificação (escaneamento) de 7 (sete) aplicações de negócio, desenvolvidas nas plataformas listadas no item 4.4.5 das Especificações Técnicas – Anexo I. Na etapa de Planejamento será definido o número exato de aplicações internas e externas que deverão ser verificadas.

PERGUNTA 9
As varreduras de aplicativos devem ser periódicas / programadas (histórico / dashboard) ou pontuais (ad hoc)?

RESPOSTA
Durante a execução do contrato está prevista a realização de 3 (três) avaliações de vulnerabilidade do ambiente corporativo, conforme definido no item 4.4 das Especificações Técnicas. Tudo que está relacionado a especificação do software a ser utilizado está descrito no item 5 das Especificações Técnicas.

PERGUNTA 10
No caso de solicitações de sites adicionais após os 250 iniciais (50 sites externos e 200 internos), quanto tempo a CONTRATADA teria para fornecê-los?

RESPOSTA
O prazo de entrega de licenças adicionais é de no máximo 15 dias úteis.

PERGUNTA 11
Gostaria de saber se é possível o envio de duvidas e questionamentos técnicos a fim de elaboração de uma proposta e precificação mais assertiva?

RESPUESTA
La ITAIPU deberá tener acceso a todas las bases de conocimiento de la solución ofertada.

PREGUNTA 8
La herramienta de Gestión de Vulnerabilidades debe incluir escaneo de Aplicaciones? De ser afirmativa la respuesta, cuántas aplicaciones deben considerarse en total aproximadamente? ¿Cuántas aplicaciones internas y cuántas externas?

RESPUESTA
Sí, debe incluir la verificación (escaneo) de 7 aplicaciones de negocio, desarrolladas en las plataformas listadas en el ítem 4.4.5 de las Especificaciones Técnicas – Anexo I. En la etapa de planificación será definido el número exacto de aplicaciones internas y externas que deberán ser verificadas.

PREGUNTA 9
Los escaneos de Aplicaciones deberían ser periódicos/programados (histórico / dashboard) o ser puntuales (ad hoc)?

RESPUESTA
Durante la ejecución del contrato está prevista la realización de 3 (tres) evaluaciones de vulnerabilidades del ambiente corporativo, de acuerdo con lo definido en el ítem 4.4 de las Especificaciones Técnicas. Todo lo relacionado a la especificación del software a ser utilizado se describe en el ítem 5 de las Especificaciones Técnicas.

PREGUNTA 10
En caso de solicitudes de sitios adicionales posteriores a los 250 iniciales (50 sitios externos y 200 internos), ¿cuánto tiempo tendría el Contratista para proveer las mismas?

RESPUESTA
El plazo de entrega de licencias adicionales es de máximo 15 días hábiles.

PREGUNTA 11
Nos gustaría saber si es posible el envío de dudas y cuestionamientos técnicos a fin de elaborar una oferta y precios más adecuados?

RESPOSTA
Os prazos estabelecidos para formalização de consultas estão estipulados no Calendário de Eventos do CBC. Gentileza reportar-se ao Aditamento 1, publicado em 18.11.20.

RESPUESTA
Los plazos establecidos para formalización de consultas están estipulados en el Calendario de Eventos del PBC. Favor remitirse al Aditivo 1, publicado el 18.11.20.

PERGUNTA 12
Em atenção a licitação em referência solicitamos esclarecimentos na forme de faturamento a cada membro do consórcio. O pregão indica o seguinte texto:
"CLÁUSUSLA 19 - Os pagamentos serão efetuados pela ITAIPU na moeda do país de origem de cada INTEGRANTE DO CONSÓRCIO contratado:
a) em real (R$), para a INTEGRANTE estabelecida no Brasil;
b) em guarani (G.), para a INTEGRANTE estabelecida no Paraguai."
Como a oferta não discrimina os valores a serem faturados por cada consorciado esclareça como será o processo de cobrança e definição dos valores para os consorciados.

PREGUNTA 12
En atención al concurso de referencia solicitamos nos aclaren la forma de facturación a cada miembro del consorcio. El Pliego indica textualmente:
"CLÁUSULA 19 Los pagos serán efectuados por la ITAIPU en la moneda del país de origen de cada INTEGRANTE DEL CONSORCIO contratado:
a) en real (R$), para el INTEGRANTE establecido en Brasil; b) en guaraní (G.), para el INTEGRANTE establecido en el Paraguay."
En atención a que en la oferta no se discrimina los montos a ser facturados por cada miembro, favor aclarar cómo será el proceso de facturación y definición de montos para los integrantes del consorcio.

RESPOSTA
O faturamento deverá seguir o previsto na cláusula 14 da minuta de contrato, que estabelece no § 1º "Os preços serão convertidos 50% (cinquenta por cento) para reais e 50% (cinquenta por cento) para guaraníes,...". Desta forma, cada faturamento corresponderá 50% para a(s) integrante(s) estabelecida(s) no Brasil e 50% para a(s) integrante(s) estabelecida(s) no Paraguai.
Entendimento reforçado pelo disposto no CBC, subitem 1.3.1.2 "A participação das empresas na constituição do consórcio binacional corresponderá 50% (cinquenta por cento) para a empresa estabelecida no Brasil e 50% (cinquenta por cento) para a empresa estabelecida no Paraguai."

RESPUESTA
La facturación se debe dar según lo previsto en la cláusula 14 de la minuta de contrato, que establece en el § 1° "Los precios serán convertidos 50% (cincuenta por ciento) para reales y 50% (cincuenta por ciento) para guaraníes,…". De esta manera corresponderá 50% para la(s) integrante(s) establecida(s) en el Brasil y 50% para la(s) integrante(s) establecida(s) en el Paraguay.

Entendimiento reforzado por lo dispuesto en el PBC, sub-ítem 1.3.1.2 "La participación de las empresas en la constitución del consorcio binacional corresponderá 50% (cincuenta por ciento) para la empresa establecida en el Brasil y 50% (cincuenta por ciento) para la empresa establecida en el Paraguay."

PERGUNTA 13
Com relação ao Pregão Eletrônico Binacional – AF 1271-20. O Item 5.1.1 estipula que um total de: 200 licenças para sites externos (com FQDN), 1.500 licenças para sites internos (com ou sem FQDN).
Podemos considerar que as referências a sites são endereços IP? Portanto, seria um total de 1.700 endereços IP.

PREGUNTA 13
Con relación a la Subasta a la Baja Electrónica Binacional con ID: AF 1271-20. El ítem 5.1.1. estipula que se deberán proveer un total de:
200 licencias para sitios externos (con FQDN)
1.500 licencias para sitios interno (con o sin FQDN)
¿Podemos considerar que al referirse a sitios son direcciones IP?, por lo tanto, sería un total de 1.700 direcciones IP.

RESPOSTA
Entendimento correto.

RESPUESTA
Entendimiento correcto.

PERGUNTA 14
Considerando que o item 4.10 dispõe sobre Capacitação Técnica em Padrões, Melhores Práticas e Processos de Gestão de Segurança da Informação em TI, questiona-se:

a) CURSO: Ethical Hacking e CompTIA PenTest+ (Exin): Por gentileza, informar se os dois treinamentos deverão ser ministrados ou se é para ser elaborado um material com o conteúdo dos dois treinamentos, pois os conteúdos são diferentes, assim como seus patrocinadores. O curso CompTIA Pentest+ é da CompTIA, e o Ethical Hacking mais usado no mercado é chamado C-EH Certified Ethical Hacker que é da empresa ISC².

PREGUNTA 14
Considerando que el ítem 4.10 dispone sobre la Capacitación Técnica en Estándares, Mejores Prácticas y Procesos de Gestión de Seguridad de la Información en TI, se cuestiona:

a) CURSO: Ethical Hacking y CompTIA PenTest+ (Exin): Favor informar si ambas capacitaciones deberán ser realizados o si es para ser elaborado un material con todo el contenido de ambas capacitaciones, pues los contenidos son diferentes, así como sus patrocinadores. El curso CompTIA Pentest+ es de la CompTIA, y el Ethical Hacking más utilizado en el mercado es llamado C-EH Certified Ethical Hacker que es de la empresa ISC².

RESPOSTA
Com relação aos cursos descritos no item 4.10.1, as Especificações Técnicas foram alteradas. Gentileza reportar-se ao item II deste Aditamento.

RESPUESTA
Con relación a los cursos descriptos en el ítem 4.10.1, las Especificaciones Técnicas fueron alteradas. Favor remitirse al ítem II de este Aditivo.

b) CURSO: Segurança Web com OWASP. Por gentileza, poderiam sugerir e detalhar o conteúdo esperado para o treinamento, pois não existe um curso formal no mercado.

b) CURSO: Seguridad Web con OWASP. Favor si podrían sugerir y detallar el contenido esperado para la capacitación, pues no existe un curso formal en el mercado.

RESPOSTA
O conteúdo de conteúdo deve contemplar (WSTG-v4.2):
- SQL Injection automatizado e manual (GET e POST);
- Quebra de formulários de autenticação com uso das técnicas de Sniper e Cluster Bomb;
- Exploração de campos http e https em aplicações web por meio de adulteração e inserção manual de parâmetros;
- Exploração XXE (XML eXternal Entity) via XML External Entity Attack;
- Conhecendo o XXS (Cross-site scripting) refletido e persistente;
- Explorando o XXS para obtenção de cookies de sessão (session hijacking) e reutilização com XSS (session replay);
- Explorando o SSTI (Server Side Template Injection) para realização de RCE (Remote Code Execution);
- Exploração remota de máquinas de usuários com

RESPUESTA
El contenido del curso debe abarcar (WSTG-v4.2):
- SQL Injection automatizado y manual (GET y POST);
- Quiebra de formularios de autenticación con uso de las técnicas de Sniper y Cluster Bomb;
- Exploración de campos http y https en aplicaciones web por medio de adulteraciones e inserción manual de parámetros;
- Exploración XXE (XML eXternal Entity) vía XML External Entity Attack;
- Conociendo el XXS (Cross-site scripting) reflejado y persistente;
- Explorando el XXS para obtención de cookies de sesión (sesión hijacking) y reutilización con XSS (sesión replay);
- Explorando el SSTI (Server Side Template Injection) para realización de RCE (Remote Code Execution);
- Exploración remota de máquinas de usuarios con Microsoft Windows con vulnerabilidades

Microsoft Windows com vulnerabilidade pré-existente combinado com Cross-Site Scripting XSS;

- Exploração de vulnerabilidades famosas como: Heartbleed, Shellshock, Sambacry, Eternal Blue e BlueKeep;
- Explorando servidores de CMS (CONTENT MANAGEMENT SYSTEM) como: Tomcat, Apache Struts, Joomla, Drupal e WordPress;
- Desenjaulamento de Shell Restrito;
- Server Side Request Forgery (SSRF);
- XML eXternal Entity (XXE);
- Prototype Pollution;
- Desserialização, Desserialização em Java, em PHP e outras linguagens;
- Template e Expression Language Injection;
- HTTP Request Smuggling.

PERGUNTA 15
"Referente ai item 4.4.2 do Edital abaixo:
"4.4.2 As principais atividades desta etapa: b) Avaliar os controles de segurança implementados nas plataformas das aplicações de negócio;""

a) "Quando se refere a analise de controles implantados, qual a expectativa? Analisar Baselines implantados?"

RESPOSTA
A expectativa é que o consórcio sugira uma linha de base inicial.

b) "Qual a métricas atual? Utilizam alguma solução para mensurar e/ou aplicar os controles/Baselines? Caso sim, qual?"

RESPOSTA
A expectativa é consórcio sugira as métricas de controles.

c) "Qual o framework utilizado?"

RESPOSTA
A expectativa é consórcio sugira o framework.

d) "Já existem Baselines desenvolvidos? Caso sim, qual a quantidade de Baselines e seus respectivos sistemas operacionais/plataformas?"

RESPOSTA
A expectativa é que o consórcio sugira uma linha de base inicial.

preexistentes combinado con Cross-Site Scripting XSS;
- Exploración de vulnerabilidades famosas como: Heartbleed, Shellshock, Sambacry, Eternal Blue y BlueKeep;
- Explorando servidores de CMS (CONTENT MANAGEMENT SYSTEM) como: Tomcat, Apache Struts, Joomla, Drupal y WordPress;
- Desenjaulamiento de Shell Restringido;
- Server Side Request Forgery (SSRF);
- XML eXternal Entity (XXE);
- Prototype Pollution;
- Deserialización, Deserialización en Java, en PHP y otros lenguajes;
- Template y Expression Language Injection;
- HTTP Request Smuggling.

PREGUNTA 15
Referente al ítem 4.4.2 del PBC abajo:
"4.4.2 Las principales actividades de esta etapa: b) Evaluar los controles de seguridad implementados en las plataformas de las aplicaciones de negocio;"

a) Cuando se refiere al análisis de controles implantados, cuál es la expectativa? Analizar Baselines implantados?

RESPUESTA
La expectativa es que el consorcio sugiera una línea de base inicial.

b) Cuál es la métrica actual? Utilizan alguna solución para medir y/o aplicar los controles/Baselines? Caso afirmativo, cuál?

RESPUESTA
La expectativa es que el consorcio sugiera las métricas de controles.

c) Cuál es el framework utilizado?

RESPUESTA
La expectativa es que el consorcio sugiera el framework.

d) Ya existen Baselines desarrollados? Caso afirmativo, cuál es la cantidad de Baselines y sus respectivos sistemas operacionales/plataformas?

RESPUESTA
La expectativa es que el consorcio sugiera una línea de base inicial.

PERGUNTA 16
"Em relação ao Item 5.1.2 do Edital: "5.1.2. O software deve constar no quadrante magico do Gartner de gestão de vulnerabilidades, ano 2018 ou superior, classificada como Líder, ou no Forrester Wave, em gestão de riscos de vulnerabilidades, ano 2018 ou superior, classificada como Líder."
Gostaríamos de solicitar que a Itaipu aceite a oferta da solução Kenna Security (https://www.kennasecurity.com/), classificada no Forrester Wave de Q4 de 2019 como Strong Performer, logo abaixo das soluções classificadas como Líderes. Ressaltamos que a solução Kenna Security atende os requisitos técnicos do edital, possui distribuição oficial no Brasil e apresenta custos mais otimizados que as soluções classificadas como Líderes. Portanto o aceite dessa oferta traria benefícios financeiros para a Itaipu, sem prejuízos técnicos e de qualidade.
Podemos ofertar essa solução em nossa proposta para esse projeto?"

RESPOSTA
Pedido indeferido. O software e demais componentes devem estar no quadrante Gartner ou no Forrester, como líderes, de acordo com o subitem 1.1.1.1 do Caderno de Bases e Condições.

II) Em conformidade com o disposto no subitem 2.6.2 do Caderno de Bases e Condições do Pregão Eletrônico Binacional AF 1271-20, a ITAIPU altera o subitem 4.10.1, das Especificações Técnicas – Anexo I, conforme segue:

DE
"CompTIA Security+ (EXIN)"

PARA
"CompTIA Security+ (CompTIA)"

DE
"Ethical Hacking e CompTIA PenTest+ (EXIN)"

PARA
"C-EH Certified Ethical Hacker (ISC²) ou CompTIA Pentest+ (CompTIA)"

III) Permanecem inalteradas as demais condições

PREGUNTA 16
Con relación al Ítem 5.1.2 del PBC: "5.1.2 El software debe constar en el cuadrante mágico de Gartner de gestión de vulnerabilidades, año 2018 o superior, clasificada como Líder, o en Forrester Wave, en gestión de riesgos de vulnerabilidades, año 2018 o superior, clasificada como Líder."
Nos gustaría solicita que la ITAIPU acepte la oferta de la solución Kenna Security (https://www.kennasecurity.com/), clasificada en Forrester Wave de Q4 de 2019 como Strong Performer, luego por debajo de las soluciones clasificadas como Líderes. Resaltamos que la solución Kenna Security atiende los requisitos técnicos del PBC, posee distribución oficial en el Brasil y presenta costos más optimizados que las soluciones clasificadas como Líderes. Por tanto la aceptación de esa oferta traería beneficios financieros a la ITAIPU, sin perjuicios técnicos y de calidad.
Podemos ofrecer esa solución en nuestra oferta para ese proyecto?

RESPUESTA
Solicitud denegada. El software y demás componentes deben estar en el cuadrante Gartner o en Forrester, como líderes, de acuerdo con el sub-ítem 1.1.1.1 del Pliego de Bases y Condiciones.

II) De conformidad a lo dispuesto en el ítem 2.6.2 del Pliego de Bases y Condiciones de la Subasta a la Baja Electrónica Binacional AF 1271-20, la ITAIPU altera el sub-ítem 4.10.1, de las Especificaciones Técnicas – Anexo I, conforme siegue:

DE
"CompTIA Security+ (EXIN)"

PARA
"CompTIA Security+ (CompTIA)"

DE
"Ethical Hacking y CompTIA PenTest+ (EXIN)"

PARA
"C-EH Certified Ethical Hacker (ISC²) o CompTIA Pentest+ (CompTIA)"

III) Permanecen inalteradas las demás condiciones

contidas no Caderno de Bases e Condições do Pregão Eletrônico Binacional AF 1271-20.

contenidas en el Pliego de Bases y Condiciones de la Subasta a la Baja Electrónica Binacional AF 1271-20.

Elaboração: Divisão de Suporte Técnico Data de emissão: 04.12.20	Elaboración: División de Apoyo Técnico Fecha de emisión: 04.12.20