Asunción, 14 de abril de 2015.

ACLARACION Nº 1

Señores
.....
Presente:

Tenemos el agrado de dirigirnos a ustedes, con relación a la Licitación por Concurso de Ofertas BNF LCO N° 01/2015 para la **"CONTRATACIÓN DE UNA EMPRESA DEL RAMO DE SEGURIDAD DE TI PARA SERVICIO DE TEST DE SEGURIDAD HACKEO INTERNO Y EXTERNO, IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES DE SEGURIDAD DE TI EN LA PLATAFORMA TECNOLÓGICA DEL BNF, EXIGIDO POR LAS NORMAS VIGENTES SU REALIZACIÓN EN FORMA ANUAL** - ID Nº **285.547.**

Al respecto, cumplimos en informar que conforme a las consultas recibidas por potenciales oferentes, han surgido las siguientes aclaraciones, conforme a lo detallado a continuación:

Consulta N° 1:
Página 42 del documento:
Hacking Ético de Aplicaciones Web, no se detalla la cantidad de aplicaciones Web que hay que testear como tampoco la modalidad con o sin usuarios.
Respuesta:
La respuesta se encuentra explícita dentro del Tema "ALCANCE" bajo el subtítulo "Seguridad de las Aplicaciones Web". La cantidad no superan de 5 sistemas o aplicaciones.

Consulta N° 2:
Página 48 del documento:
Las distintas fases de la metodología deben ser: a partir de aquí se enumeran 4 puntos y no se entiende si es la metodología a emplear, o si esta metodología conforma parte del alcance ya que hay textos como los siguientes:

3. Mejoramiento de Infraestructura: Diseñar junto con el personal del Banco una visión futura para su programa de seguridad, basado en la reducción del riesgo a través de un adecuado esquema de seguridad de la información. Para el efecto se realiza el Análisis del Modelo de Seguridad y las Políticas aplicadas en el Banco (revisión de controles administrativos: Internet, intranet, extranet, acceso remoto) con el fin de identificar fortalezas y debilidades de su puesta en práctica.

4. Implementación: Asistir al Banco en la implementación e integración de su nueva visión de la seguridad de la información. Específicamente en cuanto a:

4.1. Respuesta a Incidentes

4.2. Monitoreo y Control de Aplicaciones

4.3. Estrategia del Negocio:
4.3.1. Definición de la política de seguridad del Banco
4.3.2. Perfil Tecnológico

4.3.3. Perfil de Riesgos
4.3.4. Arquitectura de Seguridad Informática
4.3.5. Especificaciones de la Organización
4.3.6. Especificaciones Técnicas
4.3.7. Especificaciones de Pre-implementaciones

4.4. Mantenimiento:
4.4.1. Soluciones PKI
4.4.2. Soluciones VPN
4.4.3. Servicios de Directorio
4.4.4. Soluciones de Detección de Intrusos
4.4.5. Soluciones de Encriptación
4.4.6. Soluciones de Acceso Remoto
4.4.7. Soluciones de Firewall/router

Respuesta:
La metodología conforma parte del alcance.

Consulta N° 3:
Página 52 del documento:
No está claro también lo referente al Plan de Acción, Plan de acción o Soluciones Propuestas?
C. Soluciones Propuestas en formato electrónico de presentación en diapositivas del Plan de Acción con la elaboración de un plan de actividades orientado a la mitigación de los riesgos obtenidos y resolución de las debilidades y vulnerabilidades detectadas a ser ejecutadas por el Banco. El Plan de Acción se entregará conjuntamente con el personal que el Banco indique, en la medida que crea conveniente incorporar personal interno en la generación del Plan de Acción. El mismo debe incluir también:
a) Ajustes de sistemas ya existentes, especialmente en lo que hace a la configuración de determinados equipos donde normalmente se apoyan las prestaciones de seguridad.
b) Ajuste de los procedimientos, a fin de mantener estable y efectiva la seguridad al incorporarla como una rutina diaria.

Respuesta:
Las soluciones propuestas son las recomendaciones de la firma para que el Banco las ejecute como Plan de Acción para la mitigación de los riesgos encontrados. La UASTIC será la intermediaria en el caso de necesitar la asistencia de personal del Banco para los ajustes finales del mismo en forma conjunta y viable.

Consulta Nº 4:
En la página del pliego **nro.62 – Punto 6 – sub índice "b"**, donde habla de una póliza de seguro de Responsabilidad Profesional.
Por favor, necesitaríamos que nos aclarasen de ser necesario esta póliza y de qué valor o porcentaje de la oferta debería ser, como así el periodo de vigencia del mismo.
Respuesta: Remitirse a la Adenda Nº 3, se excluye este requisito para la presentación de la propuesta técnica.

Consulta Nº 5:

Para el caso de este llamado, no hemos encontrado en el pliego, si corresponde un Seguro afectado al mantenimiento de oferta.

Por favor, indicarnos si es necesario y el importe o porcentaje del mismo, como así el periodo de vigencia del mismo.

Respuesta: Remitirse a la Adenda Nº 3. Conforme a la Ley Nº 5386 que aprueba el Presupuesto General de la Nación para el Ejercicio Fiscal 2015; que establece en el Artículo 169 " En los procesos que tengan por objeto la contratación de consultorías en el marco de la Ley Nº 2051/03 DE CONTRATACIONES PUBLCAS y sus modificaciones, los Oferentes deberán garantizar su oferta mediante declaración jurada. En caso de retirarla o alterarla durante el plazo de validez requerido en las bases de la contratación, podrá iniciarse el procedimiento de aplicación de sanciones a los Oferentes, proveedores y contratistas del Título Séptimo de la citada Ley".

Consulta Nº 6:

En la **página 64 en el punto 1** – Elegibilidad, indica "Carta de Presentación de la propuesta: FORMULARIO".

Por favor necesitaríamos que nos indiquen en que parte del pliego está el formulario mencionado o como procedemos.

Respuesta:

Remitirse al Formulario TEC -1 (página 28 del PBC).

Consulta Nº 7:

En la página del pliego **nro.62 – Punto 2** – solicita una "Carta Compromiso"

Por favor, podrían indicarnos si Uds. nos dan un modelo, si la redactamos nosotros o si no aplica a este llamado.

Respuesta:

El oferente deberá redactar.

Consulta Nº 8:

En la página del pliego **nro.62** – **Punto 3** – solicita una "Carta de PROPUESTA TECNICA"

Por favor, podrían indicarnos si Uds. nos dan un modelo, si la redactamos nosotros o si no aplica a este llamado.

Respuesta:

Remitirse al Formulario TEC -1 (página 28 del PBC).

Consulta Nº 9:

En la página del pliego **nro.62** – **Punto 6** - **Sub Índice (a)** – solicita una "Carta de PROPUESTA"

Por favor, podrían indicarnos si Uds. nos dan un modelo, si la redactamos nosotros o si no aplica a este llamado.

Respuesta:

Remitirse al Formulario TEC -1 (página 28 del PBC).

Consulta Nº 10:

En la página 24 figura "DOCUMENTOS DEL ADJUDICATARIO".

Por favor, indicarnos si todos los puntos (A a la K) incluidos en ese documento, solo deben ser complementados por el oferente en el caso de serle adjudicado el proyecto.

Respuesta:

Es correcta la interpretación.

Consulta Nº 11:

En la **página 66** del pliego, se encuentra un **cuadro 5 – SITUACION FINANCIERA**. En una de las columnas "Documentación Requerida" indica formulario FIN-1 con Anexos y formulario FIN-2 con anexos.

Por favor, indicarnos si estos formularios mencionados en el párrafo anterior son parte del pliego y donde se ubican y si debemos presentarlos, de que sobre forman parte?

Respuesta:

Remitirse a la Adenda Nº 3; la Documentación Requerida: ***Balances y/o Formulario de Declaración Jurada del Impuesto a la Renta (Formulario 101), de los 3 (tres) últimos ejercicios fiscales (Años: 2011, 2012 y 2013).***

Consulta Nº 12:

Sección 2. Instrucciones para los Consultores. El ítem Criterio de Desempate (página 23) menciona "Mayor Cantidad de Contratos ejecutados satisfactoriamente y/o referencias que confirmen un desempeño satisfactorio, según formulario de Referencias Comerciales de la Sección IV... "Consulta: No hemos logrado individualizar el formulario de referencia Comerciales en la Sección IV; podría clarificar el documento a ser utilizado".

Respuesta:

Remitirse a la Adenda Nº 3; se elimina la palabra Sección IV.

Consulta Nº 13:

Sección 2. Instrucciones para los Consultores. Documentos del Adjudicatario (página 24). Los documentos indicados en los literales b), c), d), e) y g), indicados en este apartado deben ser presentados por el proveedor en la etapa de adjudicación?

Nota: es importante mencionar que la gestión de estos documentos llevan un tiempo de procesamiento el cual se extendería con posterioridad a la fecha de presentación de propuestas.

Respuesta:

El oferente adjudicado deberá presentar todas las documentaciones indicadas en la página 24 para la suscripción del contrato respectivo.

Consulta N° 14:

Sección 5. Alcance. Cuántas aplicaciones Web deberán ser contempladas para realizar las pruebas?

Respuesta:

Remitirse a la Adenda Nº 3. La cantidad no superan de 5 sistemas o aplicaciones.

Consulta N° 15:
Sección 5. Alcance (página 43). Menciona "Cincuenta exposiciones del sitio central y remotos del Banco". Podría clarificar a qué se refiere el requerimiento?
Respuesta:
Se refiere a la cantidad de accesos remotos con el sitio central del Banco cuya exposición debe ser testeada como parte de la arquitectura de comunicaciones.

Consulta N° 16:
Sección 5. Alcance (página 43). Cuál será el porcentaje de muestra requerido por el Banco para las pruebas de las estaciones de trabajo e impresoras?
Respuesta:
La cantidad no superan de 50 entre estaciones de trabajo e impresoras.

Consulta N° 17:
Sección 5. Alcance (página 44). Podría indicar cuántos servidores Web deben ser evaluados?
Respuesta:
Remitirse a la Adenda Nº 3. La cantidad no superan de 6 servidores.

Consulta N° 18:
Sección 5. Metodología (página 47). En esta sección se menciona qu la modalidad de prueba será de Gray Box y Black Bos, sin embargo en la sección Objetivos (página 41) se menciona el método Black Box (Caja Negra) y White Box (Caja Blanca). Podría clarificar el método White Box o Gray Box?
Respuesta:
Remitirse a la Adenda Nº 3. La modalidad será preferentemente Caja Negra y Caja Blanca según lo establecido en los objetivos.

Consulta N° 19:
Sección 5. Metodología literal 3 (página 47), Mejoramiento de Infraestructura. Considerando que el objetivo del proyecto hace referencia a realizar pruebas o test de intrusión sobre determinados componentes tecnológicos del Banco, podría aclarar cuál es el alcance específico requerido en este punto?
Respuesta:
Remitirse a la Adenda Nº 3: El test de intrusión sobre componentes tecnológicos del Banco debe desembocar en sus correspondientes informes de vulnerabilidades (entre ellos el análisis del modelo y políticas de seguridad en uso en la infraestructura, detectados durante los trabajos con asistencia del personal del Banco) y recomendaciones de mitigación de riesgos en el Plan de Acción propuesto al Banco para la implementación, integración y mantenimiento de su seguridad de información.

Consulta N° 20:

Sección 5. Metodología literal 4 (página 47), Implementación. Considerando que el objetivo del proyecto hace referencia a realizar pruebas o test de intrusión sobre determinados componentes tecnológicos del Banco, podría aclarar cuál es el alcance específico requerido en este punto?

Respuesta:

El test de intrusión sobre componentes tecnológicos del Banco debe desembocar en sus correspondientes informes de vulnerabilidades (entre ellos el análisis del modelo y políticas de seguridad en uso en la infraestructura, detectados durante los trabajos con asistencia del personal del Banco) y recomendaciones de mitigación de riesgos en el Plan de Acción propuesto al Banco para la implementación, integración y mantenimiento de su seguridad de información.

Consulta N° 21:

Sección 5. Metodología literal 4 (página 49), Mantenimiento. Considerando que el objetivo del proyecto hace referencia a realizar pruebas o test de intrusión sobre determinados componentes tecnológicos del Banco, podría aclarar cuál es el alcance específico requerido en este punto?

Respuesta:

El test de intrusión sobre componentes tecnológicos del Banco debe desembocar en sus correspondientes informes de vulnerabilidades (entre ellos el análisis del modelo y políticas de seguridad en uso en la infraestructura, detectados durante los trabajos con asistencia del personal del Banco) y recomendaciones de mitigación de riesgos en el Plan de Acción propuesto al Banco para la implementación, integración y mantenimiento de su seguridad de información.

Consulta N° 22:

Sección 5. Informes (página 52). Entendemos que no se requiere el re-testeo de los puntos reportados en el Informe de revisión. Es correcta nuestra interpretación?

Respuesta:

Remitirse a la Adenda Nº 3: Los informes de avances son, como lo indica el nombre, informes técnicos parciales a la UASTIC sobre los trabajos realizados en un periodo de tiempo. Los informes: Técnico y Gerencial son los finales consensuados con la UASTIC.

Consulta N° 23:

Sección 5. Referencias (página 62), apartado (a). Solicitamos presentación de declaración jurada y en caso de ser adjudicados gestionaremos las autorizaciones de nuestros Clientes a efectos de presentar los contratos solicitados.

Respuesta:

Remitirse a la Adenda Nº 3. Se admitirán también en forma paliativa una Constancia de Servicios de Seguridad de TI para Servicio de Test de Seguridad Hackeo Interno y Externo, Identificación de Amenazas y Vulnerabilidades de Seguridad de TI en la plataforma tecnológica realizados a empresas públicas y/o privadas en los últimos 3 (tres) años, como mínimo 1 (un) Contrato por año.

Consulta N° 24:
Sección 5. Criterios de calificación (página 68). Son aceptadas las certificaciones CCNA y/o CCNA SECURITY; CISA; CEH?
Respuesta:
Remitirse a la Adenda Nº 3. Se admitirán también certificaciones CCNA SECURITY, CISA, CEH.

Consulta N° 25:
Solicitamos prórroga de 15 días.
Respuesta:
El llamado ha sido prorrogado.

Consulta N° 26:
En el ítem Requisitos Generales Técnica y Económica. Sección C. "Consultores en Consorcio". Solicitamos sean aceptados consorcios con empresas internacionales.
Respuesta:
No se aceptarán consorcios con empresas internacionales; debido a que no es una contratación de carácter internacional.

Consulta N° 27:
Copia de Contratos o facturas donde el oferente demuestre haber proveído servicios de Seguridad de TI para Servicio de Test de Seguridad Hackeo Interno y Externo, Identificación de Amenazas y Vulnerabilidades de Seguridad de TI ... a empresas públicas y/o privadas en los últimos 3 (tres) años, como mínimo 1 (un) Contrato por año.
Respuesta:
Lo que se pretende es acreditar la experiencia del oferente en Servicio de Test de Seguridad Hackeo Interno y Externo, Identificación de Amenazas y Vulnerabilidades de Seguridad de TIC

Consulta Nº 28:
Respecto de la denominación "Hacking Ético Externo Caja Blanca" utilizada en las páginas 41/42, cual es la información que se plantea brindar al equipo de consultoría (Mapas de red?, Credenciales de Acceso a las Aplicaciones?)
Respuesta:
Se brindará la información necesaria para el trabajo, a ser establecida en la primera reunión con el adjudicado.

Consulta Nº 29:
Respecto a la denominación "Hacking Ético de Aplicaciones Web" (página 42), cuantas aplicaciones deberán ser revisadas como parte del alcance y con qué nivel de profundidad?.
Respuesta:
La cantidad no supera de 5 sistemas o aplicaciones, de acuerdo a lo especificado en las páginas 47 y 48 "Seguridad de las Aplicaciones Web".

Consulta Nº 30:
A que se refiere cuando se menciona en el alcance, la frase "Cincuenta exposiciones del sitio central y remotos del banco"? (Son accesos VPN que se deberán testar tomando como origen de las conexiones el laboratorio de nuestra empresa, o la casa central?)
Respuesta:
Se refiere a la cantidad de accesos remotos con el sitio central del Banco cuya exposición debe ser testeada como parte de la arquitectura de comunicaciones.

Consulta Nº 31:
Podrían por favor confirmar si como parte del alcance para test externo se ha fijado un número de 2 IPS públicas? Cuántas aplicaciones web publicadas externamente se debe revisar como parte del test externo?.
Respuesta:
Son 2 IPs públicas y 5 aplicaciones web como máximo.

Consulta Nº 32:
En la página 48 se hace referencia como parte de la metodología, a diferentes aspectos tales como "Implementación: Asistir al banco en la implementación e integración de su nueva visión de seguridad" los servicios allí descriptos, como se relacionan con el test de intrusión? Mas allá de la ejecución del proceso de evaluación, y la entrega de informes de resultado, se espera que la consultora ganadora lleve adelante los puntos allí mencionados? (Ej: Mantenimiento: Soluciones PKI, Soluciones VPN, etc.)
Respuesta:
Dichos puntos deben figurar también en el informe técnico como parte de las recomendaciones.

Consulta Nº 33:
En "Actividades" (página 49), se hace referencia en la sección "Aspectos de Seguridad de las Conexiones Externas" a temas tales como por ejemplo: "Análisis de ACL", se entregaran configuraciones de dispositivos que deberán ser analizados en modalidad caja blanca como parte del test?
Respuesta:
Se refiere a la evaluación de la seguridad de los routers de conexión. Se brindará la información necesaria para el trabajo, a ser establecida en la primera reunión con el adjudicado.

Consulta Nº 34:
Respecto de la prestación de los servicios y horarios de trabajo, se hace referencia en la página 57 a que deberán realizarse las tareas relacionadas al Hackin Etico Externo "en un fin de semana". Ese es todo el tiempo que se espera, sean realizadas las pruebas externas (Ej: desde las 00:01 hs del sábado hasta las 23:59 del domingo)?
Respuesta:
El objetivo es que los trabajos no interfieran con la operatoria normal del Banco. Se establecerá en la primera reunión con el adjudicado.

Consulta Nº 35:
Se están considerando pruebas del lado del cliente (Phishing, SpearPhishing, Client Side Attacks)?
Respuesta:
No considerados.

Consulta Nº 36:

(Página 42/93 Sección Alcance). Hacking Ético de Aplicaciones Web: se simulan los intentos de ataque reales a las vulnerabilidades de las aplicaciones determinadas por la UASTIC. No es necesaria la entrega del código fuente de la aplicación:

Cuantas aplicaciones WEB deberán ser testeadas?

La modalidad de testing, para estas aplicaciones Web, es BLACK BOX? GREY BOX? WHITE BOX?. Una sola? Dos (combinación de cualquier de las tres) o las tres?

Respuesta:

La cantidad no superan de 5 sistemas o aplicaciones.

La modalidad será preferentemente Caja Negra y Caja Blanca según lo establecido en los objetivos.

Atentamente,

DIRECCIÓN DE ADMINISTRACIÓN
UNIDAD OPERATIVA DE CONTRATACIONES
SECCIÓN COMPRAS MAYORES

DIRECCIÓN DE ADMINISTRACIÓN BNF Unidad Operativa de Contrataciones

ELIO ESPINOLA ROLON
Func. Responsable
Licitación por Concurso de Ofertas

CAROLINA AUADA DE GARDEL
Jefa
Sección Compras Mayores

P/A
RUBEN CENTURION MENDEZ
Jefe
Unidad Operativa de Contrataciones