BNF
BANCO NACIONAL DE FOMENTO
nuestro banco

Asunción, 04 de abril de 2013

SEÑOR (ES)
.....
RUC:
Teléfono:

Ref. : ACLARACIÓN Nº 1

De nuestra consideración:

Tenemos el agrado de dirigirnos a ustedes, en atención a las consultas realizadas sobre la Contratación Directa BNF CD Nº 10/2013, para el "Servicio de Test de Seguridad Hackeo Interno y Externo" para el Banco Nacional de Fomento.".

Al respecto, cumplimos en informarles cuanto sigue:

1. **Anexo 3.** Podrían indicar la cantidad de sitios web y servicios publicados en internet que deberán ser evaluados?

R= El sitio Web es el www.bnf.gov.py los servicios son 2, Banca Consumo y Control de Saldo

2. **Anexo 3.** Podrían indicar la cantidad de sitios web y servicios publicados en intranet que deberán ser evaluados?

R=La cantidad de sitios en la intranet son 5, los cuales serán dados al oferente ganador

3. **Anexo 3 (página 19).** FASES DE LA METODOLOGÍA, Item 3 – Mejoramiento de Infraestructura. Menciona que se realizará, en conjunto con el personal del Banco, un diseño de la Visión futura de su programa de seguridad, realizando el Análisis del Modelo de Seguridad y las Política. Consultas:
   - Considerando que el objetivo del proyecto hace referencia a realizar pruebas o test de intrusión sobre determinados componentes tecnológicos del Banco, podrían aclarar cuál es el alcance específico requerido en este punto?

R=La firma adjudicada deberá detectar las vulnerabilidades del esquema de seguridad y sugerir puntualidades que son necesarias a su parecer, incluir en el Plan de Seguridad del Banco.

4. **Anexo 3 (página 19).** FASES DE LA METODOLOGÍA, Item 4 – Implementación. Menciona que se debe asistir al Banco con la Implementación e Integración de su nueva visión de la seguridad de información. Consulta:
   - Considerando que el objetivo del proyecto hace referencia a realizar pruebas o test de intrusión sobre determinados componentes tecnológicos del Banco, podrían aclarar cuál es el alcance específico requerido en este punto?

R=La firma adjudicada deberá recomendar medidas de seguridad que puedan mitigar al máximo cualquier intento que viole cualquier falla de seguridad en los ítems mencionados.

5. **Anexo 3 (página 21).** ACTIVIDADES, Item 4 – Evaluación de la Seguridad de Activos Críticos. Menciona que se realizará una prueba intensiva de la seguridad lógica, sobre el control de accesos y los procedimientos de seguridad a los sistemas informáticos Seleccionados por la División de Administración de Seguridad de TI. Consultas:
   - Considerando que el objetivo del proyecto hace referencia a realizar pruebas o test de intrusión sobre determinados componentes tecnológicos del Banco, podrían aclarar cuál es el alcance específico requerido en este punto?

R=La firma adjudicada deberá juzgar el grado de seguridad de acceso a ciertas aplicaciones y bases de datos del Banco, ajustándose a los resultados esperados según el pliego.

6. **Anexo 3 (página 25).** PLAZO Y PLAN DE ENTREGA DE LA PRESTACIÓN DE SERVICIOS. Menciona que los trabajos a ser desarrollados antes del primer informe debe realizarse a distancia, y en un fin de semana, iniciando luego de los procesos afines al cierre del Banco.
   - Podrían aclarar a que se refiere el Pliego con el "*Primer Informe*"?

R=Es el informe de avances de tareas según los requerimientos del Banco, considerado como informe preliminar o resumen de actividades realizadas antes del informe formal final.

   - Los trabajos de testeo externo deben realizarse los fines de semana?

R=El objetivo final es el de no arriesgar e interferir con ninguna operatoria del Banco, teniendo en cuenta procesos críticos y días de acreditación masiva de sueldos que tiene el Banco. Sujeto a coordinación conjunta con el área de informática y de seguridad informática.

   - Por la experiencia en este tipo de trabajos, lo realizamos durante la semana, con las debidas precauciones en cada caso. Sería aceptable para el Banco adoptar esta metodología de trabajo?

R=ídem anterior.

7. **Anexo 1.** CRITERIOS DE CALIFICACIÓN. En la página 8 menciona las certificaciones CISM y/o CISSP.

Dichas certificaciones confirman la idoneidad de los técnicos que realizarán los testeos y los informes.

CISM (Certified Information Security Management) es una certificación para administradores de seguridad de la información respaldada por la ISACA (Information Systems Audit and Control Association). A diferencia de otras certificaciones de seguridad CISM define los principales estándares de competencias y desarrollo profesionales que un director de seguridad de la información debe poseer, competencias necesarias para dirigir, diseñar, revisar y asesorar un programa de seguridad de la información.

CISSP (Certified Information Systems Security Professional) es una certificación de alto nivel profesional otorgada por la ISC (International Information Systems Security Certification Consortium, Inc), con el objetivo de ayudar a las empresas a reconocer a los profesionales con formación en el área de seguridad de la información. CISSP es considerada como una de las credenciales de mayor representatividad en el ámbito de la seguridad informática a nivel mundial.

- Las certificaciones CCNA y/o CCNA SECURITY son aceptadas?

La Certificación Cisco es un plan de capacitación en tecnología de redes informáticas que la empresa Cisco ofrece. Se divide en tres niveles, de menor a mayor complejidad: Cisco Certified Network Associate,Cisco Certified Network Professional y Cisco Certified Internetwork Expert, más conocidos por sus siglas: CCNA, CCNP y CCIE. Los certificados con CCNA Security están capacitados para desarrollar tareas de administración de dispositivos en una infraestructura segura, reconocer las vulnerabilidades de la red y mitigar las amenazas de seguridad. Será aceptada con puntuación el CCNA SECURITY por ser similar a las certificaciones en seguridad mencionadas, para los trabajos en cuestión, en cuanto a redes e internet.

- La certificación CISA es aceptada para aplicar en este caso?

Certified Information Systems Auditor (CISA) es una certificación para auditores respaldada por la Asociación de Control y Auditoría de Sistemas de Información (ISACA) (Information Systems Audit and Control Association). Los candidatos deben cumplir con los requisitos establecidos por la ISACA. Serán aceptadas con puntuación por ser similar a las certificaciones en seguridad mencionadas, para los trabajos en cuestión, en cuanto a normas vigentes referentes a seguridad.

Atentamente,

CAROLINA AJADA DE GARDEL
Encargada
Sección Compras Menores

RUBEN DARIO CENTURION MENDEZ
Jefe
Unidad Operativa de Contrataciones