Asunción,.....

Señores

.....

Presente:

Tenemos el agrado de dirigirnos a ustedes, con el objeto de invitarles a participar en el procedimiento de **Contratación Directa BNF CD Nº 38/2011, ID Nº 221802 para el "Servicio de test de seguridad – Hackeo Ético – Interno y Externo para el Banco Nacional de Fomento",**

El plazo límite para la presentación de la oferta es el día: **miércoles 20 de julio de 2011 a las 10:55 hs.**

Las ofertas deberán en **DOS SOBRES CERRADOS, POR SEPARADO, INDICANDO EN CADA SOBRE CUAL CONTIENE LA PROPUESTA TECNICA Y LA PROPUESTA ECONOMICA Y AMBOS SOBRES ENDOSADOS EN UNO SOLO.**

Las ofertas deberán ajustarse a las condiciones del presente procedimiento de contratación establecidas en los siguientes documentos que se adjuntan:

Anexo 1. Instrucciones a los oferentes y datos del procedimiento de contratación directa.

Anexo 2. Formulario de presentación de oferta.

Anexo 3. Cantidad, descripción y especificaciones técnicas de los bienes/servicios requeridos. Plazo y lugar de entrega o ejecución y condiciones de pago.

Anexo4. Declaración jurada de no hallarse comprendido en las prohibiciones o limitaciones para contratar establecidas en el artículo 40 y de integridad conforme al artículo 20, inc. "w", ambos de la Ley N° 2051/03.

Anexo 5. Declaración Jurada por la cual se garantiza que no se encuentra involucrado en las practicas que violen los derechos de los niños, niñas y adolescentes referentes al trabajo infantil, estipulados en la Constitución Nacional, los convenios 138 y 182 de la Organización Internacional del Trabajo (OIT), el código del trabajo, el Código de la Niñez y la Adolescencia, demás leyes y normativas vigentes en la Republica del Paraguay.

Anexo 6. Formulario - Descripción del enfoque, metodología y plan de actividades para la ejecución del trabajo.

Anexo 7. Formulario – Composición del equipo y asignación de responsabilidades.

Anexo 8. Formulario – Curriculo del/Los Profesionales/Es Propuestos.

Anexo 9. Formulario – Calendario de actividades del personal.

Anexo 10. Formulario – Plan de trabajo.

Atentamente,

MARIA ELENA CAMPOS KRAUER
RESPONSABLE UOC
BANCO NACIONAL DE FOMENTO

DIRECCION DE ADMINISTRACION Y FINANZAS
UNIDAD OPERATIVA DE CONTRATACIONES
BNF

Anexo 1

Instrucciones para los oferentes y datos del procedimiento de Contratación Directa.

1. La Convocante, BANCO NACIONAL DE FOMENTO emite estos Documentos que forman parte de las condiciones de la **Contratación Directa BNF CD Nº 38/2011, ID Nº 221802 para el "Servicio de test de seguridad – Hackeo Ético – Interno y Externo para el Banco Nacional de Fomento".**

La cantidad, descripción, las especificaciones técnicas, plazo y lugar de entrega (o de prestación de servicios o de realización de las obras) y condiciones de pago se especifican en el Anexo 3.

2. Los fondos para la presente contratación se encuentran expresamente previstos en el rubro **"260 "SERVICIOS TECNICOS Y PROFESIONALES"** del Presupuesto General de la Nación.

3. Podrán participar en este procedimiento los Oferentes domiciliados en la República del Paraguay, que no se encuentren comprendidos en las prohibiciones o limitaciones para presentar propuestas o para contratar establecidas en el artículo 40 de la Ley N° 2051/03.

4. Los Oferentes que participen en este procedimiento de contratación deberán observar los más altos niveles éticos. La Convocante actuará frente a cualquier hecho o reclamación que se considere fraudulento o corrupto. Si se comprueba que un funcionario público, o quien actúe en su lugar, y/o el Oferente o adjudicatario propuesto en un proceso de contratación, ha incurrido en prácticas fraudulentas o corruptas,
   - Se descalificará la oferta del oferente directamente involucrado en las prácticas fraudulentas o corruptivas;
   - Se remitirán los antecedentes del oferente directamente involucrado en las prácticas fraudulentas o corruptivas, a la Dirección Nacional de Contrataciones Públicas, a los efectos de la aplicación de las sanciones previstas en el Título Séptimo de la Ley N° 2051/03.
   - Se presentará la denuncia penal ante las instancias correspondientes si el hecho conocido se encontrare tipificado en la legislación penal.

5. Ninguna de las condiciones contenidas en este documento, así como en las ofertas presentadas por los participantes podrán ser negociadas

6. Todo Oferente potencial que requiera alguna **Aclaración** sobre estos Documentos deberá comunicarse con la Convocante por escrito hasta el **día martes 12 de julio de 2011 hasta las 12:00 hs**. en la dirección *Independencia Nacional y 25 de Mayo – Unidad Operativa de Contrataciones BNF - Casa Matriz – Planta Baja*. La Convocante responderá por escrito a todas las solicitudes de aclaración, siempre que dichas solicitudes las reciba hasta la fecha límite para realizar consultas. La Convocante enviará copia de las respuestas, incluyendo una descripción de las consultas realizadas, sin identificar su fuente, a todos los oferentes invitados. Así mismo, difundirá dichas respuestas a través del Portal de la Dirección Nacional de Contrataciones Públicas (www.contratacionesparaguay.gov.py)

7. La Convocante podrá, modificar estos documentos mediante adendas numeradas hasta **el día viernes 15 de julio del 2011 hasta las 12:00 hs**. Toda Addenda emitida por la Convocante, formará parte integral de los Documentos y serán notificadas por escrito a los oferentes invitados. Además, serán difundidas a través del Portal de la Dirección Nacional de Contrataciones Públicas (www.contratacionesparaguay.gov.py). La Convocante podrá, prorrogar el plazo de presentación de ofertas a fin de dar a los posibles Oferentes un plazo razonable para que puedan tomar en cuenta las adendas en la preparación de sus ofertas.

DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS – UNIDAD OPERATIVA DE CONTRATACIONES – BNF

8. El Oferente financiará todos los costos relacionados con la preparación y presentación de su oferta, y la Convocante no estará sujeto ni será responsable en ningún caso por dichos costos, independientemente de la modalidad o del resultado del proceso de contratación.

9. La Oferta, así como toda la correspondencia y documentos relativos a la oferta intercambiados entre el Oferente y la Convocante deberán ser redactados en idioma castellano. ***No*** se permitirán la presentación de catálogos y/o folletos en el idioma de origen de los bienes, que no sean en idioma español (castellano).

10. **El oferente deberá presentar con su oferta los siguientes documentos:**

Sobre Nº 1 – OFERTA TECNICA

a) Fotocopia simple de la cédula de identidad del firmante de la oferta;
b) Fotocopia simple de la cédula tributaria del oferente (RUC);
c) Fotocopia simple de su última declaración de IVA y/o del Impuesto a la Renta;
d) Fotocopia simple de la patente Municipal del Oferente;
e) Fotocopia simple de los estatutos y sus modificaciones (en caso de ser persona jurídica);
f) Fotocopia simple del documento que acredite la capacidad del firmante, cuando corresponda (poder o documentos estatutarios como acta de asamblea o de directorio).
g) Declaración jurada de no hallarse comprendido en las prohibiciones o limitaciones para contratar establecidas en el artículo 40 y de integridad conforme al artículo 20, inc. "w", ambos de la Ley N° 2051/03, de acuerdo con lo dispuesto en la Resolución N° 330/07 de la Dirección Nacional de Contrataciones Públicas. Según modelo que se adjunta.
h) Declaración Jurada por la cual se garantiza que no se encuentra involucrado en las practicas que violen los derechos de los niños, niñas y adolecentes referentes al trabajo infantil, estipulados en la Constitución Nacional, los convenios 138 y 182 de la Organización Internacional del Trabajo (OIT), el código del trabajo, el Código de la Niñez y la Adolescencia, demás leyes y normativas vigentes en la Republica del Paraguay.
i) Anexo 6: Formulario - Descripción del enfoque, metodología y plan de actividades para la ejecución del trabajo.
j) Anexo 7: Formulario – Composición del equipo y asignación de responsabilidades.
k) Anexo 8: - Formulario – Curriculo del/Los Profesionales/Es Propuestos.
l) Anexo 9: - Formulario – Calendario de actividades del personal.
m) Anexo 10 – Formulario – Plan de trabajo.
n) El curriculum del oferente, - presentación del consultor- incluyendo un breve relato de la trayectoria donde se haga constar su experiencia específica, en instituciones públicas y/o privadas y/o con Organismos Internacionales para las cuales ha trabajado, los años de trabajo y tareas desarrolladas.
o) Fotocopias de por lo menos 2 (dos) contratos suscriptos con otras empresas, en trabajos similares a lo solicitado.

10.1 **El oferente deberá presentar con su OFERTA ECONOMICA: (Sobre Nº 2)**

a) El Formulario de oferta suscripto por el oferente en base al formulario estándar que se adjunta en Anexo 2.

Observaciones:
Los oferentes que tengan la constancia del Sistema de Información de Proveedores del Estado (SIPE) no necesitarán presentar los documentos indicados en los incisos a, b), c), d), e), f), g) y h), cuando en el mismo conste que dichos documentos se hallan activos, para la presentación de la oferta.

En caso de no estar inscripto y de salir adjudicado, deberá hacerlo en el plazo de 24 (veinticuatro) horas de haber recibido la notificación de adjudicación, **debiendo presentar la constancia de la inscripción a la Unidad Operativa de Contrataciones, para la comunicación de la adjudicación a la Dirección Nacional de Contrataciones Públicas.**

11. La moneda de oferta y pago será expresada en **GUARANÍES**. **La cotización en moneda diferente será motivo de rechazo de la oferta.** Se mantendrá la moneda de la oferta como moneda del contrato.

12. **Las ofertas deberán permanecer válidas por 60 (sesenta) días,** contado a partir de la fecha límite para la presentación de ofertas establecida por la Convocante. Toda oferta con un período de validez menor será rechazada por la Convocante. El Oferente garantizará el mantenimiento de su oferta durante dicho plazo de validez mediante la declaración jurada que suscribe al firmar el formulario de oferta adjunto como anexo 2.

13. **Las ofertas deberán presentarse en 2 (dos) sobres cerrados, por separados, indicando en cada sobre cual contiene la Propuesta Técnica y la Propuesta Económica y ambos sobres ensobrados en uno solo, dirigidos a la Convocante**. La apertura de la oferta técnica se realizará conforme se detalla más abajo. Las ofertas económicas quedaran en guarda en la UOC del BNF, hasta la fecha fijada para el acto de apertura de dicha oferta económica.

14. **Todas las páginas de la oferta deberán estar firmadas y foliadas por el oferente**. Los textos entre líneas, tachaduras o palabras superpuestas serán válidos solamente si llevan la firma o la media firma de la persona que firma la Oferta. La falta de foliatura de los documentos de la oferta, podrá ser salvada, únicamente en el acto de apertura, quedando constancia de ello en el acta respectiva.

15. Las ofertas deberán ser recibidas por la Convocante en *el Banco Nacional de Fomento* y a más tardar el día **miércoles 20 de julio de 2011 hasta las 10:55 horas.** La Convocante no considerará ninguna oferta que llegue con posterioridad al plazo límite para la presentación de ofertas. Toda oferta que reciba la Convocante después del plazo límite para la presentación de las ofertas será declarada tardía y será rechazada y devuelta al Oferente remitente sin abrir.

16. La Convocante llevará a cabo el **Acto de Apertura las ofertas técnica** en público en *la Unidad Operativa de Contrataciones del BNF – Casa Matriz Planta Baja* el **día miércoles 20 de julio de 2011 a las 11:00 horas**. Al concluir el acto de apertura, se labrará un acta de conformidad a las disposiciones del artículo 54 del Decreto N° 21909.

La Convocante comunicará con 3 (tres) días hábiles de anticipación la fecha y hora de realización del acto de **Apertura de las ofertas Económica,** el cual será realizado en público en la Unidad Operativa de Contrataciones del BNF – Casa Matriz Planta Baja. Al concluir el acto de apertura, se labrará un acta de conformidad a las disposiciones del artículo 54 del Decreto N° 21909.

17. **Para la evaluación y comparación de las ofertas**, la Convocante utilizará los siguientes criterios:

Capacidad legal:

No estar comprendido en las prohibiciones o limitaciones para contratar. Este requisito se acredita con el formulario de presentación de oferta que contiene las declaraciones juradas;

Tener capacidad legal para presentar ofertas y ejecutar el contrato. Este requisito se acredita con el poder, con los estatutos y con la declaración jurada de tener las calificaciones para ejecutar el contrato. El objeto de la sociedad debe permitir que el oferente pueda ejecutar el contrato requerido. En caso de poseer la constancia del SIPE, se acredita con dicha constancia.

DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS – UNIDAD OPERATIVA DE CONTRATACIONES – BNF

Capacidad Técnica y Experiencia:

- Deberá cumplir con los requisitos mínimos exigidos y detallados en el Anexo 3 **para el "Servicio de test de seguridad – Hackeo Ético – Interno y Externo para el Banco Nacional de Fomento".**
- Curriculum de la empresa oferente, donde conste la experiencia especifica solicitada, según documentos a ser presentados descriptos en el Anexo 3.
- Fotocopias de por lo menos 2 (dos) contratos suscriptos con otras empresas, en trabajos similares a lo solicitado.

EL PRESENTE LLAMADO SERA ADJUDICADO A LA EMPRESA QUE PRESENTE LA OFERTA ECONOMICA MAS BAJA, SIEMPRE QUE LA MISMA CUMPLA CON TODOS LOS REQUESITOS TECNICOS Y LEGALES.

Para ello será utilizada la Selección basada en precio, del Art. 97 del Decreto Reglamentario, de conformidad con lo establecido en el artículo 54 inciso c) de la Ley, se podrá utilizar este método para seleccionar Consultoras que hayan de realizar trabajos de tipo estándar o rutinario.

Se invita a las Consultoras a presentar ofertas en dos sobres separados. Primero se abren los sobres con las ofertas técnicas, las que se evaluarán. Aquellas que obtienen menos del puntaje mínimo, —que para el caso será de 70 puntos sobre 100—, se rechazan y los sobres con las ofertas financieras de las Consultores restantes se abren en público, para lo cual se realizará una nueva comunicación. A continuación se selecciona a la firma Consultora que ofrece el precio más bajo. En este método, la calificación mínima se establecerá teniendo presente que todas las oferta que excedan el mínimo compiten sólo con respecto al costo.

CRITERIOS A EVALUAR

PERFIL DE LA CONSULTORA

- La firma Consultora deberá acreditar una comprobada experiencia general en realización de trabajos relacionados a Seguridad de Sistemas Informáticos y tareas afines.
- Experiencia específica, directa y comprobada sobre la realización de trabajos en actividades similares a las solicitadas en estos términos de referencia.
- La Firma deberá contar en el plantel asignado a trabajar en este proyecto, con al menos dos profesionales con la experiencia requerida y con certificaciones CCNA, CCNA SECURITY, CISM y/o CISSP, debiendo presentar junto con la oferta los documentos o certificados que lo acrediten.

DIRECCION DE ADMINISTRACION Y FINANZAS – UNIDAD OPERATIVA DE CONTRATACIONES – BNF

CRITERIOS DE CALIFICACIÓN Y EVALUACIÓN

El puntaje máximo es de 100 puntos y el mínimo requerido para precalificar es de 70 % o más del puntaje total. Los conceptos y ponderaciones se desarrollan a continuación:

CONCEPTOS	Puntaje Máximo
1. Evaluación de la Propuesta Técnica	20
1.1 Alcance de los servicios	10
1.2 Plan de Trabajo y Cronograma	10
2. Evaluación del Equipo de Trabajo	**80**
2.1 Formación Académica	30
2.2 Experiencia General	10
2.3 Experiencia Específica	40
TOTAL	**100**

Criterios de evaluación:

Alcance de los Servicios y Plan de trabajo: Se calificará de la siguiente manera:

- No presenta plan de trabajo ni Alcance de los servicios. **EL OFERENTE SERÁ ELIMINADO.**
- Presenta plan de trabajo general y una descripción sucinta del alcance de los servicios. **5 PUNTOS.**
- Presenta un plan de trabajo con un cronograma en el cual se detallan entre otras, las actividades a realizarse, las fechas de inicio y fin, la vinculación entre las mismas y la asignación del personal a cargo, de manera consistente; detallando además en forma detallada el alcance de los servicios **10 puntos.**

Evaluación del Equipo de Trabajo

- **Formación académica**: hasta un máximo de 30 puntos, 10 puntos por cada certificación poseída por los integrantes del equipo de trabajo.

- **Experiencia general**: hasta un máximo de 30 puntos. A la firma consultora que posea experiencia profesional en realización de trabajos relacionados a experiencia general en realización de trabajos relacionados a Seguridad de Sistemas Informáticos (definición de políticas, implantación de procesos basados en ISO 27001) y tareas afines, se le otorgaran 6 puntos por cada experiencia general, hasta un máximo de 5 experiencias.

- **Experiencia específica**: A la firma que posea experiencia profesional específica con objetivos similares (test de seguridad o hacking ético) a los solicitados en estos términos de referencia, se otorgarán 10 puntos por cada proyecto. Hasta un máximo de 40 (cuarenta) puntos.

Además se aplicarán, en lo pertinente, las disposiciones establecidas en los artículos 56, 57, 58, 59, 60, 61, 62, 63, 91 y 96 del Decreto Reglamentario de la Ley N° 2051/03.

Las ofertas se aceptarán siempre que provengan de personas físicas o jurídicas que cuenten con la solvencia técnica, económica y legal suficiente para responder a los compromisos asumidos frente al Estado Paraguayo y que su actividad comercial o industrial se encuentre vinculada con el tipo de bienes, servicios u obras a contratar.

18. El Sistema de Adjudicación de la presente contratación es: **POR EL TOTAL**

19. La adjudicación se efectuará conforme con los criterios establecidos en el artículo 63 del Decreto Reglamentario de la Ley N° 2051/03 de Contrataciones Públicas. **La Convocante se reserva el derecho de declarar desierta o cancelar el proceso de contratación, únicamente conforme con lo dispuesto en los artículos 30 y 31 de la Ley Nº 2051/03 de Contrataciones Públicas**, sin que por ello incurra en responsabilidad alguna frente a los Oferentes.

20. La adjudicación será notificada por nota a cada uno de los oferentes. Deberá difundirse además en el Portal de la Dirección Nacional de Contrataciones Públicas (www.contratacionesparaguay.gov.py).

21. Las personas interesadas podrán protestar por escrito ante la Dirección Nacional de Contrataciones Públicas, contra los actos que contravengan las disposiciones que rijan la materia objeto de este documento, dentro de los diez (10) días hábiles siguientes a aquel en que éste ocurra o el Oferente tenga o deba haber tenido conocimiento del acto impugnado, de acuerdo a la Ley N° 2051/03 de Contrataciones Públicas.

22. Cualquier persona puede realizar las denuncias de supuestos hechos de corrupción o de irregularidades en este proceso de contratación o en cualquier otro, que tenga conocimiento, a través del Portal de Contrataciones Públicas (www.contratacionesparaguay.gov.py), utilizando el Programa de Protección al Denunciante, que garantiza la confidencialidad de los datos del denunciante, y cuya investigación puede monitorearse a través del Portal.

23. En caso de que al momento de la entrega y apertura de ofertas no se contare con el número mínimo de tres oferentes, la convocante podrá prorrogar las citadas fechas conforme a lo establecido por la resolución Nº 805/09.

MARIA ELENA CAMPOS KRAUER
RESPONSABLE UOC
BANCO NACIONAL DE FOMENTO

DIRECCION DE ADMINISTRACION Y FINANZAS
UNIDAD OPERATIVA DE CONTRATACIONES
BNF

Anexo 2
Formulário de carta/oferta. Procedimiento de Contratación Directa.

Asunción,.....

Señores:

BANCO NACIONAL DE FOMENTO

Contratación Directa BNF CD Nº 38/2011 para el "Servicio de test de seguridad – Hackeo Ético – Interno y Externo para el Banco Nacional de Fomento".

ID Nº 221802

Nos dirigimos a ustedes en el procedimiento de contratación directa de referencia, con el objeto de presentar oferta y declarar bajo juramento cuanto siguiente:

1. No nos encontramos comprendidos en las prohibiciones o limitaciones para contratar establecidas en el artículo 40 de la Ley N° 2051/03;

2. Nos abstenemos, por nosotros mismos o a través de interpósitas personas, de adoptar conductas orientadas a que los funcionarios o empleados de la Convocante induzcan o alteren las evaluaciones de las propuestas, el resultado del procedimiento u otros aspectos que nos otorguen condiciones más ventajosas con relación a los demás participantes.

3. Contamos con las calificaciones requeridas para ejecutar el contrato.

4. Hemos examinado y no hallamos objeción alguna a las condiciones de este procedimiento de contratación directa, incluyendo las adendas No: _____*[indicar el número y la fecha de emisión de cada Enmienda];*

5. En las condiciones requeridas en los documentos de este procedimiento de contratación directa, ofrecemos proveer los Bienes/Servicios cuya descripción y precios unitarios y totales, incluidos los tributos o gravámenes que correspondieran, se indican en la planilla siguiente:

1	2	3	4	5	6
Ítem	**Código Catalogo**	**Descripción del Bien**	**Unidad de Medida**	**Cantidad**	**Precio Unitario (IVA Incluido)**
1	80101507-003	**Contratación del "Servicio de test de seguridad – Hackeo Ético – Interno y Externo para el Banco Nacional de Fomento", según especificaciones técnicas.**	Unidad	1	
GENERAL			**TOTAL**		

El precio total es de guaraníes_____
en letras)_____

6. **Nuestra oferta se mantendrá vigente por un período de 60 (sesenta) días**, contados a partir de la fecha límite fijada para la presentación de las ofertas. Esta oferta nos obligará y podrá ser aceptada en cualquier momento antes de la expiración de dicho período.

7. Entendemos que esta oferta, junto con su debida aceptación por escrito incluida en la notificación de adjudicación, constituirán una obligación contractual entre nosotros, hasta que el Contrato formal (o la Orden de compra) haya sido perfeccionado por las partes.

8. Entendemos que la Convocante tiene el derecho de cancelar o declarar desierto el procedimiento de contratación o rechazar todas las ofertas en cualquier momento con anterioridad a la adjudicación del Contrato, conforme con lo dispuesto en los artículos 30 y 31 de la Ley Nº 2051/03 de Contrataciones Públicas, sin que por ello incurra en responsabilidad alguna frente a los Oferentes.

_____*(firma)*_____
Oferente

Datos del oferente: (Especificar el nombre completo de la empresa, si la oferta es presentada por una persona jurídica.)

Datos del firmante de la oferta: (Indicar el nombre, documento de identidad y cargo del firmante de la oferta).

Notas

1. Las ofertas deben ser presentadas en forma **IMPRESA**
2. En cumplimiento a la Resolución Nº 936/09, queda prohibida la utilización de decimales en los precios totales y unitarios. El incumplimiento de esta normativa conllevará el rechazo de la oferta.

DIRECCION DE ADMINISTRACION Y FINANZAS
UNIDAD OPERATIVA DE CONTRATACIONES
BNF

Anexo 3.

1. **Cantidad del bien y/o Servicio solicitado:**
   1 (un) Servicio

2. **Descripción**

"Servicio de test de seguridad – Hackeo Ético – Interno y Externo para el Banco Nacional de Fomento",

3. **Especificaciones técnicas del servicio requerido**

Item	Código de Catalogo	Descripción
1	81111801-001	Contratación del **"Servicio de test de seguridad – Hackeo Ético – Interno y Externo para el Banco Nacional de Fomento"**, según Especificaciones Técnicas.

OBJETIVOS

La Superintendencia de Bancos emitió la resolución 179/2005, por la cual reglamenta los procedimientos de seguridad para las transacciones electrónicas. Como parte de dicha normativa establece la necesidad de realizar pruebas de intrusión por lo menos una vez al año. El Banco Nacional de Fomento considera importante la adecuación de sus sistemas a los requisitos de la mencionada normativa, motivo por el cual solicita asistencia en la revisión de la seguridad de sus sistemas internos con el fin de garantizar la disponibilidad y confiabilidad adecuada para soportar la dinámica del negocio y el crecimiento proyectado.

En este contexto ha decidido realizar una contratación de servicios profesionales de una empresa de consultoría y servicios profesionales en el área de Seguridad de la Información, sin compromisos vigentes con proveedores de hardware y/o software para el Banco, para la realización de un intento de intrusión controlado interno, con conocimiento de la infraestructura tecnológica, con el fin de identificar el grado de exposición a las amenazas y vulnerabilidades de sus equipos conectados a internet e intranet que soportan la provisión de servicios a sus clientes y empleados. El servicio de Test de Penetración Interno y Externo permite determinar en forma precisa el nivel de seguridad real y actual instalado y operativo, detectar los expuestos de seguridad existentes de información y aplicaciones sensibles y/o críticas del Banco además de en los equipos de comunicación y servidores donde corren dichos sistemas y aplicaciones, proponer las soluciones generales y específicas a los mismos y definir planes de acción para mitigar los riesgos remanentes, concurriendo al logro del objetivo general que es el de elevar el nivel de seguridad real de toda la instalación del Banco, preservando la Confidencialidad, Integridad y Disponibilidad de los Sistemas.

DIRECCION DE ADMINISTRACION Y FINANZAS
UNIDAD OPERATIVA DE CONTRATACIONES
BNF

Los objetivos específicos son:

- Detectar vulnerabilidades y/o problemas de seguridad que puedan ser aprovechados por atacantes.
- Evaluar la efectividad y respuesta de los sistemas de seguridad implementados (firewalls, detección de intrusos y otros sistemas).
- Analizar y determinar el nivel de exposición de la infraestructura tecnológica de acuerdo con las vulnerabilidades detectadas.
- Presentar recomendaciones concretas que permitan corregir los problemas y brechas de seguridad detectados y minimizar los riesgos asociados.

ALCANCE

El Diagnóstico se focalizará en determinar el nivel de seguridad de los equipos de comunicación, servidores y aplicaciones que la soporta.

A continuación se citan las tareas a desarrollar:

Realizar el descubrimiento de la infraestructura presente en la red interna, incluyendo entre otras, las siguientes actividades

- Identificación de equipos que se encuentren dentro de los rangos de direcciones IP accesibles desde el punto de acceso otorgado al personal de la firma contratada.
- Identificación de los servidores y servicios asociados que dan soporte a la infraestructura de red (servidores, estaciones de trabajo, dispositivos de comunicaciones, otros dispositivos)
- Identificación de otras conexiones de la red LAN / WAN accesibles desde el punto de acceso otorgado al personal de la firma contratada.

Estimar los siguientes equipos de la red interna, pudiendo el Banco incluir más equipos, los que serán considerados como adicionales

- Siete Servidores Windows.
- Cuatro Servidores AS400 (Incluido el centro alterno).
- Cuatro Servidores Físicos
- Diez y nueve Switches.
- Ocho Ruteadores.
- Cincuenta Estaciones de Trabajo.
- Una Central IP
- Tres Dispositivos Wireless/Access Points (únicamente vía LAN) de Casa Matriz
- Nueve Enlaces VPN/WAN contra redes del Banco
- Tres Firewalls entre sitio central y remotos del Banco

DIRECCION DE ADMINISTRACION Y FINANZAS
UNIDAD OPERATIVA DE CONTRATACIONES
BNF

El número de estaciones de trabajo e impresoras mencionado es una muestra representativa del universo del Banco. Los resultados obtenidos a partir de esta muestra permitirán inferir en forma estimada el nivel de seguridad de la instalación del Banco.

El alcance comprende los siguientes dispositivos y servidores:

- Tres direcciones IP Pública.

Análisis del sistema de acceso remoto

- Identificación, si lo hubiera, del sistema de acceso remoto RAS utilizado.
- Determinación del tipo de sistema operativo y el software en uso.
- A partir de la identificación del posible acceso remoto, intento de acceder a la red interna a través de dicho vínculo.
- Pruebas de ataques "de fuerza bruta" sobre usuarios *default* del sistema que se detecten, tratando de determinar passwords triviales.
- Análisis e intento de explotación de vulnerabilidades de seguridad que afectan a nivel de sistema operativo y el software utilizado.
- Determinación del nivel de seguridad del sistema de validación utilizado (usuario y password, token de acceso, one-time-passwords, etc).

Situación de la seguridad en la conexión a Internet

- Aplicación de un conjunto completo de pruebas orientadas a determinar los rangos de direcciones IP involucradas, así como equipos y dispositivos activos en los rangos identificados.
  - Intento de transferencias de zonas desde servidores DNS
  - Enumeración de sistemas por técnicas de diccionario contra DNS
  - Enumeración de información mediante SNMP, en los casos que sea posible.
  - Seguimiento de rutas (UDP, TCP e ICMP)
  - Detección de hosts activos mediante técnicas de estímulo/respuesta
  - Obtención de información en registros públicos de Internet.
- Relevamiento lógico de plataforma, intentando detectar:
  - Routers.
  - Firewalls/IPS.
  - Balanceadores de carga
  - Servidores de Correo Electrónico.
  - Servidores de DNS.
  - Servidores Proxy.
  - Servidores FTP.
  - Servidores WEB.
  - Terminadores VPN y sistemas de Acceso Remoto
  - Sistemas de Bases de Datos.
  - Otros sistemas inusuales.
- *Scanning* de todos los puertos (1 al 65535) abiertos a nivel TCP, en los diferentes sistemas de la Empresa que se detecten en el barrido de las direcciones IP en Internet.
- *Scanning* de todos los puertos (1 al 65535) abiertos a nivel UDP, en los diferentes sistemas de la Empresa que se detecten en el barrido de las direcciones IP en Internet.

DIRECCION DE ADMINISTRACION Y FINANZAS
UNIDAD OPERATIVA DE CONTRATACIONES
BNF

- Análisis de las direcciones IP involucradas, evaluando vínculos de conexión y proveedores de Internet.
- Sobre cada uno de los equipos activos detectados, pruebas remotas para determinar qué sistemas operativos están utilizando (OS Fingerprinting) y qué aplicaciones se están ejecutando (Service Fingerprinting).
- Sobre todos los equipos detectados, se realizará una evaluación del nivel de seguridad tratando de determinar todos los puntos débiles y las vulnerabilidades que posean.
  - Se analizará, por cada servicio brindado, los expuestos que estos pudieran manifestar por configuraciones incorrectas o vulnerabilidades reportadas que afecten a la versión del software en cuestión.
- Análisis de los protocolos de ruteo (RIP, OSPF, BGP, EIGRP etc.) y de los protocolos ruteados (TCP/IP, IPX/SPX, etc.) por los gateways de perímetro.
- Pruebas de acceso en sistemas con autenticación mediante la identificación de los mismos y el uso de credenciales por defecto documentadas por el fabricante.
- Investigación sobre la existencia de *backdoors* en los Servidores y ruteadores detectados de forma externa.
- Evaluación del nivel de autenticación utilizado en los Concentradores de VPN y otros mecanismos de acceso remoto implementados (RAS, Terminal Servers, Citrix, etc.),
- Testeo de la cobertura existente contra ataques de denegación de servicio (Denial of Service), mediante la realización de un conjunto completo de pruebas que incluyen ataques del tipo Bonk, Boink, NewTear, Nestea, Land, La Tierra, Ping of Death y otros.

Intento de acceso a través de los vínculos encontrados

- Búsqueda y enumeración de cuentas y usuarios de correo electrónico válidas. Generación de diccionarios de ataque utilizando como entrada las cuentas obtenidas.
- Ataques por método de diccionario sobre los mecanismos de autenticación de los servicios de acceso remoto detectados:
  - Servicios con bloqueo de cuenta habilitado: Sólo se realizarán 2 pruebas por cada usuario enumerado y cuentas por defecto.
  - Servicios sin bloqueo de cuenta habilitado: Se realizarán ataques sobre la contraseña de los usuarios enumerados con diccionarios cuyo tamaño será acorde a los tiempos estipulados para el testeo.
- Intento de evitar los controles de seguridad impuestos por los Firewalls y Routers de perímetro detectados, mediante las siguientes pruebas:
  - Identificación de direcciones IP asignadas en cada subred.
  - Envío de paquetes TCP/IP malformados.
  - Medición del alcance los sistemas protegidos por técnicas de spoofing y source port attack.
  - Explotación de vulnerabilidades conocidas en un entorno controlado.
- Intento de evasión de IDS/IPS, mediante las siguientes pruebas:
  - Ataques de denegación de servicio para IDS/IPS.
  - Fragmentación de tráfico.
  - Envío de tráfico mal formado en los distintos niveles del stack TCP/IP.
- Intento de escalación de privilegios sobre todos los sistemas del perímetro. Intento de acceso a los principales sistemas internos de la empresa empleando los privilegios obtenidos sobre la plataforma pública.
- Pruebas de concepto sobre manipulación de información en bases de datos de backend de servicios Web.

DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS – UNIDAD OPERATIVA DE CONTRATACIONES – BNF

- **Seguridad de las Aplicaciones Web**
  - Análisis del nivel de seguridad que poseen los servidores de Web, Aplicaciones y el software que utilizan para administrarlo. Se investigarán las diferentes vulnerabilidades existentes y se las probará realizando:
    - Detección remota del Web Server utilizado y versión.
    - Detección remota del sistema operativo base del Web Server utilizado.
    - Detección de extensiones utilizadas: WebDAV, ASP.NET, Frontpage, OWA, IIS ISAPI, PHP, OpenSSL, etc.
    - Análisis de vulnerabilidades conocidas.
    - Análisis de aplicaciones demo instaladas.
    - Análisis de instalaciones default.
    - Intento de explotación de vulnerabilidades sobre el Web Server, en un entorno controlado.
    - Análisis de código fuente HTML.
    - Análisis de aplicaciones utilizadas.
    - Análisis del Application Server utilizado.
    - Prueba de seguridad sobre la Base de Datos de backend detectada.
    - Análisis de mecanismos de manejo de sesión.
    - Análisis de la posibilidad de explotar SQL-Injection sobre la Base de Datos.
    - Test de XPath Injection, Response Splitting, Cross-Site Scripting, Directory Trasversal, Parameter Tampering, Remote File Inclusion, Phishing Vectors, NULL Bytes, Cross Site Request Forgeries, LDAP Injection, Inverse Lookup Log Corruption, Directory Enumeration, Source Disclosure, OS Commanding.
    - Intento de acceso a interfaces Administrativas.
    - Evaluación de mecanismos de autenticación empleados.
    - Testing de WebServices públicos.
    - Intento de Vertical Privilege Escalation y Horizontal Privilege Escalation.
    - Análisis de WAF.

Más datos, como podrían ser direcciones IP o usuarios, serán proporcionados a la empresa que resulte adjudicada.

METODOLOGÍA

La metodología a ser utilizada debe ser altamente efectiva en la detección de conjuntos y/o combinaciones de expuestos y orientada a detectar combinaciones no lineales de vulnerabilidades e identificar potenciales vías de intrusión a través de las mismas.

Al mismo tiempo debe ser compatible a los siguientes estándares:

- ISO-17799 (BS 7799) Remote Auditing and Testing requirements.
- ISO 27001 y sus relacionadas
- Metodología OSSTMM (Open Source Security Testing Methodology Manual)
- Metodología OWASP (Open Web Application Security Project)
- Best Practices in Computer Security
- GNU Public License, HIPAA
- BASILEA II, Sarbanes Oaxley y COBIT AUDIT GUIDELINES (COBIT: Control Objectives for Information and Related Technology)

DIRECCION DE ADMINISTRACION Y FINANZAS
UNIDAD OPERATIVA DE CONTRATACIONES
BNF

Debe utilizar un enfoque de trabajo que va de lo general al detalle, metodología de trabajo con bases de conocimiento y uso de herramientas automáticas, alineándose con estándares internacionalmente aceptados para la práctica de seguridad informática.

A fin de alcanzar el objetivo definido, se desarrollarán las actividades necesarias para conocer, en forma detallada y objetiva, el efectivo nivel de seguridad de los equipos que el Banco utiliza y detectar eventuales vulnerabilidades ante posibles ataques informáticos perpetrados de forma interna y externa.

En línea con la realización de un profundo análisis y la no interferencia con la operatoria diaria del Banco, se empleará la modalidad Gray Box para el diagnóstico de la aplicación y Black Box para el servidor Web, dispositivos, aplicaciones y sistemas que se detecten en forma remota a través de Internet.

Se aplicará metodología de análisis recursivo de capas, orientada a detectar combinaciones no lineales de vulnerabilidades e identificar potenciales vías de intrusión a través de las mismas. Esta metodología ha demostrado ser altamente efectiva en la detección de conjuntos y/o combinaciones de expuestos que no surgen de la aplicación de sistemas de testeo estándar. Consecuentemente, permite elaborar un diagnóstico de seguridad completo y objetivo, como base imprescindible para la definición e implantación de soluciones eficaces.

El Estudio se desarrollará en etapas caracterizadas por las siguientes **Pruebas Técnicas y Trabajo de Campo:**

1. **Reconocimiento Superficial:** Network Footprinting (se intentará obtener la mayor cantidad de información posible del objetivo), rangos IP válidos, host vivos, ruteo hasta el objetivo, información de DNS (rangos IP Internos, servidores, transferencia de zona, subdominios), whois, presencia en internet, ingeniería social, dumpster diving, copia del sitio web, information gathering.
2. **Reconocimiento en Profundidad y Enumeración:** Fingerprint de Sistemas Operativos, Servidores, Dispositivos de Red, Dispositivos de protección (Detectores de Intrusos, Firewalls, filtros); escaneo de puertos, reconocimiento de servicios puestos en escucha, banner grabbing, sniffing de protocolos.
3. **Enumeración de vulnerabilidades** comunes a los servicios puestos en escucha, tests manuales de cada uno de los host vivos. Vulnerability Assessment de Dispositivos, Sistemas Operativos, Servidores, Aplicaciones mediante el uso de herramientas automáticas. Web assessment, wireless assessment.
4. **Definición de las Herramientas a Utilizar:** Se analizan los resultados arrojados por las etapas anteriores y se preparan los ambientes para realizar las etapas posteriores.
5. **Ataque Puro o Penetración:** Se ejecutan los ataques predefinidos en ambiente controlado, dependiendo de los objetivos los ataques pueden ser sniffing pasivo, sniffing activo, recolección de credenciales de acceso, password cracking, ataques a los servidores, ejecución de código exploit, Inyección de código malicioso en aplicaciones (SQL Injection, Cross Site Scripting, Representación Canónica), ataques a los dispositivos, búsqueda de credenciales default, wep cracking, etc. Se obtienen evidencias del acceso o del ataque.

puede ser captura de un trofeo, sembrado de un trofeo o reducción de la capacidad del servicio. Ataques de denegación de servicio en ambientes controlados a servidores y dispositivos de comunicación.

6. **Redefinición de pruebas y herramientas** a utilizar en base a resultados obtenidos
7. **Borrado de rastro y evidencias**: Se intentará borrar los rastros de accesos: logs, registro de eventos, huellas en dispositivos, aplicaciones y sistemas operativos.
8. **Consolidación:** Mediante el uso de técnicas no destructivas se intentará lograr un acceso a los sistemas para evidenciar el compromiso del sistema, pueden ser credenciales de usuario obtenidas durante el test, dando de alta un nuevo usuario, levantando algún servicio cerrado. Posteriormente se volverá al estado anterior a la consolidación.

Las distintas fases de la metodología deben ser:

1. **Detección y Evaluación del Perfil de Seguridad Informática del Banco:** Comprender la actual arquitectura de seguridad de la información del Banco y el riesgo para el entorno de procesamiento de la misma. Para el efecto se realizan procesos de **Ataque y Penetración** que examinan la funcionalidad de la seguridad informática del Banco (evaluación de seguridad: internet, intranet, extranet, acceso remoto) y explotan los puntos vulnerables de los sistemas y redes como lo haría un "usuario no autorizado", y/o intruso.
2. **Estrategia de Seguridad:** Identificar los requerimientos de seguridad específicos, y los riesgos y mecanismos de control necesarios para mitigarlos. Para el efecto se realiza el **Análisis de Amenazas y Vulnerabilidades** encontradas, involucrando a los sistemas operativos, bases de datos, firewalls, routers, bridges, switches y dispositivos de acceso remoto que soportan la seguridad en el ambiente de redes.
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:
   1. **Respuesta a Incidentes**
   2. **Monitoreo y Control de Aplicaciones**
   3. **Estrategia del Negocio:**
      1. Definición de la política de seguridad del Banco
      2. Perfil Tecnológico
      3. Perfil de Riesgos
      4. Arquitectura de Seguridad Informática
      5. Especificaciones de la Organización
      6. Especificaciones Técnicas
      7. Especificaciones de Pre-implementaciones
   4. **Mantenimiento:**
      1. Soluciones PKI
      2. Soluciones VPN
      3. Servicios de Directorio
      4. Soluciones de Detección de Intrusos
      5. Soluciones de Encriptación
      6. Soluciones de Acceso Remoto
      7. Soluciones de Firewall/router

Actividades:

1. Testing del nivel de seguridad general de la red Interna

1) Análisis de protocolos utilizados (TCP/IP).
2) Relevamiento y detección de equipos.
3) Scanning de vulnerabilidades en la red.
4) Testing para determinar si es posible acceder a los recursos de otro usuario sin estar debidamente autorizado.
5) Pruebas de acceso local en consola y vía la red.
6) Pruebas de seguridad sobre los diferentes dispositivos de red que se detecten, incluyendo Routers, Switches, Hubs, Bridges, etc.
7) Pruebas de seguridad sobre las estaciones de trabajo típicas (Windows, NT, XP y 2000), incluyendo:
   a. Scanning de estaciones de trabajo.
   b. Búsqueda de programas troyanos en forma remota.
   c. Análisis de recursos compartidos inseguros.
   d. Búsqueda de vulnerabilidades de seguridad informática conocidas (RPC de Windows 2000, ataques de denegación de servicio en Windows 95 y 98, etc).
   e. Determinación del nivel de seguridad vigente en la red Interna de acuerdo a los estándares internacionales.

2. Aspectos de seguridad de las conexiones externas

1) Análisis de la seguridad de los vínculos que posee el Banco.
2) Análisis de las conexiones con el sitio de contingencia.
3) Evaluación de la seguridad de los routers de conexión, analizando:
   a. Router, marca, modelo y versión del software utilizado.
   b. Puertos TCP y UDP abiertos.
   c. Nivel de encriptación utilizado.
   d. Análisis de ACL (access control lists).

3. Testing de seguridad de servidores

1) Análisis de la seguridad de los Servidores Unix/Linux, evaluando:
   a. Configuraciones de Seguridad.
   b. Patches instalados.
   c. Conexión con la red.
   d. Puertos TCP/IP abiertos.
   e. Seguridad de los servicios habilitados.
   f. Análisis de los usuarios.
2) Análisis de la seguridad de los Servidores Windows NT, 2000 y 2003, evaluando:
   a. Configuraciones de seguridad.
   b. Permisos.
   c. Patches instalados.
   d. Conexión con la red.
   e. Puertos TCP/IP abiertos.
   f. Servicios Activos.
   g. Protocolo NetBIOS utilizando.
   h. Recursos compartidos.
   i. Análisis de Usuarios.
3) Análisis de la seguridad de los Servidores AS/400:

a. Configuraciones de Seguridad.
b. Patches instalados.
c. Conexión con la red.
d. Puertos TCP/IP abiertos.
e. Seguridad de los servicios habilitados.
f. Análisis de los usuarios.

4) Análisis de la seguridad de los Controladores POS evaluando:
   a. Configuraciones de seguridad.
   b. Permisos.
   c. Patches instalados.
   d. Conexión con la red.
   e. Puertos TCP/IP abiertos.
   f. Servicios Activos.
   g. Análisis de Usuarios.
5) Scanning de protocolos TCP/IP para determinar las diferentes vulnerabilidades que poseen los servidores.

4. Evaluación de la Seguridad de Activos Críticos

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 Administración de Seguridad de TI, dependiente de la Dirección de Administración y Finanzas y la Dirección Tecnología Informática y Comunicaciones y que se consideren críticos basados en la importancia de la información que se posee o la funcionalidad que se ha asignado, en las condiciones que se producen durante la realización de un ataque y/o intento de intrusión desde adentro de la instalación, incluyendo los que se consideren críticos basados en la importancia de la información que posean o la funcionalidad que se les ha asignado, seleccionados por la División Administración de Seguridad de Tecnología Informática y la Dirección de Informática.

Como resultado de este proceso, se obtendrá valiosa información que permitirá:

a. Determinar qué niveles de acceso, a los distintos sistemas informáticos, puede lograr un intruso accediendo a la aplicación.
b. Evaluar las fortalezas y debilidades de los controles existentes en materia de seguridad de accesos y procedimientos de seguridad informática.
c. Identificar las posibilidades de un ataque interno/externo que pueda afectar la disponibilidad de los datos que administra el Banco, y/o el uso de los sistemas y analizar medidas preventivas activas.
d. Detectar la existencia de vectores de ataque que permitan realizar algún tipo de fraude financiero.

5. Presentación de Conclusiones y Recomendaciones

La información obtenida y los resultados del análisis se integran en los correspondientes informes que contienen, también, las recomendaciones pertinentes para eliminar los expuestos detectados y también aquellas que se considere deban ser incluidas como una prestación estándar en la instalación o minimizar el riesgo por acciones indebidas y/o fraudulentas.

Como resultado de dichas actividades, se dispondrá de un diagnóstico preciso, que es

indispensable para definir, generar e instalar, con un alto grado de eficiencia, las medidas de seguridad necesarias para evitar intrusiones y/o ataques externos a los sistemas y los datos mantenidos.

Dichos Informes serán presentados a la División Administración de Seguridad de Tecnología Informática y analizados conjuntamente con la Dirección de Tecnología Informática y Comunicaciones y los técnicos que realizaron los testeos a fin de satisfacer acabadamente las expectativas de información y profundizar sobre las recomendaciones en un plazo no mayor a 60 días calendario de la fecha inicial de la agenda o cronograma de trabajos aprobada en la minuta de la reunión inicial del proyecto. Luego los informes serán elevados a las instancias necesarias para la toma de conocimiento de las autoridades del Banco y para solicitar la ejecución de las recomendaciones entregadas por la empresa adjudicada. El Banco es totalmente responsable del criterio de negocio a aplicar para tomar decisiones de implementación o determinar cursos de acción respecto de cualquier cuestión tratada dentro de las sugerencias, recomendaciones, servicios e informes de la empresa adjudicada.

COMUNICACIONES ORALES Y REUNIONES DE AVANCE

Durante la evaluación, la empresa adjudicada proveerá resultados verbales sobre todos los riesgos de importancia encontrados y mantendrá reuniones de avance, si fuera necesario, informando la evolución de los objetivos planteados.

INFORMES

Durante el desarrollo de la consultoría podrán presentar Informes de Avances de tareas según los requerimientos del Banco.

Los informes a ser proporcionados son:

A. Informe Técnico detallado en formato electrónico e impreso que incluirá, los siguientes ítems:

- Detalle y secuencia de pruebas realizadas y resultados obtenidos en cada etapa del test.
- Evidencias de las vulnerabilidades y/o accesos obtenidos (Capturas de trofeo, sembrado de pruebas y pruebas de denegación de servicio). Debilidades y/o expuestos de seguridad detectados.
- Informe con "cuerpo" narrativo que incluirá la evaluación de riesgos de las vulnerabilidades encontradas, su análisis y recomendaciones técnicas. Las vulnerabilidades serán presentadas priorizadas según el nivel de riesgo que representen mediante una matriz de riesgo asociada a cada uno de los equipos bajo revisión y una matriz de riesgo general del perímetro externo. Los hallazgos detallados serán estructurados para facilitar una acción inmediata por parte del staff técnico, listando la siguiente información para cada vulnerabilidad como parte de las tareas de evaluación:

  1- Descripción de la vulnerabilidad

2- Identificación del Host afectado por la vulnerabilidad
3- Clasificación de la vulnerabilidad (Alta, Media y Baja) y determinación del riesgo
4- Posibilidad de ocurrencia (Alta, Media y Baja)
5- Solución / Recomendaciones

B. Informe Gerencial describiendo el estado inicial y al término de los trabajos en materia de Seguridad Informática. Documento en formato electrónico e impreso con las descripciones no técnicas de todos los hallazgos críticos, con su riesgo inherente de negocio y su probabilidad de ocurrencia (Alta, Media y Baja), los resultados obtenidos. Sumario ejecutivo orientado al personal superior del Banco, haciendo foco en el impacto en el negocio.

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.
c) Incorporación de funcionalidades no disponibles en el Banco. En este caso, se definirá y detallará la funcionalidad que sea necesaria incorporar para que el Banco recurra a los proveedores del mercado.

PERSONAL TÉCNICO

El trabajo deberá llevarse a cabo por un equipo multidisciplinario de expertos en hacking ético y su correspondiente supervisión de un Líder de Proyecto quien verificará la calidad del proyecto como así también su desarrollo y presentará los resultados.

No se podrá realizar ningún tipo de subcontratación de "hackers" ni personal "freelance" para ningún trabajo, en virtud de lo determinado por la pauta de "compromiso ético" sino que todos los profesionales de seguridad implicados en el proyecto deben ser empleados de tiempo completo de la firma y avalados por ésta luego de una rigurosa averiguación de antecedentes para asegurar que tengan una historia ética, personal y profesional adecuada. Además, los mismos deberán contar con cursos de capacitación específicos al proyecto en el transcurso de sus carreras profesionales.

Todo el personal del equipo de trabajo debe tener amplios conocimientos en los temas de la presente propuesta, así como una amplia experiencia comprobable en trabajos similares en

bancos o compañías de primera línea a nivel local e internacional. El equipo deberá contar con al menos dos personas con certificaciones CISM y/o CISSP, debiendo presentar junto con la oferta los documentos o certificados que lo acrediten.

El número de consultores puede variar de acuerdo a las necesidades surgidas de un cambio de alcance y los perfiles de los mismos se encontrarán en relación directa a las tareas solicitadas. En caso de ser necesario el reemplazo de los consultores para este proyecto, se le informará al banco formalmente y se pondrá a disposición el currículum vitae de los consultores que ingresen al proyecto.

LIMITACIONES DEL ALCANCE

El trabajo no incluirá:

1. La realización de pruebas que puedan generar una caída de las aplicaciones propias ejecutadas en los servidores, salvo expresa autorización por parte de la Dirección de Informática.

2. Pruebas del tipo de DoS (Negación de servicio) o brute-force attacks (ataque de fuerza bruta) que impliquen el riesgo de dejar sin servicio a cualesquiera de los entornos a evaluar, salvo expresa autorización por parte de la Dirección de Informática una vez informada la posibilidad de ejecución de las mismas.

3. Análisis de la configuración de los equipos intervinientes.

En todos los casos, durante las pruebas no se modificará ninguno de los datos y/o configuraciones a los que eventualmente se pudiera acceder en los entornos a evaluar.

VALIDACIÓN DE OBJETIVOS Y ALCANCE

A los efectos de confirmar y validar los objetivos del proyecto, se convocará una reunión inicial con el área de seguridad informática para ratificar las expectativas del Banco en cuanto a los servicios requeridos y la validación de la planificación definitiva. El Banco hará entrega del mapa de redes y aplicaciones para lograr una planificación más precisa, al conocer en forma exacta la dimensión de la arquitectura, de forma que no se necesite realizar ajustes a la planificación durante la ejecución de la misma a partir de los datos obtenidos.

La Agenda y Minuta correspondientes serán remitidas a los participantes para su aprobación formal. La reunión deberá llevarse a cabo dentro de los 15 días corridos luego de la firma del contrato. Los resultados serán tomados como conclusión de la Etapa I del Proyecto.

Para llevar a cabo los trabajos mencionados por parte de la empresa adjudicada es necesario el cumplimiento de los siguientes requisitos:

a) Aprobación formal del Cronograma de Trabajo y Minuta por parte de los participantes de Reunión de Validación de Objetivos y Alcances.

b) Firma de Contrato de Confidencialidad, Integridad y Disponibilidad entre las partes.
c) Asignar un Responsable por ambas partes, que actúen como contrapartes del trabajo.

CONFIDENCIALIDAD

En relación con el proyecto, cada una de las partes podrá eventualmente tener acceso a información confidencial puesta a disposición por la otra parte; cada una de las partes protegerá esta información confidencial de la misma manera en que protege su propia información confidencial. El Banco será propietario de los productos terminados, los cuales no incluyen la metodología ni las herramientas y técnicas utilizadas en el desarrollo del proyecto. Cada una de las partes podrá usar libremente los conceptos, técnicas y know-how utilizados y desarrollados durante el presente proyecto.

Cláusula de Confidencialidad

Cada una de las partes protegerá la información obtenida durante el desarrollo del trabajo de la misma manera en que protege su propia información confidencial, haciéndose responsable por cualquier daño/perjuicio que se pudiera ocasionar por el uso indebido de la información accedida.

Nuestros documentos entregables y papeles de trabajo serán de acceso exclusivo para los responsables del Banco. El Banco podrá disponer para su uso de todos los entregables, que no incluyen metodología ni software utilizado.

Salvo autorización de los responsables del Banco, una vez finalizado el trabajo se procederá a eliminar toda copia electrónica y/o impresa de la información obtenida de cualquiera de los equipos informáticos del personal afectado al trabajo.

DISTRIBUCIÓN DEL RIESGO

La responsabilidad máxima por todo concepto de la empresa adjudicada hacia el Banco en relación con los servicios descriptos se limita a los honorarios abonados a la misma por los servicios prestados que fueran causa o motivo de tal responsabilidad, salvo la existencia de culpa grave o dolo. Asimismo, el Banco mantendrá indemne a la empresa adjudicada y a su personal de toda responsabilidad, costos y gastos relacionados con los servicios profesionales aquí descriptos, salvo la existencia de culpa grave o dolo.

La responsabilidad de la empresa adjudicada ante el Banco como consecuencia de un incumplimiento de contrato u obligación, culpa o negligencia o por cualquier otra causa respecto o derivada del presente trabajo deberá limitarse a la proporción de la pérdida o daño (incluidos los costos e intereses) que el Banco haya sufrido, la cual será acordada por la empresa adjudicada o se le atribuirá mediante resolución de un tribunal competente que distribuya la responsabilidad proporcional teniendo en cuenta la intervención en la pérdida o daño en cuestión de cualquier persona obligada y/o responsable ante el Banco por dicha pérdida o daño. La empresa adjudicada no será responsable ante el Banco por ninguna pérdida o daño mediato o indirecto, salvo la existencia de culpa grave o dolo.

Puede ser que para el desarrollo del trabajo se precise utilizar los servicios de los socios o el personal de otras firmas independientes miembros de la empresa adjudicada para que contribuyan a la prestación de sus servicios al Banco. Cuando utilizan los servicios de dichos socios o personal con relación al presente trabajo, se considerará que dichas personas actúan como colaboradores o representantes pero no como los socios, colaboradores o representantes de cualquier otra persona (incluido cualquier otro miembro de la empresa adjudicada), y serán responsables por sus actividades como si fueran los socios o personal en todos los aspectos.

El Banco acuerda al contratar los servicios de la empresa adjudicada que cualquier reclamo de cualquier índole relacionado o no con el desarrollo de este trabajo será llevado en forma exclusiva contra la empresa adjudicada y que ningún reclamo relacionado con este trabajo será efectuado en forma personal contra ninguna persona que participe en la realización del mismo, independientemente que sean o no supuestos o verdaderos colaboradores o representantes de la empresa adjudicada.

Personal

A los fines de dar cumplimiento a las normas de seguridad vigentes en el Banco, la empresa adjudicada deberá entregar una nómina de las personas que prestarán servicios en virtud del trabajo encomendado. Dicha nómina deberá contener el nombre completo y el tipo y número de documento de todo empleado o profesional del estudio que ingresará al Banco o a sus dependencias, a quienes les podrá ser solicitada su debida identificación. A los fines de mantener la objetividad en el desempeño de los trabajos encomendados, la empresa adjudicada declara que el personal asignado al proyecto objeto de este acuerdo no posee vinculación de ninguna especie con el Banco más allá de la que surja de la aceptación de esta propuesta o de cualquier otro que se encuentre vigente con el Banco.

Disposiciones Generales

La empresa adjudicada entregará al Banco una copia de los papeles de trabajo de respaldo de los informes finales a emitir.

El Banco podrá, exclusivamente, utilizar, copiar y distribuir internamente los informes entregados por la empresa adjudicada y a la Superintendencia de Bancos.

El Banco no ofrecerá empleo ni contratará a ningún socio ni empleado profesional actual o anterior de la empresa adjudicada ni de cualquiera de sus firmas relacionadas, en la medida que dicho empleado profesional participa o ha participado en la prestación de los servicios cubiertos por el presente contrato, por un plazo de doce meses contados a partir de la fecha de la terminación de los servicios de la empresa adjudicada.

DIRECCION DE ADMINISTRACION Y FINANZAS
UNIDAD OPERATIVA DE CONTRATACIONES
BNF

LUGAR DE PRESTACIÓN DE LOS SERVICIOS Y HORARIO DE TRABAJO

Presentación de Conclusiones y Recomendaciones: Ver ítem 1.

Lugar de prestación de los servicios y horario de trabajo: Los trabajos a ser desarrollados antes del primer informe deberán realizarse a distancia, y en un fin de semana, iniciando luego de los procesos afines al cierre del Banco, con el objetivo de evitar cualquier inconveniente que pueda darse con el funcionamiento de las aplicaciones del Banco o Contratante.

PLAN DE ENTREGA DEL TRABAJO

La presentación del informe ejecutivo, necesariamente deberá ser efectuada **en las oficinas de la Dirección Tecnología Informática y Comunicaciones,** por el técnico responsable de la Firma Adjudicada y en presencia de los técnicos de la División Administración de Seguridad de TI, dependiente de la Dirección de Administración y Finanzas y la Dirección Tecnología Informática y Comunicaciones, de manera a discutir sobre todas las recomendaciones y hallazgos.

SEGURO DE RESPONSABILIDAD PROFESIONAL

El adjudicado deberá presentar una garantía de **Responsabilidad Profesional por el 10% del monto del contrato, en cumplimiento del Art. 53 de la Ley Nº 2051/2003**

4. PLAZO DE EJECUCIÓN DEL SERVICIO.

La prestación del Servicio se realizará a partir de la suscripción del Contrato respectivo, y tendrá una vigencia de 90 (noventa) días.

5. CONDICIONES DE PAGO.

Dentro de los 30 (treinta) días de recibida la factura correspondiente previo VºBº de la División Administración de Seguridad de TI, dependiente de la Dirección de Administración y Finanzas y la Dirección Tecnología Informática y Comunicaciones, en prueba de conformidad. La moneda de pago será la moneda nacional Guaraníes.

EL PAGO:

Se realizará contra aprobación del Informe final por la contraparte asignada por el Banco. La forma de pago será según detalle:

Concepto	Inicio del Proceso de Pago
Primer pago	30% de ANTICIPO previa presentación de factura correspondiente y la Garantía de Anticipo por el 100% de lo Anticipado
Segundo pago	40 % luego de la realización de los trabajos que involucren los test correspondientes y la presentación del informe técnico con todas las pruebas de las posibles vulnerabilidades o hallazgos, tipificados por niveles de riesgo (alto, medio, etc).
Tercer Pago	30 % del valor del contrato, contra presentación y aprobación del informe ejecutivo, las recomendaciones o plan de acción y factura correspondiente.

Se efectuará una vez obtenido el Código de Contratación (CC), emitido por la Dirección Nacional de Contrataciones Públicas

6. **RETENCIONES:**

Deberá dar cumplimiento al Art. 41 de la Ley Nº 2051/03 "De Contrataciones Públicas", modificado por la ley 3439/07 que establece una contribución sobre contratos suscriptos equivalente al cero punto cuatro por ciento (0.4%) sobre el importe de cada factura, deducidos los impuestos correspondientes.

RUC: 80000856-1

7. **MULTAS**

Multas a ser aplicadas al Oferente adjudicado: por cada semana de atraso en la prestación del servicio, por causas imputables al Oferente Adjudicado, se aplicará al mismo una multa equivalente al 0,5% del valor total de la factura correspondiente a dicho servicio. El BNF queda autorizado a deducir estas multas en forma automática, sin ninguna interpelación judicial o extrajudicial. El monto máximo de las multas será del 10 % del monto total del contrato.

Multas a ser aplicadas a la Convocante: La convocante pagará al Oferente adjudicado un interés del 0,01% una vez vencido el plazo establecido en las condiciones de pago 30 (treinta) días.

AJUSTE DE PRECIOS

El precio del contrato queda sujeto a reajustes: El **BNF** reconocerá reajuste en los precios del Servicio, siempre y cuando: Exista una variación sustancial de precios en la economía nacional y ésta se vea reflejada en el índice de precios de consumo publicado por el Banco Central del Paraguay, en un valor igual o mayor al quince por ciento sobre la inflación oficial esperada para el mismo periodo. La formula de reajuste a ser utilizada en este caso es la siguiente:

$$V1 = \frac{P \times I.I.BCP}{15\%}$$

P= Precio del Servicio

I.I. BCP= Índice de Inflación emitido por el Banco Central del Paraguay.

15%= Mínimo necesario para reajuste del precio.

Los precios reajustados, solo tendrán incidencia sobre los servicios aún no ejecutados y no tendrán ningún efecto retroactivo respecto a los servicios que fueron ejecutados antes de la verificación del reajuste.--------

MARIA ELENA CAMPOS KRAUER
RESPONSABLE UOC
BANCO NACIONAL DE FOMENTO

DIRECCION DE ADMINISTRACION Y FINANZAS – UNIDAD OPERATIVA DE CONTRATACIONES – BNF

Anexo 4

Declaración Jurada de no encontrarse comprendido en las inhabilidades previstas en el Art. 40 y de integridad establecida en el Art. 20, Inciso "W", ambos de la Ley 2051/03 de Contrataciones Públicas.

Fecha:_____

Proceso de Contratación: Modalidad: **Contratación Directa BNF CD Nº 38/2011**
Descripción del llamado: **Servicio de Test de Seguridad – HACKEO ÉTICO – Interno y Externo para el Banco Nacional de Fomento.**
ID (Portal) Nº : 221802

A la Convocante:
Banco Nacional de Fomento

Yo/Nosotros, quien suscribe/n, declaro/amos Bajo Fe de Juramento que, no me/nos encuentro/encontramos comprendido/s en ninguna de las inhabilidades previstas por el Artículo 40 de la Ley Nº 2.051/03 para presentar propuestas y/o contratar con el Estado Paraguayo en general, y con esta Convocante en particular y al proceso de contratación arriba individualizado.-

Asimismo, declaro/amos Bajo Fe de Juramento, que me/nos abstengo/abstenemos de adoptar conductas orientadas a que los funcionarios o empleados de la Convocante en el presente llamado, induzcan o alteren las exigencias del llamado, las evaluaciones de las propuestas, el resultado del procedimiento, la ejecución contractual u otros aspectos que pudiera/n otorgarme/nos condiciones más ventajosas con relación a los demás participantes, como por ejemplo, y de manera enunciativa y no limitativa, el soborno y la colusión.-

Asumo/imos el compromiso de comunicar por medios fehacientes a la Entidad Convocante, de manera inmediata a su surgimiento, cualquier alteración en la situación jurídica respecto de las citadas inhabilidades, dejando expresa constancia que independiente a esta situación, automáticamente resta eficacia y validez a la presente.-

La presente declaración jurada, la hago/hacemos, en los términos y condiciones del Artículo 47 del Decreto Reglamentario Nº 21.909/03 y el artículo 20, inciso "W", de la Ley 2051/03, de "Contrataciones Públicas". Así mismo, declaro conocer y aceptar el contenido y las disposiciones de la Resolución N° 330/07 de la Dirección General de Contrataciones Públicas.-

Firma El/los Oferente/s Aclaración de Firma

Adjunto/amos copia/s de documentos Si No

OBSERVACIONES IMPORTANTES: La presente deberá estar firmada por el oferente o sus/s representante/s debidamente acreditado/s, con la correspondiente aclaración/es de firma/s y fotocopia perfectamente legible, del documento que acredite la identidad y representación, en su caso, del/los firmante/s, y deberá ser emitida por el Oferente, para cada proceso en particular y presentada en formato original, adjunto a la oferta; siendo de carácter SUSTANCIAL y su no presentación o presentación en forma deficiente, no será subsanable, teniendo como consecuencia la DESCALIFICACIÓN DE LA OFERTA. (Art. 3 de la Res.330/07)

Anexo 5

DECLARACIÓN JURADA POR LA CUAL SE GARANTIZA QUE NO SE ENCUENTRA INVOLUCRADO EN LAS PRACTICAS QUE VIOLEN LOS DERECHOS DE LOS NIÑOS, NIÑAS Y ADOLECENTES REFERENTES AL TRABAJO INFANTIL, ESTIPULADOS EN LA CONSTITUCION NACIONAL, LOS CONVENIOS 138 Y 182 DE LA ORGANIZACIÓN INTERNACIONAL DEL TRABAJO (OIT), EL CÓDIGO DEL TRABAJO, EL CÓDIGO DE LA NIÑEZ Y LA ADOLESCENCIA, DEMAS LEYES Y NORMATIVAS VIGENTES EN LA REPUBLICA DEL PARAGUAY.

Asunción, __de _____de 2011

Señores

.....

Presente

REF.: **Servicio de Test de Seguridad – HACKEO ÉTICO – Interno y Externo para el Banco Nacional de Fomento.**

ID: **221802**

De mi/nuestra consideración:

La empresa....., con RUC ....., en su calidad de oferente del llamado de referencia, por medio de su/s representante/s legal/es....., con Cédula de identidad Nº.....,formula la presente DECLARACIÓN BAJO FE DE JURAMENTO:

1. QUE no empleamos niños, niñas y adolecentes en tipos de labores considerados como Trabajos Prohibidos y en particular "TRABAJO INFANTIL PELIGROSO" de conformidad a lo dispuesto en el Art. 125 del Código del Trabajo, el Art. 54 del Código de la Niñez y la Adolescencia y el Decreto Nº 4951/05 que reglamenta la Ley 1657/01.
2. QUE, en caso de tomar conocimiento de alguna conducta que se aparta de las disposiciones citadas precedentemente y que involucre a nuestros proveedores de bienes y servicios que componen la cadena de producción y comercialización de lo ofertado, denunciaremos ese hecho ante la instancia pertinente, de conformidad a lo dispuesto en el Artículo 5 del Código de la Niñez y la Adolescencia.
3. QUE en el caso de que empleemos adolescentes lo haremos de conformidad a lo que establece el Código del Trabajo y el Código de la Niñez y la Adolescencia, y sus disposiciones concordantes y complementarias salvaguardando todos los derechos y garantías del mismo y teniendo presente las obligaciones que como empleadores menos competen.

RECONOCEMOS QUE cualquier violación de esta Declaración facultará a la Convocante a descalificar durante la etapa de evaluación de ofertas y/o rescindir el contrato respectivo cualquiera sea su etapa de ejecución, de conformidad a la forma establecida en el Articulo 59 de la Ley 2051/03. En estos casos reconozco que no tendré derecho a reembolso de gastos ni a indemnización alguna y seré pasible de la aplicación del procedimiento para imposición de sanciones previstos en la Ley 2051/03, independientemente de las demás responsabilidades que pudieran generar.

Atentamente,

DIRECCION DE ADMINISTRACION Y FINANZAS – UNIDAD OPERATIVA DE CONTRATACIONES – BNF

Firma El/los Oferente/s Aclaración de Firma/s

( ) En el caso de que emplee/mos adolescentes trabajadores/as entre 14 y 17 años, adjunto/amos copia del Registro del Adolescente Trabajador/a, de conformidad a lo que establece 55 del Código de la Niñez y la Adolescencia.

El presente texto no podrá ser modificado ni alterado, siendo de carácter formal su presentación.

ANEXO 6

FORMULARIO: DESCRIPCIÓN DEL ENFOQUE, METODOLOGÍA Y PLAN DE ACTIVIDADES PARA LA EJECUCIÓN DEL TRABAJO

[El enfoque técnico, la metodología y el plan de trabajo son componentes claves de la propuesta técnica. Se le sugiere que presente su propuesta técnica dividida en las tres partes siguientes:

a) Enfoque técnico y metodología
b) Plan de trabajo, y
c) Organización y dotación de personal.

a) Enfoque técnico y metodología. En este capítulo el Consultor deberá explicar su comprensión de los objetivos del trabajo, enfoque de los servicios, metodología para llevar a cabo las actividades y obtener el producto esperado, y el grado de detalle de dicho producto. Usted deberá destacar los problemas que se están tratando y su importancia, y explicar el enfoque técnico que usted adoptaría para tratarlos. El Consultor deberá explicar la metodología que propone adoptar y resaltar la compatibilidad de esa metodología con el enfoque propuesto.

b) Plan de Trabajo. En este capítulo deberá proponer las actividades principales del trabajo, su contenido y duración, fases y relaciones entre sí, etapas (incluyendo las aprobaciones provisionales del Contratante), y las fechas de entrega de los informes. El plan de trabajo propuesto deberá ser consistente con el enfoque técnico y la metodología, demostrando una compresión de los TDR y habilidad para traducirlos en un plan de trabajo factible. Aquí se deberá incluir una lista de los documentos finales, incluyendo informes, planos y tablas que deberán ser presentadas como producto final. El plan de trabajo deberá ser consistente con el Programa de Trabajo.

c) Organización y Dotación de Personal. En este capítulo deberá proponer la estructura y composición de su equipo. Deberá detallar las disciplinas principales del trabajo, el especialista clave responsable, y el personal técnico y de apoyo designado.]

DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS
BNF
UNIDAD OPERATIVA DE CONTRATACIONES

ANEXO 7

FORMULARIO: COMPOSICIÓN DEL EQUIPO Y ASIGNACIÓN DE RESPONSABILIDADES

1. Personal Profesional

Nombre del personal	Firma	Área de Especialidad	Cargo asignado	Actividad asignada

DIRECCION DE ADMINISTRACION Y FINANZAS
UNIDAD OPERATIVA DE CONTRATACIONES
BNF

ANEXO 8

FORMULARIO: CURRÍCULO DEL/LOS PROFESIONAL/ES PROPUESTOS

1. **Cargo propuesto** [*solamente un candidato deberá ser nominado para cada posición]:*_____

2. **Nombre de la firma:** *[inserte el nombre de la firma que propone al candidato]:*_____

3. **Nombre del individuo:** *[inserte el nombre completo]:* _____

4. **Fecha de nacimiento:** _____ Nacionalidad: _____

5. **Educación:** [*Indicar los nombres de las universidades y otros estudios especializados del individuo, dando los nombres de las instituciones, grados obtenidos y las fechas en que los obtuvo.*]

6. **Asociaciones profesionales a las que pertenece:** _____

7. **Otras especialidades** *[Indicar otros estudios significativos después de haber obtenido los grados indicados en el 5 – Dónde obtuvo la educación]:*

8. **Países donde tiene experiencia de trabajo:** *[Enumere los países donde el individuo ha trabajado en los últimos diez años]:* _____

9. **Idiomas** *[Para cada idioma indique el grado de competencia: bueno, regular, pobre, en hablarlo, leerlo y escribirlo]:*_____

10. **Historia Laboral** *[Empezando con el cargo actual, enumere en orden inverso cada cargo que ha desempeñado desde que se graduó el candidato, indicando para cada empleo (véase el formulario siguiente): fechas de empleo, nombre de la organización, cargos desempeñados]:*

Desde [*Año]:* _____ Hasta [*Año*] _____
Empresa: _____
Cargos desempeñados: _____

11. Detalle de las actividades asignadas	**12. Trabajos que ha realizado que mejor demuestran la capacidad para ejecutar las tareas asignadas**
[Enumere todas las tareas que desempeñará bajo este trabajo]	[*Entre todos los trabajos que el individuo ha desempeñado, complete la siguiente información para aquellos que mejor demuestran su capacidad para ejecutar las tareas enumeradas bajo el punto 11.]* Nombre de la tarea o proyecto: _____

	Año: _____ Lugar: _____ Contratante: _____ Principales características del proyecto: _____ Actividades desempeñadas: _____

13. Certificación:

Yo, el abajo firmante, certifico que, según mi mejor conocimiento y mi entender, este currículo describe correctamente mi persona, mis calificaciones y mi experiencia. Entiendo que cualquier declaración voluntariamente falsa aquí incluida puede conducir a mi descalificación o la cancelación de mi trabajo, si fuera contratado.

_____ Fecha: _____

[Firma del individuo o del representante autorizado del individuo] *Día / Mes / Año*

Nombre completo del representante autorizado: _____

Observación: Esta planilla deberá ser llenada por cada uno de los profesionales propuestos para el trabajo de elaboración del proyecto, debiendo acompañar documentos respaldatorios de las manifestaciones vertidas en el mismo, pudiendo consistir estos documentos en copias de contratos, certificaciones de trabajos realizados. También podrá presentar notas con carácter de declaración jurada de clientes a quienes hayan prestado servicios similares a los descritos en los Términos de referencia.

ANEXO 9

FORMULARIO: CALENDARIO DE ACTIVIDADES DEL PERSONAL [1]

N°	Nombre del personal	Contribución del personal (en un gráfico de barras)[2]													Total de la contribución persona-meses		
		1	2	3	4	5	6	7	8	9	10	11	12	n	Sede	Campo[3]	Total
Extranjero																	
1		[*Sede*]															
		[*Campo*]															
2																	
3																	
n		.															
											Subtotal						

Local																	
1		[*Sede*]															
		[*Campo*]															
2																	
n																	
											Subtotal						
											Total						

1 Para el personal profesional el aporte deber ser indicado individualmente; para el personal de apoyo, deberá ser indicado por categoría (por ejemplo, dibujante, empleado de oficina; etc.)
2 Los meses se cuentan desde el inicio del trabajo. Para cada empleado indique separadamente el aporte en la sede y en el campo.
3 Trabajo en el campo significa el trabajo realizado fuera en un lugar que no es la oficina sede del Consultor.

Tiempo completo

Tiempo parcial

DIRECCION DE ADMINISTRACION Y FINANZAS
UNIDAD OPERATIVA DE CONTRATACIONES
BNF

ANEXO 10

FORMULARIO: PLAN DE TRABAJO

N°	Actividad[1]	Meses [2]												
		1	2	3	4	5	6	7	8	9	10	11	12	n
1														
2														
3														
4														
5														
n														

1. Indique todas las actividades principales del trabajo, incluyendo entrega de informes (por ejemplo, inicial, provisional, informes finales), y otras etapas tales como aprobaciones por parte del Contratante. Para tareas en varias fases, indique separadamente las actividades, entrega de informes y etapas para cada fase.
2. La duración de las actividades deberán ser indicadas en un gráfico de barras.

DIRECCION DE ADMINISTRACION Y FINANZAS
UNIDAD OPERATIVA DE CONTRATACIONES
BNF