Contrato BNF P Nº_____2013

SERVICIO DE TEST DE SEGURIDAD HACKEO INTERNO Y EXTERNO PARA EL BANCO NACIONAL DE FOMENTO.

Entre el Banco Nacional de Fomento, domiciliado en las calles Independencia Nacional entre Cerro Corá y 25 de Mayo, de la ciudad de Asunción, representado en este acto por su Presidente, ……., con Cédula de Identidad Civil Nº ……., nombrado por Decreto Nº…… del …… de …….. de 20…., del Poder Ejecutivo de la Nación, denominado en adelante **BNF**, y el ……., con Registro Único del Contribuyente Nº ……., con Cédula de Identidad Civil N° ……., domiciliado en……., de la ciudad de ……., en adelante **CONSULTOR**, acuerdan celebrar el presente Contrato para el **"Servicio de Test de Seguridad Hackeo Interno y Externo para el BNF"**, el cual estará sujeto a los siguientes puntos y condiciones:

1. OBJETO Y DESCRIPCION DEL SERVICIO

El **BNF** contrata al **CONSULTOR** para el **"Servicio de Test de Seguridad Hackeo Interno y Externo para el BNF"**, en las mismas condiciones establecidas en los términos de referencia y especificaciones técnicas de la **Contratación Directa CD N° 10/2013**, y la Oferta presentada por el **CONSULTOR**, de fecha……. de…….. de 2013, a cuyo fiel cumplimiento se obligan las partes.---

2. ALCANCE DEL SERVICIO Y TAREAS A REALIZAR

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

El **CONSULTOR** deberá realizar las siguientes tareas:

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 BNF incluir más equipos, los que serán considerados como adicionales.

- Veintisiete Servidores Windows.
- Cuatro Servidores AS400.

- Tres Servidores Linux
- Dieciocho Switches.
- Siete Ruteadores.
- Cincuenta Estaciones de Trabajo.
- Una Central IP
- Cuatro Dispositivos Wireless/Access Points (únicamente vía LAN) de Casa Matriz
- Trece Enlaces VPN/WAN contra redes del Banco
- Tres Firewalls entre sitio central y remotos del Banco

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

El alcance comprende los siguientes dispositivos y servidores:

- Tres direcciones IP Públicas.

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.
  - 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, 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 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.

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 al **CONSULTOR**.

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).

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 **BNF** 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 **BNF**, 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 que 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 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, 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 IBM 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 **BNF** y para solicitar la ejecución de las recomendaciones entregadas por la empresa adjudicada. El **BNF** 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 **BNF**. 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 **BNF**, 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 **BNF**. El Plan de Acción se entregará conjuntamente con el personal que el **BNF** 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 de seguridad informática, 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 **BNF** en cuanto a los servicios requeridos y la validación de la planificación definitiva. El **BNF** 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 la Reunión de Validación de Objetivos y Alcances.
b) 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 **BNF** 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.

Clausula 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 **BNF**. El **BNF** podrá disponer para su uso de todos los entregables, que no incluyen metodología ni software utilizado.

Salvo autorización de los responsables del **BNF**, 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 **BNF** 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 **BNF** 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 **BNF** 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 **BNF** 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 **BNF** por dicha pérdida o daño. El **CONSULTOR** no será responsable ante el **BNF** 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 del **CONSULTOR** para que contribuyan a la prestación de sus servicios al **BNF**. 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 **BNF** acuerda al contratar los servicios del **CONSULTOR**, que cualquier reclamo de cualquier índole relacionado o no con el desarrollo de este trabajo será llevado en forma exclusiva contra el **CONSULTOR** 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 del **CONSULTOR**.

Personal

A los fines de dar cumplimiento a las normas de seguridad vigentes en el **BNF**, el **CONSULTOR** 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 **BNF** 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, el **CONSULTOR** declara que el personal asignado al proyecto objeto de este acuerdo no posee vinculación de ninguna especie con el **BNF** más allá de la que surja de la aceptación de esta propuesta o de cualquier otro que se encuentre vigente con el **BNF.**

Disposiciones Generales

El **CONSULTOR** entregará al **BNF** una copia de los papeles de trabajo de respaldo de los informes finales a emitir.

El **BNF** podrá, exclusivamente, utilizar, copiar y distribuir internamente los informes entregados

por la empresa adjudicada y a la Superintendencia de Bancos.

El **BNF** no ofrecerá empleo ni contratará a ningún socio ni empleado profesional actual o anterior del **CONSULTOR** 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 del **CONSULTOR**.

3. PLAZO Y PLAN DE ENTREGA DE LA PRESTACIÓN DEL SERVICIO

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 **BNF**, con el objetivo de evitar cualquier inconveniente que pueda darse con el funcionamiento de las aplicaciones del **BNF**.

Plazo de Entrega final: 30 (treinta) días.----------

4. DOCUMENTOS INTEGRANTES DEL CONTRATO.

Forman parte integral del contrato los siguientes:

(a) La invitación a la Convocatoria y las Especificaciones Técnicas del llamado.
(b) La Oferta presentada por el **CONSULTOR**, de fecha…….. de…….. de 2013.
(c) Resolución de Adjudicación Nº…….. Acta……. de fecha…… de……. de 2013, del Consejo de Administración del **BNF**.
(d) Seguro de Responsabilidad Profesional.
(e) Las comunicaciones que las partes emitieren con relación al presente contrato.

5. IDENTIFICACIÓN DEL CRÉDITO PRESUPUESTARIO

El crédito presupuestario para cubrir el compromiso derivado del presente contrato está previsto en el **Rubro OG 260 – "SERVICIOS TECNICOS Y PROFESIONALES",** del Presupuesto General de la Nación. Esta contratación está incluida en el Plan Anual de Contrataciones (PAC) con el **Código ……/2013**, **ID Nº 255726/2013**.----------

7. PROCEDIMIENTO DE CONTRATACIÓN

El presente contrato es el resultado del procedimiento de la **Contratación Directa CD Nº 10/2013**, según Resolución Nº……. Acta …… del ….. de …… de 2013, por la cual se aprobó el este Servicio.----------

8. PRECIO Y FORMA DE PAGO

El Precio del servicio contratado, es de conformidad a la oferta presentada por el **CONSULTOR**, de fecha…….. de…….. de 2013, según el siguiente detalle: **(DETALLAR OFERTA)**

El **BNF** abonará al **CONSULTOR**, a plazo. Dentro de los 30 (treinta) días de presentada la fractura, previo visto bueno por la **Dirección de Tecnología Informática y Comunicaciones**, en prueba

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

El Pago final 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.

Conforme al Art. 41º de la Ley 2.051/03 "De Contrataciones Públicas" modificado por Ley Nº 3439/07, de los servicios contratados se retendrá el 0,4% (cero punto cuatro por ciento) sobre el importe de cada factura, deducido los impuestos correspondientes, al momento de su cobro.--

La moneda de pago será la moneda nacional Guaraníes.----------

9. REAJUSTES DE PRECIOS

El precio del contrato queda sujeto a reajustes (a petición de parte y por escrito): 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.----------

10. VIGENCIA DEL CONTRATO

La vigencia del contrato será de **3 (tres) meses**, a partir de su suscripción.----------

La vigencia del presente documento queda sujeta a la disponibilidad presupuestaria del **BNF**, de acuerdo a lo previsto en el Artículo 14 de la Ley 2051/03.----------

11. LUGAR DE PRESTACIÓN DE LOS SERVICIOS.

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.----------

12. RESPONSABILIDAD DEL CONSULTOR

Será responsable de la cabal, eficiente, y satisfactoria prestación del servicio y no podrá eludir sus responsabilidades por no haber solicitado a su debido tiempo las instrucciones o aclaraciones necesarias con relación a los documentos del Contrato.----------

Queda prohibido el remplazo del personal técnico clave, con la única excepción de aquellas que se encuentren debidamente justificadas y fuera del control del **CONSULTOR** (Art. 53 de la Ley 2051/03 de Contrataciones Públicas.).----------

Brindará el Servicio de conformidad a las condiciones establecidas en este Contrato salvo motivo de fuerza mayor o caso fortuito debidamente comprobado y a satisfacción del **BNF**.----------

Para los fines de este Contrato se considerarán casos fortuitos o de fuerza mayor los que como ejemplo, pero no limitativamente se mencionan a continuación siempre que tales casos hayan tenido efectiva influencia o producida interrupción en la ejecución del Contrato y se haya utilizado la debida diligencia para prevenir o limitar sus influencias:

1. Guerra y hostilidades bélicas, invasiones armadas, guerra civil, revoluciones, insurrecciones o destrucciones;
2. Huelgas, actos de sabotaje, maniobras subversivas;
3. Catástrofes naturales tales como sismos, terremotos etc.;
4. Incendios y naufragios.

Al producirse un caso fortuito o de fuerza mayor la parte afectada deberá comunicarlo a la otra de inmediato, en un plazo de 15 (quince) días para aportar las pruebas correspondientes a menos que existan graves impedimentos para ello, anexando a esta comunicación la documentación correspondiente.----------

El **CONSULTOR** no podrá ceder o transferir sus derechos y obligaciones establecidos en este Contrato, sin el previo consentimiento por escrito del **BNF**.----------

13. RESPONSABILIDAD DEL BNF

- Pagar al **CONSULTOR** por el servicio realizado, en la forma establecida en el punto Nº 8 de este Contrato.----------
- Efectuar el control y calidad del servicio realizado por el **CONSULTOR**.----------

14. RESCISION POR EL BNF

El **BNF**, podrá rescindir este contrato por justos motivos, que son entre otros:

- Si el servicio realizado por el **CONSULTOR** no fuese de la calidad y características especificadas en su propuesta. ----------
- Por violación, alteración e incumplimiento de los términos del Contrato o de los documentos que forman parte de él.- ----------
- En caso de darse algunos de los motivos enumerados en el Art. 59, de la Ley 2051/03 de Contrataciones Públicas. ----------

15. TERMINACIÓN POR MUTUO ACUERDO

En caso fortuito o de fuerza mayor por el cual se imposibilite el cumplimiento del presente contrato, las partes podrán resolver o rescindir el mismo por mutuo acuerdo, previa conciliación de cuentas.----------

16. CONFIDENCIALIDAD

La información que el **CONSULTOR**, reciba u obtenga en el marco de este Contrato o por efecto de éste, relacionada con el **BNF**, sus actividades, tecnología, finanzas, clientes, operaciones, sistemas de seguridad, etc., tendrá carácter reservado y confidencial, debiendo ser tratada como tal por el **CONSULTOR**, quien se compromete a no darlos a conocer a terceros, sin perjuicio de que la información hubiese sido proveída o llegase a su conocimiento antes, durante o una vez completada la ejecución del Contrato. ----------

El incumplimiento de esta obligación dará derecho al **BNF** a reclamar daños que se originen por ello.----------

La obligación del **CONSULTOR** de conformidad con los Sub-Puntos, no se aplicará a aquella información que:

(a) El **BNF** o el **CONSULTOR** requieran compartir con otras instituciones públicas, conforme a la legislación vigente; o

(b) en el presente o a futuro se haga pública sin culpa de ninguna de las partes; o

(c) pueda probarse que era conocida por esa parte en el momento en que fue divulgada y que no fue obtenida previamente, directa o indirectamente, de la otra parte; o

(d) haya sido puesta a disposición de esa parte por un tercero que no tiene obligación de confidencialidad.

Las disposiciones precedentes de este Punto no modificarán de manera alguna los compromisos de confidencialidad que hubiesen asumido las partes con anterioridad a la fecha del Contrato, con respecto al suministro o cualquiera de sus componentes.----------

Las disposiciones de este Punto se mantendrán en vigor con posterioridad a la finalización o terminación de este Contrato, cualquiera hubiese sido la causa de dicha terminación.----------

17. SOLUCIONES DE DIFERENCIAS

El **BNF** y el **CONSULTOR** se comprometen a resolver, en forma amistosa, mediante negociaciones informales directas, cualquier desacuerdo o disputa que pudieran surgir entre ellos de las resultas de este Contrato.----------

18. MODIFICACIONES DEL CONTRATO

No habrá variaciones o modificaciones de los términos de este Contrato, excepto por mutuo acuerdo por escrito de las partes.----------

19. SEGURO DE RESPONSABILIDAD PROFESIONAL

El **CONSULTOR** deberá presentar al **BNF**, a la firma del contrato un **SEGURO DE RESPONSABILIDAD PROFESIONAL**, equivalente al **10 % (diez por ciento)** del monto total adjudicado, extendida mediante una Póliza de Seguro emitida por una compañía de seguros que cumpla con el Margen de Solvencia y Fondo de Garantía establecidos por la Superintendencia de Seguros, a satisfacción y a la orden del **BNF**, por un plazo que exceda en 30 (treinta) días la vigencia del contrato (Art. 53 de la Ley 2051/03 de Contrataciones Públicas.).----------

20. PENALIZACIONES

Multas a ser aplicadas al **CONSULTOR**: por cada semana de atraso en la prestación del servicio, por causas imputables al **CONSULTOR**, se aplicará al mismo una multa equivalente al 0,5% del valor total de la factura mensual 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 al **BNF**: El **BNF** pagará al **CONSULTOR** un interés del 0,1% (cero coma un por ciento), una vez vencido el plazo establecido en las condiciones de pago 30 (treinta) días.----------

21. LEYES Y REGLAMENTOS

El **CONSULTOR** deberá observar y cumplir todas las leyes y reglamentos vigentes en la República, que de una u otra forma afecten la ejecución del servicio adjudicado, además de todas las leyes y reglamentos laborales y sociales, convenios laborales y cualesquiera otras disposiciones que regulen las relaciones obrero-patronales.----------

22. COMPETENCIA

En caso de conflicto en la interpretación de las disposiciones que regulan el presente Contrato, si ellas no pueden ser solucionadas de común acuerdo, las partes contratantes se someterán a la Competencia de los Tribunales Ordinarios de la ciudad de Asunción, capital de la República del Paraguay, siendo aplicables las leyes de la República.----------

En prueba de conformidad y con el compromiso de fiel cumplimiento, firman ambas partes, en dos ejemplares de un mismo tenor y a un solo efecto, en la ciudad de Asunción, Capital de la República del Paraguay a los.....días del mes de.....del año dos mil trece.----------

CONSULTOR **BNF**