



## BANCO AGRÍCOLA DE LA REPÚBLICA DOMINICANA

### TÉRMINOS DE REFERENCIA PARA LA ADQUISICIÓN DEL SERVICIO DE PRUEBA DE PENETRACION (PENTESTING) AL INTERNET BANKING Y A LA APLICACIÓN MOBIL DEL BANCO.

Ref. BAGRICOLA-DAF-CM-2021-0010

El **BANCO AGRÍCOLA DE LA REPÚBLICA DOMINICANA (BAGRICOLA)**, les invita a participar en el procedimiento de compra menor, de referencia No. BAGRICOLA-DAF-CM-2021-0010, a los fines de presentar su mejor oferta para la adquisición del servicio de prueba de penetración (Pentesting) al Internet Banking y a la Aplicación Móvil del Banco.

La presente invitación se hace de conformidad con los Artículos Nos. 16 y 17 de la Ley No. 340-06, sobre Compras y Contrataciones Públicas de Bienes, Servicios, Obras y Concesiones, de fecha Dieciocho (18) de Agosto del Dos Mil Seis (2006), y su posterior modificación contenida en la Ley No. 449-06, de fecha Seis (06) de Diciembre del Dos Mil Seis (2006).

#### 1. PRESENTACIÓN DE LAS OFERTAS:

La fecha límite para presentar su oferta será el día **MIÉRCOLES 23 DE JUNIO, HASTA LA 2:00 PM**, en la unidad de Compras y Contrataciones en la dirección de Servicios Administrativos en la sede principal del Banco, ubicada en la **Av. George Washington # 601, Santo Domingo de Guzmán, D.N.** El oferente deberá entregar su oferta sobre cerrado, debidamente identificado con la siguiente información:

Nombre del Oferente

Dirección

BANCO AGRICOLA DE LA REPUBLICA DOMINICANA

Presentación de Oferta: Un (1) sobre con el contenido de la oferta

Referencia del Procedimiento: **BAGRICOLA-DAF-CM-2021-0010**

Los Oferentes presentaran su oferta en pesos dominicanos (RD\$).

#### 2. DOCUMENTACIÓN A PRESENTAR:

- Registro de Proveedor del Estado (**RPE**) con documentos legales-administrativos actualizados, emitido por la Dirección General de Contrataciones Públicas. El oferente debe estar inscrito en el rubro correspondiente la naturaleza del servicio a contratar.
- **Oferta Económica** (cotización) en pesos dominicanos (RD\$), reflejando el monto de **ITBIS**.
- Copia certificación emitida por la **DGII**, donde se manifieste que el Oferente se encuentra al día en el pago de sus obligaciones fiscales.
- Copia certificación emitida por la **TSS**, donde se manifieste que el Oferente se encuentra al día en el pago de sus obligaciones de la Seguridad Social.
- **Registro mercantil actualizado**, emitido por la Cámara de Comercio y Producción correspondiente.
- Certificación Pentesting o Ethical Hacking, entre los cuales pueden ser: CISSP, CEH, GPEN, GWAPT, LPT, CHFI, ECSA).
- Experiencia de por lo menos dos proyectos de ethical hacking o penetration testing en los dos últimos años, dentro o fuera del país.

- Conocimiento sobre normativa de seguridad informática vigente para el sistema financiero e instituciones públicas de República Dominicana.
- La empresa deberá tener oficina local y deberá estar domiciliada en República Dominicana.

**Nota:** Las propuestas que no presenten toda la documentación y especificaciones requeridas no serán consideradas para la adjudicación.

### **3. OBJETIVOS ESPECIFICOS DE LA CONTRATACIÓN:**

El contratista deberá ejecutar como mínimo la siguiente lista de Pruebas de Pentesting y Ethical Hacking, si el contratista considera que hay pruebas adicionales que se deban hacer debe incluirlas en su oferta y detallarlas.

- Prueba de carga (load testing);
- Prueba de estrés (stress);
- Prueba de resistencia (endurance);
- Prueba de escalabilidad (scalability);
- Escaneo y análisis de puertos;
- Escaneo y análisis de vulnerabilidades;
- Evaluación de las seguridades tecnológicas implementadas en el servicio de acceso a Internet;
- Desbordamiento de buffer;
- Fuerza bruta sobre el servicio de autenticación de las Aplicaciones
- Google Hacking;
- Ataque de aplicaciones web;
- Inyección de SQL, SSI, LDAP;
- Inyección de comandos del sistema operativo;
- XSS Secuencias de Comandos entre sitios (Cross Site Scripting);
- Falsificación de petición en sitios cruzados (Cross Site Request Forgeries);
- Control de autorización erróneo sobre aplicaciones del sitio Web;
- Explotar vulnerabilidades de los servidores Web con el uso de programas exploit;
- Análisis y aprovechamiento de vulnerabilidades de los servidores, mediante el uso de programas exploit;
- Ataques de vulnerabilidades;
- Ataques de autenticación;
- Escalamiento de privilegios;
- Suplantación de credenciales;
- Usuarios o Claves en aplicaciones en texto plano;
- Manejo de sesiones;
- Remote File Access "Posibilidad de re-escribir archivos del servidor utilizando puertos conocidos.

El proveedor deberá utilizar al menos una herramienta de software comercial de escaneo de vulnerabilidades y otra de explotación presentes en el cuadrante de Gartner y/o Forrester. Las herramientas de escaneo de vulnerabilidades y explotación deben incluir Bases de Datos actualizadas a la fecha de realización de la consultoría.

#### **4. FASES DE EJECUCIÓN**

##### **1. Etapa de Análisis.**

Etapa en la que se realizará el análisis de la plataforma y sus configuraciones de acuerdo al alcance establecido en el punto “Objetivos específicos” del presente documento.

##### **2. Plan de Acción.**

La empresa consultora adjudicada establecerá una metodología y cronograma para la ejecución del servicio. El contratista deberá proponer un plan de ejecución del servicio de Pentesting Black Box, el cual, deberá ser aprobado por la Dirección de Ciberseguridad y Dirección General de Tecnología de la Información.

##### **3. Ejecución del Servicio.**

La empresa adjudicada realizará el estudio de Pentesting Black Box de acuerdo al cronograma aprobado, en la ejecución de las pruebas intervendrán funcionarios de la Dirección de Ciberseguridad y Gerencia de Informática.

#### **5. ENTREGABLES**

La empresa adjudicada deberá entregar:

- Informes tanto técnicos, como ejecutivos especificando las vulnerabilidades encontradas, nivel de riesgo, y las recomendaciones y/o posibles soluciones a dichas vulnerabilidades.
- Informe con los resultados de todas las pruebas realizadas.
- Plan de remediación para eliminar vulnerabilidades encontradas.

#### **6. RESPONSABILIDAD Y CONFIDENCIALIDAD**

La empresa adjudicada asume la responsabilidad sobre el manejo de la información, debiendo garantizar la integridad y disponibilidad de la misma durante la ejecución de las pruebas, además mantendrá la información tanto institucional como del resultado de las pruebas bajo estricta confidencialidad; pudiendo el Banco Agrícola realizar las verificaciones necesarias en cualquier momento.

Para tales efectos se tendrá como confidencial cualquier información no divulgada que posea legítimamente su titular que pueda usarse en alguna actividad productiva, industrial o comercial, y que sea susceptible de transmitirse a un tercero, en la medida en que dicha información sea secreta, en el sentido que como conjunto o en la configuración y reunión precisa de sus componentes no sea generalmente conocida ni fácilmente accesible a quienes se encuentran en los círculos que en forma usual manejan la información respectiva, tenga un valor comercial por ser secreta, y haya sido objeto de medidas razonables tomadas por su legítimo poseedor para mantenerla secreta.

La obligación de reserva consiste en abstenerse de usar, facilitar, divulgar o revelar, sin causa justificada y sin consentimiento del titular, la información sobre cuya confidencialidad se la haya prevenido en forma verbal o escrita; dicha obligación subsistirá durante la vigencia del contrato, y luego de su terminación mientras subsistan las características para considerarla como información confidencial.

## **7. TIEMPO DE EJECUCIÓN DEL CONTRATO**

El plazo de ejecución del contrato será de cuarenta y cinco (45) días laborables, contados a partir de la fecha de inicio de ejecución señalada por el Banco Agrícola, el lugar de ejecución será en las oficinas de la Matriz del Banco Agrícola en la ciudad de Santo Domingo.

## **8. REQUISITOS PARA PARTICIPAR**

- Especificar el **tiempo de validez de la oferta**.
- El suplidor del servicio debe **hacer constancia mediante una carta que evidencie y especifique el tiempo de entrega** y que se compromete a cumplir con el mismo.

## **9. CONDICIONES DE PAGO**

El pago se realizará en **treinta (30) días** luego de recibida la factura original en la Gerencia de Tesorería del Banco.

- 6. INFORMACIÓN DE CONTACTO:** Para cualquier consulta o aclaración, conforme al Procedimiento de Referencia, los datos de contacto son los siguientes:

**BANCO AGRÍCOLA DE LA REPÚBLICA DOMINICANA**  
**SECCIÓN DE COMPRAS Y CONTRATACIONES / DIRECCION DE SERVICIOS ADMINISTRATIVOS**  
Av. George Washington # 601, Santo Domingo de Guzmán, D.N.  
Teléfono: 809.535.8088 ext. 4316  
E-mail: [compras@bagricola.gob.do](mailto:compras@bagricola.gob.do)

## **7. ADJUDICACIÓN DE LA COMPRA**

La adjudicación será en favor de aquel oferente que: 1) Cumpla con los requerimientos establecidos en el numeral **2. Documentación a Presentar**, 2) Que cumpla con los requerimientos establecidos en el numeral **3. Objetivos Específicos de la Contratación** y 3) Que presente el menor precio.

Si se presentase una sola oferta, ella deberá ser considerada y se procederá a la adjudicación, si cumple técnica y económicamente con lo requerido.

## **8. PROHIBICIÓN A PARTICIPAR**

Los Oferentes/Proponentes deberán cumplir con las disposiciones establecidas en el Artículo 14 de la Ley No. 340-06 en el sentido de no encontrarse dentro de las prohibiciones indicadas en el mismo; además de no encontrarse impedidos de ejercer; ni han estados ni están, sancionados administrativamente con inhabilitación temporal o permanente para ofertar a entidades del sector público e involucradas en demandas o procesos judiciales relacionadas relación con el ejercicio de la profesión. Además, de que las firmas, ni sus socios, tienen conflictos de intereses con el Banco, incluyendo sus principales funcionarios o ejecutivos.

En adición a las disposiciones del Artículo 14 de la Ley No. 340-06 con sus modificaciones NO podrán contratar con el Estado dominicano los proveedores que no hayan actualizado sus datos en el Registro de Proveedores del Estado.

## **9. CONOCIMIENTO Y ACEPTACIÓN DE LOS TÉRMINOS DE REFERENCIA**

El sólo hecho de un oferente/proponente participar en el presente proceso de Compra Menor implica pleno conocimiento, aceptación y sometimiento por él, por sus miembros, ejecutivos y su Representante Legal, a los procedimientos, condiciones, estipulaciones y normativas, sin excepción alguna, establecidos en el presente documento, el cual tiene carácter jurídicamente obligatorio y vinculante.

## **10. ANEXOS**

- Solicitud de Compra
- Ficha Técnica
- Certificado de existencia de fondo No. 2021/000031

**DIONISIO E. JIMENEZ H.**  
Enc. Sección de Compras y Contrataciones