Programa Exportando Calidad e Inocuidad (ECI) y
El Centro para el Desarrollo Agropecuario y Forestal (CEDAF).

Consultoría para desarrollo, implementación y mantenimiento de la seguridad Informática a ser aplicada en la red y centro de datos del Centro para el Desarrollo Agropecuario y Forestal.

Santo Domingo, 26 de mayo del 2017

1. Introducción

El **Programa Exportando Calidad e Inocuidad (ECI),** ejecutado en la República Dominicana, es financiado por el Departamento de Agricultura de los Estados Unidos (USDA), con el objetivo de ofrecer asistencia para incrementar la productividad y venta de frutas y vegetales de alta calidad para el mercado doméstico e internacional. Tiene previsto mejorar el manejo post-cosecha y el cumplimiento de los requerimientos de calidad e inocuidad en las cadenas de valor de piña, aguacate, cacao, vegetales orientales e invernaderos para la mejora de sus niveles de competitividad. El Centro para el Desarrollo Agropecuario y Forestal (CEDAF), es el socio principal y sede del Programa ECI en el país y tiene el objetivo de apoyar al mismo en la ejecución y cumplimiento de las actividades definidas en el proyecto en pro del desarrollo agroexportador del país.

Para contribuir con esta iniciativa, el CEDAF dentro de las actividades del proyecto facilita el uso de un Sistema de Trazabilidad a los empacadores y exportadores de frutas y vegetales desde hace varios años.

Con el fin de garantizar el óptimo funcionamiento del sistema y su actualización a través del tiempo, el CEDAF y el programa ECI ejecutaron una consultoría con un especialista internacional de trazabilidad para la evaluación y diagnóstico del funcionamiento del Sistema de Trazabilidad de acuerdo a parámetros mundialmente aceptados. Como uno de los resultados de dicha evaluación surgió la necesidad de realizar una consultoría de seguridad informática que analice las vulnerabilidades en la red, equipos, sistemas, procesos y operaciones de datos del CEDAF.

La consultoría de seguridad informática mostrará la estructura tecnológica (hardware y software ofrecidos por CEDAF) y políticas de seguridad para implementar las mejoras necesarias con el fin de garantizar la confidencialidad, integridad y la disponibilidad de la información de la institución.

2. Objetivo General

La consultoría tiene como objetivo principal realizar un diagnóstico de las vulnerabilidades de la red, equipos y sistemas informáticos de la institución, proponer la estructura tecnológica (hardware y software) para implementar las mejoras necesarias con el fin de garantizar la confidencialidad, la integridad y la disponibilidad de la información de la institución.

Objetivos Específicos

- Efectuar un análisis y evaluación de los diferentes elementos de la red tales como firewalls, servidores de datos, servidores DNS, routers, switches, etc.; a fin de detectar posibles vulnerabilidades desde el Internet.

- Proponer la estructura y diagrama de la topología de la red en el cual se presenten las debilidades identificadas, con sus características y respectiva explicación, para cada uno de los componentes principales de la red.

- Diseñar e implementar los métodos, hardware y políticas de seguridad que garanticen la integridad, disponibilidad y confidencialidad de los datos registrados en la web tomando en cuenta el nivel de acceso a los datos por parte de los usuarios de los sistemas, como también rutinas de respaldo de la información y recuperación en caso de fallas o desastres.

3. Actividades y/o Productos de la Consultoría

El consultor tendrá la responsabilidad de realizar o entregar, en versión física y digital, los productos siguientes:

- **Producto1: ***
  Entrega de plan de trabajo y cronograma de actividades.

- **Producto 2:***
  Evaluación de las vulnerabilidades de los diferentes elementos de la red y/o sistemas, identificando debilidades de configuración que puedan ser explotadas. Presentar un diagrama e informe de la topología de la red en la cual se presenten las debilidades identificadas para cada uno de sus componentes principales. Asimismo, se debe presentar las posibilidades de hardware y metodologías necesarias para poner en funcionamiento la seguridad.

- **Producto 3:**

  Aplicar e implementar los métodos, hardware y políticas de seguridad que garanticen la integridad, disponibilidad y confidencialidad de los datos. Priorizando las recomendaciones para mitigar y/o eliminar las debilidades.

- **Producto 4:**

  - Entrega de documento que explique la política de seguridad de la estructura tecnológica del CEDAF (niveles de seguridad, políticas usadas, etc.) y donde se detallen las recomendaciones a seguir para garantizar la integridad y confidencialidad de los datos.

  - Impartición de charlas de sensibilización relacionada con seguridad, dirigida a los directivos de la institución y personal de tecnología.

- **Producto 5**
  Entrega del informe final detallado (técnico) con los resultados del estado de la seguridad implementado en la infraestructura tecnológica.

Los entregables deberán ser revisados y aprobados por el personal correspondiente del programa ECI y el CEDAF.

*Los derechos de propiedad intelectual, derechos de autor y demás derechos que surjan sobre cualquier material producido en el desarrollo de la consultoría, corresponden exclusivamente al contratante.

Nota: Todo lo que sea de conveniencia para el desarrollo y buen funcionamiento de la seguridad informática que no esté incluido dentro de los puntos mencionados, deberá ser considerado en la etapa de análisis y diseño e implementación de la consultoría, por parte del consultor(a) y/o empresa contratada para tales fines.

4. Supervisión

La **Supervisión** estará a cargo de la División de Informática del CEDAF para velar que la consultoría cumple con los requerimientos en términos de metodologías y su manejo.

Los entregables deberán ser revisados y aprobados por el Programa ECI y el CEDAF.

5. Período de Ejecución

El diagnóstico, diseño e implementación de la seguridad informática deberá realizarse en un plazo no mayor a (30) días y el período de tiempo tendrá vigencia a partir de la firma del contrato.

6. Calificaciones Requeridas

El consultor(a) y/o empresa deberá cumplir con los siguientes requisitos:

a) Ingeniero en sistemas, tecnología de la información o ciencias afines a la computación.
b) En caso de ser una empresa, contar con la documentación que demuestre que la empresa o consultor(a) está legalmente constituido (RNC, registro tributario, etc).
c) Más de 5 años de experiencia en implementación de sistemas de seguridad informática.
d) Experiencia suficiente y comprobable en, por lo menos, dos (2) consultorías en: i) proyectos similares de aplicación de seguridad informática, cobertura nacional y con accesos web; y ii) en la realización de pruebas de penetración, utilización de herramientas avanzadas para el análisis y evaluación de vulnerabilidades internas y externas de los sistemas computacionales.

e) Deberá tener, por lo menos, una (1) certificación internacional en seguridad que lo acredite, tales como: CISSP; Cisco CCNA Security; *CompTIA Security+;* CEH; CISM; GIAC; entre otros.

f) Experiencia y conocimiento en seguridad informática, pruebas de penetración, hacking, tráfico de datos, sistemas operativos, protocolos, arquitectura, topologías de red, estándares y/o políticas internacionales en materia de seguridad informática y auditoria de sistemas.

g) Experiencia en coordinación de proyectos de tecnologías de información con instituciones u Organizaciones No Gubernamentales.

7. Honorarios y Forma de Pago de la Consultoría

Los honorarios de la consultoría serán realizados contra entrega y aprobación de los productos citados. El número de pagos y porcentaje a realizar es el siguiente:

Pago	Productos contra entrega y aprobación	Porcentaje
1er. pago	**Producto 1:** Entrega de plan de trabajo y cronograma de actividades. **Producto 2:** Presentar un diagrama e informe de la topología de la red en la cual se presenten las debilidades identificadas para cada uno de los componentes principales de la red.	25%
2do. pago	**Producto 3:** Aplicar e implementar los métodos, hardware y políticas de seguridad que garanticen la integridad, disponibilidad y confidencialidad de los datos.	40%
3er. pago	**Producto 4:** Entrega de documento que explique la política de seguridad del y donde se detallen las recomendaciones a seguir para garantizar la integridad y confidencialidad de los datos. Impartición de charlas de sensibilización relacionada con seguridad, dirigida a los directivos de la institución y personal de tecnología. **Producto 5:** Entrega final de un informe detallado (técnico) con los resultados del estado de la seguridad implementado en la infraestructura tecnológica, priorizando las recomendaciones para mitigar y/o eliminar las debilidades detectadas.	35%
	TOTAL:	**100%**

8. Requisitos para Presentar Oferta Técnica Financiera

El consultor(a) y/o empresa seleccionado deberá presentar su oferta técnica (*productos a realizar, cronograma*) – económica (honorarios / *presupuesto de gastos*), en la que detallará la metodología a utilizar en la prestación de sus servicios, a los fines de la implementación de la seguridad informática; debiendo ser entregada en copia electrónica dirigida a **recursoshumanos@cedaf.org.do**, adjuntando, además, **el CV y/o portafolio de la empresa**, los documentos legales que avalen la existencia legal de dicho consultor(a) y/o empresa.

Plazo límite para recepción de aplicaciones: 12 de junio del 2017.