Al servicio
de las personas
y las naciones

ACLARATORIA N°1
SDC/00118949/167/2020 Adquisición de Auditoría de Seguridad Informática

Proyecto 00118949 Programa de apoyo para la eficiencia y la transparencia del proceso de modernización del documento nacional de identificación en Honduras

El Programa de las Naciones Unidas para el Desarrollo (PNUD), por este medio da las siguientes respuestas a consultas presentadas por empresas interesadas en el marco del proceso SDC/00118949/167/2020 Adquisición de Auditoría de Seguridad Informática:

PREGUNTA 1:
Para el requerimiento: **Análisis de vulnerabilidades en aplicaciones:**

a) ¿Cuántas aplicaciones de negocio y cuentas aplicaciones de terceros son requeridas escanear?
b) De las anteriores, ¿Cuántas serian en modelo caja blanca y cuántas serían en modelo caja negra?
c) ¿Cuántas aplicaciones web son?
d) ¿Cuántos módulos/funcionalidades tiene aproximadamente cada aplicación?
e) ¿En qué tecnología está desarrollada cada plataforma, y cuál es su número estimado de líneas de código? (para dimensionar análisis de código fuente - estático).

Respuesta 1:
a) Aplicaciones desarrolladas internamente: 1 (Aplicación A)
Aplicaciones desarrolladas por terceros: 1 (Aplicación B)
b) Caja blanca: una, la Aplicación A. Es importante recalcar que el análisis de caja blanca se requiere solo para la parte relacionada a la seguridad informática.
Caja negra: dos, las aplicaciones A y B.
c) Una, la Aplicación A, cuenta con ambiente web based y servicios web
La Aplicación B corre en clientes distribuidos en ambiente Windows, con consolidación a una base de datos central.
d) La Aplicación A (análisis de caja blanca y caja negra) tiene 4 opciones de menú y web services de consulta
La Aplicación B (solo caja negra) tiene una sola opción de menú que conduce a 8 pantallas.
e) Aplicación A: desarrollada .net 2019, aproximadamente 200,000 líneas de código. De nuevo, se recalca que el análisis de caja blanca solo es de lo relacionado con seguridad informática.
Aplicación B: no requiere revisión de código.

PREGUNTA 2:
Para el requerimiento: **Pruebas de penetración a aplicaciones móviles**:

a) ¿Cuántas aplicaciones móviles de negocio y cuentas aplicaciones de terceros son requeridas realizar las pruebas de penetración?
b) De las anteriores, ¿Cuántas serian en modelo caja blanca y cuántas serían en modelo caja negra?
c) ¿Cuántas aplicaciones móviles son?
d) ¿Cuántas Android y cuantas iOS?
e) ¿Cuántos módulos/funcionalidades tiene aproximadamente cada aplicación?
f) ¿En qué tecnología está desarrollada cada plataforma, y cuál es su número estimado de líneas de código? (para dimensionar análisis de código fuente - estático).

Respuesta 2:
a) Hay 4 aplicaciones móviles, todas desarrolladas internamente.
b) Se requiere análisis de caja blanca y caja negra para las 4 aplicaciones móviles.
c) 4
d) 3 en Android únicamente, y una en Android y iOS
e) App1: 4 módulos principales
App2: 4 módulos principales
App3: 2 módulos principales
App4: Un solo módulo principal
f) Las 4 aplicaciones están desarrolladas usando Java, HTML/JavaScript y XML. La cantidad aproximada de líneas de código es la siguiente:

	App1		App 2		App 3		App 4	
	Archi-vos	**Líneas codigo**	**Archi-vos**	**Líneas codigo**	**Archi-vos**	**Líneas codigo**	**Archi-vos**	**Líneas codigo**
.JAVA	45	12,139	36	18,275	48	15,503	13	3,319
.XML	60	6,964	42	23,976	54	6,833	26	836
.HTML	19	8,827	6	9,973	19	8,825	14	4,068

Es importante recalcar que el análisis de caja blanca se requiere solo para la parte relacionada a la seguridad informática.

PREGUNTA 3:
Para el requerimiento: **Test de Intrusión:**

a) Se indica que es requerido acceder a los sistemas, por favor, confirmar a qué se refiere ¿a servicios que están expuestos a Internet, o si se desea un test de intrusión a redes Wireless? ¿o ambos escenarios?
b) Confirmar si es un test interno (LAN) o externo (Internet).
c) Confirmar número aproximado de activos incluidos dentro del alcance.

Respuesta 3:
a) Solo a servicios expuestos en Internet
b) Solo externo (Internet)
c) Aproximadamente 10 servidores expuestos a IP pública

PREGUNTA 4:
Para el requerimiento: **Auditoría de páginas web:**

a) ¿Cuántos sitios web externos son parte del alcance?
b) Confirmar número de sitios incluidos dentro del alcance.
c) Del total ¿Cuántos sitios web externos parte del alcance tienen funcionalidades transacciones y o de consultas de usuarios externos a la organización?

Respuesta 4:
a) Tres
b) Tres
c) Dos son informativos, y uno tiene consultas de usuarios externos.

PREGUNTA 5:
Para el requerimiento: **Test de ingeniería social:**

a) ¿Cuántos usuarios son parte del alcance?
b) Confirmar número de usuarios aproximados para una prueba de Phishing Dirigido.
c) ¿Se deben hacer pruebas en diferentes idiomas?

Respuesta 5:
a) Máximo 8 técnicos de soporte
b) Máximo 8 técnicos de soporte
c) Solo Español

PREGUNTA 6:
Sobre la ejecución del proyecto se indica que la sede va a ser Tegucigalpa, Honduras, con trabajo presencial y remoto desde la oficina del contratista, solicitamos por favor, aclarar si es la expectativa que ciertas actividades se deben ejecutar en sus oficinas de modo presencial.

Respuesta 6:
El análisis de caja blanca de las aplicaciones preferiblemente presencial, el resto puede hacerse remotamente.

PREGUNTA 7:
Para el proceso ¿cuántas aplicaciones web son las que se van a evaluar?

Respuesta 7:
Una aplicación web, que incluye pantallas ambiente web y web services.
Una segunda aplicación que corre en clientes distribuidos en ambiente Windows, con consolidación a una base de datos central

PREGUNTA 8:
Para el proceso ¿Cuántas aplicaciones móviles se van a evaluar?

Respuesta 8:
Tres

PREGUNTA 9:
¿Cuántos servidores, equipos de comunicaciones y firewalls se van a evaluar?

Respuesta 9:
No es necesario evaluar equipos de comunicaciones ni firewalls. Servidores, solo los expuestos en IP pública, que son aproximadamente 10.

PREGUNTA 10:
En el alcance al realizar las evaluaciones de vulnerabilidades ¿posteriormente tienen que ser re-evaluadas a efectos de verificar que han sido solventadas?

Respuesta 10:
Si

PREGUNTA 11:
¿El nivel de madurez se puede realizar bajo la norma ISO 27001?

Respuesta 11:
Si

PREGUNTA 12:
Favor ampliar los alcances requeridos de la ingeniería social a realizar.

Respuesta 12:
Phishing a técnicos de soporte para tratar de obtener información que ponga en riesgo los sistemas de a la organización.

PREGUNTA 13:

a) ¿Se realizará análisis de vulnerabilidades a las PC de la empresa?
b) ¿a cuántas PCs?

Respuesta 13:
a) No
b) Ninguna

PREGUNTA 14:
¿Se evaluarán redes inalámbricas?

Respuesta 14:
No

PREGUNTA 15:
¿Cuál es el presupuesto indicativo-aproximado que posee el presente proyecto?

Respuesta 15:
El PNUD no indica valores referenciales de los concursos y promueve la libre competencia entre las empresas participantes, quienes deberán hacer su mayor esfuerzo para ofertar sus mejores precios.

PREGUNTA 16:
Respecto a la actividad Análisis de vulnerabilidades en aplicaciones (4.1):

a) Favor especificar la cantidad de aplicaciones que serán objeto de las pruebas
b) Brindar en detalle el lenguaje de programación y la versión del mismo con que fue creado el código que las conforma.
c) De igual manera confirmar si requiere hacer retest o reevaluación posterior.

Respuesta 16:
a) Favor ver respuesta a esta consulta en la Pregunta # 1
b) Favor ver respuesta a esta consulta en la Pregunta # 1
c) Favor ver respuesta a esta consulta en la Pregunta # 10

PREGUNTA 17:
Respecto a la actividad **Pruebas de penetración a aplicaciones Móviles (4.2):**

a) Favor especificar la cantidad de aplicaciones móviles que serán objeto de las pruebas
b) Brindar en detalle el lenguaje de programación y la versión del mismo con que fue creado el código que las conforma.
c) De igual manera confirmar si requiere hacer retest o reevaluación de las pruebas.
d) Indicar si estas aplicaciones existen para las plataformas de Android y iOS.

Respuesta 17:
a) Favor ver respuesta a esta consulta en la Pregunta # 2
b) Favor ver respuesta a esta consulta en la Pregunta # 2
c) Favor ver respuesta a esta consulta en la Pregunta # 10
d) Favor ver respuesta a esta consulta en la Pregunta # 2

PREGUNTA 18:
Respecto a la actividad **Pruebas de intrusión a nivel de red (4.3):**

a) Favor especificar si las pruebas de intrusión requeridas deben incluir en su alcance la ejecución de explotación de vulnerabilidades a criterio del analista según su criticidad.
b) Indicar si es para la red interna o externa.
c) Indicar la cantidad de activos o direcciones IP que serán objeto de los análisis.
d) Es importante confirmar si se requiere retest posterior.

Respuesta 18:
a) Si, debe incluirse.
b) Favor ver respuesta a esta consulta en la Pregunta # 3
c) 20 IPs públicas y 10 servidores
d) Favor ver respuesta a esta consulta en la Pregunta # 10

PREGUNTA 19:
En cuanto al alcance - **Auditoria de páginas WEB (4.4):**

a) Favor especificar textualmente si se requiere análisis de código estático y dinámico como parte del alcance.
b) Indicar la cantidad y nombre de cada una de las aplicaciones que serán objeto del análisis.

Respuesta 19:
a) Se requiere estático y dinámico.
b) Favor ver respuesta a esta consulta en la Pregunta # 4

PREGUNTA 20:
En cuanto al **Test de Ingeniería Social (4.5):** Existen varias pruebas que pueden ejecutarse como parte de este requerimiento: Phishing, Vishing, USB, entre otras.

a) Favor especificar ¿qué tipo de prueba requieren y cuál será el alcance de las mismas?
b) Si es Phishing indicar cantidad de buzones de correo;
c) Si es Vishing indicar cantidad de extensiones telefónicas y
d) Si es USB indicar cantidad requerida.

Respuesta 20:
a) Favor ver respuesta a esta consulta en la Pregunta # 5
b) Favor ver respuesta a esta consulta en la Pregunta # 5
c) Favor ver respuesta a esta consulta en la Pregunta # 5
d) No se requiere USB.

En la Ciudad de Tegucigalpa, M.D.C., a los 23 días del mes de noviembre de 2020