



Tegucigalpa, MDC
7 de septiembre de 2021

ABN-9559/2021

Señores
OFERENTES
Ciudad

Ref.: Concurso Privado No.02/2021

Estimados señores:

Hacemos referencia a consultas efectuadas al Concurso Privado No.02/2021 para la contratación de los servicios de consultoría para la gestión de ciberseguridad, análisis de vulnerabilidades y hacking ético del Banco Central de Honduras; al respecto, se informa lo siguiente:

Consulta No.1:

1. *"¿Qué tipo de arquitectura SWIFT tiene el Banco Central de Honduras?"*

Respuesta

A2.

Consulta No.2:

2. *"¿Cuántos operadores tienen acceso a la plataforma de SWIFT?"*

Respuesta

Entre 10 y 20 operadores.

Consulta No.3:

3. *"¿En cuántos sitios de datos tienen distribuida la arquitectura de SWIFT?"*

Respuesta

La arquitectura principal de SWIFT se encuentra en un sitio de datos.

Consulta No.4:

4. *"Considerando que el objetivo principal de este servicio es evaluar la efectividad de los controles existentes en servicios DMZ e Implementación del Programa de Seguridad del Cliente SWIFT, Red Interna y Sistemas que soportan los procesos críticos del BCH, ¿desean agregar una reevaluación de cumplimiento después de que se apliquen las recomendaciones para el cierre de las brechas encontradas en la primera evaluación?"*

f

*Una pequeña decisión puede cambiar la economía.
Ahorra energía y combustible hoy!*



Respuesta

La reevaluación de cumplimiento solamente es para el Programa de Seguridad del Cliente SWIFT y se contempla su ejecución en la fase IV.

Consulta No.5:

5. *"¿Desean que se incluyan horas de acompañamiento por parte de un Consultor de SISAP para la remediación de las brechas encontradas o solamente compartir el Plan de Remediación para ejecución propiamente por el BCH?"*

Respuesta

Se espera que, durante la vigencia de la consultoría, la empresa brinde asesoría técnica para implementar las acciones correctivas que se consideren necesarias para remediar las potenciales vulnerabilidades encontradas; según se estable en el Anexo No.2: Condiciones y Requerimientos Técnicos, Condiciones que debe cumplir el consultor, numeral 2.11.

Consulta No.6:

6. *"¿Podrían por favor indicar la cantidad de direcciones IP privadas que forman parte de su red de SWIFT?"*

Respuesta

Entre 10 y 20 direcciones IP privadas.

Consulta No.7:

7. *"¿Podrían por favor indicar si desean incluir una re-evaluación de esta prueba después de que hayan aplicado las recomendaciones brindadas para la mitigación de las vulnerabilidades encontradas? Es decir, ¿aclarar si requieren un retest en cada nueva fase?"*

Respuesta

No se requiere; sin embargo, se puede evaluar y aceptar cualquier otra evaluación o servicio que el consultor estime conveniente y que agregue valor y no represente costo adicional al BCH, según se establece en el Anexo No.2: Condiciones y Requerimientos Técnicos, Condiciones que debe cumplir el consultor, numeral 2.19.

Consulta No.8:

Fase II Servicios en DMZ (Internet y Extranet) **Aclarar:**

8. *"¿Por favor indicar la cantidad de direcciones IP privadas y públicas que forman parte de su red de servicios DMZ?"*

48

*Una pequeña decisión puede cambiar la economía
¡Ahorra energía y combustible hoy!*



Respuesta

Entre 15 a 25 segmentos de IP privadas, 95 a 125 direcciones IP públicas.

Consulta No.9:

9. "¿Por favor indicarnos la cantidad de SSID que están dentro del alcance de la evaluación?"

Respuesta

Entre 5 a 10 SSID.

Consulta No.10:

"Fase III Sistema que Soportan Procesos Críticos

Literal c) Realizar en coordinación con el Gerente de Proyecto del BCH, adscrito al Departamento de Gestión de Riesgos, el análisis de los activos de información de al menos tres (3) sistemas que soportan procesos críticos del BCH para determinando: 1) Valoración de los Activos de Información

Aclarar:

10. *¿Esta valoración se refiere a una valoración del riesgo cualitativo o cuantitativo de los activos a evaluar, confirmar qué tipo de Valoración de Activos de información es la esperada?"*

Literal d) La evaluación sobre los activos de información de los sistemas que soportan los procesos críticos que se definan deben incluir como mínimo: 5) Aplicaciones web en producción y su correspondiente análisis utilizando la metodología Guía de Pruebas OWASP".

Respuesta

Valoración cualitativa.

Consulta No.11:

Aclarar

11. "¿Por favor indicarnos la cantidad de aplicaciones web que soportan los procesos críticos?"

Respuesta

Al menos 3 aplicaciones web.

Consulta No.12:

12. "¿Por favor indicarnos con la cantidad de IP de los 3 sistemas que soportan los procesos críticos?"

H

*Una pequeña decisión puede cambiar la economía
'Ahorra energía y combustible hoy'*



Respuesta

Entre 2 a 4 direcciones IP por sistema que soporta procesos críticos.

Consulta No.13:

"Fase IV Red Interna, Concientización en Ciberseguridad, SWIFT y Cierre de Proyecto, Respecto a la Red Interna

Aclarar:

13. *¿Por favor indicarnos la cantidad de IP internas que serán evaluadas en la fase 4?"*

Respuesta

Una muestra mínima del 10% el BCH cuenta con un estimado entre 950 a 1200 estaciones de trabajo.

Consulta No.14:

"Respecto a la Concientización en Ciberseguridad

Literal f) Debe evaluar el grado actual de conciencia de ciberseguridad de los empleados del BCH, a través de aplicación de pruebas de conocimiento e ingeniería social disponibles, con el objeto de determinar áreas de oportunidad que permitan reforzar la conciencia sobre esta temática, para enfrentar diferentes escenarios de riesgos que podrían presentarse y afectar a la disponibilidad, integridad y confidencialidad de los activos del BCH

Aclarar:"

14. *¿Por favor indicar la cantidad de usuarios (cantidad de buzones) a las que se aplicará la prueba de conocimiento e ingeniería social?"*

Respuesta

Considerando que la información que se generará de la ejecución del literal f) será la base para la ejecución literal g), por lo que, se estiman todos los buzones de correo electrónico (950 a 1150) esto depende del tipo de prueba de ingeniería social que realizarán, ya que se desea que las pruebas reflejen diferentes escenarios de riesgos.

Consulta No.15:

"Todas las fases inician con el enunciado que se debe dar seguimiento a las fases anteriores, revisando el avance del plan de remediación propuesto referente a la mitigación de potenciales vulnerabilidades, nos podrían confirmar por favor si:

15. *¿Requieren que en cada nueva fase de realice un retest de las pruebas realizadas en fases anteriores?"*

HP

*Una pequeña decisión puede cambiar la economía
"Ahorra energía y combustible hoy"*



Respuesta

No se requiere; sin embargo, se puede evaluar y aceptar cualquier otra evaluación o servicio que el consultor estime conveniente y que agregue valor y no represente costo adicional al BCH, según se establece en el Anexo No.2: Condiciones y Requerimientos Técnicos, Condiciones que debe cumplir el consultor, numeral 2.19.

Consulta No.16:

16. "¿Requieren solamente la propuesta Plan de Remediación o también la ejecución por parte del Consultor?".

Respuesta

Se espera que, durante la vigencia de la consultoría, la empresa brinde asesoría técnica para implementar las acciones correctivas que se consideren necesarias para remediar las potenciales vulnerabilidades encontradas, según se establece en el Anexo No.2: Condiciones y Requerimientos Técnicos, Condiciones que debe cumplir el consultor, numeral 2.11

Nota: Los valores proporcionados son estimaciones, que podrán variar. Estos se definirán en el Plan de Trabajo.

Atentamente,



FANNY MARISABEL TURCIOS BARRIOS

Secretaria de la Comisión de Compras y Evaluación y
Jefe Departamento de Adquisiciones y Bienes Nacionales

SDM/IMP/TMG

