SUPERINTENDENCIA DE BANCOS
REPÚBLICA DOMINICANA

Informe Final de Evaluación de Ofertas Técnicas
SUPBANCO-CCC-CP-2021-0015

A : Eblin Pena
Analista de Compras

Asunto : Informe final rendido por los peritos designados para evaluar la oferta técnica propuesta del proceso SUPBANCO-CCC-CP-2021-0015, referente a Pruebas de Penetración (Pentesting) Ciberseguridad.

Fecha : 30 de junio 2021

I. Introducción

En atención a su solicitud, fuimos designados peritos del proceso para realizar **Prueba de Penetración (Pentesting) Ciberseguridad, llevado a cabo mediante** el proceso SUPBANCO-CCC-CP-2021-0015, procederemos a evaluar las propuestas recibida de los oferentes Siguientes:

- Multicomputos
- Grupo Tecnológico Adexus
- KPMG dominicana, SA
- Infosec Latin America, SISAP
- NAP Del Caribe

II. Objetivo

El objetivo de este informe consiste en revisar las propuestas técnicas enviadas por los oferentes y validar el cumplimiento de estas con las especificaciones técnicas del proceso "SUPBANCO-CCC-CP-2021-0015" definidas en el Pliego de Condiciones.

III. Criterios

Para la revisión se consideraron los requisitos indicados en el Pliego de condiciones y las correspondientes Especificaciones Técnicas y documentos a presentar.

IV. Conclusión

Luego de analizar las informaciones suministradas en la propuesta técnica remitida por los oferentes, relacionadas a la adquisición de servicios Pruebas de Penetración (Pentesting) Ciberseguridad para la Superintendencia de Bancos, les informamos que el oferente indicado a continuación no cumple con las

condiciones indicadas en el Pliego de Condiciones del proceso "SUPBANCO-CCC-CP-2021-0015":

1. Multicómputos. En su propuesta no incluyen documentación de la calificación del personal que realizará el Análisis de Vulnerabilidades y Prueba de Penetración. De igual forma deben incluir un cuadro resumen indicando el cumplimiento de nuestros requerimientos y las secciones donde se dan respuestas a estos.

Los oferentes indicados a continuación cumplen con las condiciones indicadas en el Pliego de Condiciones del proceso "SUPBANCO-CCC-CP-2021-0015", como se puede observar en la matriz de cumplimiento anexa:

1. Grupo Tecnológico Adexus
2. KPMG dominicana, SA
3. Infosec Latin America, SISAP
4. NAP Del Caribe

Atentamente,

Eduard Encarnación
Especialista Senior

Kendra Mazara
Encargado de División

Levin Torres
Encargado de
División

	A	B	C	D	E	F
1	Requerimientos	KPMG Dominicana	Infosec Latin America (SISAP)	NAP del Caribe	Multicómputos	Grupo Tecnológico Adexus
2	Realizar un Análisis de Vulnerabilidades y Prueba de Penetración a la red de la Superintendencia de Bancos, sin tener información previa de la infraestructura y sistemas de la red (Blackbox).	Cumple	Cumple	Cumple	Cumple	Cumple
3	Realizar los Pentests y Análisis de Vulnerabilidades de manera interna (red interna Superintendencia de Bancos), tanto a nivel de la capa de red como de la capa de aplicación.	Cumple	Cumple	Cumple	Cumple	Cumple
4	Implementar una metodología basada en las mejores prácticas de la industria. Ejemplo: OWASP, NIST, OSSTMM	Cumple	Cumple	Cumple	Cumple	Cumple
5	Personal está calificado, presentando certificaciones que prueben sus competencias.	Cumple	Cumple	Cumple	No presentó documentación para este requerimiento. Hay uno de los archivos enviados que no abre, Documentación sobre A SUPBANCO.pdf	Cumple
6	10 años de experiencia realizando Análisis de Vulnerabilidades y Pruebas de Penetración a organizaciones con infraestructuras y tamaño similares o superior a la Superintendencia de Bancos	Cumple	Cumple	Cumple	No presentó documentación para este requerimiento. Hay uno de los archivos enviados que no abre, Documentación sobre A SUPBANCO.pdf	Cumple
7	Formalizar la planeación del proyecto, definir los alcances detallados de cada una de las fases y etapas, así como determinar la organización y administración del proyecto.	Cumple	Cumple	Cumple	Cumple	Cumple
8	Recolectar la información inicial para identificar de forma precisa los procesos, recursos e infraestructura de TI.	Cumple	Cumple	Cumple	Cumple	Cumple
9	Identificar los componentes que integran la Infraestructura Tecnológica de Superintendencia de Bancos de la República Dominicana, cómo se relacionan y enlazan entre sí, y los posibles vectores de ataque que podrían ser usados. o Enumeración de la red, usuarios y recursos o Queries a los DNS o Escaneo de servicios y mapeo de la red o Identificación de patrones en los datos recolectados.	Cumple	Cumple	Cumple	Cumple	Cumple
10	Realizar búsquedas de vulnerabilidades específicas de acuerdo a la información obtenida de la fase de recolección de información. o Realizar análisis de la seguridad de los protocolos de la red y su backbone o Auditar el diseño y la configuración de los servicios, servidores y aplicaciones, bases de datos, firewall, routers, sistemas de prevención de intrusos, switches y otros recursos. o Investigar las vulnerabilidades que afectan a los recursos de TI identificados o Verificar y probar manualmente las vulnerabilidades encontradas o Cuantificar y priorizar los hallazgos.	Cumple	Cumple	Cumple	Cumple	Cumple
11	Realizar pruebas controladas, sin afectar la disponibilidad de los servicios de la Superintendencia de Bancos, las cuales están encaminadas en explotar activamente las vulnerabilidades identificadas en los diferentes recursos de TI. o Configuraciones débiles o inseguras o Falta de implementación de las mejores practicas o Fallas en el kernel de los sistemas operativos evaluados o Buffer overflows a nivel de los sistemas operativos, aplicaciones o servicios o Sistemas sin los últimos parchos de seguridad o Exploits que explotan vulnerabilidades no publicadas. o Hacer intentos de escalar privilegios para ganar control total sobre el sistema afectado. o Analizar el sistema comprometido para encontrar brechas que nos permitan ganar acceso a otros sistemas. o Instalar herramientas adicionales de penetración en el equipo afectado para comprometer la infraestructura tecnológica y sistemas.	Cumple	Cumple	Cumple	Cumple	Cumple

	A	B	C	D	E	F
12	Realizar pruebas de penetración contra las aplicaciones Web HTTP/S identificadas dentro de la infraestructura tecnológica. o Mapeo Web o Evaluación de la Configuración o Pruebas de Autenticación o Evaluación de la Gestión de Sesiones o Análisis del Esquema de Autorización o Pruebas de Lógica de Negocio o Validación de la Entrada de Datos.	Cumple	Cumple	Cumple	Cumple	Cumple
13	Realizar la Clasificación y Ponderación de Vulnerabilidades, utilizando una metodología basada en estándares, que permita asignar un valor cuantitativo a cada una de las vulnerabilidades identificadas.	Cumple	Cumple	Cumple	Cumple	Cumple
14	Realizar el Análisis de Riesgos a la Infraestructura Tecnológica en el alcance de la Superintendencia de Bancos de la República Dominicana considerando vulnerabilidades, amenazas e impactos al negocio, mediante el uso de metodologías de análisis de riesgos.	Cumple	Cumple	Cumple	Cumple	Cumple
15	Realizar un documento de proyecto donde indique: tiempo de implementación, tiempo de entrega y recomendaciones.	Cumple	Cumple	Cumple	Cumple	Cumple