ACLARACIONES CONVOCATORIA 489 COMFENALCO TOLIMA ESTÁ INTERESADO EN CONTRATAR SERVICIO ESPECIALIZADO QUE REALICE PRUEBAS DE ETHICAL HACKING A LOS DOMINIOS DE LAS PÁGINAS WEB DE LA CAJA

N°	PREGUNTA	RESPUESTA
1	Observación 1: Agradecemos a la entidad que, para el componente de ingeniería social, se aclare aproximadamente hacia cuantas personas ira dirigido el ejercicio. Adicionalmente, solicitamos nos indiquen si el proveedor puede proponer el tipo de prueba realizar o Comfenalco tiene un plan para esto.	La prueba de ingeniera social es propuesta(s) y ejecución del ejercicio que por parte de Comfenalco se apruebe de acuerdo a la propuesta del oferente. Respecto a la cantidad de personas que va dirigido, tiene la condición que si la propuesta requiere la presencia física del personal de la Caja se tiene una estimación de 300 y si la prueba es a través de herramientas tecnológicas que no requieren la presencia física del personal de la Caja se puede estar hablando de 500.
2	Observación 2: Para el componente de transferencia de conocimiento, solicitamos nos indiquen hacia cuantas personas aproximadamente van dirigidas las capacitaciones (workshop y las jornadas de capacitación).	Para el workshop virtual en temas de seguridad ofensiva (de mínimo 9 horas): se estima un total de 15 personas Para las dos (2) capacitaciones virtuales en temas de ingeniería social cada una de 4 horas: 500 personas, en donde cada capacitación un estimado de 250 personas.
3	En las condiciones del servicio a contratar, requieren textualmente: “El proponente debe especificar y certificar claramente los acuerdos de niveles de servicio establecidos ofertados para el servicio”. Es importante nos aclaren los servicios que requieren tener niveles de servicio, y cuáles serían estos en términos de métricas.	El oferente dentro de su oferta; debe especificar para los posibles riesgos y hallazgos que se encuentren los tiempos en que se debe cumplir la subsanación para la siguiente evaluación de acuerdo con la oferta.
4	También en las condiciones del servicio a contratar, requieren textualmente: “En el evento que exista la necesidad de realizar desplazamiento a algunas de las sedes fuera de las oficinas principales por el tipo de contratación, esta deberá estar a cargo del oferente, por lo tanto, deberá ser incluida en la oferta”. Solicito por favor enumerar las sedes de COMFENALCO TOLIMA, y si se encuentran dentro de la ciudad de Ibagué.	A continuación se comparte información de la sedes en la ciudad de Ibagué La sede principal de Comfenalco Tolima: Ibagué, Tolima - Colombia: Calle 37 con Cra. 5 esquina Instituto Técnico: Ibagué, Tolima - Colombia: Calle 14 No. 7 - 53 Barrio Pueblo Nuevo Centro recreacional Urbano Carlos M. Arango: Ibagué, Tolima - Colombia: Kilómetro 6 vía Bogotá Instituto Educativa Augusto E. Medica: Ibagué, Tolima - Colombia: Calle 125 entre Cra. 18 D Sur y 18 Bis Sur - Ciudadela Comfenalco Para cumplimiento del objeto de la convocatoria, no se requiere desplazamiento a sedes fuera de la ciudad de Ibagué
5	En la sección de ámbito de ataque, indican textualmente: “APP Comfenalco Tolima (Sistema Android y IOS)”. Con relación a estas aplicaciones, es importante conocer cuántas son las APP a evaluar; si fueron desarrolladas por COMFENALCO TOLIMA, o si fueron contratadas. Si ya se hicieron otros análisis de vulnerabilidades previos y si se tiene el resultado de éstos	El APP es una sola, la cual fue desarrollada para los servicios de la Caja, este desarrollo fue realizado por parte del mismo proveedor de software ERP y se encuentra integrada al mismo, no se cuenta con análisis de vulnerabilidades anterior.
6	No se puede dar información al respecto, por el servicio de hosting se paga arrendamiento. El detalle será compartido únicamente con el oferente a quien se le asigne el contrato	El servicio es Alojado en un Datacenter TIER IV con sede en tocancipa, el detalle de las aplicaciones alojadas se dará una vez se adjudique el contrato al oferente elegido.

ACLARACIONES CONVOCATORIA 489 COMFENALCO TOLIMA ESTÁ INTERESADO EN CONTRATAR SERVICIO ESPECIALIZADO QUE REALICE PRUEBAS DE ETHICAL HACKING A LOS DOMINIOS DE LAS PÁGINAS WEB DE LA CAJA

N°	PREGUNTA	RESPUESTA
7	Como observación, esto podría llegar a subir mucho el precio de la consultoría para COMFENALCO Por eso, aconsejamos que se analicen las funciones de estas estaciones de trabajo, y si todas ellas son totalmente diferentes y cumplen roles críticos para COMFENALCO, se deben analizar todas; pero si existe un modelo similar para las estaciones de trabajo de un área específica, se recomienda sacar una o dos, y a partir del resultado de ellas, corregir las demás. Si la gran mayoría se usan para trabajos de ofimática, y simplemente tienen un anti malware instalado, no se justifica invertir tanto dinero en el análisis de vulnerabilidades y pen testing de estas. Basta con sacar una muestra, y el resultado se aplicará a las demás estaciones. También se recomienda seleccionar para este análisis, aquellas estaciones de trabajo que realmente se tienen para actividades críticas, tales como Tesorería o Gestión de Personal, entre otras.	Es viable con una muestra representativa de acuerdo con la criticidad la cual podemos establecer con el contratista una vez se adjudique el contrato
8	PRUEBAS DE INGENIERÍA SOCIAL: Es importante que indiquen el alcance de esta prueba: Por ejemplo, si deciden realizar phishing, a cuántas cuentas de correo se lanzará. Si deciden Prueba de Smishing – Vising, a cuántas personas se lanzará; si deciden pretexting: A cuántas personas se lanzará el ataque.	La prueba de ingeniera social es propuesta(s) y ejecución del ejercicio que por parte de Comfenalco se apruebe de acuerdo a la propuesta del oferente. Respecto a la cantidad de personas que va dirigido, tiene la condición que si la propuesta requiere la presencia física del personal de la Caja se tiene una estimación de 300 y si la prueba es a través de herramientas tecnológicas que no requieren la presencia física del personal de la Caja se puede estar hablando de 500.
9	EXPERIENCIA EXIGIDA: Con relación a esta experiencia, ¿es necesario que los tres contratos ejecutados hayan tenido un precio similar al de la propuesta? ¿O la suma de los tres contratos debe ser similar al de la propuesta?	La suma de los tres contratos debe ser similar al de la propuesta.
10	FECHA MÁXIMA DE ENTREGA: Con el fin de determinar el recurso humano necesario para cumplir con el alcance de este proyecto, es importante que se aclare si COMFENALCO TOLIMA tiene fecha límite de entrega de este proyecto.	Entregables por el oferente: (Informe Técnico, Matriz de Hallazgos, Informe Ejecutivo, Presentación, Remisión de los entregables) y Transferencia del Conocimiento; no deberán superar la vigencia 2023. y las Pruebas de Re-testing para vigencia 2024
11	1.¿A qué hacen referencia al número de clientes promedio por aplicación y al número de tablas de bases de datos de aplicación? ¿Dentro de la infraestructura hay aplicaciones? Esto se encuentra descrito en la página 8, numeral 2.	El numero de clientes promedio por aplicación; hace referencia a la cantidad de usuarios finales que se tienen en las aplicaciones. El numero de tablas base de aplicación; es la cantidad de tablas en base de datos. En la infraestructura se encuentran alojadas las aplicaciones a las que se requiere realizar las pruebas de ethical
12	2. ¿Se debe presentar una propuesta técnica o únicamente los requisitos descritos en el anexo 3?	La propuesta debe describir lo requerido por el anexo 3 y la propuesta ecónomica
13	3. ¿Hay algún formato para presentar la propuesta económica?	No, no hay formato definido

ACLARACIONES CONVOCATORIA 489 COMFENALCO TOLIMA ESTÁ INTERESADO EN CONTRATAR SERVICIO ESPECIALIZADO QUE REALICE PRUEBAS DE ETHICAL HACKING A LOS DOMINIOS DE LAS PÁGINAS WEB DE LA CAJA

N°	PREGUNTA	RESPUESTA
14	1.1. Con respecto al objeto por favor aclarar si la entidad requiere pruebas de penetración o un ejercicio de ethical hacking. Pruebas de penetración: Este servicio también llamado test de penetración está diseñado para determinar el alcance de los riesgos, vulnerabilidades o fallas de seguridad de los sistemas bajo evaluación. El pentester simula la ejecución de pruebas que podría realizar un atacante malintencionado desde una perspectiva: • Atacante externo sin privilegios o acceso a las aplicaciones o tecnologías que soportan los servicios. • Atacante externo con un usuario válido de bajos privilegios de las aplicaciones web. • Atacante interno con un usuario válido de bajos privilegios de las aplicaciones web. Son pruebas estructuradas que buscan la posible explotación de esas vulnerabilidades detectadas a través de un ejercicio previo de descubrimiento. Ethical hacking: Esta actividad tiene como objetivo buscar resquicios de seguridad mediante actividades no estructuradas de ataque. Esto significa que no se emplean metodologías estándares de penetración, sino que se emplea la experiencia y conocimiento del experto con el fin de buscar acceder a la plataforma de manera no autorizada de la misma forma que lo haría un Ciberdelincuente (Hacker Malicioso).	Es Ethical Hacking
15	2. Personal calificado 2.1. Solicitamos retirar como opciones de certificaciones la CISSP, CCSP y CompTIA CASP+ ya que éstas certificaciones son utilizadas para servicios consultivos de ciberseguridad y no para servicios de diagnóstico o pruebas lo cual es el objeto del contrato.	Los pliegos se mantienen Las certificaciones requeridas no son de cumplimiento en su totalidad, solo se requiere al menos una de las mencionas
16	3. Evaluación de proveedores 3.1. Sugerimos a la entidad solicitar que las empresas que se postulen para prestar el servicio estén certificadas como mínimo en ISO 27001 y como valor estar con certificación ISO 9001; esto asegura en gran medida que la gestión de información recopilada dentro del ejercicio sea manejada dentro de las mejores prácticas asegurando su confidencialidad,	Los pliegos se mantienen
17	4. Especificaciones técnicas 4.1. Por favor indicarnos si las pruebas a los componentes de infraestructura se pueden realizar de manera remota a través de una VPN.	El medio de ejecución de las pruebas lo define el proponente, por lo que se requiere pruebas de ethical de Caja Negra
18	4.2. Por favor indicarnos los horarios de ejecución de las pruebas (5x8 o 7x24)	El horario será definido por el proponente. Puede escoger los horarios que estime dentro de la propuesta.

ACLARACIONES CONVOCATORIA 489 COMFENALCO TOLIMA ESTÁ INTERESADO EN CONTRATAR SERVICIO ESPECIALIZADO QUE REALICE PRUEBAS DE ETHICAL HACKING A LOS DOMINIOS DE LAS PÁGINAS WEB DE LA CAJA

N°	PREGUNTA	RESPUESTA
19	4.3. Por favor aclararnos si se debe realizar pruebas a todas las estaciones de trabajo; como sugerencia de parte de SecPro se podría hacer un análisis de vulnerabilidades a todos los equipos de computo y pruebas a un porcentaje (10% equivalente a 50 equipos) esto con el fin de optimizar recursos (humanos y financieros) y resultados de la entidad. Es importante resaltar que no se incluyen las otras 450 estaciones de trabajo, dado a que en nuestra experiencia, en las organizaciones respecto a la configuración están bajo una línea base especifica, por lo tanto, al tomar una muestra de los dispositivos se puede tener una visión general del estado de las demás estaciones de trabajo, lo que indica, que las vulnerabilidades detectadas, identificadas y comprobadas (explotación) pueden estarpresentes en las otras 450 estaciones de trabajo, por tal razón, el equipo de Comfenalco Tolima podría verificar si las vulnerabilidades identificadas y comprobadas pueden estar en las otras 450 estaciones de trabajo; ej.: falta de parches de seguridad.	Es viable con una muestra representativa de acuerdo con la criticidad la cual podemos establecer con el contratista una vez se adjudique el contrato
20	4.4. Agradecemos indicar qué tipo de ejercicio de ingeniería social se desea realizar (phishing, vishing, Smishing, etc.) y la cantidad de usuarios objetivo.	La prueba de ingeniera social es propuesta(s) por parte del proponente. Si la propuesta requiere la presencia física del personal de la Caja se tiene una estimación de 300 y si la prueba es a través de herramientas tecnológicas que no requieren la presencia física del personal de la Caja se puede estar hablando de 500.
21	4.5. Por favor indicar la cantidad de personas aproximadas y roles dentro de Comfenalco a quienes estará dirigido el workshop y la capacitación. Sugerimos a la entidad separar el requerimiento en 2 fases: primera un ejercicio tipo table top en el que se simula un ataque y se vinculan los niveles decisorios de la organización (alta gerencia) y segunda una capacitación en seguridad ofensiva (red team) para un grupo determinado de personas	Es viable la propuesta. Se tiene estimado un total de 15 personas
22	4.6. Por favor indicar la cantidad de personas aproximadas y roles a la que estará dirigida la capacitación de ingeniería social.	Dos (2) jornadas de capacitación virtual en temas de ingenieria social cada una de 4 horas, con la participación en cada jornada de 250 personas aproximadamente. Para un total de 500 trabajadores de la Caja
23	5. Generales 5.1. Solicitamos a la entidad extender el tiempo de entrega teniendo en cuenta que se requieren las respuestas a las preguntas para el dimensionamiento del servicio y posterior solicitud de la garantía de seriedad requerida.	Los pliegos se mantienen
24	Se indica que: "4. El oferente debe presentar los informes estructurados tanto impreso como en medio magnetico", sin embargo, teniendo en cuenta el volumen de información que se relaciona en los informes tecnicos, solicitamos que los informes sean presentados únicamente en medio digital.	Los pliegos se mantienen
25	Para la prueba de ingenería social, solicitamos inidcar el número aproximado de colaboradores.	Dos (2) jornadas de capacitación virtual en temas de ingenieria social cada una de 4 horas, con la participación en cada jornada de 250 personas aproximadamente. Para un total de 500 trabajadores de la Caja

DIANA MAGALLY KANDIA TRONCOSO

Firmado digitalmente por DIANA MAGALLY KANDIA TRONCOSO
DN: T=SECRETARIO GENERAL Y APOYO A LA GESTION, SN=KANDIA TRONCOSO, STREET=CR 5 CL 37 ESQ, S=TOLIMA, OU=OTROS - 2 ANOS - TOKEN FISICO, SERIALNUMBER=1614439, OID.1.3.6.1.4.1.23267.2.3=8907001484, OID.1.3.6.1.4.1.23267.2.2=52082808, OID.1.3.6.1.4.1.23267.2.1=154, O=CAJA DE COMPENSACION FAMILIAR DE FENALCO DEL TOLIMA COMFENALCO, L=IBAGUE, G=DIANA, E=DIANA.KANDIA@COMFENALCO.COM.CO, C=CO, CN=DIANA MAGALLY KANDIA TRONCOSO
Razón: Soy el autor de este documento
Ubicación: 8754
Fecha: 2023.10.19 17:13:09-05'00'
Foxit PDF Reader Versión: 12.1.2

DIANA MAGALLY KANDIA TRONCOSO
Directora Administrativa Suplente

Edna Oviedo Ruiz

Vb. Edna Mayerly Oviedo-Jefe Unidad de Auditoria Interna