

Consultas Realizadas

Licitación 305787 - Servicio de Asistencia Técnica para virtualización de servidores, test de seguridad y antiphishing

Consulta 1 - En el Pliego de Bases y Condiciones

Consulta	Fecha de Consulta	11-04-2017
<p>En el Pliego de Bases y Condiciones, SECCIÓN II, CRITERIOS DE EVALUACIÓN Y REQUISITOS DE CALIFICACIÓN, EXPERIENCIA Y CAPACIDAD TÉCNICA, Ítem N° 2 Servicio de Test de Seguridad de Hackeo Interno y Externo, PERFILES PROFESIONALES, dice:</p> <p>EL OFERENTE deberá presentar el listado mínimo de 4 (cuatro) personas, de un equipo de profesionales altamente calificados, que podrán disponer entre otros de los siguientes perfiles:</p> <p>Audidores Especialistas Funcionales: Llevará a cabo las actividades de consultoría relacionadas con toda evaluación funcional y/o de compliance.</p> <p>Audidores Especialistas en Técnicas de Hacking / Seguridad Telemática: Se encargarán de las actividades de Intrusión y los análisis técnicos derivados del proyecto a realizar.</p> <p>Arquitecto de Red: Llevará a cabo las actividades de consultoría de resultados obtenidos y aportará las medidas correctoras de rediseño de red de acuerdo a los resultados obtenidos, si este aspecto fuera contratado en el Proyecto.</p> <p>Jefe de Proyecto: Realizará las actividades de coordinación de recursos e interlocución con el BNF.</p> <p>Responsable de alto nivel: Realizará la interlocución de alto nivel con el BNF, en los casos en que esta fuera necesaria.</p> <p>Documentalista: Llevará a cabo todas las labores de documentación del Proyecto.</p> <p>Solicitamos respetuosamente a la convocante que pueda ser aceptada la subcontratación de empresas o profesionales técnicos especialistas en este ámbito de servicios para así permitir una mayor participación de potenciales oferentes en beneficio de la convocante, conforme a lo que preceptua el artículo 4 inc b) de la Ley de Contrataciones 2051/03. PRINCIPIO DE IGUALDAD Y LIBRE COMPETENCIA que deben regir las compras públicas inc. b del Art. 4 de la Ley N° 2051 DE CONTRATACIONES PÚBLICAS -. Dicha solicitud, se realiza asimismo en virtud del Art. 20, a razón de que el mismo establece que: Las especificaciones técnicas () se establecerán con la mayor amplitud de acuerdo con la naturaleza específica del contrato, con el objeto de que concurra el mayor número de oferentes; sin embargo, deberán ser lo suficientemente claras, objetivas e imparciales, para evitar favorecer indebidamente a algún participante.</p>		

Respuesta	Fecha de Respuesta	18-05-2017
<p>Será aceptada la subcontratación de empresas consultoras especializadas en el área de Seguridad Informática, No se podrá realizar ningún tipo de subcontratación de hackers ni personal freelance para ningún trabajo, en virtud de lo determinado por la pauta de compromiso ético sino que todos los profesionales de seguridad implicados en el proyecto deben ser empleados de tiempo completo de la firma subcontratada y avalados por ésta luego de una rigurosa averiguación de antecedentes para asegurar que tengan una historia ética, personal y profesional adecuada, por lo tanto el Equipo del OFERENTE deberá reunir un conjunto adecuado de certificaciones internacionales directamente relacionadas con el área de Seguridad de la Información</p> <p>Certified Ethical Hacker (CEH) - Certified Information Systems Security Professional (CISSP) Certified Information Security Manager (CISSM) Certified Secure Software Lifecycle Professional (CSSLP) Certificate of Cloud Security Knowledge (CCSK) ISO Leader Auditor.</p> <p>También deberá tener aprobada experiencia en el ámbito internacional, respecto de la provisión de servicios de Ethical Hacking.</p> <p>Es de suma importancia y será excluyente que los implementadores posean el nivel técnico solicitado pues el análisis de la seguridad será de gran magnitud debido a la infraestructura que posee el Banco Nacional de Fomento.</p> <p>Por lo expuesto precedentemente, remitirse a la Adenda N° 3.</p>		

Consulta 2 - En el Pliego de Bases y Condiciones

Consulta	Fecha de Consulta	11-04-2017
<p>En el Pliego de Bases y Condiciones, SECCIÓN II, CRITERIOS DE EVALUACIÓN Y REQUISITOS DE CALIFICACIÓN, EXPERIENCIA Y CAPACIDAD TÉCNICA, Ítem N° 2 Servicio de Test de Seguridad de Hackeo Interno y Externo, dice:</p> <p>Presentar copias de Contratos o facturas donde el oferente demuestre haber proveído servicios de Seguridad de TI para Servicio de Test de Seguridad Hackeo, a empresas públicas y/o privadas en los últimos 3 (tres) años, como mínimo 1 (un) Contrato por año (Años: 2013, 2014 y 2015).</p> <p>Solicitamos respetuosamente a la convocante que puedan ser aceptados Contratos o facturas de la empresa subcontratada o de profesionales técnicos especialistas en este ámbito de servicio en donde demuestren la capacidad y experiencia técnica requerida en este Pliego de Bases y Condiciones y de esta forma se pueda permitir la mayor participación de potenciales oferentes en beneficio de la convocante., conforme lo preceptua el Artículo 4 inc b) de la Ley de Contrataciones Públicas: al PRINCIPIO DE IGUALDAD Y LIBRE COMPETENCIA que deben regir las compras públicas inc. b del Art. 4 de la Ley N° 2051 DE CONTRATACIONES PÚBLICAS -. Dicha solicitud, se realiza asimismo en virtud del Art. 20, a razón de que el mismo establece que: Las especificaciones técnicas () se establecerán con la mayor amplitud de acuerdo con la naturaleza específica del contrato, con el objeto de que concurra el mayor número de oferentes; sin embargo, deberán ser lo suficientemente claras, objetivas e imparciales, para evitar favorecer indebidamente a algún participante.</p>		

Respuesta	Fecha de Respuesta	18-05-2017
<p>Serán aceptados Contratos o facturas de las empresas consultoras especializadas en el área de Seguridad subcontratada, para que de esta forma se pueda permitir la mayor participación de potenciales oferentes en beneficio de la convocante. Por lo tanto remitirse a la Adenda N° 3.</p>		

Consulta 3 - En la sección 3 "REQUISITOS DE LOS BIENES Y/O SERVICIOS REQUERIDOS" ítem 3

Consulta	Fecha de Consulta	17-04-2017
<p>En la sección 3 "REQUISITOS DE LOS BIENES Y/O SERVICIOS REQUERIDOS" ítem 3 dice "Disponer de monitoreo proactivo de vigilancia digital que incluya (Monitoreo de marca, fuga de información, antiphishing, entro otros) ¿Que significa específicamente el punto de fuga de información? ¿Que se requiere?"</p>		

Respuesta	Fecha de Respuesta	18-05-2017
<p>Se refiere al monitoreo online de la información confidencial del BNF en el ciber espacio. Se requiere que este monitoreo cumpla con los servicios detallados en el pliego.</p>		

Consulta 4 - En la sección 3 "REQUISITOS DE LOS BIENES Y/O SERVICIOS REQUERIDOS"

Consulta	Fecha de Consulta	17-04-2017
<p>Seccion 3:"Poder Realizar Spoofing WEB." ¿Es posible enviar mayor detalle de lo que se requiere en este punto?</p>		

Respuesta	Fecha de Respuesta	18-05-2017
<p>El servicio debe poder rastrear sitios fraudulentos sobre dominios del Banco.</p>		

Consulta 5 - seccion 3: "La solución de monitoreo

Consulta	Fecha de Consulta	17-04-2017
----------	-------------------	------------

Seccion 3 punto 5: "La solución de monitoreo debe detectar y alertar en tiempo real correos electrónicos de dudoso origen." ¿Es posible enviar mayor detalle de lo que se requiere en este punto?

Respuesta	Fecha de Respuesta	18-05-2017
-----------	--------------------	------------

El servicio debe tener la capacidad de obtener la reputación de los correos entrantes para determinar su tratado.

Consulta 6 - seccion 3 item 4: El servicio monitoreo de Phishing

Consulta	Fecha de Consulta	17-04-2017
----------	-------------------	------------

"El servicio monitoreo de Phishing para el Banco Nacional de Fomento deberá incluir a los dominios del BNF publicados." ¿Cuántos dominios son? ¿Cuales?

Respuesta	Fecha de Respuesta	18-05-2017
-----------	--------------------	------------

El BNF cuenta con un dominio, el www.bnf.gov.py.

Consulta 7 - Seccion 3 : patrones de comportamientos

Consulta	Fecha de Consulta	17-04-2017
----------	-------------------	------------

Se requiere la posibilidad de identificar patrones y comportamientos específicos que ocurren típicamente en las primeras etapas de un ataque de phishing ¿Es posible especificar más este requerimiento?

Respuesta	Fecha de Respuesta	18-05-2017
-----------	--------------------	------------

Se refiere a datos relevantes que pudieren ser utilizados para actuar con proactividad en caso que ocurra un ataque de phishing.

Consulta 8 - ÍTEM 3:) Detección de mediciones en el Ciberespacio que comprometan la marca

Consulta	Fecha de Consulta	17-04-2017
----------	-------------------	------------

Detección de mediciones en el Ciberespacio que comprometan la marca del Banco Nacional de Fomento o comprometa su información ¿Es posible especificar más este requerimiento?

Respuesta	Fecha de Respuesta	18-05-2017
-----------	--------------------	------------

Se requiere que, mediante el uso de palabras clave, se encuentre información valiosa expuesta en redes sociales e Internet que sea indicio de su uso fraudulento.

Consulta 9 - ITEM 3: La solución debe de identificar y desactivar el uso no autorizado de materia

Consulta	Fecha de Consulta	17-04-2017
----------	-------------------	------------

La solución debe de identificar y desactivar el uso no autorizado de material con contenido protegido por leyes de propiedad intelectual ¿Es posible acotar más este punto?

Respuesta	Fecha de Respuesta	18-05-2017
-----------	--------------------	------------

En caso de detectar información considerada confidencial por parte del banco y publicada en el ciberespacio, el proveedor debe gestionar la baja de los mismos.

Consulta 10 - ITEM 3: La solución debe de identificar y desactivar el uso no autorizado

Consulta	Fecha de Consulta	17-04-2017
La solución debe de identificar y desactivar el uso no autorizado de material con contenido protegido por leyes de propiedad intelectual ¿Es posible acotar más este punto?		

Respuesta	Fecha de Respuesta	18-05-2017
En caso de detectar información considerada confidencial por parte del banco y publicada en el ciberespacio, el proveedor debe gestionar la baja de los mismos.		

Consulta 11 - ITEM 3: La solución debe de identificar y desactivar el uso no autorizado

Consulta	Fecha de Consulta	17-04-2017
La solución debe de identificar y desactivar el uso no autorizado de material con contenido protegido por leyes de propiedad intelectual ¿Es posible acotar más este punto?		

Respuesta	Fecha de Respuesta	18-05-2017
En caso de detectar información considerada confidencial por parte del banco y publicada en el ciberespacio, el proveedor debe gestionar la baja de los mismos		

Consulta 12 - Sección 3 "REQUISITOS DE LOS BIENES Y/O SERVICIOS REQUERIDOS"

Consulta	Fecha de Consulta	17-04-2017
En la sección 3 "REQUISITOS DE LOS BIENES Y/O SERVICIOS REQUERIDOS" - La solución debe de identificar y desactivar el uso no autorizado de material con contenido protegido por leyes de propiedad intelectual ¿Es posible acotar más este punto?		

Respuesta	Fecha de Respuesta	18-05-2017
En caso de detectar información considerada confidencial por parte del banco y publicada en el ciberespacio, el proveedor debe gestionar la baja de los mismos.		