Port de Barcelona

RESPUESTAS A LAS CONSULTAS EFECTUADAS A LA LICITACIÓN:

"SERVICIO DE LA OFICINA TÉCNICA DE SEGURIDAD TIC DE LA AUTORIDAD PORTUARIA DE BARCELONA". Clave de expediente: 2015R320054. Ref. Servicio de Contratación: 151/15

CONSULTA:

S'ha registrat l'assentament Q0867012G-1-2015-025654-2
Assumpte: Exp.151/2015

ASSUMPTE: Dins del quadre-resum de característiques a l'apartat E- Requisits per a licitar, dins del punt 1 c) s'indica que s'han tingut que realitzar en els últims 3 anys, un mínim de 3 projectes i/o serveis en les tecnologies incloses en el concurs, sumant els (3) un import de 100.000 i a l'apartat G- Contingut de les ofertes a l'apartat c) diu que s'ha d'acreditar mitjançant certificats emesos per clients, un mínim de 3 projectes amb un imports superior a 75.000 realitzats en els últims 3 anys. Com existeix una contradicció perquè en el apartat E és la suma de 3 o més projectes han de ser 100.000€ i en canvi al apartat G han de ser cadascun superior a 75.000€, entendem que la petició valida es la de l'apartat E. Us prego si us plau confirmació d'aquest punt. Gràcies per avançat. Qualsevol cosa estic a la vostra disposició. Salutacions cordials.

RESPUESTA:

L'import correcte que s'ha d'acreditar és un mínim de 3 projectes i/o serveis en les tecnologies incloses en el concurs, sumant els (3) un import de 100.000 €, en els últims 3 anys.

CONSULTA:

S'ha registrat l'assentament Q0867012G-1-2015-025957-1
Procedència: Telefonica soluciones de informatica y Comunicaciones de España, S.A.
Assumpte: Exp.151/2015

A continuación planteamos las siguientes consultas:
1.- Necesitaríamos conocer información sobre la planta de seguridad que desean monitorizar, es decir qué tipo de elementos (FW, IPS, etc...) y el número de los mismos (fuentes) para poder dimensionar correctamente el SIEM (herramienta de monitorización). En el apartado 2.7 (Disaster Recovery Plan) de la pag.9 del Pliego de prescripciones ´técnicas hay un listado de arquitectura, sería confirmar que esos son los tipos de elementos a monitorizar y necesitamos saber el nº de cada uno de ellos.

2.- Periodo de retención de logs.

3.- Necesitaríamos conocer la volumetría actual de incidencias para poder dimensionar correctamente el servicio de gestión de incidencias de seguridad.

4.- Respecto al servicio de monitorización, también se indica en el pliego un apartado de detección, análisis y gestión de vulnerabilidades. Necesitaríamos confirmación de que realmente se desea dicha gestión de vulnerabilidades. En caso afirmativo necesitaríamos conocer la siguiente información:

a) Qué tipo de auditoría necesitaría: Caja negra (ejecución de intentos de intrusión orientados a la detección de vulnerabilidades sin conocimiento previo de los detalles de la infraestructura tecnológica del cliente. Se realiza desde internet) o Caja blanca (ejecución de intentos de intrusión orientados a la detección de vulnerabilidades con conocimiento previo de los detalles de la infraestructura tecnológica auditada del cliente, bien porque se realiza desde la red interna, porque se facilitan ficheros de configuración, tablas de rutas, reglas de firewall, documentación sobre la arquitectura, cuentas de usuario de pruebas o cualquier otro dato del que no dispondría, a priori, un usuario malicioso)?

b) ¿Las auditorías podrían realizarse en horario laboral o fuera del horario laboral?

c) ¿Se requiere desplazamiento o se puede realizar en remoto?

d) Cuantas IPs están en el alcance? Son públicas o privadas?

e) Detalle del Entorno a auditar: aplicaciones web, sistemas/servidores, servicios, dominios. Si existe WIFI cuantos SSID deben auditarse.

5.- Equipo presencial. No nos queda del todo claro el número de consultores necesarios ya que solicitan un perfil muy extenso (Seguridad, software, seguridad Tic del código, bastionado de sistemas...) ¿Un Service Manager y un Consultor Senior sería suficiente?.

RESPUESTA.-

1- La planta de seguridad actual consta de:

- 2 UTM de seguridad físicos que virtualizan 3 FW/IPS.
- 2 balanceadores que virtualizan dos parejas de balanceadores uno para tráfico interno de servidores y otro externo.
- 2 routers para la conexión a proveedores de internet.
- 2 equipos para el Servicio DNS
- Unos 150 equipos de red distribuidos por todo el territorio.
- 3 routers/FW adicionales para conexión a redes especiales de territorio que requieren más seguridad.
- Unos 200 servidores virtuales de los que un 10 % se consideran expuestos a ataques de seguridad.

Independientemente de la plataforma actual y dada la duración máxima que puede tener este contrato se ha de tener en cuenta que es un escenario cambiante y el proveedor deberá adaptarse a los cambios que ocurran en los sistemas a lo largo del mismo.

El apartado 2.7 del pliego de condiciones lista las diferentes infraestructuras básicas de que dispone la APB actualmente pero no da el volumen de las mismas y no se puede garantizar que estas no cambien a lo largo del contrato.

2 - No está definido el periodo de retención de logs que se desea mantener. El proveedor deberá hacer su propuesta en función del equipamiento existente y las buenas prácticas en seguridad.

3 - No existe actualmente un registro específico de incidentes de seguridad y la detección de las mismas se hace de forma manual. A lo largo del 2015 ha habido tres incidentes que se han clasificado cómo de seguridad. Sin embargo se estima que una vez se pongan sistemas automáticos de detección de eventos este número puede llegar a multiplicarse varias veces.

a) Para la gestión de vulnerabilidades lo que se necesita es que el proveedor nos informe cuando aparezca una nueva vulnerabilidad que afecte a alguno de nuestros servicios monitorizados. Será decisión del proveedor cómo se realiza la detección de esas vulnerabilidades (con auditorias automáticas externas, gestión de versiones de software, etc.). En la oferta se deberá explicar la metodología utilizada para esta detección.
b) La realización de las auditorias podrá realizarse dentro del horario habitual cuando se considere que estas tienen un riesgo bajo de afectación al servicio. No debe descartarse de que en caso de que se realicen pruebas de alto riesgo estas deban realizarse en horarios de bajo impacto para el negocio.
c) Las auditorias pueden realizarse en remoto siempre que sea posible y no se comprometa ni la seguridad ni la disponibilidad de los sistemas.
d) L'APB dispone actualmente de direccionamiento privado interno, y dos proveedores de conexión a Internet que proporcionan 256 IPs públicas uno y 64 IPs el segundo. Está la situación actual pero la misma puede cambiar en las renegociaciones de los contratos con los distintos operadores. El servicio debe ser lo suficientemente flexible para poder adaptarse a ello.
e) El entorno a auditar es complejo y cambiante. El proveedor deberá adaptarse al mismo a lo largo del contrato. Actualmente existen como servicios externos dos grupos principales de servicios web con múltiples URLs en entornos de producción y preproducción, un servicio de escritorios virtuales, correo web, correo SNMP, servicio de VPNs SSL.

5 – El equipo presencial.

- El perfil de Service Manager como responsable global del servicio, con conocimiento y experiencia como consultor de seguridad, y que deberá de asumir el rol de jefe de proyectos para poner en marcha la OTS, ha de trabajar de manera presencial en las dependencias de la APB, de forma continua y con una dedicación parcial estimada de 5 h a la semana.
- Para otros perfiles especialistas en diferentes áreas de seguridad, se estima que puedan dedicar una media de 8 horas semanales de forma presencial en la APB, pero no se considera una dedicación continuada, tampoco todos ellos de forma solapada, se tratará de colaboraciones puntuales en función de los proyectos o líneas de trabajo que se vayan definiendo en cada momento en la OTS por el Service Manager.

CONSULTA:

S'ha registrat l'assentament Q0867012G-1-2015-025658-2

Assumpte: l'expedient 151/2015 2 de 2realitzats en els últims 3 anys. Com existeix una contradicció perquè en el apartat E és la suma de 3 o més projectes han de ser 100.000 i en canvi al apartat G han de ser cadascun superior a 75.000 , entendem que la petició valida es la de l'apartat E. Us prego si us plau confirmació d'aquest punt. Gràcies per avançat. Qualsevol cosa estic a la vostra disposició. Salutacions cordials.

RESPOSTA:

L'import correcte que s'ha d'acreditar és un mínim de 3 projectes i/o serveis en les tecnologies incloses en el concurs, sumant els (3) un import de 100.000 €, en els últims 3 anys.

CONSULTA:

S'ha registrat l'assentament Q0867012G-1-2015-025968-2

Port de Barcelona

Assumpte:- Número i tipologia de sistemes a monitoritzar Comentaris . En el punt 2. Situació actual s'inclouen esquemes de les infraestructures de l'APB. Per dimensionar i valorar el servei agrairíem les volumetries associades al mateix. Per exemple, elements de seguretat 5, servidors crítics 10, etc.

RESPOSTA:

La planta de seguridad actual consta de:

- 2 UTM de seguridad físicos que virtualizan 3 FW/IPS.
- 2 balanceadores que virtualizan dos parejas de balanceadores uno para tráfico interno de servidores y otro externo.
- 2 routers para la conexión a proveedores de internet.
- 2 equipos para el Servicio DNS
- Unos 150 equipos de red distribuidos por todo el territorio.
- 3 routers/FW adicionales para conexión a redes especiales de territorio que requieren más seguridad.
- Unos 200 servidores virtuales de los que un 10 % se consideran expuestos a ataques de seguridad.

Independientemente de la plataforma actual y dada la duración máxima que puede tener este contrato se ha de tener en cuenta que es un escenario cambiante y el proveedor deberá adaptarse a los cambios que ocurran en los sistemas a lo largo del mismo.

CONSULTA:

S'ha registrat l'assentament Q0867012G-1-2015-025969-2

Assumpte.- Solució SIEM SaaS Comentaris .- Al plec s'inclou tant el projecte d'implementació de la solució SIEM, com la seva posterior operació a partir de l'any 2. Agrairíem aclarir com s'ha de tractar el cost de provisió del SIEM (que inclouria el maquinari, programari, així com el manteniment i suport associat)

RESPOSTA:

El SIEM constarà de tres parts en quant a cost:

1- Definició de la solució o projecte SIEM. Aquesta part anirà a la borsa d'hores com tasca a realitzar per la OTS.
2- Servei d'operació del SIEM, a partir del moment que el SIEM estigui operatiu, esta inclòs a la part fixe del servei que es facturarà periòdicament.
3- Provisió, desplegament, i/o implantació del SIEM. Tant si es proposa una solució de compra o una solució Saas (o similiar al cloud), el cost no forma part d'aquest contracte tot i que pel punt 1 si es col·laborarà en la definició e implantació del projecte.

CONSULTA:

S'ha registrat l'assentament Q0867012G-1-2015-025971-

Port de Barcelona

Apartat.- 4.3.3. Planificació de Peticions Pàgina(es) 18-19Consulta ANS corresponents a les peticions Comentaris L'apartat conté 2 taules d'ANS que entenem solapen alguns indicadors, sent la primera variable segons prioritat, mentre la segona no. Agrairíem si podem veure si hi ha possible error i en cas que no aclariment.

RESPOSTA:

Es considera que al llarg del servei hi haurà dos grups de peticions de canvis e intervencions: les que tindran per les seves característiques una prioritat associada i peticions que no en tindran. Cada taula fa referència un d'aquests grups de peticions i s'aplicarà en conseqüència.

CONSULTA:

S'ha registrat l'assentament Q0867012G-1-2015-025972-2

Apartat.- 4.4.1. Horari i lloc de treball Pàgina(es) 20-21Consulta .- Horari de servei de l'equip presencial.- Comentaris : Al primer paràgraf s'especifica de 9 a 18 hores, posteriorment hi ha una nota on especifica entre les 08:00h i les 18:00h. Agrairíem aclariment.

RESPOSTA:

L'horari de servei de l'equip presencial serà d'una jornada de 8 hores que s'haurà de realitzar dintre del horari d'oficines que és des de 8:00 a 18 hores.

CONSULTA:

S'ha registrat l'assentament Q0867012G-1-2015-025974-2

Assumpte: Nombre de reunions de Gestió de servei establertes en el model de relació no realitzades per motius atribuïbles a l'adjudicatari Comentaris. Trobem que l'indicador està duplicatt

RESPOSTA:

L'indicador no està duplicat. El primer indicador fa referència a la reunions convocades y no realitzades. El segon indicador fa referència a reunions no realitzades de les previstes en el model de relació. El segon indicador implica que hi haurà penalització si no es poden convocar les reunions previstes al model de relació per causes atribuïbles al proveïdor.

SERVICIO DE CONTRATACIÓN.

Barcelona, a 4 de novembre del 2015

Port de Barcelona
Secretaria General
Contractació