XXX

UNIÓN EUROPEA

RESPUESTAS A CUESTIONES PLANTEADAS SOBRE DETERMINADOS ASPECTOS DE LOS PLIEGOS. EXPEDIENTE "Acuerdo marco de servicios de Auditorías de Certificación, de Auditorías Técnicas, y de Formación y Concienciación en el ámbito de la ciberseguridad" (CONTR 2023 0000934533)

Pregunta 1: No encontramos la memoria económica, y en la memoria justificativa cuando se exponen los datos en los que se basa el cálculo del importe de cada servicio solo se incluyen en actividades constitutivas horas de personal, en ningún caso medios materiales como alquiler de instalaciones o entrega de materiales al alumnado obligatorios en PPT. ¿Han publicado otra memoria económica?
Respuesta: Se ha realizado el cálculo en base a horas de perfiles asociados a los de la Instrucción 1/2023, de 4 de mayo, de la Agencia Digital de Andalucía sobre perfiles, precios de referencia y desglose de costes en contratos de bienes y servicios TIC. Se ha considerado que el material y las instalaciones están incluidas, si bien es cierto que la gran mayoría de las actividades presenciales se realizarán en instalaciones de la propia Junta de Andalucía.

Pregunta 2: La facturación o forma de pago prevista es ¿mensual, al final del servicio, dependerá del contrato?
Respuesta: Al tratarse de un acuerdo marco, cada contrato basado posterior indicará la forma de pago del precio. Así se indica en el PCAP, apartado 4.9.3 (Pago del precio):

> La persona adjudicataria tiene derecho al abono del precio convenido, con arreglo a las condiciones establecidas en el contrato, correspondiente a los trabajos efectivamente realizados y formalmente recibidos por la Administración.
> La forma de pago vendrá determinada en el Documento de licitación y, en su caso, en la correspondiente invitación a licitación.

Pregunta 3: Las acciones formativas presenciales no llevan asociadas pólizas de seguro independientes, entendemos que, porque las consideran cubiertas con el seguro de RC de la actividad de la empresa, ¿correcto?
Respuesta: Así lo entendemos. En todo caso, se especificarán requisitos en cada contrato basado.

Pregunta 4: En el apartado 3.2.2.4. A4: Revisión técnica de aplicaciones mediante análisis dinámico, del Pliego de Prescripciones Técnicas se indica:

> **"Con los sistemas en ejecución, el adjudicatario analizará el entorno en busca de posibles vulnerabilidades de seguridad. Deberán llevarse a cabo pruebas de "caja negra" y de "caja blanca"."**

Entendemos que este tipo de pruebas se hacen con las herramientas indicadas en el párrafo siguiente del PPT:

> **"(BoundsChecker, Cenzic, ClearSQL, Dmalloc, Gcov, IBM Rational AppScan, Intel Thread Checker, Parasoft Insure++, Valgrind, etc.)"**

Sin embargo cuando describen las actividades de Caja Negra y Caja Blanca hacen referencia a actividades de Pentesting de Aplicaciones Web o (Web Penetration Testing) como definen otros fabricantes y otras soluciones.
¿Qué tipo de actividades requieren realmente en el apartado 3.2.2.4: Revisión de aplicaciones mediante análisis dinámico o Pentesting de Aplicaciones Web?
Respuesta: En el apartado "actividades a desarrollar" de cada lote se han descrito un conjunto de actividades frecuentes y posibles, con mayor o menor detalle, pero las actividades que se soliciten en los contratos basados serán las que concreten las actuaciones. Sobre este ejemplo en concreto, se ha tratado de definir las actividades de revisión de aplicaciones en ejecución, en contraposición con el análisis estático de código reflejado en el apartado siguiente (3.2.2.5). Eso incluye tanto actividades de pentesting como uso de herramientas.

Pregunta 5: En el anexo III del pliego administrativo, se indica que se tiene que descargar el fichero xml desde el perfil del contratante pero, salvo error por nuestra parte, no hemos visto este documento. ¿Se va publicar este archivo o serviría con utilizar directamente el publicado en la web oficial?
Respuesta: Se ha publicado en el perfil de contratante el XML para el Documento Europeo Único de Contratación (DEUC).

Pregunta 6: En cuanto a los contratos basados que superen los 50.000 euros, ¿se establecerán nuevos criterios o seguirán las mismas pautas que en el acuerdo marco? En este último caso, ¿se decidirá el ganador en función de la puntuación más alta en el acuerdo marco?
Respuesta: Los criterios de adjudicación de los contratos basados serán independientes para cada contrato, y se tomarán de entre los indicados en el anexo XIX del PCAP. Entre ellos no se incluye la puntuación obtenida en los criterios de adjudicación del Acuerdo Marco (aquellos del anexo VIII).
Esta puntuación, sin embargo, sí se utilizará en la selección de empresas a invitar (caso de contratos basados con segunda licitación) o a adjudicar (caso de contratos de adjudicacón directa).

NOTA:
Reflejamos a continuación un conjunto de preguntas realizadas sobre los servicios del lote 2 (auditorías técnicas de seguridad), aclarando que la respuesta a la mayoría de ellas es en el siguiente sentido:

Al tratarse de un acuerdo marco, se han especificado como "actividades a desarrollar" para cada lote un conjunto de actividades frecuentes y posibles, con mayor o menor detalle. Los contratos basados que se realicen al amparo de este acuerdo marco concretarán las actividades a desarrollar, que podrán ser las especificadas en el PPT u otras que estén en el ámbito del lote (el Objeto del servicio). También especificarán los contratos basados el alcance de las actividades en cuanto a sedes, sistemas, infraestructuras, tecnologías, duración...

Pregunta: LOTE 2 A1: AUDITORÍAS TÉCNICAS SOBRE INFRAESTRUCTURA En el punto 3.2.2.1. A1 (pag. 12 del pliego técnico) se indica que se plantea la revisión técnica de seguridad de una infraestructura o entorno en modalidad de caja negra o gris. No obstante, en el tercer párrafo de dicho punto se indica lo siguiente: "El equipo auditor no dispondrá de información sobre los objetivos, simulando así el comportamiento que pueda tener cualquier usuario externo malintencionado". Este enfoque corresponde sólo con caja negra. Por tanto, ¿las pruebas a plantear en este escenario deben ser todas en caja negra o se desea considerar alguna en caja gris? En caso de que se quiera alguna prueba en caja gris, ¿qué asunciones y/o información para cada uno de los 3 planos (interconexión sedes, publicación y bastionado) se deberán tener en cuenta para el alcance de las pruebas?
Respuesta: Las descripciones de actividades a desarrollar indicadas en el PPT corresponden a las actividades más frecuentes, y no son exhaustivas, pudiéndose realizar contratos con otras actividades, siempre dentro del objeto del servicio. Cada contrato basado explicitará las características específicas de las actividades, y en concreto para auditorías de caja gris, indicará qué información se pondrá a disposición de la empresa.

Pregunta: LOTE 2 A1: AUDITORÍAS TÉCNICAS SOBRE INFRAESTRUCTURA ¿Cuántas sedes se deben considerar dentro del alcance de las pruebas de infraestructura en el plano de interconexión?
Respuesta: Cada contrato basado en el acuerdo marco indicará la sede o sedes en que se deban desarrollar las actuaciones. La Junta de Andalucía cuenta con varios miles de sedes de datos, aunque las actuaciones de auditoría técnica podrán ser realizadas en sedes muy concretas, en número menor.

Pregunta: LOTE 2 A1: AUDITORÍAS TÉCNICAS SOBRE INFRAESTRUCTURA ¿El servicio VPN es el mismo para todas las sedes o hay servicios diferentes que se deban considerar dentro del alcance? En caso de que haya varios, ¿cuántos serían?
Respuesta: El servicio VPN, en principio, es el proporcionado por la Red Corporativa de Telecomunicaciones de la Junta de Andalucía (RCJA en adelante). Sin embargo, cada contrato basado especificará el ámbito de las actuaciones, que podría abarcar otros servicios VPN existentes.

Pregunta: LOTE 2 A1: AUDITORÍAS TÉCNICAS SOBRE INFRAESTRUCTURA A fin de poder dimensionar el esfuerzo necesario para las pruebas de pentesting de infraestructura ¿Cuántas aplicaciones, servicios, sistemas y rangos de IPs y de qué tipo se deben considerar dentro del alcance de estas pruebas?

Respuesta: Cada contrato basado especificará el ámbito de las actuaciones. Como orientación muy general, el número de aplicaciones en uso en la Junta de Andalucía está en el orden de varios centenares, el número de equipos en el orden de los cien mil, y los rangos de IP principales incluyen subredes /20.

Pregunta: LOTE 2 A1: AUDITORÍAS TÉCNICAS SOBRE INFRAESTRUCTURA ¿Qué tipo de servicios o sistemas estarán dentro del alcance de las pruebas solicitadas en el plano de publicación? ¿qué se entiende como publicación?
Respuesta: Nos referimos a los servicios (aplicaciones web, principalmente) publicados hacia el exterior de la RCJA. Hay una gran variedad de tecnologías implicadas, dada la cantidad de servicios expuestos. Cada contrato basado especificará el ámbito de las actuaciones.

Pregunta: LOTE 2 A1: AUDITORÍAS TÉCNICAS SOBRE INFRAESTRUCTURA Para el escenario de " Suplantación de credenciales con el objetivo de intentar modificar publicaciones.", ¿se proporcionarán dichas credenciales y se partirá de un enfoque de brecha asumida o se busca que las credenciales sean extraídas por el proveedor mediante técnicas de phishing y/o fuerza bruta durante el ejercicio de pentesting?; ¿cuántos servicios se deberán contemplar en el alcance de estas pruebas?
Respuesta: Cada contrato basado especificará el ámbito de las actuaciones.

Pregunta: LOTE 2 A1: AUDITORÍAS TÉCNICAS SOBRE INFRAESTRUCTURA Para el escenario de "ataques de denegación de servicio", ¿contra qué sistemas o aplicaciones se deberán realizar?, ¿se espera que los servicios/aplicaciones objetivo esténd alojados en un proveedor cloud, on-premise, otros? ¿se dispone de sistemas de prevención/antiDOS activos que protejan la infraestructura contra este tipo de ataques? ¿en qué ventana horaria se deberán realizar?
Respuesta: Contra los sistemas publicados. Mayoritariamente on-premise, pero podrían solicitarse actividades ante sistemas en nube. RCJA dispone de protección anti DDoS. La ventana horaria y demás parámetros se especificarían en los contratos basados o, más probablemente, al inicio de la ejecución de las pruebas.

Pregunta: LOTE 2 A1: AUDITORÍAS TÉCNICAS SOBRE INFRAESTRUCTURA Para las pruebas en el plano de bastionado: ¿qué capas y sistemas se deberán considerar?, ¿se considera como parte del alcance la realización de una línea base de seguridad basada en algún estandar (p.e. benchmarks del CIS) o el enfoque deseado es más de pruebas de pentest manuales?
Respuesta: Ambas actividades son posibles, y se concretarán en los contratos basados.

Pregunta: LOTE 2 A1: AUDITORÍAS TÉCNICAS SOBRE INFRAESTRUCTURA Tenemos dudas sobre el enfoque a considerar en las pruebas de pentest sobre el plano de bastionado de la infraestructura (apartado 3.2.2.1. A1; págs 12-13) y el apartado específico de bastionado (apartado 3.2.2.6. A6: "Revisión de bastionado y verificación de la correcta aplicación de procedimientos de instalación y empleo seguro de sistemas"; págs. 18-19) En concreto, en el apartado de "Análisis de bastionado a nivel de sistemas". ¿Podrían aclararnos las diferencias de alcance que se buscan en cada caso, por favor?
Respuesta: En las auditorías de infraestructura (A1) pueden incluirse análisis de la fortaleza de los sistemas desde el exterior, en tanto que en las revisiones de bastionado (A6) se considera más una visión desde el interior del sistema, y con una línea base como referencia.

Pregunta: LOTE 2 A3: AUDITORÍAS TÉCNICAS SOBRE RED WIFI ¿Cuántas redes Wi-Fi y de qué tipo se deberán considerar dentro del alcance?, ¿sobre qué sedes se deberá realizar y cuántos SSIDs y APs tiene cada una?
Respuesta: Cada contrato basado indicará el alcance.

Pregunta: LOTE 2 A4: AUDITORÍAS TÉCNICAS DE APLICACIONES - ANÁLISIS DINÁMICO ¿Cuántas aplicaciones y qué tamaño (nº de pantallas, nº de fomrularios, nº de endpoints) tienen las aplicaciones a contemplar dentro del alcance de la auditoría?, ¿cuántas están públicas en Internet y cuántas son internas?
Respuesta: No se dispone de esa información. Cada contrato basado indicará el alcance.

Pregunta: LOTE 2 A4: AUDITORÍAS TÉCNICAS DE APLICACIONES - ANÁLISIS DINÁMICO Para poder evaluar "la protección e integridad de los logs, prioritariamente los relativos a accesos (aplicaciones y tablas) y su grado de exposición al riesgo" que se indica en la página 16 del pliego técnico, ¿se dará acceso al proveedor a los sistemas que los alojan para revisar la configuración de los mismos o qué enfoque se quiere dar a estas pruebas?
Respuesta: Se dará acceso.

Pregunta: LOTE 2 A4: AUDITORÍAS TÉCNICAS DE APLICACIONES - ANÁLISIS DINÁMICO Para las pruebas en caja blanca de las aplicaciones, ¿cuántos roles diferentes habrá que considerar en el alcance de cada aplicación?, ¿qué tamaño tienen las aplicaciones a revisar 8(nº de pantallas, nº de fomrularios, …)?
Respuesta: No se dispone de esa información. Cada contrato basado indicará el alcance.

Pregunta: LOTE 2 A5: AUDITORÍAS TÉCNICAS DE APLICACIONES - ANÁLISIS ESTÁTICO ¿Cuántas aplicaciones se consideran dentro del alcance y en qué tecnologías están desarrolladas?, ¿qué volumen de líneas de código tiene cada una de ellas?
Respuesta: No se dispone de esa información. Cada contrato basado indicará el alcance.

Pregunta: LOTE 2 A6: REVISIÓN DE BASTIONADO Dentro de las pruebas para el apartado 3.2.2.6. A6 del pliego (Análisis de bastionado a nivel de sistemas): ¿qué tipo de sistemas (tecnologías, versiones, servidores, moviles, equipos de escritorio, etc.) se deberán evaluar? ¿cuántos sistemas?
Respuesta: No se dispone de esa información concreta. Cada contrato basado indicará el alcance.

Pregunta: LOTE 2 A6: REVISIÓN DE BASTIONADO Cuando se habla de dispositivos de propósito específico o de control industrial ¿se refiere a dispositivos OT?
Respuesta: Nos referimos a dispositivos IoT y OT, entre otros.

Pregunta: LOTE 2 A6: REVISIÓN DE BASTIONADO Para las pruebas de análisis de componentes y software base: ¿qué tecnologías se deberán evaluar? ¿cuántos componentes/softaware base?
Respuesta: No se dispone de esa información. Cada contrato basado indicará el alcance.

Pregunta: LOTE 3 A6: REVISIÓN DE BASTIONADO La revisión de los procedimientos de instalación, ¿se entiende como una revisión de los documentos o guías de instalación y configuración de los que disponga cada sede?
Respuesta: Exacto. Y de su alineamiento con estándares, guías y buenas prácticas.

Pregunta: LOTE 2 A6: REVISIÓN DE BASTIONADO La revisión de los procedimientos de instalación, ¿se espera del adjudicatario que además de identificar carencias en los procedimientos también se defina y redacte aquellos procedimientos de los que se carezca?
Respuesta: Cabría esa actividad, al estar en el objeto del servicio y en base al texto

> Consistirá en analizar el nivel de seguridad de una infraestructura o plataforma tecnológica y definir un conjunto de configuraciones que permitan minimizar los riesgos identificados debidos a malas configuraciones o defectos del sistema.

Pregunta: LOTE 2 A6: REVISIÓN DE BASTIONADO Para las pruebas de "revisión de procedimientos de instalación y configuración": ¿qué tipo de sistemas (tecnología, SO, versiones, ….) se deberán evaluar? ¿cuántos sistemas?
Respuesta: No se dispone de esa información. Cada contrato basado indicará el alcance.

Pregunta: LOTE 2 A6: REVISIÓN DE BASTIONADO Cuando se habla sobre "Revisión de componentes software base" de los desarrollos ¿podría considerarse un análisis SCA (Aoftware Component Analysis) y realizarse como parte de los analisis estáticos o se prefiere un análisis del repositorio de librerías puntual?
Respuesta: ambos casos podrían darse.

Pregunta: LOTE 2 A7: PRUEBAS DE INTRUSIÓN / RED TEAM ¿Para la ejecución de estas pruebas estará avisado el equipo de Blue Team de la ADA y/o algún otro (p.e.: IT) o se busca medir el nivel de respuesta/resiliencia ante posibles ataques? En el caso de que sea lo segundo, si durante las pruebas de intrusión somos detectados y bloqueados, ¿se considerará terminado el ejercicio o se podrá continuar con el mismo levantando el modo bloqueo y quedando sólo el de detección durante el resto del tiempo del ejercicio?
Respuesta: Cada contrato basado indicará el alcance, las responsabilidades RACI y el procedimiento de ejecución.

Pregunta: LOTE 2 A7: PRUEBAS DE INTRUSIÓN / RED TEAM Para la realización de este ejercicio, ¿qué sede(s) se deberán considerar? En el caso de ejecutar pruebas in-situ, ¿sobre qué sede u organismo se podrán realizar?
Respuesta: Cada contrato basado indicará el alcance, dentro de los sistemas y sedes de la Junta de Andalucía, como se especifica en el PPT, página 8:

> Lotes 2 y 3: los trabajos a ejecutar, en el contexto del Centro de Operaciones de Seguridad (SOC) de la Junta de Andalucía, en tanto que recurso común (art. 6.3.o del citado Decreto 128/2021), podrán beneficiar a todos los organismos del sector público andaluz, y en concreto a los del ámbito subjetivo del Decreto 70/2017, de 6 de junio, por el que se modifica el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

Pregunta: LOTE 2 A7: PRUEBAS DE INTRUSIÓN / RED TEAM Para la realización de ataques de ingeniería social como vector de entrada a la organización, ¿se deberá consensuar previamente con la Dirección del Proyecto el listado de personas, teléfonos, etc., que se utilizarán durante el ataque o podrán utilizarse todos aquellos que sean encontrados a través de técnicas OSINT durante la fase de

enumeración del ejercicio sin previa autorización?; ¿La Dirección del proyecto querrá sugerir posibles víctimas a incluir dentro del ataque?
Respuesta: Cada contrato basado indicará el alcance, las responsabilidades RACI y el procedimiento de ejecución, así como los posibles contactos, aunque podrán ser establecidos también al inicio de la ejecución.

Pregunta: LOTE 2 A7: PRUEBAS DE INTRUSIÓN / RED TEAM En caso de que no sea posible lograr el acceso a red interna desde los activos expuestos y/o técnicas de ingeniería social efectuados durante las primeras fases, ¿se podrá ejecutar un escenario de brecha asumida ("assume the breach") que parta del supuesto de haber comprometido una máquina ubicada en red interna a la que la Dirección del Proyecto proporcione acceso al proveedor para poder continuar el ejercicio de pentest interno o se daría por concluido el mismo?
Respuesta: Es posible.

Pregunta: LOTE 2 A7: PRUEBAS DE INTRUSIÓN / RED TEAM ¿La duración del ejercicio de red team será fijada por la Dirección del Proyecto o puede el proveedor proponer una? En caso de que vaya a ser fijada por la Dirección del Proyecto, ¿de cuánto tiempo como máximo podríamos considerar el ejercicio?
Respuesta: Los contratos basados especificarán la duración máxima del ejercicio.