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: En relación con el criterio de Solvencia Técnica 2, ¿se requiere que el licitador sea (i) una entidad certificadora o (ii) una entidad certificada por alguna entidad certificadora acreditada por la ENAC?

Respuesta: aplicaría (i), puesto que el PCAP, en su Anexo I, punto 2º, establece lo siguiente: <<Para el lote 1, las empresas auditoras deberán ser entidades certificadoras acreditadas por la Entidad Nacional de Acreditación (ENAC) para la certificación en al menos una de las siguientes normas: ISO27001, ENS>>. Debe observarse que el objeto del lote 1 es la realización de auditoría de certificación de sistemas, incluyendo, si procede, la expedición de la certificación, para lo cual (ii) no resulta suficiente.

Pregunta 2: Conforme a la guía CCN-CERT IC-02/20 del Centro Criptologico Nacional (guía para la contratación de auditorías de certificación del Esquema Nacional de Seguridad, indicado en el apartado 5.2, puntos 24, 25, 26), necesitaríamos conocer los servicios y definición concisa de los alcances de los certificados a emitir del ENS, identificando la categoría por cada alcance (básica/media/alta), sistemas de información afectados, así como la sede física de cada uno de los certificados y el número de trabajadores (vinculados directamente con el alcance).

2. Relacionado con el alcance de ENS, de los certificados ya emitidos anteriormente, cuales desean realizar la renovación y con que categoría?

3.Tanto para ENS como para ISO 27001, necesitaríamos conocer las ubicaciones físicas de los CPDs junto con el número y localización de sedes alternativas?

4.Referido a la ISO 27001, igualmente necesitaríamos, alcance, sedes y trabajadores implicados directamente con el alcance, así como si disponen de certificados vigentes y si es necesaria la transferencia de los certificados acreditados?.

5.Cabe mencionar que conforme a la guía CCN mencionada anteriormente apdo 5.3, punto 28, donde aclara que la contratación debe ser realizada a entidades de certificación acreditadas por el propio CCN-ENAC, ¿Es necesario que las entidades de certificación estén a su vez certificadas en ENS y 27001 e ISO 20000 para LOTE 1?.

Respuesta: Los detalles referidos serán acotados en cada contrato basado, pudiendo estos acogerse al catálogo de unidades de servicio predefinidas o bien no predefinidas, en cuyo caso resultará aplicable el punto 27 de la citada guía CCN-CERT IC-02/20.

En los contratos basados se ofrecerá, cuando sea el caso, la información relativa a certificaciones preexistentes que sean objeto de renovación.

Con las mismas consideraciones, también se ofrecerá en los contratos basados la información relativa a ubicación y número de CPDs y sedes alternativas.

De manera análoga, en el ámbito de la ISO 27001, los datos que se enumeran serán detallados en los contratos basados.

Conforme a lo exigido en el PCAP, Anexo I, punto 2º, <<Para el lote 1, las empresas auditoras deberán ser entidades certificadoras acreditadas por la Entidad Nacional de Acreditación (ENAC) para la certificación en al menos una de las siguientes normas: ISO27001, ENS>>. No se exige, por tanto, que las entidades de certificación estén certificadas en ISO 27001 e ISO 20000, si bien están contemplados como criterios valorables para la adjudicación del Acuerdo Marco, considerándose además una certificación en ENS en nivel medio o alto como equivalente a ISO 27001. De otra parte, como pudiera deducirse, no resulta obligatoria la posesión de certificación en ENS en el Acuerdo Marco, pero no se debe perder de vista que en los contratos basados se aplicarán, conforme al PCAP, las medidas de seguridad correspondientes al ENS en el nivel que se determine por el responsable del contrato basado, así como lo expresado en el punto 5.10 del PPT.

Pregunta 3: Para justificar la solvencia técnica: ¿sería posible usar declaraciones responsables firmadas por la empresa en el caso de que los proyectos se hayan ejecutado en el sector privado y no en el público y por lo tanto no haya CPVs?

Respuesta: El PCAP permite la posibilidad de justificar trabajos realizados aún sin coincidencia de CPV, pero siempre que

> "tengan como objeto principal de los trabajos la realización de servicios de auditoría de certificación, de auditoría técnica de seguridad, o de formación y concienciación en materia de ciberseguridad, según el lote".

Recordamos también que

> "La acreditación de la relación de los trabajos presentada por el interesado tendrá que estar avalada por los correspondientes certificados de buena ejecución, que deberán ser aportados junto con la declaración Responsable".

Pregunta 4: En relación al valor estimado del lote 2 de este procedimiento encontramos una discrepancia entre lo indicado en el PCAP y lo reflejado en los datos básicos de esta licitación en el perfil del contratante. Datos del Pliego de Cláusulas Administrativas: LOTE 2: 2 Servicios de auditorías técnicas Valor estimado 1.961.869,82 € Datos del perfil: LOTE 2: 2 Servicios de auditorías técnicas Valor estimado 1.963.759,87€

Respuesta: Prevalece el valor indicado en el Pliego de Cláusulas Administrativas Particulares.

Pregunta 5: Respecto a la elaboración de dicho acuerdo para la norma ISO 27001, sería de ayuda conocer de una manera aproximada el personal sujeto a dicha norma que habría en cada institución (al menos en intervalos) a certificar.

Respuesta: Estos datos serán establecidos en cada contrato basado, sin que puedan quedar predefinidos en el Acuerdo Marco.

Pregunta 6: En referencia al LOTE 3 de Formación y Concienciación, tendríamos las siguientes consultas de cara a poder dimensionar las unidades de servicio predefinidas que se demandan:
Cursos presenciales: Aunque el pliego indica que los servicios podrían requerir el desplazamiento a cualquier punto de la Comunidad Autónoma de Andalucía, ¿podrían dar una estimación de los cursos

que se realizarían en Sevilla o en el resto de las capitales de provincia? ¿podrían indicar qué % de cursos harían uso de las instalaciones de la Junta de Andalucía para la impartición de los mismos?
Cursos semipresenciales: ¿Qué % de presencialidad se espera que tengan los cursos?
Para la planificación de los cursos, ¿se puede considerar que se realizarían en jornadas consecutivas? Es decir, para los cursos presenciales ¿se podría tener en cuenta que se realizarían en 2 jornadas, siendo estas en días consecutivos tanto para los cursos de 10 horas como para los de 15 horas?
En referencia al servicio de "Preparación del campus virtual para la formación on-line", ¿podrían ampliarnos la información del servicio al respecto? ¿Estamos hablando de una plataforma de Formación dedicada? ¿Estamos hablando del uso de plataformas tipo Teams?
Formación on-line: la formación impartida a distancia, ¿puede llevarse a cabo a través de plataformas tipo Teams, Zoom o similar (no siendo obligatorio el uso de ninguna Plataforma E-learning)? ¿o es obligatorio el uso de una plataforma E-learning?
Los vídeos solicitados, ¿qué formato han de tener? ¿qué objetivo tienen? Introducción al curso, resumen del mismo…
En referencia al video tutorial (ELEM-DFS-VT) ¿Cuál sería el objetivo del curso? ¿En qué ámbito? ¿Qué formato y duración mínima ha de tener?
En referencia a los cursos MOOC ¿Qué se espera en cuanto a contenido? ¿Qué se espera de la tutorización de los alumnos? ¿Debemos incluir el coste de la plataforma donde alojar el SCORM y a los alumnos?

Respuestas:

- No se dispone ahora mismo de estimación sobre distribución de los cursos presenciales. En anteriores planes de formación se han realizado cursos en Sevilla, Granada o Málaga, pero no hay compromiso ni estimación sobre los futuros cursos.
- No podemos indicar un valor concreto, pero un porcentaje elevado de los cursos presenciales se realizarán en instalaciones de la Junta de Andalucía.
- No se dispone de estimación sobre el porcentaje de semipresencialidad de los cursos semipresenciales.
- Las jornadas de formación suelen realizarse de forma contigua, pero no hay compromiso sobre ello.
- La plataforma de formación a usar para los cursos será propuesta por el adjudicatario en función de su experiencia y conocimientos, y se valorará, considerando que forma parte del "Modelo general de prestación del servicio", en el marco del criterio 1 del Anexo VIII del PCAP.
- La unidad predefinida "ELEM-DFS-VT" busca la realización de elementos audiovisuales para la de sensibilización en materia de ciberseguridad con formato atractivo, concisos y con carátulas específicas del proyecto de inicio y cierre. Su duración rondará los 2-5 minutos. El formato deberá ser archivo MP4 o similar de alta calidad para distribución en redes sociales.
- Los MOOC se alojarán habitualmente en plataformas de la Junta de Andalucía, aunque no hay compromiso para ello. Los detalles sobre los mismos serán propuestos por el adjudicatario en función de su experiencia y conocimientos, y se valorarán en el marco del criterio 1 del Anexo VIII del PCAP.

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... Los presupuestos base de licitación de los contratos basados, como es lógico, estarán dimensionados de acuerdo a la amplitud y exigencias de las actuaciones requeridas.

3.2.2.1. A1: Revisión técnica de seguridad de una infraestructura o entorno en modalidad de caja negra o gris 3.2.2.2. A2: Revisión técnica de seguridad de una infraestructura o entorno en modalidad de caja blanca En estas iniciativas (caja negra, blanca o gris) , ¿Podrían indicarnos qué se espera de la revisión con el enfoque de plano de bastionado de los activos?
3.2.2.1. A1: Revisión técnica de seguridad de una infraestructura o entorno en modalidad de caja negra o gris En relación al punto Plano de interconexión: Sobre los accesos sede contra sede ¿Entendemos que se refieren a un pentesting para medir la segmentación entre las distintas sedes de la compañía?
3.2.2.1. A1: Revisión técnica de seguridad de una infraestructura o entorno en modalidad de caja negra o gris Sobre el punto Plano de publicación, y entre otros se realizarán test de: - Suplantación de credenciales con el objetivo de intentar modificar publicaciones. ¿Implicaría el análisis y búsqueda de todas las credenciales que se encuentren en internet, ya sea en mercados negros o en leaks, verificando si todavía siguen presentes?
3.2.2.2. A2: Revisión técnica de seguridad de una infraestructura o entorno en modalidad de caja blanca Al tratarse de una revisión de caja blanca, entendemos que el objetivo de este apartado es aplicar las técnicas de pentesting en los planos internos del cliente. ¿Es por tanto el objeto de la revisión los sistemas internos o el perímetro de red?
3.2.2.2. A2: Revisión técnica de seguridad de una infraestructura o entorno en modalidad de caja blanca ¿Se incluye dentro del alcance los equipos de escritorio o portátiles corporativos?
Respuesta: Así es.

3.2.2.3. A3: Revisión técnica de seguridad de entornos wifi, con enfoque de caja blanca y/o negra Respecto al punto "Estado de salud y comportamiento de los dispositivos (AP y Cliente)" ¿Se espera desde el punto de vista de ciberseguridad que se revisen configuraciones relacionadas con detección de comportamientos anómalos como fakeap?
3.2.2.3. A3: Revisión técnica de seguridad de entornos wifi, con enfoque de caja blanca y/o negra Respecto al punto "Identificación de vulnerabilidades en el cifrado y en la implementación y revisión de la asociación y autenticación MAC" ¿Se requiere realizar algún tipo de prueba o se puede realizar una revisión basada en configuraciones y buenas prácticas?
3.2.2.3. A3: Revisión técnica de seguridad de entornos wifi, con enfoque de caja blanca y/o negra Respecto al punto "Estado de salud y comportamiento de los dispositivos (AP y Cliente)" ¿Se espera revisar configuraciones relacionadas con detección de comportamientos anómalos como fakeap?

3.2.2.3. A3: Revisión técnica de seguridad de entornos wifi, con enfoque de caja blanca y/o negra

Respecto al punto "Revisión de la monitorización y la captura." ¿Se espera la activación de las opciones de monitorización y estado de las integraciones de logs con SIEM?

ACLARACIÓN A PREGUNTAS Para las preguntas que vienen a continuación, se trata de aclarar si vuestro objetivo es el de hacer una revisión del bastionado de los sistemas o de arquitectura de la red. Dado que la metodología que incluiremos es diferente, nos gustaría saber qué esperáis.

3.2.2.6. A6: Revisión de bastionado y verificación de la correcta aplicación de procedimientos de instalación y empleo seguro de sistemas Para el punto "Análisis de la protección a nivel de red del servicio objeto de análisis: reglas de cortafuegos; reglas de Web Application Firewall (WF); protección respecto a ataques Denial of Service (DoS) o Distributed." ¿Entendemos que la revisión es desde un punto de vista teórico en base a evidencias y en ningún caso se entraría a las herramientas de seguridad a revisar configuraciones?

Respuesta: Así es, en este caso. Recordamos que estas actividades son orientativas y no exhaustivas, en todo caso.

3.2.2.6. A6: Revisión de bastionado y verificación de la correcta aplicación de procedimientos de instalación y empleo seguro de sistemas Para el punto "Análisis del firmware o software de dispositivos o appliances, sus versiones e identificación de aquellos con vulnerabilidades reconocidas, discontinuados o con versiones muy desfasadas (más de 1 año) respecto a la última versión estable disponible." ¿Entendemos que se proporcionará un inventario con las versiones del software y firmware de las aplicaciones para poder realizar las comprobaciones? ¿Qué se espera de este punto?

3.2.2.6. A6: Revisión de bastionado y verificación de la correcta aplicación de procedimientos de instalación y empleo seguro de sistemas Para el punto "Denial of Service (DDoS), escaneo de puertos, etcétera. También, el análisis de la idoneidad de reglas de enrutado de tráfico aplicado, de la limitación de privilegios en el acceso, o de la situación y disposición correcta de los componentes del servicio en la infraestructura de red y cloud del organismo. En todos los casos, tanto desde el punto de vista de una persona externa a la organización, como de una persona interna a la misma." ¿Se espera de este punto que se revise la existencia de una herramienta para la protección contra DDoS o que se realicen pruebas para identificar los puertos abiertos de cada uno de los sistemas y el nivel de tolerancia frente a ataques DDoS? Si es necesario la realización de pruebas ¿Se tendría que proporcionar dicha herramienta para la revisión de este tipo de controles?

3.2.2.6. A6: Revisión de bastionado y verificación de la correcta aplicación de procedimientos de instalación y empleo seguro de sistemas Para el punto "Análisis de la protección a nivel de red de las comunicaciones entre distintos módulos del servicio analizado." ¿Se espera un análisis de la matriz de visibilidad entre distintas vlan, análisis del mapa de red y como está distribuidas las herramientas para el control de red? ¿Cuál es el resultado final esperado con respecto a este punto?