QUESTIONS AND ANSWERS - REFERENCE: CO/2022-28

Nombre de la licitación: Auditoría del sistema informático
Referencia: CO/2022-28

Pregunta 3:

Dudas de carácter documental/administrativo

1. La oferta deberá contener un original completo con la firma original del representante autorizado del licitador, ¿se admite firmar el documento en pdf o tiene que ser manuscrita? ¿basta con firmar en la primera pagina o se precisa firmar el documento completo?¿serviría con un sello de empresa?
2. Sobre el documento Modelo de contrato, se entiende que es para el adjudicatorio pero hay que hacer alguna mención sobre que se aceptan los términos de forma previa o se ponen objeciones a los mismos?
3. Cuando en el sobre 1 se indica que hay que aportar los datos del licitador se refiere al documento PARTE B: Formulario de identificación del licitador?
4. La oferta estará acompañada de una carta firmada por el licitador ¿Qué contenido se espera tenga esa carta?
5. Para presentar en el sobre 1 el PARTE C: FORMULARIO DE ENTIDAD JURÍDICA se dispone de ese modelo en formato Word para su cumplimentación?¿se puede adjuntar en un formato similar o tiene que ser ese modelo?
6. el formulario de FORMULARIO DE IDENTIFICACIÓN FINANCIERA debe incluirse en el sobre 1 o solo se aporta en caso de adjudicación? En caso de tener que adjuntar se dispone de ese modelo en formato Word para su cumplimentación? o ¿se puede adjuntar en un formato similar? ¿ tiene que ser ese modelo?
7. Prueba de capacidad técnica o profesional si no puede aportarse con cartas de referencia, bastaría con un certificado firmado por la empresa que indique claramente el volumen de trabajo realizado?
8. En los criterios de adjudicación se observa que los baremos indicados no suman 100% sino un 90% ¿a qué criterio corresponde el 10% que falta? Ciertamente, falta un criterio: “Puntos de control adicionales ofrecidos de acuerdo con la norma ISO 27002 (10%)”

Dudas orientadas a la auditoria

- Aunque la RFP indica que se trata de una auditoría con 2 informes diferenciados, el texto de cada uno de los puntos a tratar da pie a interpretaciones distintas a esta (Además, hay una frase en la que indican que esta RFP es interpretable por su Secretaría Ejecutiva). Dicho esto, sería conveniente que nos aclararan que se trata de una auditoría per sé y que no entra en el alcance del proyecto ningún tipo de implantación, desarrollo, configuración y/o propuesta similar que se escape de la revisión y análisis llevados a cabo en el propio proceso de auditoría. Es obvio que sin contar la parte de pruebas de seguridad que hubiera que llevar a cabo por parte de Auditoría.
- Por otro lado, necesitaríamos más detalle del alcance:
  - Tecnologías en el alcance de la auditoría y de cada uno de los puntos a revisar
  - Tipo y orden de magnitud de cada tecnología.
- Idioma de los entregables.
- Idioma de los interlocutores y países involucrados, en el caso de que no sea exclusivamente desde España

- Localizaciones físicas en el alcance (oficinas, CPDs, etc.) y ubicaciones de las mismas (a nivel de país).
- Se entiende que los trabajo se desarrollaran siempre en horario laboral Cual es el horario de la entidad?

Dudas orientados a trabajos de hacking:

1. Para el Pentest Externo
   Dudas para el dimensionamiento del servicio:
   * Conocer el enfoque:
     1) el cliente nos facilita los sistemas del alcance, o
     2) nosotros identificamos los sistemas del alcance (y luego confirma cliente)
   * Idioma del entregable (español o ingles).
   * Existencia de IDS/IPS actuando en el alcance (para pruebas de IDS/IPS)

   * Existencia de servidores de correo entrante en el alcance (para pruebas de correo)
   * Existencia de WAF en el alcance (para pruebas de WAF). * Número de aplicaciones web expuestas y tipo (web corporativa, intranet, tienda online, etc.):
   En caso de que el cliente nos facilite el alcance, necesitaremos:
   * Rangos y/o direcciones IP del alcance
   En caso de que el cliente no nos facilite el alcance, necesitaremos:
   * conocer si el alcance es global o limitado a algún país:

2. Para el Pentest Interno
   Dudas para el dimensionamiento del servicio:

   * Conocer el enfoque:
     1) simular usuario que se conecta a un punto de red, sin información, y/o
     2) simular empleado que se conecta desde su maqueta y con la información estándar
     3) los 2 escenarios anteriores
   * Idioma del entregable (español o ingles)
   * Número de segmentos de red que componen el alcance.
   * Número de servidores y estaciones de trabajo
   * Ubicación desde la que se realizará el pentest :
   * En caso de estar en el Cloud:
     - conocer donde se encuentra (AWS, Azure, etc.)

Respuesta 3:

Dudas de carácter documental/administrativo

1. La oferta deberá contener un original completo con la firma original del representante autorizado del licitador, ¿se admite firmar el documento en pdf o tiene que ser manuscrita? Se admite la firma en pdf ¿basta con firmar en la primera pagina o se precisa firmar el documento completo? la primera página es suficiente, salvo los documentos que tengan una casilla específica para poner la firma ¿serviría con un sello de empresa? No, se requiere firma del representante autorizado del licitador
2. Sobre el documento Modelo de contrato, se entiende que es para el adjudicatorio pero hay que hacer alguna mención sobre que se aceptan los términos de forma previa o se ponen objeciones a los mismos? No es necesario hacer ninguna mención expresa sobre la aceptación de los términos, al enviar la documentación se entiende que se aceptan todos los términos del contrato. Cualquier duda sobre los mismos contactar con el COI
3. Cuando en el sobre 1 se indica que hay que aportar los datos del licitador se refiere al documento PARTE B: Formulario de identificación del licitador? Es necesario el DNI y el documento de identificación del licitador.
4. La oferta estará acompañada de una carta firmada por el licitador ¿Qué contenido se espera tenga esa carta? La carta de presentación es una carta de cortesía que se utiliza para confirmar la voluntad de la empresa en presentarse a la licitación. Dado que es la primera oportunidad de dirigirse a la empresa licitante, se suele utilizar para destacar cualquier aspecto relevante que pueda suponer un valor diferencial frente a sus competidores. No existe un modelo específico de carta.
5. Para presentar en el sobre 1 el PARTE C: FORMULARIO DE ENTIDAD JURÍDICA se dispone de ese modelo en formato Word para su cumplimentación? Sí, se dispone de dicho modelo en formato editable ¿se puede adjuntar en un formato similar o tiene que ser ese modelo? Ha de ser este modelo
6. el formulario de FORMULARIO DE IDENTIFICACIÓN FINANCIERA debe incluirse en el sobre 1 o solo se aporta en caso de adjudicación? En caso de tener que adjuntar se dispone de ese modelo en formato Word para su cumplimentación? Sí, se dispone de dicho modelo en formato editable. Cabe resaltar que este documento debe de ser firmado y sellado por la entidad financiera o ¿se puede adjuntar en un formato similar? ¿ tiene que ser ese modelo? Ha de ser este modelo
7. Prueba de capacidad técnica o profesional si no puede aportarse con cartas de referencia, bastaría con un certificado firmado por la empresa que indique claramente el volumen de trabajo realizado? Sí, sería suficiente cualquier documento certificado y auditable que demuestre la capacidad técnica de la empresa.
8. En los criterios de adjudicación se observa que los baremos indicados no suman 100% sino un 90% ¿a qué criterio corresponde el 10% que falta? Ciertamente, falta un criterio: “Puntos de control adicionales ofrecidos de acuerdo con la norma ISO 27002 (10%)”

Dudas orientadas a la auditoria

Aunque la RFP indica que se trata de una auditoría con 2 informes diferenciados, el texto de cada uno de los puntos a tratar da pie a interpretaciones distintas a esta (Además, hay una frase en la que indican que esta RFP es interpretable por su Secretaría Ejecutiva). Dicho esto, sería conveniente que nos aclararan que se trata de una auditoría per sé y que no entra en el alcance del proyecto ningún tipo de implantación, desarrollo, configuración y/o propuesta similar que se escape de la revisión y análisis llevados a cabo en el propio proceso de auditoría. Es obvio que sin contar la parte de pruebas de

seguridad que hubiera que llevar a cabo por parte de Auditoría. Efectivamente, se trata de un proyecto de auditoría y no de un proyecto de otra índole (desarrollo, configuración, implantación, …)

Por otro lado, necesitaríamos más detalle del alcance:

Tecnologías en el alcance de la auditoría y de cada uno de los puntos a revisar. En el capítulo SISTEMAS ANALIZADOS del ANEXO I, se detallan los componentes que se solicita analizar (funciones I/O, servlets, conectores de base de datos, códigos SSL, ….) en los Sistemas del COI (excepto el ERP, llamado SAGE). Y para ello, se entiende que serán necesarias herramientas tales como analizadores de tráfico, escáner de puertos, generador de paquetes IP, … (sugeridas también en ANEXO I)

Tipo y orden de magnitud de cada tecnología. Esta respuesta será enviada por correo electrónico a quien lo solicite después de firmar el acuerdo de confidencialidad pertinente.

Idioma de los entregables. Español ó inglés

Idioma de los interlocutores y países involucrados, en el caso de que no sea exclusivamente desde España. La geografía del proyecto es España y por tanto los idiomas de interlocución será siempre español o inglés.

Localizaciones físicas en el alcance (oficinas, CPDs, etc.) y ubicaciones de las mismas (a nivel de país). c/Principe de Vergara 154 – 28002 MADRID. Adicional, los servicios en la nube.

Se entiende que los trabajo se desarrollaran siempre en horario laboral Cual es el horario de la entidad? 7:30 – 18:00 (L-J), 7:30-17:00 (V)

<u>Dudas orientados a trabajos de hacking:</u>

1. Para el Pentest Externo
   Dudas para el dimensionamiento del servicio:
   * Conocer el enfoque:
     1) el cliente nos facilita los sistemas del alcance, o
     2) nosotros identificamos los sistemas del alcance (y luego confirma cliente) Sí

   * Idioma del entregable (español o ingles). Cualquier de los dos
   * Existencia de IDS/IPS actuando en el alcance (para pruebas de IDS/IPS) No

   * Existencia de servidores de correo entrante en el alcance (para pruebas de correo) Servicio de correo de Microsoft (nube)
   * Existencia de WAF en el alcance (para pruebas de WAF). Ninguno privado. Los que suministra el proveedor de la plataforma web
   * Número de aplicaciones web expuestas y tipo (web corporativa, intranet, tienda online, etc.): Esta respuesta será enviada por correo electrónico a quien lo solicite después de firmar el acuerdo de confidencialidad pertinente.

   En caso de que el cliente nos facilite el alcance, necesitaremos:

   * Rangos y/o direcciones IP del alcance

   En caso de que el cliente no nos facilite el alcance, necesitaremos:

   * conocer si el alcance es global o limitado a algún país: es sólo para nuestra sede en Madrid

2. Para el Pentest Interno
   Dudas para el dimensionamiento del servicio:

   * Conocer el enfoque:
     1) simular usuario que se conecta a un punto de red, sin información, y/o
     2) simular empleado que se conecta desde su maqueta y con la información estándar
     3) los 2 escenarios anteriores ambos

   * Idioma del entregable (español o ingles) cualquiera de los dos

   * Número de segmentos de red que componen el alcance. Esta respuesta será enviada por correo electrónico a quien lo solicite después de firmar el acuerdo de confidencialidad pertinente.
   * Número de servidores y estaciones de trabajo Esta respuesta será enviada por correo electrónico a quien lo solicite después de firmar el acuerdo de confidencialidad pertinente.
   * Ubicación desde la que se realizará el pentest : Se aceptan sugerencias, pero la sede del COI puede ser una ubicación para realizar el pentest

   * En caso de estar en el Cloud:
     - conocer donde se encuentra (AWS, Azure, etc.) Esta respuesta será enviada por correo electrónico a quien lo solicite después de firmar el acuerdo de confidencialidad pertinente.