GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

INTECO
Instituto Nacional de Tecnologías de la Comunicación

SERVICIOS DE AUDITORÍA DE SEGURIDAD DE APLICACIONES SOFTWARE

EXPEDIENTE 42/13

PLIEGO DE CARACTERÍSTICAS TÉCNICAS

JULIO 2013

ÍNDICE

Nota: Cualquier consulta en relación a este procedimiento de adjudicación debe dirigirse por correo electrónico a la dirección contratacion@inteco.es, indicando:

Asunto: número de expediente.

Cuerpo: nombre de la empresa, datos de la persona que realiza la consulta y texto de la consulta.

El presente documento cumple con las condiciones de accesibilidad del formato PDF (Portable Document Format).

Se trata de un documento estructurado y etiquetado, provisto de alternativas a todo elemento no textual, marcado de idioma y orden de lectura adecuado.

Para ampliar información sobre la construcción de documentos PDF accesibles puede consultar la guía disponible en la sección Accesibilidad > Formación > Manuales y Guías de la página http://www.inteco.es.

1. ALCANCE Y OBJETO DEL CONTRATO

1.1. OBJETO

El objeto del contrato es la prestación de servicios de auditorías de seguridad de aplicaciones software en ejecución y de código.

El detalle de los trabajos a realizar por el equipo de trabajo está recogido en el apartado 2. Requisitos Técnicos.

2. REQUISITOS TÉCNICOS

2.1. CONSIDERACIONES PREVIAS

En este apartado se describen los servicios, características y requisitos que conforman el objeto del contrato y que el adjudicatario deberá prestar, no siendo el listado que aparece a continuación una relación exhaustiva de las características de los servicios contratados, sino las líneas generales demandadas por INTECO, cubriendo los aspectos de tareas a realizar y resultados esperados.

Los referidos requisitos deben entenderse como mínimos pudiendo los licitadores ampliarlos y mejorarlos en sus ofertas. Las propuestas que ofrezcan características inferiores no serán tomadas en consideración en el presente procedimiento de adjudicación. El licitador puede ofertar prestaciones superiores a las solicitadas, que se considerarán positivamente en la valoración técnica de la oferta.

El adjudicatario deberá aportar los conocimientos, metodologías y apoyarse en las herramientas necesarias para asegurar el resultado óptimo del proyecto.

El adjudicatario se obliga a guardar secreto y a hacerlo guardar al personal que emplee para la ejecución del contrato, sobre toda la información proveniente de INTECO, o que pueda afectar a INTECO, o que sea resultado del servicio que INTECO le haya encargado, que con motivo del desarrollo de los trabajos llegue a su conocimiento. En ningún caso podrá usar esta información para sí, ni para otra persona o entidad, sin el acuerdo expreso previo de INTECO.

2.2. ALCANCE

El objetivo del contrato es la evaluación de la seguridad de aplicaciones software a través de los siguientes dos tipos de servicio:

1. Auditoría de seguridad. Con la aplicación en ejecución, y mediante técnicas de *hacking*, el adjudicatario analizará la aplicación software en busca de posibles vulnerabilidades de seguridad. Las pruebas y análisis de seguridad a realizar deberán incluir, donde proceda, al menos los siguientes: posibilidades de inyección de código, gestión de sesiones, escalada de privilegios, gestión de errores, propagación de vulnerabilidades, posibles *exploits* que se pudieran usar, sistemas de autenticación, posibles suplantaciones, de entrada de datos y de tráfico y comunicaciones.

2. Auditoría de código. A través del código fuente de la aplicación, el adjudicatario analizará la aplicación en busca de posibles vulnerabilidades de seguridad. Las

aplicaciones a analizar podrán hacer uso de cualquiera de los siguientes lenguajes: PHP, C, C++, C#, Objective C, Java (SE/EE, JMF, Java RTS, RMI, JAXB, SOAP, CORBA, ODBC/JDBC, Struts, JSTL, Portlets, GWT, Spring, Hibernate, AXIS, etc), Python, VB/VB.net, ASP/ASPX, COBOL, mod_plsql (PL/SQL), Dalvik Java (Android) y Perl

INTECO podrá solicitar al adjudicatario la realización de auditorías en cualquier momento durante la vigencia del contrato, siempre y cuando no se haya alcanzado el límite presupuestario. Ver apartado de metodología.

En el apartado siguiente se establecerán las características técnicas de las aplicaciones a auditar.

2.3. DESCRIPCIÓN DE LOS TRABAJOS

Los análisis de seguridad que podrán ser solicitados pueden clasificarse de la siguiente manera:

Clasificación	Servicio	Objeto del servicio	Volumen
Tipo 1	Auditoría de seguridad	Aplicación web	La aplicación tiene entre 0 y 5 formularios de entrada (con cualquier número de páginas sin formularios).
Tipo 1.X	Auditoría de seguridad	Aplicación web	Donde X es un múltiplo que señala cada bloque de hasta 5 formularios (con cualquier número de páginas sin formularios) adicionales al primer bloque.. Ejemplo. Una aplicación de 12 formularios sería Tipo 1.2
Tipo 2	Auditoría de código	Aplicación web	La aplicación tiene hasta 10.000 líneas de código.
Tipo 2.X	Auditoría de código	Aplicación web	Donde X es un múltiplo que señala cada bloque de hasta 10.000 líneas de código adicionales a las de Tipo 2. Ejemplo. Una aplicación de 34.000 líneas de código sería Tipo 2.3.
Tipo 3	Auditoría de seguridad	Aplicación cliente-servidor	La aplicación muestra entre 0 y 5 formularios de entrada (con cualquier número de páginas sin formularios).
Tipo 3.X	Auditoría de seguridad	Aplicación cliente-servidor	Donde X es un múltiplo que señala cada bloque de hasta 5 formularios (con cualquier número de páginas sin formularios) adicionales al primer bloque. Ejemplo. Una aplicación de 12 formularios sería Tipo 1.2
Tipo 4	Auditoría de código	Aplicación cliente-servidor	La aplicación tiene hasta 10.000 líneas de código.
Tipo 4.X	Auditoría de código	Aplicación cliente-servidor	Donde X es un múltiplo que señala cada bloque de hasta 10.000 líneas de código adicionales a las de Tipo 4. Ejemplo. Una aplicación de 93.000 líneas de código sería Tipo 4.9

Aspectos a tener en cuenta en las auditorías de seguridad:

1. Para realizar ambos tipos de auditorías, dinámicas o de código, el adjudicatario podrá apoyarse en el uso de herramientas de seguridad. Sin embargo, siempre que sea posible, las vulnerabilidades explotables serán reportadas indicando los pasos que se han seguido para su explotación mediante técnicas de *hacking*.

2. En los casos en los que sean requeridas ambas auditorías (dinámicas y de código) para una misma aplicación, los resultados de ambas auditorías deberán ser cruzados (relación de las vulnerabilidades detectadas en ambas auditorías) y se elaborará un único informe de resultados por aplicación.

3. Las auditorías de seguridad serán normalmente realizadas en entornos de pruebas imagen de los entornos de producción en los que se encuentren desplegadas las aplicaciones. Siempre que INTECO pueda disponer de estos entornos se facilitará su acceso al adjudicatario. En caso contrario, el adjudicatario deberá disponer de la infraestructura necesaria para la construcción de estos entornos desde donde se realizarán las pruebas.

Cada auditoría consistirá en una doble iteración, es decir, el adjudicatario evaluará la aplicación y emitirá el correspondiente informe. Una vez corregidas las vulnerabilidades detectadas, se facilitará al adjudicatario una nueva versión de la aplicación, y éste verificará que se han corregido las vulnerabilidades reportadas en la primera iteración, y que debido a su corrección no se han incluido nuevas vulnerabilidades. La metodología a seguir ha sido descrita en detalle en el siguiente apartado.

2.3.1. Metodología

La **metodología de trabajo** a seguir para cada aplicación de la que se quiera realizar una auditoría de seguridad será la siguiente:

1. El Director Técnico de INTECO solicitará al adjudicatario la realización de cada auditoría, indicando de que tipo sería.

2. El adjudicatario deberá responder, en un plazo no superior a 5 días laborables, cuando podrá comenzar los trabajos y el tiempo estimado que le llevaría ejecutarlos.

3. Tras el análisis de la propuesta de plazos, y si estos se consideran adecuados por INTECO, el Director Técnico de INTECO proporcionará al adjudicatario todo lo necesario para la correcta realización de la auditoría/s: la información, documentación, código fuente si necesario, etc. En el caso de no poder facilitar un entorno de ejecución para la realización de las pruebas, el adjudicatario se encargará de desplegar el entorno de pruebas.

4. El adjudicatario realizará la auditoría/s según su propia metodología (1ª iteración), que tendrá que ser descrita en la oferta por los licitadores. Una vez finalizada la auditoría/s, el adjudicatario enviará un informe completo al Director Técnico de INTECO.

5. El informe de auditoría será revisado por INTECO, que si lo ve necesario podrá convocar una reunión con el equipo de auditoría del adjudicatario, que podrá ser a través de audio o video-conferencia, y en la que podrá contar con el proveedor de desarrollo de la aplicación auditada, u otras partes implicadas según criterio de INTECO.

6. El Director Técnico de INTECO procederá a dar el visto bueno a la auditoría, o propondrá los cambios pertinentes que tendrán que ser revisados y realizados por el adjudicatario. En caso de que INTECO considere que el informe no tiene la calidad adecuada, podrá justificárselo al adjudicatario y devolverle el informe, no considerándose por tanto el trabajo como realizado.

7. Una vez aceptado el informe por el Director Técnico de INTECO, se planificarán los trabajos de corrección de la aplicación y la posterior verificación de las correcciones por parte del adjudicatario (2ª iteración).

8. El Director Técnico de INTECO facilitará una nueva versión de la aplicación corregida al adjudicatario.

9. El adjudicatario verificará que las correcciones han sido realizadas emitiendo un nuevo informe. En el caso de no estar conforme con la solución aplicada, emitirá nuevas recomendaciones para la solución correcta de las vulnerabilidades detectadas.

Tal y como se ha establecido en el punto 3, los licitadores incluirán en su oferta la metodología a seguir durante los análisis y evaluaciones de las aplicaciones y, en concreto, cuáles serán los métodos o técnicas utilizados para definir y abordar los trabajos.

Los licitadores incluirán además el nombre y características de las herramientas que utilicen como soporte.

2.3.2. Documentación entregable

El adjudicatario deberá proporcionar a INTECO dos informes de auditoría de seguridad por aplicación. El primer informe corresponderá a la primera iteración y el segundo informe, basado en el anterior, se corresponderá con la segunda iteración.

En el caso de ser requerida auditoría dinámica y auditría estática sobre la misma aplicación, se generará un único informe por iteración con los resultados de ambas auditorías relacionados.

Los informes de auditoría incluirán, como mínimo, los siguientes apartados:

- Objeto y alcance de la auditoría.
- Metodología empleada: análisis realizado, clasificación de vulnerabilidades y estado de seguridad del aplicativo.
- Resultados obtenidos: vulnerabilidades detectadas, descripción de las vulnerabilidades, evidencias y recomendaciones de solución.
- Otras consideraciones: todas aquellas observaciones relacionadas con seguridad u otras características de la aplicación (funcionalidad, eficiencia, etc.) que hayan sido detectadas en las auditorías y que se consideren relevantes para el correcto funcionamiento de la aplicación.
- Conclusiones: resumen de las principales vulnerabilidades detectadas y recomendaciones de mejora de la aplicación.

3. DIRECCIÓN Y SEGUIMIENTO DE LOS TRABAJOS

Corresponde a la Dirección Técnica del proyecto, la completa supervisión y dirección de los trabajos, proponer las modificaciones convenientes o, en su caso, proponer la suspensión de los mismos si existiese causa suficientemente motivada.

Para la supervisión de la marcha de los trabajos, INTECO indicará al comienzo del proyecto, la persona designada como Director/a Técnico/a del proyecto. Sus funciones en relación con el presente Pliego serán:

a) Velar por el adecuado cumplimiento de los servicios contratados.

b) Emitir las certificaciones parciales de recepción de los mismos.

c) Fijar reuniones periódicas entre la Sociedad y el adjudicatario con el fin de determinar, analizar y valorar las incidencias que, en su caso, se produzcan durante la ejecución del contrato.

Independientemente de las reuniones ya establecidas en el Plan de Proyecto, el Director de Proyecto podrá convocar cuantas reuniones de seguimiento del proyecto considere oportunas para asegurar el cumplimiento del calendario del proyecto así como la correcta consecución de los objetivos propuestos. El adjudicatario será responsable de la redacción y distribución de las correspondientes actas de reunión.

Con el fin de garantizar que se satisfacen las necesidades y prioridades establecidas por el Director de Proyecto, este marcará las directrices de los trabajos a realizar, siendo estas directrices de obligado cumplimiento por parte del adjudicatario.

Durante el desarrollo del proyecto se podrán solicitar, como parte de las tareas de seguimiento y control, entregas intermedias que permitan tanto la verificación del trabajo realizado, como reducir y evitar riesgos a lo largo del proyecto.

La rectificación de los trabajos no aceptados no se computarán como nuevos servicios realizados por el adjudicatario.

Las rectificaciones derivadas de decisiones sobrevenidas que no tengan como origen errores u omisiones del adjudicatario, si se podrán computar como nuevos servicios realizados por el adjudicatario.

4. FORMA DE EJECUCIÓN

4.1. LUGAR DE REALIZACIÓN DE LOS TRABAJOS

El adjudicatario deberá realizar el trabajo en las instalaciones de la adjudicataria, salvo acuerdo en contrario para casos especiales por motivos de seguridad y confidencialidad.

4.2. OBLIGACIONES DE INFORMACIÓN Y DOCUMENTACIÓN

Durante la ejecución de los trabajos objeto del contrato, el adjudicatario se compromete, en todo momento, a facilitar al Director Técnico, la información y documentación completa de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos.

Asimismo el adjudicatario estará obligado a asistir y colaborar, a través del personal que designe a este propósito, en las reuniones de seguimiento del proyecto definidas por el Director Técnico, quién se compromete a citar con la debida antelación al personal del adjudicatario.

Toda la documentación generada por el adjudicatario durante la ejecución del contrato será propiedad exclusiva de INTECO sin que el contratista pueda conservarla, ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización por escrito de INTECO, que la podrá conceder, en su caso y con expresión del fin, previa petición formal del adjudicatario.

Salvo indicación expresa en contrario, las especificaciones, informes, diagramas, planos, dibujos y cualquier otro documento relativo al objeto del contrato, serán aportados en castellano, cualquiera que sea el soporte y/o formato utilizado para la transmisión de información.

4.3. CONTROL ECONÓMICO E HITOS FACTURACIÓN

4.3.1. Control de Facturación

Debido a las características propias del objeto del contrato, la facturación se realizará por cada servicio prestado: por cada auditoría de seguridad o de código o mixta

Se considerará el servicio como prestado cuando el Director Técnico de INTECO de por recibidos y aceptados los entregables resultado de cada servicio.

4.3.2. Hitos de Facturación

Por cada servicio ejecutado y aceptado por el director técnico de INTECO, el adjudicatario deberá emitir una factura por la cantidad correspondiente al servicio prestado.

4.4. CONTROL DE CALIDAD

Sin perjuicio de las obligaciones asumidas en su oferta, el adjudicatario, a través del supervisor designado a tal efecto, deberá seguir los procedimientos de aseguramiento de la calidad existentes en la ejecución del contrato.

El adjudicatario reconoce el derecho de la Sociedad para examinar por medio de auditores, externos o propios, el fiel cumplimiento de los trabajos por él realizados.

INTECO tendrá derecho a llevar a cabo auditorías de las actividades de los adjudicatarios para asegurarse de que la ejecución de los trabajos se lleva de acuerdo con lo establecido en el presente Pliego. Todo el material e información requerida para dichas inspecciones y auditorías por los representantes de la Sociedad estará disponible sin restricciones. La Sociedad notificará al adjudicatario con dos semanas de antelación la auditoría y con un día de antelación la inspección a realizar, y el adjudicatario tendrá la obligación de:

- Facilitar el acceso al material solicitado por el grupo auditor.
- Designar personas responsables que acompañen a los auditores.
- Facilitar un entorno de trabajo adecuado en el mismo lugar en que tiene lugar la auditoría.
- Cooperar con el auditor.
- Participar en las reuniones que convoque el auditor.
- Analizar los datos encontrados para que el informe sea real.
- Emprender rápidamente acciones correctoras y/o preventivas.
- Emitir una respuesta oficial para cada uno de los defectos que haya detectado el grupo de auditores.

5. PRESENTACIÓN DE LAS OFERTAS TÉCNICAS

5.1. Datos generales

La presentación de la documentación para su admisión como licitador supone la aceptación de lo dispuesto en la Instrucción de Contratación de la Sociedad incluida en el Perfil de Contratante y publicada en la web, así como todas las disposiciones del presente Pliego.

Toda la documentación que se presente por los licitadores deberá estar redactada en castellano, salvo los supuestos que hayan podido especificarse en este Pliego de Características Técnicas. En caso de que se presentasen en lengua distinta deberá presentarse la correspondiente traducción oficial a la lengua castellana primando esta última en caso de duda o discrepancia.

De todos los datos que se aporten por el licitador, INTECO podrá exigir la correspondiente justificación documental o aclaraciones antes de la adjudicación, condicionando ésta a que dicha justificación o aclaraciones sean suficientes a juicio de la Sociedad.

En el sobre Nº 2 no debe incluirse la oferta económica, pues es un criterio de adjudicación cuantificable; solo deben incluirse los documentos técnicos expresados en el punto siguiente. La inclusión en el sobre nº 2 de los documentos que deben constar en el sobre 3 es causa de exclusión.

5.2. Formato de la propuesta técnica (sobre nº 2)

Los licitadores deberán presentar una propuesta técnica que deberá contener los siguientes apartados y en el mismo orden:

1. Descripción de los contenidos de cada uno de los entregables a entregar por cada tipo de servicio según el pliego de características generales.

2. Descripción de las metodologías y herramientas que el licitador seguiría para desarrollar cada uno de los tipos de servicio solicitado. Donde sea pertinente, el licitador podrá incluir una comparativa con otras metodologías o herramientas alternativas.

6. CRITERIOS DE VALORACIÓN

La oferta económicamente más ventajosa se determinará según los criterios de valoración recogidos en el anexo VI del Pliego de Características Generales.

León, 24 de julio de 2013.

DIRECTOR GENERAL DE INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN