PLIEGO DE CONDICIONES

Licitación n° CO/10-19 Ad.

TÍTULO: CONTRATACION DE UNA AUDITORÍA DEL SISTEMA INFORMÁTICO DEL CONSEJO OLEÍCOLA INTERNACIONAL.

1. Introducción

El Consejo Oleícola internacional ha iniciado desde hace unos años un proceso de modernización de sus sistemas informáticos.

El objeto de este pliego es auditar la seguridad del sistema informático del COI, así como proponer posibles mejoras al sistema.

Como marco principal para este análisis, y dada la naturaleza de organismo intergubernamental del COI, se ha determinado seguir un estándar público e internacional, de modo que los niveles de exigencia y criterios a comprobar en la auditoría quedan enmarcados en el estándar que establece la ISO/IEC 27002:2005 'Código de buenas prácticas para la gestión de la seguridad de la información', norma que actuará como supletoria de lo establecido en el anexo I "Alcance de los trabajos" del presente pliego. La ejecución en detalle de los trabajos deberá de tomar como marco de referencia por tanto dicha norma.

2. Objeto del contrato

El objeto del presente pliego es la contratación de una auditoría del nuevo sistema informático del COI, así como elaboración de un informe proponiendo soluciones a las incidencias encontradas y posibles mejoras al sistema.
Queda excluido del ámbito de este contrato el ERP del Organismo (SageX3) pues se audita anualmente por la firma que audita los Estados Financieros del Organismo.

Deberán tenerse en cuenta los siguientes puntos, que se detallan en el anexo I:

- Política de seguridad
- Organización y planificación de la seguridad
- Seguridad física
- Autenticación
- Confidencialidad
- Integridad
- Disponibilidad
- Control de Accesos
- Acceso a través de redes
- Protección de soportes de información y copias de respaldo
- Desarrollo y explotación de sistemas
- Gestión y registro de incidencias
- Análisis y gestión de riesgos
- Firma Electrónica
- Plan de contingencias
- Auditoría y control de la seguridad
- Identificación y clasificación de activos a proteger
- Salvaguardas ligadas al personal.

3. PARTICIPACIÓN EN LA LICITACIÓN

La presente licitación está abierta a cualquier persona jurídica que acepte estas condiciones en su totalidad, tenga capacidad de actuación, pueda demostrar su capacidad económica, financiera y técnica o profesional y no tenga ninguna responsabilidad en relación con la Secretaría Ejecutiva del COI.

Asimismo, su objeto social o actividad debe estar directamente relacionada con el objeto del contrato y ha de contar con una estructura empresarial con suficientes recursos humanos y equipamiento para la ejecución del contrato.

2.1. Licitaciones conjuntas

En caso de presentar una licitación conjunta, el licitador debe definir claramente la estructura de la oferta:

2.1.1. Un consorcio ya existente

La oferta la presentan proveedores de servicios que ya han constituido un consorcio como entidad jurídica separada con estatutos y/o reglas de funcionamiento propios y capacidad técnica y financiera independiente, así como contribuciones de los proveedores de servicios definidas. El consorcio será la entidad que asumirá la responsabilidad técnica y financiera del contrato.

2.1.2. Intención de constituir un consorcio

La oferta la presentan proveedores de servicios que aún no han constituido un consorcio como entidad jurídica separada, pero tienen previsto hacerlo de conformidad con el anterior punto 2.1.1. si se acepta su oferta conjunta. En ese caso, el licitador tendrá que facilitar documentación sobre su naturaleza jurídica y la versión preliminar de los estatutos previstos. Asimismo, ha de proporcionar una descripción clara de la modalidad

de funcionamiento del consorcio y de las distintas contribuciones técnicas y financieras de cada proveedor de servicios.

2.2. Subcontratación

Las ofertas presentadas por proveedores de servicios que no deseen constituir un consorcio como entidad jurídica separada se presentarán en forma de subcontratación y, en ese caso, uno de los proveedores de servicios asumirá toda la responsabilidad de la oferta. Dicho proveedor de servicios (“adjudicatario principal”) firmará un contrato a su nombre con las demás empresas o personas físicas que, por tanto, se consideran subcontratistas del “adjudicatario principal”.

Todos los proveedores de servicios que actúen como subcontratistas han de facilitar una declaración firmada reconociendo al proveedor de servicios que

actúa como adjudicatario principal. Asimismo, ha de indicarse la proporción (%) del contrato que se imputa al adjudicatario principal y de cada uno de los subcontratistas.

3. **Alcance de los trabajos**

El alcance de los trabajos a que hace referencia este pliego se encuentra en el Anexo I, en el que se detallan los aspectos que necesariamente tendrá que considerar el informe de auditoría, así como el contenido mínimo que deberá abarcar el informe sobre soluciones a las incidencias encontradas y mejoras del sistema.

4. DESCRIPCIÓN DE LOS REQUISITOS TÉCNICOS Y CUALIFICACIONES PROFESIONALES REQUERIDAS

El adjudicatario deberá cumplir los servicios y prestaciones ofertados, y en todo caso, los detallados en este pliego de condiciones.

El adjudicatario deberá aportar certificaciones, homologaciones, autorizaciones, y en general toda aquella documentación exigida por la legislación vigente para la prestación de los servicios.

El adjudicatario deberá cumplir en todo momento la legislación vigente que le sea de aplicación.

El adjudicatario deberá proveer a su cargo los medios y recursos necesarios para llevar a cabo los servicios y prestaciones ofertados.

El adjudicatario se comprometerá a tratar con estricta confidencialidad toda información y todo documento relacionados con la ejecución del contrato, y a no utilizarlos ni divulgarlos a terceros. El adjudicatario seguirá obligado por este compromiso una vez concluidas las tareas.

El adjudicatario será el responsable de los daños a personas, materiales o terceros por las acciones realizadas en la ejecución del servicio; por lo que deberá disponer de una póliza de seguros con cobertura suficiente para cubrir cualquier tipo de incidencia que pudiera ocurrir en la ejecución de los servicios.

5. CALENDARIO

Está previsto que la auditoría se realice en el cuarto trimestre de 2019. La fecha concreta será fijada de común acuerdo entre las partes.

6. DOCUMENTACIÓN

La documentación se presentará en **tres sobres** cerrados, precintados y sellados que contendrán:

SOBRE 1 – Documentación administrativa:

Se deberán incluir los siguientes datos: nombre del licitador / denominación social de la Sociedad; números de teléfono; dirección de correo electrónico; número de identificación fiscal; persona de contacto; carta de presentación y anexos cumplimentados.

El licitador deberá declarar sobre su honor, utilizando el formulario que aparece en la lista de control, parte F, que su empresa/organización dispone de la capacidad económica, financiera, técnica y profesional necesaria para llevar a cabo los servicios/suministros objeto de la presente licitación

SOBRE 2: Oferta financiera

El precio de las ofertas debe expresarse en euros (cifras y palabras), IVA y demás tributos incluidos.

Los precios ofertados incluirán todos los derechos y obligaciones establecidos en este pliego de condiciones. Asimismo, incluirán todos los gastos en los que incurrirá o pueda incurrir el licitador para la prestación de los servicios en cuestión, en particular los materiales necesarios, el transporte y los viajes, así como los honorarios y sueldos de cualquier empleado.

SOBRE 3: Memoria técnica

La oferta deberá contener una relación detallada, clara y completa de todos los servicios ofertados, así como un calendario de ejecución que refleje la asignación de medios a cada tarea.

7. CRITERIOS DE EXCLUSIÓN

Los licitadores serán excluidos de participar en un procedimiento de adjudicación si:

a) se encuentran en situación concursal, quiebra o en liquidación, están bajo administración concursal o administración judicial, han alcanzado un acuerdo con acreedores, han suspendido sus actividades comerciales, son objeto de procedimientos en relación con dichos asuntos o se encuentran en cualquier otra situación análoga derivada de un procedimiento similar contemplado en la legislación o normativa de carácter nacional;

b) han sido condenados por algún delito relacionado con su conducta profesional mediante sentencia con valor de cosa juzgada (*res judicata)*;
c) han sido declarados culpables de mala conducta profesional grave demostrada por cualquier medio que pueda justificar el órgano de contratación;
d) no han cumplido con sus obligaciones relativas al pago de cotizaciones a la seguridad social o pago de impuestos de cualquier tipo;

e) han recibido una sentencia con valor de cosa juzgada (*res judicata)* por fraude, corrupción, participación en organización criminal o cualquier otra actividad ilegal;
f) en relación con otro proceso de licitación, se les ha condenado por incumplimiento grave y culpable de sus obligaciones contractuales.

8. CRITERIOS DE SELECCIÓN

La selección de los licitadores se realizará en función de su capacidad técnica, profesional, financiera y económica para la ejecución del contrato.

9. CRITERIOS DE ADJUDICACIÓN

Finalmente, se valorarán las ofertas admitidas de conformidad con los siguientes parámetros:

- Precio (50%)
- Metodología de trabajo y equipo puesto a disposición (30%)
- Experiencia en otros trabajos similares (20%)

10. DURACIÓN DEL CONTRATO

El contrato correspondiente entrará en vigor en el momento de su firma y se extinguirá con el cumplimiento por ambas partes de sus obligaciones.

11. PUNTO DE CONTACTO

El punto de contacto autorizado para preguntas sobre la presente convocatoria de licitación es:

Consejo Oleícola Internacional
C/Príncipe de Vergara, 154
28002 Madrid, España
E-mail: iooc@internationaloliveoil.org

Cualquier contacto deberá realizarse por escrito. Las preguntas y las respuestas correspondientes se publicarán en el sitio web del Consejo Oleícola Internacional: http://www.internationaloliveoil.org/

12. VARIOS

El procedimiento de adjudicación se regirá por las condiciones de este pliego de condiciones, los documentos de la oferta, las disposiciones del Reglamento Financiero del Consejo Oleícola Internacional, las disposiciones sobre los procedimientos de ejecución y cualquier otra disposición presente o futura aplicable.

Una vez recibidas las ofertas, la Secretaría Ejecutiva se reserva el derecho de no adjudicar el contrato y renegociar con los licitadores objeto de la mejor evaluación.

Hasta el momento de la firma, el órgano de contratación puede cancelar el procedimiento de adjudicación sin que los candidatos o licitadores tengan derecho a reclamar ninguna compensación. Dicha decisión ha de motivarse y notificarse a los candidatos o licitadores.

La Secretaría Ejecutiva se reserva el derecho a interpretar este pliego de condiciones.

La participación en este procedimiento de adjudicación implica la plena aceptación por parte del licitador de todas las cláusulas contempladas en el pliego de condiciones y cualquier obligación derivada de las mismas.

Anexo I

ALCANCE DE LOS TRABAJOS

Se realizarán dos informes. Cada uno de ellos deberá contener los resultados de la auditoría practicada (en el caso de que aparezcan incidencias se categorizarán como muy grave, grave o leve), las soluciones que se proponen y aquellas mejoras que si ben no son obligatorias sería conveniente realizar (graduándolas entre muy conveniente, conveniente y deseable)

1. PRIMER INFORME

1.1. Política de seguridad

Por política de seguridad se entiende el conjunto de normas, reglas y prácticas, que regulan el modo en que los bienes que contienen información sensible son gestionados, protegidos y distribuidos dentro de una organización. (ITSEC)
La política de seguridad afecta en general a los cuatro subestados de autenticidad, confidencialidad, integridad y disponibilidad.

En relación con la protección de los datos de carácter personal, se tendrá en cuenta un cumplimiento de nivel medio.

1.2. Organización y planificación de la seguridad

La función de seguridad de sistemas de información, con dedicación completa o compartida con otras funciones, incluye unos contenidos de carácter general, como la aplicación de la política de seguridad, desarrollo de normas, sistemas y procedimientos de detección de amenazas, protección de activos y acción ante eventos; así como la administración de la seguridad y de las correspondientes salvaguardas frente a las anomalías antes (preventivas) o cuando se presenten (correctivas).

Se verificará que el personal y la organización de seguridad de IT cumplen con los criterios establecidos por este punto.

1.3. Seguridad física

La seguridad física proporciona protección ante accesos no autorizados, daños e interferencias a las instalaciones de la organización y a la información.
Los requisitos sobre seguridad física varían considerablemente según las organizaciones y dependen de la escala y de la organización de los sistemas de información. Pero son aplicables a nivel general los conceptos de asegurar la protección de ciertas áreas, controlar perímetros, controlar las entradas físicas e implantar equipamientos de seguridad.

Se analizará el nivel existente de protección física del sistema.

1.4. Autenticación

La autenticación se refiere a la capacidad de verificar que un usuario, convenientemente identificado, que accede a un sistema o aplicación es quien dice ser; o que un usuario que ha generado un documento o información es quien dice ser (mediante la firma electrónica, que tiene su propio capítulo aparte).

La identificación de los usuarios y la verificación de la autenticidad de la misma es un requisito previo a la autorización del acceso a los recursos del sistema.

1.5. Confidencialidad

Este apartado trata sobre la protección de la confidencialidad, sin perjuicio de que dicha protección reclama en general tener en cuenta al mismo tiempo a los otros tres subestados de la seguridad (autenticación, integridad o la disponibilidad). En cualquier caso, las medidas de protección han de ser proporcionadas a la naturaleza de los datos y de los tratamientos, los riesgos a los que están expuestos y el estado de la tecnología. En general será precisa la aplicación conjunta de parte o de todos los 'Criterios de seguridad'.

El nivel de seguridad que se desea considerar para este Criterio es de nivel Protegida, con restricciones altas. Se comprobará el cumplimiento de los criterios a este nivel.

1.6. Integridad

En este capítulo se tratan los aspectos más estrechamente relacionados con la protección de la integridad, sin perjuicio de que dicha protección reclama en general tener en cuenta al mismo tiempo a los otros tres subestados de la seguridad (autenticación, confidencialidad y disponibilidad). En cualquier caso, las medidas de protección han de ser proporcionadas a la naturaleza de los datos y de los tratamientos, los riesgos a los que están expuestos y el estado de la tecnología.

El nivel de seguridad que se desea aplicar a este criterio es Alta, por considerarse que el activo de información es de difícil reconstrucción. Se comprobará el cumplimiento de los criterios para este nivel.

1.7. Disponibilidad

En la disponibilidad intervienen múltiples aspectos: unas adecuadas instalaciones y equipamiento físico, un adecuado dimensionamiento de la plataforma tecnológica que permita hacer frente a escenarios variables de carga de trabajo, o posibles fallos, procedimientos de explotación y de mantenimiento,

protección contra código dañino y frente a intentos de intrusión o ataques de denegación de servicio, así como procedimientos relativos a la gestión de la información que pueda almacenarse cifrada o codificada que garanticen la gestión de claves. La eliminación de errores de codificación y la adopción de estándares y especificaciones públicas de programación pueden facilitar el control de la aplicación (software libre).

Se establece como tiempo máximo aceptable de carencia del activo como “72 horas”. Se estimará si las medidas de disponibilidad actuales cumplen este criterio.

1.8. Control de Accesos

Se entienden por privilegios (de acceso) los mecanismos de salvaguarda que permiten a ciertos usuarios alterar los controles de seguridad del sistema o de las aplicaciones. La asignación de privilegios especiales innecesarios es una de las causas de vulnerabilidad más frecuentes en los sistemas que han sufrido ataques, por lo que se deberá controlar mediante un procedimiento formal de autorización de privilegios.
Se analizará la posibilidad de que personas distintas de cada usuario puedan acceder a sus datos sin el permiso del mismo.

1.9. Acceso a través de redes

Se entiende por acceso a través de redes cualquier tipo de comunicación, con los sistemas informáticos o de comunicaciones de una organización, realizada mediante enlaces de telecomunicaciones.

El enfoque de la seguridad en relación con el acceso a través de redes debe contemplar cuestiones como las siguientes:

- ¿En qué medida puede un intruso acceder a los recursos del sistema o de la aplicación desde la red?
- ¿En qué medida estas intrusiones pueden afectar a los datos y a los tratamientos?
- ¿Los datos son fáciles de ser modificados o leídos cuando son transmitidos?

Se analizarán las medidas de protección de ataques, tanto a nivel de aplicación como a nivel de sistema, con el fin de determinar su suficiencia. Para ello se emplearán los criterios marcados en el presente punto.

1.10. Protección de soportes de información y copias de respaldo

La protección de los soportes de información (discos duros, disquetes, cd-rom, cintas, ordenadores portátiles, etc.) debe incluir un conjunto equilibrado de medidas proporcionado a la naturaleza de los datos y documentos que contengan.

En la preparación de los procedimientos de protección de los soportes de información ha de tenerse en cuenta que los ordenadores personales, incluyendo los portátiles, agendas electrónicas, etc., con discos fijos u otros dispositivos de almacenamiento no volátiles, operando de forma aislada o conectados en red, deben ser considerados como dispositivos de almacenamiento de información en el mismo sentido que otros soportes electrónicos de almacenamiento de información extraíbles.

Se determinará la validez de los sistemas y procedimientos relacionados con las copias de respaldo, tanto desde el punto de vista de integridad como desde el punto de vista de confidencialidad, incluyendo un inventario tanto de los procedimientos internos tipificados en el organismo como de los soportes materiales y de software para la ejecución de los mismos. De igual forma se valorará el control de acceso a dichos soportes cuando contienen datos.

Se determinará también si se están llevando a cabo correctamente las pruebas de recuperación de las copias realizadas y si el calendario previsto para las mismas es razonable.

1.11. Desarrollo y explotación de sistemas

En relación con el desarrollo:

- Establecer criterios de aceptación para nuevos sistemas, así como en los desarrollos de nuevas versiones y funciones.
- Para la realización de las pruebas previas a la puesta en explotación (relativas a la seguridad, rendimientos, diseño, etc.) es conveniente la disposición de un entorno de pruebas independiente de los entornos de desarrollo y de explotación.
- En condiciones de determinados requisitos de seguridad cabe desarrollar un Perfil de Protección conforme con los Criterios Comunes de evaluación de la seguridad de las tecnologías de la información.

En relación con la explotación:

- Implantar y mantener actualizado el software de detección y protección ante código dañino y de detección de intrusiones.
- Formar a los usuarios en la utilización adecuada de la aplicación, del software antivirus y en la notificación de incidencias relacionadas con los ataques de este tipo y todo lo relativo a la gestión y responsabilidades relacionadas con el código dañino.

Se valorará y analizará el ciclo de vida de la aplicación, su implantación y soporte en producción, utilizando los criterios de este punto como guia, incluyendo procedimientos de control y gestión de actualizaciones, correcciones de errores, soporte y respuesta rápida ante contingencias.

1.12. Gestión y registro de incidencias

Se trata de una función esencial para el análisis de los problemas informáticos y en especial de los incidentes de seguridad.
Se entiende la 'informática forense' como aquella que se ocupa de investigar los incidentes o intrusiones, una vez que estos ya se han producido, para tratar de averiguar las causas, a los autores y los daños que han conllevado.

Se estudiará y diagnosticará el nivel de registro de todo el sistema, en los diferentes niveles tipificados por este punto, tanto a nivel de aplicación como de sistema y de accesos telemáticos, teniendo en cuenta tanto los registros automáticos como las incidencias notificadas por los usuarios.

2. SEGUNDO INFORME

2.1. Análisis y gestión de riesgos

Se comprobará si existe un estudio de riesgo/impacto que determine los distintos niveles de vulnerabilidad en los que se puede enmarcar el sistema, así como la definición de las medidas que tendría que adoptar el organismo y los riesgos implícitos y explícitos asociados para quedar encuadrado en uno u otro.

2.2. Firma Electrónica

Firma electrónica: La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
(...)

La firma electrónica avanzada basada en certificados reconocidos o los dispositivos seguros de creación de la firma electrónica se utilizarán cuando el correspondiente análisis y gestión de los riesgos así lo aconseje.

Se determinará si, a día de hoy, los sistemas de firma electrónica que utiliza el Organismo cumplen con los estándares de seguridad.

2.3. Plan de contingencias

El plan de contingencias es la forma detallada en que la organización debe reaccionar para asegurar que las aplicaciones sigan activas ante determinados eventos, accidentales o deliberados.

Se analizará si el Plan de contingencias del COI es suficiente, si existe un calendario de pruebas periódicas, si se documenta su utilización y si en base a la experiencia se introducen mejoras. Se analizará si cubre al menos los siguientes puntos y si la manera en que trata estos apartados es razonable:

- Objetivos del Plan.
- Escenarios de desastre y tiempos críticos de recuperación para cada servicio. Establecimiento de criticidades por recurso (equipos, servicios, aplicaciones…).
- Procedimientos de localización de las personas involucradas en el Plan y procedimientos de comunicación existentes (a terceros o a personal interno).
- Identificación de Roles y Responsabilidades del equipo de recuperación ante desastres implicado.
- Procedimientos y jerarquía en la activación de servicios informáticos críticos. Existencia de centro alternativo, en su caso.
- Procedimientos de prueba a realizar para verificar correcta recuperación.
- Procedimientos de vuelta a la situación de normalidad.

Recomendamos, adicionalmente que, una vez elaborado, se someta el mismo a pruebas y actualizaciones periódicas.

2.4. Auditoría y control de la seguridad

Definición de auditoría:
Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar el alcance al que se cumplen los procedimientos o requisitos contra los que se compara la evidencia. (ISO 9000: 2000).

Se verificará la necesidad de establecer un calendario periódico de auditorías (de seguridad, funcionales, etc.) y en caso afirmativo el alcance y la periodicidad del mismo.

2.5. Identificación y clasificación de activos a proteger

El COI mantiene un inventario contable de todos los informáticos propiedad del organismo. Se deberá determinar si este inventario es suficiente o se debería completar con otros atributos como la importancia de cada elemento en términos cualitativos o cuantitativos en función de los requisitos de autenticidad, integridad,

confidencialidad y disponibilidad que le son aplicables. También se deberá determinar si es necesario documentar a qué usuarios se autoriza el acceso y los atributos relacionados con el referido acceso.

2.6. Salvaguardas ligadas al personal

Garantizar que el usuario de datos de carácter personal, esté sensibilizado respecto de los riesgos que puede implicar un tratamiento incorrecto de esta información. Asimismo, conviene instruir a los usuarios acerca de los detalles de la Política de Seguridad de la Organización que les afecten.

Se analizará si la formación que ha recibido el personal respecto de este asunto (riesgos del manejo incorrecto de la información, sobre la obligación de confidencialidad, etc.) es suficiente.

Madrid 2 de octubre

Abdellatif Ghedira
Director Ejecutivo

Príncipe de Vergara, 154
28002 Madrid (España)
iooc@internationaloliveoil.org
Tlf: +34-91 590 36 38
Fax: +34-91 563 12 63