PLIEGO DE CONDICIONES

Licitación N°: CO/2022-06

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

1. INTRODUCCIÓN

El Consejo Oleícola Internacional (en adelante COI) es una organización internacional intergubernamental con personalidad jurídica y sede en Madrid, creada en 1959 bajo los auspicios de Naciones Unidas, que se rige por el Acuerdo Internacional del Aceite de Oliva y de las Aceitunas de Mesa 2015 y cuyas relaciones con España vienen reguladas por el Acuerdo de Sede entre el Reino de España y COI firmado el 28 de noviembre de 2019.

El organismo cuenta con una Secretaría Ejecutiva encargada de administrar el Convenio, con 31 funcionarios y varios becarios de distintos países.

COI ha iniciado desde hace unos años un proceso de modernización de sus sistemas informáticos y sigue adelante con este objetivo.

COI es consciente de que la información es un activo que, al igual que otros activos empresariales importantes, es esencial para su actividad y, en consecuencia, debe protegerse adecuadamente.

2. OBJETO Y ALCANCE DEL CONTRATO

El objeto del presente pliego es la contratación de una auditoría de los actuales sistemas informáticos del COI, la cual incluirá un informe detallado sobre la situación de los mismos y una propuesta de posibles soluciones a las incidencias encontradas, así como una propuesta de posibles mejoras acompañada de un plan que sirva de guía para tener el óptimo nivel de los sistemas informáticos que precisa el COI. El COI está interesado en contratar servicios de auditoría para conocer el estado y la operatividad de sus sistemas informáticos, software y hardware.

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.

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 ‘Código de buenas prácticas para la gestión de la seguridad de la información’, norma que

proporciona una orientación general sobre los objetivos comúnmente aceptados de la gestión de la seguridad de la información.

Hay 114 controles, bajo 35 categorías y 14 cláusulas en la ISO 27002:2013 (La edición de la ISO 27002:2022 ha reducido el número de 114 controles en 14 cláusulas en la edición de 2013 a 93 controles en la edición más reciente de 2022. Sin embargo, el enfoque general sigue siendo el mismo, por lo que el propietario de la oferta debe indicar a qué edición se refiere.

COI va a priorizar algunos controles teniendo en cuenta la criticidad y el nivel de riesgo. En este sentido, a continuación, encontrará las categorías de control sustanciales y los puntos que fueron identificados como obligatorios para la Organización. Además, el resto de categorías y controles indicados en la ISO 27002 se valoran como un activo.

Puntos de control obligatorios se indican en el anexo 1.

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

PRIMER INFORME

1.1 Política de seguridad

1.2 Organización y planificación de la seguridad

1.3 Seguridad física

1.4 Autenticación

1.5 Confidencialidad

1.6 Integridad

1.7 Disponibilidad

1.8 Control de Accesos

1.9 Protección de soportes de información y copias de respaldo

1.10 Desarrollo y explotación de sistemas

1.11 Gestión y registro de incidencias

SEGUNDO INFORME

2.1 Análisis y gestión de riesgos

2.2 Firma Electrónica

2.3 Plan de contingencias

2.4 Auditoría y control de la seguridad

2.5 Identificación y clasificación de activos a proteger

2.6 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.

3.1. Licitaciones conjuntas

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

3.1.1. 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.

3.1.2. 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.

3.2. 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.

3.3. 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.

3.4. CALENDARIO

En principio, está previsto que cada auditoría anual tenga lugar antes de la sesión de noviembre del Consejo de Miembros. La auditoría podría tener lugar antes a petición del COI. La fecha concreta se fijará de común acuerdo entre las partes. Cualquier modificación del calendario acordado deberá ser aprobada previamente por el COI.

3.5. DOCUMENTACIÓN

La documentación se presentará en **cuatro 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.

SOBRE 4: Copia Electrónica

Incluirá UNA copia en soporte digital - tipo USB - del contenido íntegro DE CADA UNO de los tres sobres anteriores. Cada uno de los 3 soportes (USB) irá a su vez DENTRO un sobre cerrado, y todos los sobres dentro del sobre 4, con las siguientes anotaciones:

SOBRE 1 – Pen drive con la Documentación Administrativa
SOBRE 2 – Pen drive con la Oferta Financiera
SOBRE 3 – Pen drive con la Memoria Técnica

3.6. 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.

3.7. 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.

3.8. CRITERIOS DE ADJUDICACIÓN

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

- Precio (50%)
- Equipo puesto a disposición (sus experiencia, formación, habilidades, etc.) (10%)
- Metodología de trabajo y cumplimiento del anexo I (20%)
- Experiencia en otros trabajos similares (10%)
- Puntos de control adicionales ofrecidos de acuerdo con la norma ISO 27002 (10%)

3.9. 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. Se realizará un contrato marco con una duración máxima de cuatro años. Para cada pedido específico, se firmará un bono de pedido.

Los precios establecidos en la oferta no podrán variar o podrán revisarse. El incremento no podrá superar la subida del índice de precios al consumo en los últimos doce meses según los datos oficiales facilitados por el Instituto Nacional de Estadística de España para el índice general.

3.10. 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 *https://www.internationaloliveoil.org/*

3.11. 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).

PRIMER INFORME

1.1. Política de seguridad

El objetivo es proporcionar dirección y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos de la empresa y las leyes y reglamentos pertinentes.

La dirección debe establecer una dirección política clara en línea con los objetivos de la empresa y demostrar su apoyo y compromiso con la seguridad de la información mediante la emisión y el mantenimiento de una política de seguridad de la información en toda la organización.

La política de seguridad afecta en general a los cuatro subastados de autenticidad, confidencialidad, integridad y disponibilidad.

El documento de política de seguridad de la información debe declarar el compromiso de la dirección y establecer el enfoque de la organización para gestionar la seguridad de la información. Esta política de seguridad de la información debe comunicarse en toda la organización a los usuarios de una forma que sea pertinente, accesible y comprensible para el lector previsto.

El objetivo es proporcionar dirección y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos de la empresa y las leyes y reglamentos pertinentes.

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

El objetivo es gestionar la seguridad de la información dentro de la organización. Debe establecerse un marco de gestión para iniciar y controlar la aplicación de la seguridad de la información en la organización.

La dirección debe aprobar la política de seguridad de la información, asignar funciones de seguridad y coordinar y revisar la aplicación de la seguridad en toda la organización. La implantación de los controles de seguridad requiere una organización gestionada y la participación informada de todo el personal que trabaja con los sistemas de información. Es este personal el responsable de la operación diaria, de la reacción ante incidencias y de la monitorización en general del sistema para determinar si satisface con eficacia y eficiencia los objetivos propuestos.

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

El objetivo es impedir el acceso físico no autorizado, los daños y las interferencias a las instalaciones y a la información de la organización.

Las instalaciones de procesamiento de información crítica o sensible deben alojarse en zonas seguras, protegidas por perímetros de seguridad definidos, con barreras de seguridad y controles de entrada adecuados. Deben estar físicamente protegidas del acceso no autorizado, los daños y las interferencias.

La protección proporcionada debe ser proporcional a los riesgos identificados.

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.

Principalmente, hay que prestar atención a los 6 puntos siguientes: Perímetro de seguridad física; Controles físicos de entrada; Asegurar las oficinas, salas e instalaciones; Protección contra las amenazas externas y medioambientales; Trabajar en zonas seguras; y Zonas de acceso público, de entrega y de carga.

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.

Se auditarán las normas de seguridad para la gestión de accesos lógicos a los sistemas, así como para la definición de los requisitos de seguridad necesarios en los procesos de autenticación, autorización y registro de los sistemas, redes o aplicaciones.

1.5. Confidencialidad

El término "confidencialidad" significa preservar las restricciones autorizadas de acceso y divulgación, incluidos los medios para proteger la privacidad personal y la información de propiedad. Confidencialidad hace referencia a la habilidad para proteger, haciéndolos no visibles o no disponibles, los datos de aquellos que no están autorizados a acceder a ellos.

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 subastados 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

El término "integridad" significa la protección contra la modificación o destrucción indebida de la información, e incluye la garantía de no repudio y autenticidad de la información. Integridad hace referencia a la habilidad de prevenir la modificación de los activos por aquellos que no están autorizados o que estándolo los modifican de forma incorrecta. Esta habilidad implica la posibilidad de revertir o deshacer los cambios realizados.

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 subastados 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

Disponibilidad hace referencia a la capacidad de poder acceder a los activos informativos en el momento en que se necesiten y de poder usarlos correctamente (aquellos debidamente autorizados).

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.

No se incluyen las pruebas DDOS.

1.8. Control de Acceso

El acceso a la información, a las instalaciones de procesamiento de la información y a los procesos empresariales debe controlarse en función de los requisitos empresariales y de seguridad.

Las normas de control de acceso deben tener en cuenta las políticas de difusión y autorización de la información.

En lo que respecta a la gestión de los accesos de los usuarios y a las responsabilidades de los mismos, hay que comprobar los siguientes puntos:
- Debe existir un procedimiento formal de registro y cancelación de usuarios para conceder el acceso a todos los sistemas y servicios de información;
- La asignación y el uso de cualquier privilegio en el entorno del sistema de información debe estar restringido y controlado, es decir, los privilegios se asignan en función de la necesidad de uso, los privilegios se asignan sólo después de un proceso de autorización formal;
- La asignación y reasignación de contraseñas debe ser controlada a través de un proceso formal de gestión, y se debe pedir a los usuarios que firmen una declaración de confidencialidad de la contraseña. Si existe un proceso para revisar los derechos de acceso de los usuarios a intervalos regulares. Ejemplo: Revisión de privilegios especiales cada 3 meses, privilegios normales cada 6 meses.
- Los usuarios y contratistas deben conocer los requisitos y procedimientos de seguridad para proteger los equipos desatendidos (Ejemplo: Cerrar la sesión cuando se termine o establecer la desconexión automática, terminar las sesiones cuando se terminen, etc.,),
- La política de escritorio claro con respecto a los papeles y medios de almacenamiento extraíbles y la política de pantalla clara con respecto a la instalación de procesamiento de información son importantes para la Organización.

En lo que respecta al control de acceso a la red, deben comprobarse los siguientes puntos:
- Si los usuarios tienen acceso sólo a los servicios que han sido específicamente autorizados a utilizar.
- Si existe una política que aborde los problemas relacionados con las redes y los servicios de red.
- Si el acceso físico y lógico a los puertos de diagnóstico está controlado de forma segura, es decir, protegido por un mecanismo de seguridad.

- Si los grupos de servicios de información, usuarios y sistemas de información están segregados en las redes.
- Si la red (en la que los socios comerciales y/o terceros necesitan acceder al sistema de información) está segregada mediante mecanismos de seguridad perimetral como los cortafuegos.
- Si se tiene en cuenta la segregación de las redes inalámbricas de las redes internas y privadas.
- Si existe una política de control de acceso que establezca el control de las conexiones de red para las redes compartidas, especialmente para aquellas que se extienden más allá de los límites de la organización.
- Si la política de control de acceso establece que se deben implementar controles de enrutamiento para las redes.
- Si los controles de enrutamiento se basan en el mecanismo de identificación positiva de origen y destino.

En lo que respecta al control de acceso al sistema operativo, deben comprobarse los siguientes puntos:
- Si el acceso al sistema operativo se controla mediante un procedimiento de inicio de sesión seguro.
- Si se proporciona un identificador único (ID de usuario) a cada usuario, como los operadores, los administradores de sistemas y el resto del personal, incluido el técnico.
- Si se ha elegido una técnica de autenticación adecuada para corroborar la identidad declarada del usuario.
- Si las cuentas de usuario genéricas se suministran sólo en circunstancias excepcionales en las que hay un claro beneficio comercial. Pueden ser necesarios controles adicionales para mantener la responsabilidad.
- Si existe un sistema de gestión de contraseñas que aplique varios controles de contraseñas como: contraseña individual para la rendición de cuentas, aplicar cambios de contraseñas, almacenar las contraseñas de forma encriptada, no mostrar las contraseñas en pantalla, etc.,
- Si los programas de utilidad que podrían ser capaces de anular los controles del sistema y de la aplicación están restringidos y estrechamente controlados.
- Si la sesión inactiva se cierra después de un período definido de inactividad.
- (En algunos sistemas se puede prever una forma limitada de tiempo de espera, que borra la pantalla e impide el acceso no autorizado, pero no cierra la aplicación o las sesiones de red.
- Si existe una restricción del tiempo de conexión para las aplicaciones de alto riesgo. Este tipo de configuración debería considerarse para las aplicaciones sensibles para las que los terminales están instalados en lugares de alto riesgo.

En lo que respecta al control de acceso a la información y a las aplicaciones, deben comprobarse los siguientes puntos:
- Si el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de apoyo está restringido de acuerdo con la política de control de acceso definida.
- Si los sistemas sensibles cuentan con un entorno informático dedicado (aislado), por ejemplo, si se ejecutan en un ordenador dedicado, si comparten recursos sólo con sistemas de aplicaciones de confianza, etc.,

En cuanto a la informática móvil y el teletrabajo, deben comprobarse los siguientes puntos:
- Si existe una política formal y se adoptan las medidas de seguridad adecuadas para protegerse contra el riesgo de utilizar la informática móvil y los medios de comunicación. Algunos ejemplos de instalaciones de computación y comunicaciones móviles son: ordenadores portátiles, ordenadores de bolsillo, tarjetas inteligentes, teléfonos móviles. Si la política de informática móvil tiene en cuenta riesgos como el de trabajar en un entorno desprotegido.
- Si la política, el plan operativo y los procedimientos se desarrollan y aplican para las actividades de teletrabajo.
- Si la actividad de teletrabajo está autorizada y controlada por la dirección y si se asegura de que existen disposiciones adecuadas para esta forma de trabajo.

1.9. Protección de soportes de información y copias de respaldo

Se auditarán los intercambios de información en formato electrónico, ya sea dentro de la organización como con organizaciones ajenas a éste, evitando así la pérdida, modificación o mal uso de dicha información durante todo el proceso.

Se comprobará que se realizan regularmente copias de seguridad de la información contenida en los sistemas TIC. La frecuencia con la que se realicen las copias de seguridad depende de la criticidad de la información, de la frecuencia con que nueva información es introducida en el sistema, y de los parámetros establecidos en cada proceso de negocio.

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.

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.

1.10. 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.

1.11. 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

Las tareas de análisis y gestión de riesgos no son un fin en sí mismas, sino que se

encajan en la actividad continua de gestión de la seguridad.

El Análisis de Riesgos permite determinar cómo son, qué valoración y cómo de protegidos se encuentran los activos. En coordinación con los objetivos, estrategia y política de la Organización, las actividades de gestión de riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta y asume la organización.

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

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

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 auditará el análisis de impacto en el negocio después de la evaluación de riesgos anual de toda la organización. Cuando se realiza un análisis de impacto en el negocio, el proceso incluirá no solo una especificación del período máximo que la empresa puede pasar sin los servicios de procesamiento de información involucrados, sino que también incluirá un análisis de las pérdidas financieras potencialmente incurridas durante la interrupción, una evaluación de riesgo residual cualitativa y un análisis de criticidad de activos.

Con esto, se definirán los requisitos de Continuidad del Negocio por lo que los responsables evaluarán los riesgos asociados a la Continuidad y a la Disponibilidad del servicio además de identificar los requisitos de Continuidad y Disponibilidad, teniendo en cuenta los Planes de negocio aplicables, SLA's y riesgos.

La Continuidad y la Disponibilidad del servicio deben incluir al menos los siguientes requisitos:

► Derechos de acceso
► Tiempo de respuesta

Disponibilidad extremo a extremo

Como parte del ciclo de desarrollo de sistemas, todos los sistemas informáticos de información deben ser evaluados para determinar el conjunto mínimo de controles, el coste/beneficio de dichos controles y el presupuesto requerido para mitigar y mantener riesgo a un nivel aceptable para el (los) proceso(s) comercial(es) involucrados. Este análisis se realizará en la fase de diseño preliminar para cualquier sistema nuevo y antes de cualquier cambio significativo en cualquier sistema de producción.
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

Comprobar 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.

Se propone un cuestionario sencillo de 10-15 preguntas para obtener información sobre el grado de concienciación del personal.

SISTEMAS ANALIZADOS

Sobre las aplicaciones seleccionadas, se inspeccionarán los siguientes componentes de los sistemas:

Familia	Descripción
Componentes de entradas / salidas	Las funciones de entrada/salida son puntos de intercambio de datos con otras aplicaciones o del entorno externo, facilitando así la inserción de datos malintencionados y la filtración de información confidencial. Este es el caso por ejemplo de las funciones de lectura y escritura en el sistema.
Servlets	La mayoría de estas funciones puede recibir parámetros directamente de peticiones http, por lo que los códigos vulnerables a ataques (encabezados, URLs, respuesta HTTP), se suelen utilizar para el transporte de los ataques.
Conectores de base de datos y SQL	Funciones de ejecución de consultas SQL para los ataques de inyección de código para la realización de acciones ilegítimas (divulgación, alteración o supresión de datos).
SSL / criptografía	Los códigos que usen SSL para comunicaciones seguras pueden ser reutilizados para robar una identidad, revelar secretos de conexión o descifrar datos.

Cookies y sesiones de gestión	Las sesiones de usuario y las cookies pueden utilizarse por un atacante fraudulentamente para acceder a una cuenta o recuperar información confidencial almacenada en sesión, por ejemplo variables.
Ejecución de código	La ejecución de código permite ejecutar comandos ilegítimos (inyección OS), facilitando la intrusión en un sistema o información de robo
Funciones de los registros	Los datos contenidos en los registros pueden contener información sensible (datos bancarios, datos personales, etc.). Además, el mal manejo de los registros puede conducir a una saturación de espacio en disco provocando una denegación de servicio.

Herramientas y utilidades

Los siguientes tipos de herramientas (lista no exhaustiva) suelen usarse en los prueba de intrusión propuestos:

Generador de paquetes:

- Herramienta para generar *y* enviar paquetes IP
- Herramientas para la determinación de las rutas utilizadas por los paquetes ICMP / UDP
- Herramienta para el envío de paquetes ICMP específicos

Analizador de tráfico:

- Herramientas para capturar tráfico de red
- Herramienta para analizar *y* modificar sobre la marcha las solicitudes HTTP
- Herramienta para capturar las contraseñas que circulan por la red

Escáner de Puertos:

- Herramientas para la determinación los puertos abiertos en una máquina
- Herramienta de búsqueda de servicios SNMP

Identificación del sistema (Fingerprinting)

- Herramienta para identificar sistemas operativos mediante un análisis

TCP

- Herramienta para identificar la huella OS a través de paquetes TCP – IP stack *y* servicios accesibles
- Herramienta para identificar las versiones de los servicios accesibles a través de un puerto
- Herramienta para identificar el equipo utilizando el protocolo IKE.

Escáner de vulnerabilidades:

- Analizador de sistema de vulnerabilidades
- Vulnerabilidades Web Scanner

Explotación de vulnerabilidades

- Colección de exploits y códigos maliciosos públicos
- Colección de exploits y códigos maliciosos desarrollados específicamente (Shell, Perl, Python)
- Herramientas de confirmación de vulnerabilidad
- Herramientas de generación de código malicioso (inyección de SQL, java,...)

Determinación de contraseñas

- Herramienta para obtener contraseñas en Windows
- Herramienta para conseguir un puesto de Windows LSA secretos
- Contraseña rompiendo herramienta basada en Windows «previamente calculados» diccionarios
- Herramientas de craqueo de contraseñas
- Craqueo herramienta de huella digital MD5
- Herramienta para recuperar la contraseña de una identificación mediante un ataque de diccionario
- Herramientas para llevar a cabo ataques de diccionario en diferentes servicios (http, POP, FTP, Telnet,...)
- Herramientas para realizar ataques de diccionario en un servicio de Terminal Server.
- Herramienta para atacar servicios VNC
- Herramienta para obtener una contraseña VNC en registro
- Herramienta para obtener las contraseñas de equipos Cisco
- Herramienta para romper claves wifi WEP/WPA

- Disco de arranque para reemplazar cualquier contraseña de Windows

Herramientas de redes

- Cliente para consulta de bases de datos Whois
- Clientes para hacer peticiones de red
- Herramienta para realizar las consultas DNS
- SSH client para conectarse a un servidor SSH y el establecimiento de túneles
- Herramienta para las conexiones TCP y UDP en puertos
- Herramientas para redirigir los puertos TCP y UDP
- Herramienta para hacer un túnel SSL
- Herramienta para obtener un Shell remoto mediante inyección HTTP

Herramientas Netbios

- Conjunto de herramientas para realizar diversas acciones en Netbios (obtener una línea de comandos, lista de los procesos activos, iniciar un servicio remoto,...)
- Herramienta para la captura de contraseñas de red, enumerar los usuarios mediante sesiones y tomar el control del sistema a distancia
- Conjunto de herramientas para establecer conexiones Netbios
- Conjunto de herramientas de información de Netbios

Procesos para el análisis de la información obtenida y elaboración de los informes de resultados

Análisis de riesgo

Los análisis de riesgos se inspiran y se ajustan a la norma internacional ISO 27005. A continuación se describen las escalas de criterios que se pueden utilizar para analizar y cuantificar los riesgos, y así ayudar en la toma de decisiones de la Organización.

Estas escalas nos sirven para clasificar tanto las evidencias encontradas en los pruebas de intrusión como en las consultorías internas.

Criticidad

El nivel de criticidad (o gravedad) de un riesgo es la combinación de la potencialidad

y el impacto asociado con ese riesgo. La escala de valores asociados con el nivel de criticidad es:

Nivel de Criticidad del Riesgo	Descripción
DEBIL	Los riesgos asociados con la vulnerabilidad eran bajos y no es grave
MEDIA	Los riesgos asociados con la vulnerabilidad tienen un nivel apreciable.
ALTO	Los riesgos asociados con la vulnerabilidad tienen un nivel significativo.
CRÍTICO	Los riesgos asociados con la vulnerabilidad tienen un nivel crítico.

Potencialidad / explotabilidad

La potencialidad de un riesgo es:

- La probabilidad de ocurrencia de un evento causante del riesgo se materializa por amenazas cuyos orígenes son accidentales y/ o no intencionales.
- La facilidad de explotación de una vulnerabilidad que lleva a la materialización del riesgo de amenazas maliciosas originales y/ o intencionales.

La escala de valores asociados con el nivel de potencialidad se muestra a continuación:

Nivel de Potencialidad	Descripción
DEBIL	El evento tiene un potencial por debajo del 30% de realizarse a corto plazo (1 año) o es un evento con un

	potencial menor de 1 caso cada 3 años. La vulnerabilidad puede ser explotada por una persona con experiencia y/o un nivel de acceso y/o herramientas muy especializadas.
MEDIA	El evento tiene un potencial de entre el 30% y el 60% de realizarse a corto plazo (1 año) o es un evento con un potencial de entre 1 caso cada 3 años y 1 caso cada 1,5 años. La vulnerabilidad puede ser explotada por una persona con experiencia y/o un nivel de acceso y/o herramientas especializadas.
ALTO	El evento tiene un potencial de entre el 60% y el 90% de realizarse a corto plazo (1 año) o es un evento con un potencial de entre 1 caso cada año, y un caso cada 1,5 años. La vulnerabilidad puede ser explotada por una persona con experiencia y/o un nivel de acceso y/o herramientas básicas.
CRÍTICO	El evento tiene un potencial casi seguro (>90%) a realizarse en el corto plazo (1 año). La vulnerabilidad puede ser explotado por cualquier individuo, casi automáticamente, la explotación no requiere de habilidades o de un nivel de acceso a recursos importantes.

Impacto

Los impactos de riesgo son las consecuencias negativas sobre la actividad de la organización, desde la realización de valores risque. La escala asociada con el impacto es la siguiente:

Nivel de Impacto	Descripción
DEBIL	El impacto del riesgo en la actividad de la organización es débil y poco problemático (las actividades de la organización no se ven afectadas)
MEDIA	El impacto del riesgo en la actividad de la organización es significativa (las actividades de la organización sufren una alteración perceptible)
ALTO	El impacto del riesgo en la actividad de la organización es muy importante (las actividades de la organización sufren una perturbación importante)
CRÍTICO	El impacto del riesgo en la actividad de la organización es crítico (afecta a la actividad de la organización de manera vital)

Prioridad

La prioridad pretende definir el período de aplicación de la recomendación.

La escala de valores asociados a la prioridad es la siguiente:

Prioridad	Explanación
PLANIFICAR	Para ser implementado dentro de 1 a 6 meses.
URGENTE	Para ser implementado en un plazo inferior a tres meses.
IMMEDIATA	Para ser implementado en un plazo de menos de un mes.

Indicadores CVSS v2

Para el caso concreto de valoración de las vulnerabilidades identificadas en los sistemas, se sigue el estándar internacional CVSS.

SCORING CVSS					
CVSS Base score:					
Vector de acceso	Complejidad de acceso	Autenticación	Impacto de confidencialidad	Impacto de integridad	Impacto de disponibilidad
CVSS Temporal score:					
Explotabilidad		Nivel de Remedio		Informe de confianza	
OVERALL CVSS SCORE:					

Madrid, … de junio de 2022

Abdellatif Ghedira

Director Ejecutivo