



**CONDICIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SERVICIO DE REDACCIÓN DE UN PLAN DE ACCIÓN INTEGRADO PARA LA ADAPTACIÓN DEL CONSORCIO AL ESQUEMA NACIONAL DE SEGURIDAD, AL REGLAMENTO DE DESARROLLO DE LA LOPD Y A LA LEGISLACIÓN DE INFRAESTRUCTURAS CRÍTICAS, Y DE UN PLAN DE CONTINUIDAD DE NEGOCIO**

Por un importe de 22.000 € IVA excluído (26.620 € con el 21% de IVA incluído), el servicio a contratar tendrá las siguientes características técnicas mínimas:

**CARACTERÍSTICAS GENERALES**

- El Consorcio pretende contratar un servicio de consultoría consistente en la preparación, redacción y entrega de dos documentos:
  - un Plan de Acción Integrado que agrupe, de forma lógica, todas las actividades que el Consorcio deberá realizar con posterioridad para llegar al cumplimiento legal del Esquema Nacional de Seguridad, el Reglamento de Desarrollo de la LOPD y a la legislación de infraestructuras críticas
  - un Plan de Continuidad de Negocio, que especifique los procesos que el Consorcio considera críticos, los activos protegibles, las medidas de seguridad a implantar, y las tareas o actividades necesarias para ello.
- Asimismo, el objeto de este contrato incluirá también los servicios siguientes a prestar por el adjudicatario:
  - seis meses de soporte telefónico con los redactores de ambos documentos para la resolución de dudas durante la implantación de las medidas propuestas.
  - impartición de sesiones de concienciación para el personal del Consorcio, un mínimo de cuatro sesiones, de una duración estimada mínima de dos horas cada una, y cuya organización y planificación temporal correrá a cargo del Consorcio.
  - impartición de una sesión de formación para el personal de TI del Consorcio, de un mínimo de 4 horas, donde se expliquen en detalle las cuestiones más relevantes de ambos documentos.
  - sólo en el caso de que se aporte en la oferta del adjudicatario, sin coste adicional alguno para el Consorcio, algún software para la gestión de los planes redactados o del soporte a las actividades a realizar, se formará al personal técnico del Consorcio encargado de su manejo. En este caso, deberán quedar claras en la oferta del licitante las condiciones de uso de esa licencia o servicio, particularmente, la duración de la suscripción a ese hipotético servicio o del soporte de la aplicación, la titularidad de la licencia, en su caso, etc.



### **SOBRE EL PLAN DE ACCIÓN INTEGRADO**

- Para la redacción del Plan de Acción Integrado (PAI) para el cumplimiento del Esquema Nacional de Seguridad, el Reglamento de Desarrollo de la LOPD y a la legislación de infraestructuras críticas, el adjudicatario recopilará la información necesaria para conocer en detalle la situación del nivel de cumplimiento legal actual del Consorcio en cada uno de estos apartados. Dicha recopilación de información provendrá tanto de entrevistas con personal, como de documentos del Consorcio, de otro tipo de evidencias recopiladas in situ por el adjudicatario, y de otras fuentes de acceso público, si así se considera oportuno.
- Con todas esas evidencias, el adjudicatario redactará un breve documento de trabajo en el que se indicarán los incumplimientos legales detectados, la norma incumplida, y las posibles medidas correctoras. Este documento de trabajo se discutirá con los responsables del proyecto en el Consorcio para acordar cómo enfocar la redacción del documento final del PAI.
- En este punto, se tendrá en cuenta que, como parte de este mismo proyecto, se va a redactar un Plan de Continuidad de Negocio, por lo que las actividades que se incluyan en el PAI deberán tenerlo en cuenta, para ser un Plan completo y coherente. Asimismo, en lo que pudiese afectar, en su caso, se tendrá en cuenta el RD 4/2010, Esquema nacional de Interoperabilidad y sus Normas técnicas de Desarrollo.
- Finalmente, el adjudicatario redactará un borrador de un Plan Integrado de Acción para el cumplimiento legal de las normas objeto de este contrato, de forma detallada, en el que, para cada actividad incluida en el Plan se indicará, al menos, la siguiente información:
  - Identificador único de actividad
  - Nombre de la actividad
  - Descripción detallada de en qué consiste la actividad a realizar, las posibles alternativas para su realización (si las hay), una comparativa de ventajas e inconvenientes de cada alternativa, y los costes y/o recursos asociados estimados
  - No Conformidades que se resuelven, total o parcialmente, con esta actividad
  - Otras actividades del Plan de la que depende la actividad

En este primer borrador del Plan, se incluirán también una propuesta de priorización de las actividades.

- El primer borrador del Plan de Acción Integrado se discutirá con el personal del Consorcio responsable del Proyecto, acordándose las modificaciones que fuesen necesarias en el documento, tantas veces como fuese necesario.
- Finalmente, se entregará el documento, en su redacción final, del Plan de Acción Integrado . Éste Plan será presentado por el adjudicatario ante el Comité de Gerencia, que propondrá su aprobación por la Presidencia-Delegada, si lo estima oportuno.

### **SOBRE EL PLAN DE CONTINUIDAD DE NEGOCIO**

- Para la redacción del Plan de Continuidad de Negocio (PCN), inicialmente el adjudicatario realizará, aprovechando al máximo las entrevistas con personal del Consorcio para la



redacción del PAI anteriormente citado, un Análisis de Riesgos (RA) y un Análisis de Impacto en el Negocio (BIA).

- Análisis de Riesgos: estudio de las causas de las posibles amenazas y probables eventos no deseados, y de los daños y consecuencias que éstas puedan producir en la infraestructura de TI que da soporte a los procesos del Consorcio.
- Análisis de Impacto en el Negocio: conocer la relación entre la tecnología existente, los servicios ofrecidos por el departamento de TI y los procesos de negocio que los utilizan.
- Con esta información como base, el adjudicatario realizará un estudio de los escenarios y estrategias de Continuidad de Negocio, que se discutirán con el personal responsable del Proyecto en el Consorcio, y que se someterán a la aprobación de la Dirección del Consorcio, como requisito previo para la continuación del proyecto.
- Con toda la información obtenida, se elaborará un borrador de Plan de Continuidad de Negocio, que incluirá aquellas actividades, tareas, requisitos, sistemas y políticas organizativas y técnicas a poner en marcha para la protección de la continuidad de los procesos críticos del Consorcio. Este borrador será discutido con el personal responsable del Proyecto en el Consorcio, para su máxima adecuación a las necesidades de la organización.
- Antes de su redacción final, el PCN deberá someterse a las pruebas que ambas partes acuerden, de cara a verificar la adecuada graduación de las medidas propuestas, teniendo en cuenta que mientras no se implanten las medidas técnicas y organizativas concretas del PAI y del PCN, de forma práctica es imposible testear completamente el PCN.
- Finalmente, el adjudicatario redactará el Plan de Continuidad de Negocio, incluyendo en el PAI todo aquellas tareas que considere oportuno y que estén relacionadas con el contenido de aquel. Éste Plan de Continuidad de Negocio será presentado por el adjudicatario ante el Comité de Gerencia, que propondrá su aprobación por la Presidencia-Delegada, si lo estima oportuno.

### FORMACIÓN, CONCIENCIACIÓN Y SOPORTE

- Tras la redacción de ambos Planes, y organizadas por el Consorcio a su conveniencia, el adjudicatario realizará un mínimo de cuatro sesiones de dos horas para la presentación del Plan al personal del Consorcio y para concienciar sobre la imperiosa necesidad de su aplicación y cumplimiento.
- Asimismo, se realizará una sesión formativa específica, de mayor duración y profundidad técnica, para el personal de TI del Consorcio, donde se expliquen los documentos y los requerimientos adicionales que ambos documentos generarán en esta función del Consorcio.
- Desde el momento de la firma del Acta de Recepción, y por un periodo mínimo de seis meses, el adjudicatario prestará soporte telefónico o por correo electrónico, a las dudas o consultas que el personal del Consorcio a cargo del Proyecto les necesite plantear durante la fase de ejecución del PAI o de mantenimiento del PCN.

### EQUIPO HUMANO Y DESARROLLO DEL PROYECTO

- El adjudicatario designará un Responsable del Proyecto, que en la reunión de lanzamiento presentará una primera planificación temporal de las actividades a realizar en el proyecto. Asimismo, en esa reunión también presentará al resto del equipo del adjudicatario que



participará en el Proyecto. La dirección de los trabajos del proyecto estará bajo la responsabilidad del Responsable del Proyecto por el adjudicatario, en coordinación con el Responsable del Proyecto por el Consorcio.

- Tras la reunión de lanzamiento, el adjudicatario presentará una programación temporal, que incluya descomposición de tareas, hitos, y duraciones, de cara a acordar con el Consorcio el calendario de los trabajos.
- El plazo máximo de la ejecución de este proyecto es de seis meses.
- El personal asignado por el adjudicatario al proyecto deberá disponer de certificaciones internacionales en materia de gestión y seguridad en TI, como las certificaciones CISA, CISM y/o CRISC de ISACA, u otras similares. Asimismo, dicho personal deberá contar con una experiencia mínima demostrable de dos años en proyectos relacionados con la Seguridad de la Información, la Auditoría de Sistemas de Información, y/o la Gestión de la Continuidad de Negocio.

### **DECLARACIÓN DE CONFIDENCIALIDAD**

- El ofertante se comprometerá, y así lo hará constar explícitamente en su oferta, a mantener la más estricta confidencialidad sobre cualquier tipo de información relacionada con el proyecto a la que tuviera acceso con motivo de esta colaboración profesional.
- Asimismo, el adjudicatario quedará obligado al cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, especialmente en lo que a su art. 12 se refiere, y a aplicar las medidas de seguridad descritas en el RD 1720/2008, Reglamento de Desarrollo de la LOPD, dependiendo del nivel requerido por los datos personales que el Consorcio le va a proporcionar o que pudiera ser conocedor durante su actividad.

### **PROPIEDAD**

- La propiedad de todos los materiales entregados por el proveedor será exclusiva del Consorcio, entendiéndose como tales la documentación elaborada que se entregue con relación a estas actividades.

### **FORMATOS Y ESTÁNDARES**

- Todos los documentos elaborados durante este proyecto se entregarán en formato ODF, para facilitar posibles trabajos posteriores relacionados con la puesta en marcha del PAI y del PCN.
- Los documentos finales objeto principal de este expediente se entregarán, asimismo, en formato PDF, y firmados digitalmente por el Responsable de Proyecto del Adjudicatario.

### **NORMATIVA DE REFERENCIA**

#### 1. Legislación



- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
- Real Decreto 4/02010, de 8 de enero (BOE de 29 de enero), por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Ley 11/2008, por la que se establecen medidas para la Protección de las Infraestructuras Críticas
- Real Decreto 704/2011, por la que se aprueba el Reglamento para la Protección de las Infraestructuras Críticas

## 2. Normativa técnica

- ISO/IEC 27001: Sistema de gestión de la seguridad de la información.
- ISO/IEC 27002: Código de práctica. Gestión de seguridad de la información.
- ISO/IEC 27031: Tecnología de información - Técnicas de seguridad - Guías para preparación de tecnologías de información y comunicaciones para continuidad de negocios.
- ISO/PAS 22399: Guía para la preparación frente a incidentes y la gestión de continuidad operacional.
- ISO/IEC 24762: Directrices para los servicios de recuperación de desastres de las tecnologías de información y comunicaciones.
- ISO/IEC 22301: Gestión de la Continuidad de Negocio
- ISO/IEC 20000 Gestión de servicios de TI.

Valencia, 10 de febrero de 2015  
El Responsable de la Unidad de Sistemas  
e Innovación Tecnológica

Fdo.: Manuel D. Serrat Olmos

