Universidad Complutense

PLIEGO DE PRESCRIPCIONES TÉCNICAS

"Servicio de asistencia y asesoramiento para el cumplimiento de la normativa de seguridad asociada al Esquema Nacional de Seguridad (ENS)"

2016

INDICE

1 OBJETO DEL CONTRATO

El presente documento recoge los requisitos para la contratación de unas jornadas de soporte para dar cumplimiento legal de la normativa de seguridad asociada al Esquema Nacional de Seguridad (ENS)" consistentes en la ejecución de diversas actividades que garanticen la correcta implantación y seguimiento de los requisitos asociados a dicha normativa:

- 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 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.

La UCM ha detectado la necesidad de contar con unos servicios expertos que, por un lado, ayuden a identificar las acciones necesarias para cumplir con los requisitos del ENS y, por otro, presten un apoyo permanente a la implantación y mantenimiento de dichos requisitos, contribuyendo, en definitiva, a la gestión de la Seguridad de la Información.

2 DESCRIPCION DE LOS TRABAJOS

La contratación tendrá por objeto el disfrute de una **bolsa de jornadas/horas específica** para la realización de diferentes tareas con el fin de dar cumplimiento legal y normativo en lo referente al Esquema Nacional de Seguridad y otra **bolsa de horas general** para tareas extras (extraídas del perfil de consultor).

El esquema de asistencia planteado es el que se indica a continuación:

- 1. Análisis y Diagnóstico de Seguridad. Se partirá del que ya existe y se ampliará y modificará con nuevos servicios a acordar entre las partes (contemplando los actuales cambios en el ENS).
- 2. Plan de Seguridad: partiendo del análisis se rediseñará la hoja de ruta de implantación del ENS y gestión de riesgos para los nuevos servicios y contemplando el nuevo ENS.
- 3. Control, seguimiento y soporte a la realización de las Acciones del Plan de Seguridad. Este servicio se prestará de forma presencial: visitas programadas de control y asesoría presencial (basada en bolsa de horas).
- 4. Acciones de auditoría interna del ENS.
- 5. Reporte al órgano competente del ENS sobre el estado de seguridad y publicación de la declaración de conformidad del ENS en sede electrónica.

- 6. Puesta a disposición y utilización durante toda la duración del proyecto de una herramienta de soporte a la gestión del ENS basada en Opensource.

Conforme a este esquema, y con cargo a **la bolsa de horas específica**, se deberán llevar a cabo las siguientes tareas:

- Realización del Análisis y Gestión de Riesgos para nuevos servicios afectados por el ENS (hasta 4) bajo la metodología MAGERIT y haciendo uso de la herramienta PILAR: Elaboración del Plan de Seguridad.
- Actualización del Plan de Adecuación al ENS conforme a la guía CCN-STIC-806.
- Control, seguimiento y asesoramiento permanente para el cumplimiento de las medidas de seguridad del Plan. Dentro de esta actividad, deberá contemplarse:
    - Visitas programadas para monitorizar el cumplimiento de las acciones del ENS conforme al Plan y prestar soporte presencial.
    - Realización directa de acciones del plan: como mínimo se deberán elaborar los correspondientes a las medidas del marco organizativo del ENS (actualización o elaboración de: política, procedimientos, normativas y procesos de autorización) y definición de indicadores de seguridad (alineados con la guía CCN-STIC 815).
    - Revisión y medida de indicadores que se hayan definido.
    - Soporte para el comité de seguridad de la información bajo demanda: asistencia, revisión de la agenda, generación o revisión de acta y seguimiento de los compromisos establecidos.
    - Divulgación personalizada (según público objetivo) y presencial (en las instalaciones de la UCM) en materia del ENS, incluyendo la difusión de la documentación específica al respecto (política, normas y procedimientos) a través de acciones formativas presenciales y generación de contenidos. Se deberá proponer un calendario de acciones presenciales de formación y divulgación, así como la entrega de material divulgativo de seguridad, para poderlo publicar en diferentes medios (intranet, mailing, etc.).
- Realización de Auditoría Bienal conforme al art. 34 ENS.
- Soporte consultivo a la subsanación de las deficiencias encontradas en la Auditoría del ENS. Deberá indicarse los mecanismos que se ofrecen para este soporte (teléfono, mail, horario de consultas, tiempos de respuesta).
- Soporte en la redacción del Informe del Estado de la Seguridad del año en curso, conforme a la guía CCN-STIC 824.
- Soporte en la creación de la Declaración de Conformidad conforme al art. 41 ENS.

Con cargo a la **bolsa de horas general**, se deberán acometer otras acciones que se requieran bajo demanda, tales como la asistencia a reuniones con proveedores de soluciones técnicas y físicas, soporte a la gestión de contratos con terceros, soporte legal, desarrollo de otra documentación adicional a la indicada en el punto anterior, solicitud de acciones formativas presenciales adicionales, asesoramiento sobre la gestión de incidencias y vulnerabilidades, realización de auditorías técnicas de seguridad/hacking ético.

Los trabajos de asistencia a la implantación al ENS se deberán basar en alguna herramienta de soporte al ENS. Los requisitos mínimos que deberá cubrir la herramienta serán:

- Funcionalidad de Análisis de r i esgos conforme a la metodología MAGERIT y/o integración con la herramienta PILAR.
- Gestión de métricas e indicadores de seguridad.
- Gestión documental (con funcionalidades de flujos de aprobación y versionado).
- Gestión de activos (inventariado manual y automático).
- Gestión de servicios externalizados (contratos con terceros).
- Gestión de incidentes de seguridad.
- Gestión de Planes de Acción.
- Gestión de formación online.
- Gestión del cumplimiento normativo de protección de datos (LOPD).

No es objeto de la licitación la adquisición de la herramienta en sí, sólo su uso como plataforma de apoyo a la implantación, sin perjuicio de que la Universidad determine su compra con carácter posterior.

3 CONDICIONES DE LA ASISTENCIA

- Al comienzo del servicio deberá presentarse un calendario inicial, que se irá actualizando con la ejecución de acciones del plan.
- Particularmente, las siguientes tareas, por su naturaleza, deberán llevarse a cabo a costa de la **bolsa de horas específica**.
    - Recogida de información en los análisis de riesgos y auditoria (entrevistas).
    - Presentación de resultados de análisis de riesgos y auditorías.
    - Reuniones presenciales para revisiones conjuntas de documentos (en caso de que fuese preciso).
    - Seguimiento y control de cumplimiento de controles y medidas de

seguridad. En este caso se realizarán visitas periódicas programadas. De cada visita deberá emitirse un informe de avance que se entregará a la semana siguiente.

- Asistencia a los comités de seguridad (bajo demanda).
- Soporte en concienciación y sensibilización presencial en materia de seguridad de la información en general y de los requisitos del ENS en particular. Al menos deberán impartirse **16 horas de formación presencial** (distribuidas en un máximo de 4 días dentro del periodo del contrato), solicitadas bajo demanda con una antelación máxima de 3 semanas. El oferente deberá indicar en su propuesta los contenidos que abarcará la formación.

- El tamaño de la bolsa de horas **especifica** será:
  - Mínimo **205 horas por cuatrimestres** (por personal que pertenezca al equipo de trabajo propuesto).
- El tamaño de la bolsa de horas para la asistencia bajo demanda **(bolsa general)** será:
  - Mínimo **15 horas por cuatrimestre** (extraídas del montante de horas del perfil consultor)
- Se acordarán entre las partes los mecanismos de consumo y medición de las bolsas de horas.
- Se deberán incluir la emisión de informes cuatrimestrales de avance, que den cuenta de las actividades realizadas en todo el periodo del servicio y, particularmente, dentro del cuatrimestre en cuestión. Estos informes deberán acompañarse de los resultados asociados a dichas actividades.
- **No podrán subcontratarse los servicios ni total ni parcialmente, debiendo participar en el proyecto el equipo de trabajo que se presente en la propuesta y que, en cualquier caso, deberá responder a los requisitos de solvencia técnica.**

4 ENTREGABLES DEL SERVICIO

Los entregables se suministrarán cada cuatro meses siguiendo el orden acordado en la reunión de inicio del proyecto. Al margen de esto y sin perjuicio de lo anterior se resumen en la siguiente tabla:

Entregables	
• Documentación asociada al Análisis de Riesgos y actualización del plan de adecuación. • Suministro e instalación de la plataforma de gestión de la seguridad. • 1er Informe de Avance cuatrimestral con resultados en el soporte a la implantación del ENS. • Resultados de los trabajos solicitados bajo demanda conforme a la bolsa de horas general si los hubiera.	1º Cuatrimestre
• Documentación asociada al marco organizativo del ENS actualizada y ampliada: Política, procedimientos, normativa y procesos de autorización. • Informe de definición de indicadores de seguridad conformes a la guía CCN-STIC-815. • 2º Informe de Avance cuatrimestral con resultados en el soporte al ENS. • Resultados de los trabajos solicitados bajo demanda conforme a la bolsa de horas general si los hubiera.	2º Cuatrimestre
• Documentación asociada al marco organizativo del ENS actualizada y ampliada: Política, procedimientos, normativa y procesos de autorización. • Material divulgativo de seguridad resultante de las acciones formativas. • 3er Informe de Avance cuatrimestral con resultados en el soporte al ENS. • Resultados de los trabajos solicitados bajo demanda conforme a la bolsa de horas, si los hubiera.	3º Cuatrimestre
• Documentación asociada al Análisis de Riesgos y actualización del plan de adecuación. • Documentación asociada al marco organizativo del ENS actualizada y ampliada: Política, procedimientos, normativa y procesos de autorización. • Informe de Auditoría Bienal ENS conforme al art. 34 ENS. • Material divulgativo de seguridad resultante de las acciones formativas. • Redacción del Informe del Estado de la Seguridad conforme a la guía CCN-STIC 824. • Resultados de los trabajos solicitados bajo demanda conforme a la bolsa de horas, si los hubiera. • Informe Final de los trabajos con resultados finales en el soporte al ENS.	4º Cuatrimestre

5 EQUIPO DE TRABAJO

Para el desarrollo de los trabajos, la empresa adjudicataria deberá ofrecer un equipo consistente al menos en: un Jefe de Proyecto, dos Consultores de Seguridad, un Técnico de TI, un Auditor y un Consultor Legal.

Los miembros del equipo deberán contar con las siguientes titulaciones y certificaciones. Vigentes a la fecha de la licitación

Jefe de proyecto
Requisitos
• Titulación superior en ingeniería informática, de telecomunicaciones o ingeniería industrial.
• CISA (Certified Information System Auditor) de ISACA
• CISM (Certified Information Security Manager) de ISACA
• CSx (Cibersecurity Fundamentals Certificate) de ISACA
• CDPP (Certified Data Privacy Proffessional) del ISMS Forum
• LEAD AUDITOR en Sistemas de Gestión de la Seguridad de la Información (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...)
• ISO 27001 Implementer (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...)
• LEAD AUDITOR en Sistemas de Gestión de la Continuidad del Negocio – ISO 22302- (expedido por alguna entidad de certificación como AENOR, SGS, Bureau Veritas, BSI...)
• Experiencia: al menos 5 años en proyectos de Seguridad de la información.

2 Consultores de Seguridad
Requisitos
• Titulación superior en ingeniería informática, de telecomunicaciones o ingeniería industrial o Titulación media (grado, diplomatura, ingeniería técnica) en informática, telecomunicaciones o industrial.
• CISA (Certified Information System Auditor) de ISACA
• CISM (Certified Information Security Manager) de ISACA
• Experiencia: al menos 5 años en proyectos de Seguridad de la información

1 Auditor de Seguridad
Requisitos
• Titulación superior en ingeniería informática, de telecomunicaciones o ingeniería industrial.
• CISA (Certified Information System Auditor) de ISACA.
• CISM (Certified Information Security Manager) de ISACA.
• CRISC (Certified Risk and Information Systems Control) de ISACA.
• CDPP (Certified Data Privacy Professional) del ISMS Forum
• Experiencia: al menos 5 años en proyectos de Seguridad de la información

1 Consultor Legal
Requisitos
• Licenciado en Derecho
• Experiencia: al menos 5 años en proyectos de Seguridad de la información

1 Técnico de TI
Requisitos
• C|EH (Certified Ethical Hacker) por el EC-Council
• Experiencia: al menos 5 años en proyectos de Seguridad de la información

Los recursos presentados deben ser actualmente personal de la empresa, para ello se deberá presentar la vida laboral.

Los perfiles y horas de dedicación al proyecto serán los siguientes:

Perfiles	Horas 2016	Horas 2017
Jefe de proyecto	20	59
Consultores de Seguridad	150	445
Auditor de Seguridad	0	50
Consultor Legal	25	60
Técnico de TI	25	45

5.1.1 **Componentes**

El adjudicatario deberá describir con detalle dentro del plan de proyecto la estructura, composición y organización interna del equipo de trabajo que proponga.

Debe incluir detalle del perfil de cada persona y su dedicación a este proyecto.

También debe nombrar dentro del equipo de trabajo destinado a este proyecto un responsable con categoría suficiente dentro de su organización, que tendrá entre sus funciones mantener la relación de la empresa adjudicataria con la Universidad y será responsable de todo el servicio.

Todos los perfiles deberán consumir las horas in situ. Las horas no consumidas de las diferentes bolsas podrán ser consumidas por el perfil correspondiente o compensadas por un perfil similar.

En caso de baja de algún miembro del equipo de trabajo, este deberá ser sustituido por otro miembro con el mismo perfil al que haya causado baja.

5.1.2 **Dependencia organizativa**

El proyecto será gestionado por parte de la UCM por Miguel Angel Perote Alejandre, perteneciente al Área de Gobierno T. I. de los Servicios Informáticos de la Universidad.

5.1.3 Calendario y Horario

El adjudicatario deberá prestar el servicio todos los días laborables en función del calendario laboral de la Universidad Complutense, dentro del horario comprendido entre las 8:00 h. y las 18:00 h.

6 OTRAS CONDICIONES GENERALES DEL CONTRATO

6.1.1 Confidencialidad

El adjudicatario se compromete a tratar confidencialmente los datos, documentación e información de éste proyecto.

El adjudicatario declara expresamente que conoce quedar obligado al cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, especialmente en sus artículos 10 y 12, así como lo dispuesto en la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, especialmente en su artículo 11, y a su respectiva normativa de desarrollo. El adjudicatario se compromete expresamente a formar e informar a su personal de las normas que de tales normas dimanan.

El adjudicatario y el personal encargado de la realización de las tareas guardará secreto profesional sobre todas las informaciones, secretos y asuntos a los que tenga acceso o conocimiento durante la vigencia del contrato, estando obligado a no hacer público o enajenar cuantos datos conozcan como consecuencia o con ocasión de su ejecución, incluso después de finalizar el plazo contractual.

En el caso que el adjudicatario tenga acceso a datos de carácter personal procedentes de los ficheros responsabilidad de la UCM, quedará obligado a redactar una memoria descriptiva de las medidas de seguridad que adoptará para asegurar la confidencialidad e integridad de los datos manejados y la documentación facilitada. Estas medidas se corresponderán con el nivel de seguridad de los ficheros origen de los datos, de acuerdo con lo dispuesto en el artículo 9 de la Ley 13/1999 y su normativa de desarrollo. Esta memoria, junto con el nombre y perfil profesional de la persona encargada de ponerlas en práctica, serán comunicadas a la UCM en un plazo máximo de siete días desde la fecha de la adjudicación.

Si la empresa adjudicataria aporta equipos informáticos, una vez finalizadas las tareas y previamente a su retirada, deberá borrar de ellos toda la información utilizada o que se derive de la adjudicación del contrato, mediante el adecuado procedimiento técnico. La destrucción de la documentación de apoyo, si no se considerase necesaria, se efectuará mediante máquina destructora de papel o cualquier otro medio que garantice la ilegibilidad, efectuándose esta operación en el lugar donde se realicen los trabajos.

El adjudicatario reconoce expresamente que todo el material, escritos, procedimientos y formularios a cuyo conocimiento acceda en el desarrollo de sus servicios son propiedad de UCM. A la finalización de la relación que une a ambas partes, el adjudicatario se compromete a devolver a la UCM toda la información, documentos, programas y datos proporcionados por la UCM para el desarrollo de los trabajos. Al mismo tiempo, toda la documentación e información generada por adjudicatario y sus colaboradores como consecuencia del desarrollo de su actividad, salvo pacto en contrario, pertenece en exclusiva titularidad a la UCM, renunciando expresamente a ejercitar cualquier reclamación que sobre la misma pudiera recaer.

6.1.2 Equipamiento

Corre a cargo del adjudicatario todos los equipos informáticos, licencias de productos software y demás elementos necesarios para el personal de su equipo, pudiendo compartir algunos de los elementos y/o equipos de la UCM si ésta lo autorizase.

La infraestructura de soporte (entre los que se destacan los servidores de red y/o de desarrollo) y comunicaciones serán aportadas por la UCM.

La UCM pondrá a disposición del adjudicatario un equipo dedicado exclusivamente a este proyecto que será configurado por el personal de los Servicios Informáticos de la UCM de acuerdo a la normativa de seguridad interna establecida y no podrá, en ningún caso, ser reconfigurado ni utilizado para otra función o en otro entorno al establecido en este concurso.

7 DURACIÓN

En caso de que finalizado el periodo de servicio no se produzca la prórroga del contrato, el adjudicatario entregará toda la documentación e información necesaria para que el servicio pueda continuar siendo prestado por las personas que designe la Universidad.

PERSONA DE CONTACTO E INFORMACION ADICIONAL

En caso de necesitar alguna aclaración sobre este pliego las consultas deberán dirigirse a:

D. Miguel Angel Perote Alejandre - Área de Gobierno T. I.-Servicios Informaticos

e-mail: maperote@ucm.es

Tfno: 91.394.4791

Madrid, 25 de abril de 2016

EL DIRECTOR DEL AREA DE GOBIERNO T. I.
SERVICIOS INFORMATICOS

Fdo.: Fernando Pescador González