UNIVERSIDAD DE BURGOS | Servicio de Informática y Comunicaciones

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE SERVICIOS DE CONSULTORÍA Y ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD (ENS)

Contenido

1. OBJETO

la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, amplió el ámbito de aplicación del Esquema Nacional de Seguridad (ENS) a todo el sector público, estableciendo en su artículo 3, que regula los principios generales, la necesidad de que las administraciones públicas se relacionen entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que garanticen la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas y la protección de los datos personales, y faciliten la prestación de servicios a los interesados preferentemente por dichos medios, señalando al ENS como instrumento fundamental para el logro de dichos objetivos en su artículo 156.

Recientemente se ha publicado el nuevo Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 311/2022, de 3 de mayo, (https://www.boe.es/eli/es/rd/2022/05/03/311).

El nuevo ENS establece en la Disposición transitoria única. Adecuación de sistemas.
"1. Los sistemas de información del ámbito de aplicación de este real decreto, preexistentes a su entrada en vigor, incluidos aquellos de los que sean titulares los contratistas del sector privado en los términos señalados en el artículo 2, dispondrán de veinticuatro meses para alcanzar su plena adecuación al ENS, circunstancia que se manifestará con la exhibición del correspondiente distintivo de conformidad, atendiendo lo dispuesto en el artículo 38."

En cumplimiento de este mandato, la Universidad de Burgos (UBU) desea avanzar en el cumplimiento normativo en materia de seguridad de la información, con el objetivo de iniciar el proceso que permita obtener la Certificación de Conformidad con el Esquema Nacional de Seguridad (ENS), según el Perfil de Cumplimiento Específico para Universidades.

El presente pliego tiene por objeto la contratación de servicios de asesoría y consultoría técnica y legal, para la adecuación de la UBU al nuevo ENS, de forma que permita abordar el proceso de certificación con suficientes garantías de éxito.

2. ALCANCE DEL CONTRATO

En el alcance del contrato se incluyen los siguientes servicios y actuaciones por parte de la empresa adjudicataria:

1. Servicios de asesoría técnica y legal en seguridad de la información orientados a la adecuación y el cumplimiento del nuevo Esquema Nacional de Seguridad. Resolución de consultas técnicas y/o jurídicas, referentes al cumplimiento del ENS, así como la elaboración de plantillas.

2. Elaboración por parte de la empresa adjudicataria del Plan de Adecuación siguiendo el Anexo II Plan de adecuación al ENS de las universidades, adaptándolo a las particularidades de la UBU:

a. Identificación del alcance de los sistemas a certificar.
b. Categorizar el Sistema.
c. Declaración de Aplicabilidad Provisional- aplicando el Perfil de Cumplimiento Específico para Universidades.
d. Análisis de riesgos según lo indicado en el punto 6 de este apartado.
e. Declaración de aplicabilidad definitiva, asociada al Perfil de Cumplimiento Específico para Universidades:
    1. Identificación de las medidas de seguridad y los refuerzos recogidos en el Perfil de Cumplimiento Específico para Universidades.
    2. Identificación de las medidas del Perfil de Cumplimiento Específico para Universidades que serán reemplazadas por otras compensatorias que ofrezcan igual o superior protección, justificando su implementación de acuerdo a lo establecido en la Guía "CCN-STIC 819 Medidas compensatorias".

3. Una vez realizado el Plan de Adecuación, se pasará a la fase de Implantación de la Seguridad, mediante la definición del Plan de Implantación que contendrá los documentos a elaborar y las medidas técnicas a implementar de forma priorizada.

4. Revisión y actualización de las políticas, normativas, procedimientos e instrucciones técnicas ya existentes en la UBU y elaboración de la nueva documentación que se considere necesaria para cumplir el objetivo de conseguir la certificación en el cumplimiento del ENS según lo establecido en la **Guía de Seguridad de las TIC CCN-STIC 881- Guía de Adecuación al ENS para Universidades y sus Anexos.**

5. Registro de toda la documentación en la herramienta **AMPARO del CCN-CERT**.

6. Realización de un análisis anual de riesgos con la herramienta **PILAR del CCN-CERT** (no se usará microPilar, ni Pilar Basic) que implementa la metodología MAGERIT. Se usará la última versión (o penúltima bajo justificación y acuerdo con la UBU) de esta herramienta. La UBU proporcionará el archivo con el análisis de riesgos anterior, sobre el que se harán las correspondientes modificaciones. **La empresa adjudicataria se coordinará con el Delegado de Protección de Datos de la UBU para**

incorporar al análisis de riesgos la parte relativa al cumplimiento del RGPD. En la realización del análisis de riesgos se reflejará el estado de cumplimiento de las medidas de seguridad, indicando el nivel de madurez de las medidas de la declaración de aplicabilidad.

7. Carga automática de la información generada por PILAR en la herramienta INES del CCN-CERT y asesoría para la cumplimentación del resto de información a rellenar manualmente en dicha herramienta.

8. Toda la documentación actualizada o generada en el ámbito de este contrato deberá seguir las pautas establecidas en las **Guías CCN-STIC del CCN-CERT**.

9. Preparación de contenidos para formación online a partir de los documentos elaborados en el punto 4, para publicar en la plataforma Moodle (en formato SCORM) de forma que ayuden a difundir la normativa y procedimientos entre los miembros de la Comunidad universitaria. Se incluirá la realización de un cuestionario tras la realización del curso.

10. Elaboración de una píldora audiovisual sobre aspectos de concienciación y formación en seguridad, y en un formato audiovisual adecuado para captar la atención de los usuarios y transmitir las ideas de una forma sencilla y eficiente.

11. Realización de auditoría de seguridad de cumplimiento del nuevo ENS siguiendo lo establecido en su artículo 38 y en el Anexo III, así como en la Guía CCN-STIC 809 Declaración, certificación y aprobación de conformidad con el ENS y distintivos de cumplimiento.

    El ENS establece en el artículo 31 Auditoría de la seguridad. "2. La auditoría se realizará en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico que corresponda, según lo dispuesto en los anexos I y III y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información".

    El ENS establece en el artículo 38 Procedimientos de determinación de la conformidad con el Esquema Nacional de Seguridad:
    "Los sistemas de información comprendidos en el ámbito del artículo 2 serán objeto de un proceso para determinar su conformidad con el ENS. A tal

efecto, los sistemas de categoría MEDIA o ALTA precisarán de una auditoría para la certificación de su conformidad, sin perjuicio de la auditoría de la seguridad prevista en el artículo 31 que podrá servir asimismo para los fines de la certificación…"

12. **Establecimiento de un sistema de indicadores**. Se trata de definir y gestionar unos indicadores del SGSI (Sistema de Gestión de Seguridad de la Información) para conocer el nivel de madurez de la UBU.

13. Realización de auditorías de hacking ético anuales de **5 sistemas de información de la UBU**. Las vulnerabilidades se deberán reflejar y gestionar con la herramienta de auditoría continua ANA del CCN-CERT.

14. Asesoramiento y colaboración en todas las fases del proceso de adecuación para la consecución de los fines especificados en este PPT: implementación de medidas de seguridad, propuesta de mejoras a implantar en la UBU, etc.

15. Asesoramiento jurídico y acompañamiento en la resolución de incidentes de seguridad.

Todas las dietas, desplazamientos, licencias o trabajos que sean necesarios para el cumplimiento de lo especificado en este pliego serán por cuenta de la empresa adjudicataria.

3. CONDICIONES PARA LA PRESTACIÓN DEL SERVICIO

El objeto del presente apartado es definir los requerimientos para prestar el servicio ofertado:

1. El equipo mínimo de trabajo que tienen que ofertar las empresas para ejecutar el contrato estará formado por los siguientes perfiles profesionales que se acreditarán mediante la presentación de los correspondientes Curriculum vitae, certificados de formación, profesionales, etc.:

    a. Un consultor principal y un consultor suplente, de forma que el servicio esté siempre cubierto durante toda la duración del contrato, con la siguiente cualificación:

i. Perfil técnico en el sector de Tecnologías de la Información y las Comunicaciones
ii. Especialista en ENS y RGPD.
iii. Experiencia en el uso de la herramienta de análisis de riesgos PILAR.
iv. Experiencia en proyectos de similares características a las del objeto del contrato, en los últimos 3 años.

b. Un consultor con perfil jurídico, especialista en ENS y RGPD.

2. La Universidad proporcionará al personal de la empresa adjudicataria, la información necesaria y el acceso a los sistemas (INES, Amparo, etc.) para el cumplimiento de las cláusulas previstas en este pliego. El plazo de configuración del acceso a los sistemas y definición de protocolos de actuación será como máximo de **15 días** desde la firma del contrato.
3. La empresa adjudicataria deberá prestar soporte telefónico, por email y por videoconferencia, 8h x 5 días laborables, especificando claramente en su oferta el horario laboral, que en todo caso deberá incluir la franja de 9 a 15h. En el soporte telefónico se deberá incluir exclusivamente numeración que no sea de tarificación especial y/o adicional.
4. **Tiempo de respuesta de consultas**. La empresa deberá revisar y responder **al menos al 98%** de todas las consultas y solicitudes recibidas, en el plazo de **dos días laborables**. (Indicador medido mensualmente).
5. **Tiempo de entrega** o realización de trabajos. La empresa deberá cumplir **como mínimo en el 98%** de todas las solicitudes recibidas, con los plazos de entrega de los trabajos acordados con el responsable de la UBU. Se tratará de ajustar el alcance de los trabajos para que puedan realizarse en **5 días laborables**. (Indicador medido mensualmente).
6. La empresa adjudicataria deberá disponer de un sistema de registro de peticiones que permita hacer un seguimiento adecuado del cumplimiento de los tiempos de respuesta y entrega.
7. La oferta especificará los recursos técnicos, mecanismos para la comunicación y registro de las peticiones, medición de los tiempos de respuesta y entrega de las consultas y solicitudes, el horario efectivo de prestación del servicio cumpliendo lo especificado en este PPT, así como el detalle de la formación y experiencia de los recursos humanos puestos a disposición del contrato.

8. La empresa adjudicataria deberá implantar mecanismos de seguimiento y supervisión para garantizar el buen funcionamiento de los servicios contratados.

4. FASES, PLAZOS Y DOCUMENTACIÓN A ENTREGAR

El proyecto se realizará por fases y se elaborará como mínimo la siguiente documentación que se entregará a la Universidad de Burgos:

Fase I: plazo de entrega máximo 2 meses desde la firma del contrato.
Documentos a entregar:

1. Plan de Adecuación.
2. Fichero e informes del análisis de riesgos. Carga de datos en INES.
3. Declaración de Aplicabilidad Definitiva-Perfil de Cumplimiento Específico (se plasmará en un documento firmado por el Responsable de Seguridad).
4. Plan de Implantación que contendrá los documentos a elaborar y las medidas técnicas a implementar de forma priorizada.

Fase II: plazo de entrega máximo 6 meses desde la firma del contrato
Documentos a entregar:

5. Políticas, normativas, procedimientos e instrucciones técnicas con control de versiones.
6. Inventario de toda la documentación asociada al SGSI (Sistema de Gestión de Seguridad de la Información) y evidencias de cumplimiento de las medidas de seguridad.
7. Contenidos a publicar en Moodle y píldora formativa sobre aspectos de concienciación y formación en seguridad.
8. Sistema de indicadores.

Fase III: plazo de entrega máximo 8 meses desde la firma del contrato
Documentos a entregar:

9. Informe de auditoría de seguridad de cumplimiento del nuevo ENS.
10. Informes de auditorías de hacking ético.

Durante todo el contrato:

11. Informes mensuales de seguimiento del contrato con el detalle de consultas, peticiones y trabajos realizados y los tiempos de respuesta y entrega.

Toda la documentación deberá entregarse en castellano, en formato electrónico editable generado con herramientas ofimáticas estándar del mercado (formatos .doc, .docx u .odt), para facilitar su tratamiento y reproducción.

Se emplearán las plantillas e imagen corporativa de la Universidad de Burgos.

5. PLANIFICACIÓN, DIRECCIÓN Y SEGUIMIENTO DEL CONTRATO

Una vez formalizado el contrato, el adjudicatario se reunirá con responsable del contrato en la Universidad de Burgos y se procederá al nombramiento de una comisión de seguimiento del proyecto.

Formarán parte de la Comisión de seguimiento:

- El Responsable de Seguridad de la Información de la Universidad de Burgos que será el responsable del contrato.
- El Responsable del Sistema de la Universidad de Burgos.
- El responsable del proyecto por parte de la empresa adjudicataria.
- Un técnico asignado al proyecto por la empresa adjudicataria.

La comisión de seguimiento se reunirá a petición del responsable del proyecto de la UBU y tendrá sus reuniones por videoconferencia o en las instalaciones de la Universidad de Burgos, con la periodicidad que fije el responsable del contrato, que será como mínimo mensual.

Las funciones de esta Comisión serán las siguientes:

- Seguimiento y evaluación del progreso de las tareas y plazos planificados para la prestación de los servicios contratados.
- Coordinación de las reuniones e informes de seguimiento del proyecto.
- Verificación del cumplimiento de las actuaciones solicitadas y definición de los requisitos pendientes.
- Negociación para la incorporación de nuevas prestaciones o requisitos.
- Cualquier otro asunto que la propia Comisión considere de interés.

La empresa adjudicataria asignará un responsable del proyecto para el control y seguimiento del contrato y realizará **informes mensuales de seguimiento** donde se recojan todas las actuaciones realizadas como consecuencia de los servicios objeto de este contrato.

6. PROTECCIÓN DE DATOS

La empresa adjudicataria se compromete a tratar los datos de carácter personal en el ámbito del servicio objeto de este pliego, de conformidad con lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y la normativa que la desarrolla.

También se compromete a tratar los citados datos, únicamente conforme a las instrucciones de la Universidad de Burgos y a no aplicarlos o utilizarlos con fin distinto al del servicio objeto de este pliego ni a comunicarlos, ni siquiera para su conservación, a otras personas.

El adjudicatario se compromete asimismo a efectuar un borrado lógico de la información que garantice su irrecuperabilidad, en aquellos equipos que contengan información no cifrada de carácter reservado o de carácter personal que como consecuencia de la ejecución del contrato sea preciso sacar fuera de las instalaciones de la UBU.

7. SEGURIDAD DE LA INFORMACIÓN

De acuerdo con la resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad:

"VIII.2 Es responsabilidad de las entidades públicas contratantes notificar a los operadores del sector privado que participen en la provisión de soluciones tecnológicas o la prestación de servicios, la obligación de que tales soluciones o servicios sean conformes con lo dispuesto en el Esquema Nacional de Seguridad y posean las correspondientes Declaraciones o Certificaciones de Conformidad, según lo señalado en la presente Instrucción Técnica de Seguridad."

El personal asignado por la empresa adjudicataria deberá conocer y respetar la normativa de seguridad de información de la UBU, así como los procedimientos establecidos por la Universidad que sean de aplicación en este ámbito:

http://wwww.ubu.es/normativa/administracion-y-gestion-general-de-la-universidad/seguridad-de-la-informacion

En cumplimiento del Esquema Nacional de Seguridad el adjudicatario se compromete a:

a) Garantizar el cumplimiento del Esquema Nacional de Seguridad durante la duración del contrato.
b) Mantener un contacto permanente con el Responsable de Seguridad de la universidad para temas de interés en el ámbito de la seguridad.
c) Despliegue en toda su organización de la cultura de la seguridad en los sistemas de información.
d) Establecimiento de una figura de responsable de seguridad en su organización.
e) El intercambio de información se realizará de forma segura protegiendo especialmente la información confidencial y los datos personales.
f) El medio técnico preferente de conexión para accesos puntuales será el establecimiento de una conexión VPN.
g) Solamente se dará acceso a los servidores de aplicaciones, bases de datos, etc. estrictamente necesarios para el cumplimiento del objeto del contrato.
h) El acceso local a recursos TIC de equipos de las empresas prestadoras de servicios se deberá integrar y cumplir con las medidas de seguridad de la red de la UBU (control de acceso a la red, disponibilidad de antivirus actualizado, parches de seguridad…).
i) El servicio de acceso remoto no debe ser usado para:
    i. Cualquier transmisión de información o acto que viole la legislación vigente que le sea de aplicación.
    ii. Fines privados, personales o comerciales, no relacionados con las actividades propias y autorizadas por la UBU.
    iii. Transmisión de material que infrinja la legislación sobre propiedad intelectual (software, imágenes, video, audio, películas…). En general el usuario se compromete a no hacer uso de los recursos informáticos y de comunicación para publicar o divulgar material obsceno, difamatorio u

ofensivo que pueda suponer una violación de los derechos legales de terceros.

8. PROPIEDAD INTELECTUAL Y CONFIDENCIALIDAD

Toda información que se encuentre en las instalaciones de la Universidad de Burgos es confidencial y de su propiedad, por lo que la empresa adjudicataria y cualquier persona dependiente de la misma que desempeñe las funciones objeto de este pliego deberán mantener la confidencialidad plena sobre la información inherente a los servicios objeto del mismo. Esta obligación de confidencialidad se entenderá plenamente vigente incluso con posterioridad a la extinción del servicio prestado.

La documentación y/o ficheros generados durante la ejecución del contrato serán propiedad exclusiva de la Universidad de Burgos. El adjudicatario no podrá hacer ningún uso o divulgación de los informes, estudios y documentos elaborados en base a este pliego de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, ni facilitarlos a terceros sin la expresa autorización por escrito de la UBU.

En Burgos,
La Jefa del Servicio de Informática y Comunicaciones