Nota aclaratoria

Aclaraciones respecto al contenido mínimo establecido en la plantilla de la memoria de la categoría de ciberseguridad para certificación para el programa Kit Consulting

El Programa Kit Consulting financia diez Categorías de Servicio de Asesoramiento, destacando, entre otras, la ciberseguridad. Sobre ciberseguridad existen tres Categorías de Servicios de Asesoramiento:

VII. Servicio de Asesoramiento en Ciberseguridad (básico),

VIII. Servicio de Asesoramiento en Ciberseguridad (Avanzado), y

IX. Servicio de Asesoramiento en Ciberseguridad (Preparación para Certificación).

La categoría IX. de Servicio de Asesoramiento en Ciberseguridad (Preparación para Certificación) persigue el siguiente objetivo: *"Plan enfocado para empresas que disponen de una protección básica y un plan de seguridad adaptado y la estructura documental básica de SGSI (según ISO 27001 y ENS media-alta) y quieren implementar sistemas de protección avanzada, aprovechando además las capacidades de la inteligencia artificial, y prepararse para presentar su SGSI a la certificación (no incluida)."*

Para asegurar que los beneficiarios obtengan la mejor preparación posible para la certificación, esta nota tiene como objetivo definir la totalidad de los elementos necesarios que se contemplan en los SGSI que evalúa la certificación y que deben contenerse en la memoria técnica.

Si bien en las Bases Reguladoras se recogen los contenidos necesarios a alto nivel, **en la plantilla de memoria técnica se incluyen en detalle cada uno de los elementos evaluados en la certificación ISO27001 y ENS y que resultarán necesarios para justificar la Categoría de Servicio de Asesoramiento «Servicio de Asesoramiento en Ciberseguridad (Preparación para Certificación)»**.

Elementos evaluados en la certificación ISO27001 y ENS y en la memoria técnica de la Categoría Servicio de Asesoramiento en Ciberseguridad (Preparación para Certificación).

La certificación **ISO27001 y ENS del SGSI** evalúa once (11) elementos principales, de los cuales ocho se incluyen de forma explícita en las bases reguladoras y el resto forman parte del manual del SGSI. Atendiendo a lo anterior, los siguientes puntos deberán estar comprendidos en la memoria técnica para la

Categoría de Servicio de Asesoramiento de «Servicio de Asesoramiento en Ciberseguridad (Preparación para Certificación)».:

1. Alcance del SGSI.
2. Política de seguridad de la información.
3. Objetivos de seguridad de la información.
4. Evaluación y tratamiento de riesgos.
5. Declaración de aplicabilidad (DoA).
6. Controles y procedimientos implementados en la empresa.
7. Roles y responsabilidades del SGSI.
8. Recursos y formación para el SGSI.
9. Gestión de incidentes de seguridad.
10. Mantenimiento y mejora del SGSI.
11. Documentación y control de documentos.

Para asegurar que los beneficiarios que soliciten el «IX. Servicio de Asesoramiento en Ciberseguridad (Preparación para Certificación)» reciban el asesoramiento necesario adquiriendo las competencias para optar (con posibilidad de éxito) a la certificación, se ha incluido en la plantilla de memoria técnica información relevante y que sirve de guía para los asesores digitales, detallada a continuación.

Plantilla de memoria técnica del Programa Kit Consulting

La plantilla de memoria técnica para la Categoría de Servicio de Asesoramiento IX. «Servicio de Asesoramiento en Ciberseguridad (Preparación para Certificación)» se encuentra dividida en seis apartados, tal y como se establecen en las bases reguladoras, siguiendo el mismo orden.

A continuación, se detallan los seis puntos incluidos en la plantilla con aclaraciones adicionales a las ya incluidas en dicha plantilla:

1.1 Manual del SGSI

En esta sección se incluirá la elaboración de un manual del SGSI que refleje el ciclo PDCA de mejora continua, e incorpore el conjunto de políticas, procedimientos y directrices, junto con los recursos y actividades gestionados colectivamente por la organización para proteger sus activos de información esenciales. Además, el manual debe incluir[1]:

- **Política de seguridad**: Declaración formal de la dirección.
- **Alcance del SGSI**: Definición de los límites y aplicabilidad.
- **Roles y responsabilidades**: Asignación clara de funciones en la gestión de la seguridad.

[1] Se incluye esta puntualización con el objeto de mejorar la claridad respecto al texto de la Convocatoria.

1.2 Declaración de aplicabilidad ISO27001 y ENS

En el apartado 1.2 de la plantilla de la memoria se incluye una descripción del contenido a incluir, para asegurar la correcta comprensión de la declaración de aplicabilidad y su alineación con los marcos normativos relevantes. De este modo, la descripción que se incluye en la plantilla no sólo contiene el texto íntegro de las bases reguladoras, sino que añade una aclaración con una mención explícita al elemento 5 de los 11 evaluados para la certificación enumerados anteriormente.

Respecto al contenido, conviene aclarar que en este apartado deberá incluirse la declaración de aplicabilidad compartida entre ISO27001 y ENS, la cual debe ser aprobada por el Responsable de Seguridad. En el caso del ENS, la declaración debe estar en consonancia con el CCN-STIC 804 y alineada con la categorización del servicio. Además de los controles ya establecidos por la pyme a este respecto, se deberán incluir los controles adicionales del SGSI basados en los procedimientos de evaluación y tratamiento de riesgos.

1.3 Programa de formación en ciberseguridad

En el apartado 1.3 de la plantilla de la memoria se incluye una descripción del contenido a incluir, para asegurar la correcta identificación y desarrollo de competencias profesionales críticas en ciberseguridad. Este apartado no sólo contiene el texto íntegro de las bases reguladoras, sino que añade una mención explícita a los puntos 3 y 9 de los 11 evaluados para la certificación enumerados anteriormente. El programa de formación deberá contemplar la capacitación especializada para los perfiles y funciones clave dentro de la organización, asegurando que se aborden tanto las competencias técnicas como las de concienciación en materia de seguridad.

Respecto al contenido, conviene aclarar que en este apartado se deberá identificar y categorizar las necesidades de formación del personal, segmentadas por perfiles y departamentos, para garantizar que cada grupo reciba la formación adecuada a sus responsabilidades y riesgos asociados.

1.4 Normativa y procedimientos de seguridad avanzados

En este apartado se ha clarificado el contenido de las bases reguladoras para asegurar la comprensión de los requisitos – deben incluirse más normativas y procedimientos de seguridad avanzados además de gestión de crisis y continuidad de negocio, pero estos dos deben estar incluidos siempre[2]:

> *"Esta sección contemplará la normativa y procedimientos de seguridad avanzados en base a la norma y el alcance del SGSI; entre otros, deberá incluir los establecidos para la gestión de crisis y para la continuidad de negocio".*

[2] Se incluye esta puntualización con el objeto de mejorar la claridad respecto al texto de la Convocatoria.

1.5 Definición de un sistema de métricas de ciberseguridad

En este apartado se ha clarificado el contenido para asegurar una correcta implementación y seguimiento de un sistema de métricas de ciberseguridad. Se deberá definir un conjunto de indicadores clave de rendimiento (KPIs) que permitan medir de forma continua el desempeño en relación con los objetivos de seguridad establecidos. Estos KPIs deben ser diseñados específicamente para identificar áreas de mejora y mitigar los riesgos mediante la evaluación continua de la eficacia de los controles y medidas de seguridad. Es esencial que el sistema de métricas se revise y ajuste periódicamente para garantizar su alineación con los riesgos emergentes y la evolución de las amenazas.

1.6 Plan e informe de auditoría interna del SGSI

En el apartado 1.6 de la plantilla de la memoria se incluye una descripción del contenido necesario para asegurar la correcta planificación y ejecución de la auditoría interna del SGSI. El plan de auditoría debe definir de manera clara la frecuencia y las fechas de ejecución, el alcance de las auditorías, así como la metodología empleada. Además, se deberá detallar la asignación de interlocutores clave para la planificación, realización y presentación de los informes de resultados.

Además, deberá comprender una descripción detallada de las ubicaciones físicas, unidades organizativas, actividades y procesos que serán auditados, especificando las fechas de inicio y finalización de las auditorías internas. Es fundamental garantizar que estas auditorías sean llevadas a cabo por personal independiente que no haya participado en la implantación del SGSI, con el objetivo de asegurar la objetividad e imparcialidad del proceso. Finalmente, los resultados de las auditorías deberán ser documentados en un informe que refleje el cumplimiento de los controles y procedimientos del SGSI, identificando posibles no conformidades o áreas de mejora, y proponiendo las acciones correctivas correspondientes.

Para cualquier duda adicional, puede remitirse a las FAQs del programa, en la sección «Servicio de Asesoramiento en Ciberseguridad (Preparación para Certificación)».