Ejemplo de modelo para justificar la experiencia profesional en funciones relacionadas con los distintos dominios de la certificación GRC IA

A continuación se incluye un modelo de certificado para justificar la experiencia profesional. El ejemplo aportado es genéricos y únicamente tienen como objetivo orientar al candidato sobre la forma que puede tener un certificado para considerarse adecuado. El contenido del/los certificado/s, en cuanto a las funciones desarrolladas, debe ser veraz y adecuado a las funciones desarrolladas por el candidato.

Las funciones reflejadas deben corresponder con las recogidas en el esquema GRC IA que figuran extractadas en este documento.

Yo, XXXX, con DNI XXXXX, en calidad de XXXX de la empresa XXXXXXX con domicilio en XXXXXX y CIF XXXXXXX por la presente certifico que:

D/Dª (Candidato) con DNI XXXX ha desarrollado desde enero de 20XX a la fecha de firma de este documento labores relacionadas con la protección de datos y seguridad de la información en distintos ámbitos.

Las funciones concretas desarrolladas por D/Dª (candidato) en el periodo han sido:

- *Implementación de un marco de gobierno del dato para IA*
- *Aseguramiento del cumplimiento de normativas de privacidad como el GDPR y RIA*
- *Aplicación de estrategias de ciberseguridad relacionados con sistemas de seguridad de la información basados en la/s norma/s XXXXX y en la aplicación de metodologías de gestión de riesgos*
- *Realización de auditorías*
- *Asesoramiento y resolución de consultas para la supervisión del cumplimiento*

En ……., a…… de…… de ……..

(Firma y Sello de la Entidad)

(Nombre y Apellidos)

Tareas y competencias clave del profesional RC IA conforme al esquema de certificación

1. Supervisión del desarrollo y uso de la inteligencia artificial
   - Evaluar la aplicación de los principios fundamentales de IA, asegurando su alineación con valores éticos y objetivos estratégicos.
   - Fomentar la transparencia y explicabilidad de los modelos de IA dentro de la organización.
2. Implementación de un marco de gobierno del dato para IA
   - Definir políticas de gestión del dato que garanticen su calidad, trazabilidad y uso responsable en sistemas de IA.
   - Supervisar el acceso, almacenamiento y procesamiento de datos en cumplimiento con principios de minimización y equidad.
3. Garantía de privacidad y protección de datos en entornos de IA
   - Asegurar el cumplimiento de normativas de privacidad como el GDPR y RIA
   - Aplicar técnicas como anonimización, encriptación y control de acceso para mitigar riesgos de exposición de datos sensibles.
4. Aplicación de estrategias de ciberseguridad en sistemas de IA
   - Evaluar y mitigar riesgos de ciberseguridad específicos en IA, como ataques adversariales y manipulación de modelos.
   - Implementar controles de seguridad para proteger datos, algoritmos y procesos de inferencia.
5. Gestión de riesgos asociados a la inteligencia artificial
   - Identificar, analizar y mitigar riesgos éticos, operacionales y regulatorios en sistemas de IA.
   - Aplicar metodologías de evaluación de impacto para reducir sesgos, errores y daños potenciales.
6. Desarrollo e implementación de sistemas de gestión de IA (Dominio 6: Sistemas de Gestión)
   - Diseñar marcos de gobernanza basados en estándares reconocidos (ISO 42001, NIST….) para la gestión de IA en la organización.
   - Asegurar el cumplimiento de requisitos de calidad y supervisión en la implementación de sistemas de IA.
7. Coordinación de respuestas ante crisis e incidentes de IA
   - Diseñar planes de contingencia y protocolos de respuesta ante fallos en IA, incluyendo sesgos, discriminación y errores críticos.
   - Liderar la recuperación de incidentes y coordinar la comunicación de riesgos con stakeholders internos y externos.
8. Cumplimiento del Reglamento Europeo de Inteligencia Artificial
   - Asegurar la implementación de requisitos normativos del Reglamento Europeo de IA dentro de la organización.
   - Supervisar la clasificación de los sistemas de IA según su nivel de riesgo y aplicar las medidas de control necesarias.
9. Adaptación y cumplimiento del marco legislativo internacional de IA
   - Monitorear la evolución de regulaciones globales en IA (EE.UU., China, OCDE, ONU) y evaluar su impacto en la organización.
   - Alinear políticas internas con estándares internacionales para garantizar la interoperabilidad y el cumplimiento normativo.