Normas y estándares

Qué cubre SEVEN-G de ISO/IEC 42001, del NIST y del Reglamento Europeo de IA.

> *«Los estándares dicen qué debe existir; SEVEN-G es la capa operativa que lo hace funcionar caso a caso. Ayuda a preparar la evidencia, pero no certifica ni sustituye a una auditoría acreditada.»*

QUÉ ES

Mapear, no copiar

SEVEN-G no incorpora las normas: las mapea. Una tabla de cobertura relaciona cada requisito de ISO/IEC 42001, de otras normas ISO/IEC, del marco de riesgos de IA del NIST y del Reglamento Europeo de IA con la regla del marco, la evidencia que la sostiene y su grado de cobertura.

Implicación: ¿Sabe su compañía qué requisitos de la norma que persigue ya cubre lo que hace hoy?

Riesgo: Sin mapa, cada norma se trata como un proyecto aparte y la evidencia se pide dos veces.

QUÉ PROPONE

Una cobertura honesta

Cada fila dice si la cobertura es directa, parcial, requiere un control externo o no existe. Quedan fuera la certificación, la documentación técnica de un proveedor de alto riesgo y la evaluación de la conformidad. Cada norma ISO se resume con palabras propias y se coteja con el texto adquirido.

Implicación: ¿Qué requisitos de su objetivo normativo no cubre hoy ningún proceso interno?

Riesgo: Creer que la metodología certifica lleva a una auditoría externa sin preparación.

CÓMO SE COMPRUEBA

Una evaluación, dos lecturas

El diagnóstico de madurez da también los perfiles actual y objetivo del NIST, en la misma escala de 0 a 5, sin una segunda evaluación. Para ISO/IEC 42001, la declaración de aplicabilidad justifica cada exclusión y solo marca «implantado» lo que tiene evidencia. Certifica una entidad acreditada.

Implicación: ¿Ha aprobado la alta dirección una declaración de aplicabilidad con evidencias?

Riesgo: Un control marcado como implantado sin evidencia es el primer hallazgo de una auditoría.

CUATRO PREGUNTAS PARA EL CONSEJO

1. **¿Qué cubrimos de ISO/IEC 42001 y qué nos falta?**
   La tabla de cobertura, fila a fila: qué es parcial, qué requiere un control externo y quién lo cubre.
2. **¿Cumplimos el Reglamento Europeo de IA?**
   La respuesta va sistema a sistema: clasificación, obligaciones que aplican y evidencia. No hay una respuesta global.
3. **¿Dónde está nuestra brecha frente al perfil objetivo del NIST?**
   Perfiles actual y objetivo por subcategoría, con la brecha y su acción en el plan de mejora de la madurez.
4. **¿Quién nos certifica, si queremos certificarnos?**
   Una entidad de certificación acreditada. SEVEN-G ayuda a preparar la evidencia; no certifica ni declara la conformidad.

QUÉ FALLA SI NO SE GOBIERNA

QUÉ FALLA	NIVEL	QUÉ HACER
Presentar el marco como una certificación	ALTO	Revisar cómo se comunica el cumplimiento
Exclusiones de la norma sin justificar	ALTO	Justificar cada exclusión de la declaración
Requisitos que nadie cubre en la compañía	ALTO	Asignar un control externo a cada hueco de cobertura
Un borrador de norma usado como criterio de decisión	MEDIO	Citar los borradores solo como orientación
El resumen de una norma tomado por su texto	MEDIO	Cotejar la cobertura con el texto adquirido
Una evaluación distinta para cada marco	BAJO	Derivar los perfiles del NIST del diagnóstico

PARA SEGUIR LEYENDO

Mapeo regulatorio
Documento 34 · tabla de cobertura de normas

Perfil de gobierno de IA (NIST AI RMF)
Plantilla editable

Declaración de aplicabilidad de ISO/IEC 42001
Plantilla editable

ISO/IEC 42001 · Sistema de gestión de la IA
ISO/IEC (JTC 1/SC 42) · 18-12-2023

Fernando García Varela · CC BY 4.0 · Versión 0.x, en revisión

Ayuda genérica y gratuita, sin revisión jurídica para ningún caso concreto: cada organización la adapta, identifica la normativa que le aplica y responde de su cumplimiento. No es asesoramiento ni certificación. En la máxima medida permitida por la ley, el autor no asume responsabilidad por los efectos de su aplicación.