NUEVOS RETOS

Tu empresa ante la IA y la ciberseguridad

Cambra de Comerç de Barcelona

Grant Thornton

Grant Thornton

Responsabilidad de los administradores en ciberseguridad: Riesgos, deberes, y gobernanza

Joan Saula, Socio de Legal de Grant Thornton

Riesgos: ¿La irrupción de la IA aumenta el riesgo en ciberseguridad?

- La IA puede ampliar la superficie de ataque al integrarse en más procesos, canales y sistemas conectados.
- También facilita la automatización de ataques, aumentando su escala, velocidad y capacidad de personalización.
- El uso de proveedores, modelos de terceros y cadenas de suministro tecnológicas introduce riesgos adicionales de dependencia y control.
- El tratamiento de datos mediante sistemas de IA exige reforzar la protección de datos, la confidencialidad y las medidas de acceso.
- Los sesgos, errores o alucinaciones pueden generar decisiones inseguras o respuestas que comprometan la seguridad.
- Este escenario exige definir responsabilidades, supervisión humana y marcos de gobernanza adecuados para mitigar riesgos.

Deberes: marco normativo

Ley de Sociedades de Capital: deber de diligencia y responsabilidad de los administradores, en particular arts. 225 y 236 y ss.

Directiva (UE) 2022/2555, NIS2: obligaciones de gobernanza, gestión de riesgos y supervisión en ciberseguridad.

Reglamento (UE) 2022/2554, DORA: exigencias reforzadas para entidades financieras en resiliencia operativa digital.

RGPD: relevancia en brechas de seguridad, medidas técnicas y organizativas y deberes de notificación, cuando proceda.

Ley 8/2011 y normativa de protección de infraestructuras críticas: aplicables a operadores críticos y servicios esenciales, según el caso.

Marco nacional futuro de transposición y gobernanza de ciberseguridad en España: referencia de contexto regulatorio y refuerzo supervisor (Ley de Coordinación y Gobernanza de la Ciberseguridad).

Gobernanza: relevancia estratégica de la ciberseguridad

Ciberseguridad como Pilar Estratégico
La ciberseguridad es esencial para la continuidad del negocio y la confianza digital en el entorno corporativo moderno.

Supervisión y Liderazgo de Consejos
Los consejos deben supervisar activamente el riesgo cibernético y demostrar liderazgo en su gestión y mitigación.

Evaluación y Políticas de Riesgo
Es fundamental evaluar riesgos digitales periódicamente y establecer políticas robustas para proteger la organización.

Formación y Cambio Cultural
La capacitación continua en ciberseguridad es clave para adaptarse a amenazas emergentes y fomentar un cambio cultural.

Gobernanza: preguntas que debemos hacer al consejo

1. ¿Conoce el Consejo el nivel de exposición a posibles ciberataques?
2. ¿La Empresa está preparada para responder a un ciberataque?
3. ¿Existe comprensión sobre las técnicas de la ciberdelincuencia y como puede afectar a nuestra empresa?
4. ¿Se cuenta con el personal o los proveedores y tecnología necesarios para dar adecuada respuesta?
5. ¿Se ha previsto la formación tanto de los técnicos responsables como de los directivos?
6. ¿Se ha incluido en el presupuesto anual una partida suficiente para atender las necesidades en la materia?

Gobernanza: pasos esenciales

Grant Thornton

Reglamento EU de Inteligencia Artificial (RIA)

Eloi Font, Socio de Legal de Grant Thornton

CONTEXTO

El uso de la Inteligencia Artificial (IA) crece:

- **11,4%** empresas españolas de +10 trabajadores utilizan IA / 44% grandes empresas (ONTSI, 2024).
- **20%** de las empresas españolas encuestadas emplean sistemas de IA (Banco de España, 2025).
- La IA transformará el **25%** de los puestos de trabajo en Catalunya (Cambra de Comerç BCN, 2026).

CONTEXTO

El RIA regula por 1ª vez el uso de la IA en la UE y establece obligaciones específicas.

- Muy técnico y de interpretación compleja.

España:

Anteproyecto Ley para el buen uso y la gobernanza de la inteligencia artificial (trámite): autoridades de vigilancia (AEPD, Banco España, CNMV, etc.).

Entrada en vigor

- El RIA entró en vigor en **agosto de 2024** y, con carácter general, **aplicable en agosto de 2026.**

- **Particularidades:**
  - **Febrero 2025**: Alfabetización y Sistemas prohibidos.
  - **Agosto 2025**: Modelos de Propósito General y Gobernanza de la IA.
  - **Agosto 2026:** Sistemas de Alto Riesgo del Anexo III.
    ÓMNIBUS DIGITAL: DICIEMBRE 2027
  - **Agosto 2027:** Sistemas de Alto Riesgo del Anexo I.
    ÓMNIBUS DIGITAL: AGOSTO 2028

Ámbito de aplicación

- **Reglamento UE:** aplicación directa en todos los EM de la UE.
- **Sistemas de IA introducidos en el mercado de la UE en la UE**, con independencia de si están establecidos/ubicados en la UE o en un tercer país.
- Sistemas de IA **establecidos/ubicados en un tercer país, cuando la información de salida generada** por el Sistema de IA **se utilice en la UE**.

El RIA propone enfoque basado en el riesgo, diferenciado en niveles, con obligaciones y garantías específicas.

1. Riesgo Inadmisible: prohibidos

Sistemas de IA con usos especialmente nocivos y contrarios a los valores de la UE.

2. Alto Riesgo

Pueden tener un impacto negativo en la seguridad de las personas o sus DDFF: objeto de una **estricta regulación.**

3. Riesgo Limitado

No suponen un riesgo relevante para los DDFF y los valores de la UE: incluyen **obligaciones de transparencia.**

4. Riesgo Bajo

Impacto bajo en la seguridad de las personas o en sus DDFF: **sin obligaciones adicionales.**

Grant Thornton

Riesgo inadmisible

Manipulación subliminal del comportamiento de personas que pueda causarles daños físicos o psicológicos.

Explotación de vulnerabilidades de grupos sociales para manipular su comportamiento de forma que pueda causarles daño.

Evaluación o **clasificación de personas** o grupos por su **comportamiento social** que pueda perjudicarlos.

Identificación biométrica en tiempo real en espacios de acceso público para autoridades policiales (salvo casos tasados y con autorización).

ÓMNIBUS DIGITAL: Sistemas de IA que generen **contenido sexualmente explícito e íntimo** sin consentimiento, así como **material de abuso sexual infantil.**

Alto Riesgo

- Implementaciones de IA en **productos o componentes de seguridad de productos** detallados en **Anexo I RIA** como, por ejemplo, maquinaria, juguetes, productos sanitarios, entre otros.
- Los previstos en el **Anexo III del RIA** (excepto no supongan un **riesgo importante** para la salud, seguridad o DDFF):
    - **Biometría** (Identificación biométrica remota; categorización biométrica; reconocimiento de emociones).
    - **Infraestructuras críticas** (Infraestructuras digitales críticas, funcionamiento del tráfico rodado, suministros de agua, gas, calefacción o electricidad).
    - **Educación y FP** (Asignación de personas físicas a Centros de educación o de FP; evaluación de los estudiantes; detectar comportamientos prohibidos en exámenes, entre otros).
    - **Empleo, gestión de los trabajadores y acceso al autoempleo** (Contratación o selección de personal; decisiones relativas a la promoción o resolución de relaciones laborales; asignación de tareas o seguimiento del rendimiento y conducta de los trabajadores, entre otros).
    - **Acceso y disfrute de servicios públicos y privados esenciales** (Acceso a beneficios sociales; calificación crediticia (salvo detección de fraude financiero); evaluación de riesgos y fijación de precios en seguros de vida y salud; triaje en asistencia sanitaria de urgencia, entre otros).

Alto Riesgo

- **Garantías del cumplimiento de la Ley** (Actividades de fuerzas y cuerpos de seguridad, como por ejemplo en la valoración de pruebas, personas sospechosas, entre otras).
- **Gestión de la migración, el asilo y el control fronterizo** (Valoración de las solicitudes, utilización de polígrafos, entre otros).
- **Administración de justicia y procesos democráticos** (Asistencia a una autoridad judicial en la investigación o interpretación y aplicación de hechos o de la Ley).

Alto Riesgo

Obligaciones técnicas

1. **Sistema de Gestión de Riesgos:** identificación riesgos conocidos y previsibles y adopción de medidas para gestionarlos (atendiendo especialmente a riesgos sobre la salud, seguridad y DDFF).

2. **Sistema de Gobernanza de los datos de entrenamiento y prueba,** asegurando buenas prácticas en su diseño, recolección y preparación, y evitando sesgos que afecten negativamente a las personas.

3. **Documentación Técnica y actualizada** que acredite que se cumplen los requisitos exigidos antes de su puesta en el mercado (durante todo el tiempo que se encuentre en el mercado).

4. **Registros de Actividad del Sistema ("logs")** durante toda la vida del Sistema de IA para facilitar la vigilancia de funcionamiento y detectar situaciones de riesgo.

5. **Diseñarse para que funcionen de forma transparente** para que los Responsables del despliegue interpreten y usen correctamente sus resultados de salida.

Alto Riesgo

Obligaciones técnicas

6 **Diseñarse para permitir la supervisión humana** durante su uso para minimizar los riesgos a la salud, seguridad y DDFF, con especial atención, a los riesgos residuales tras la aplicación de medidas contempladas en el Sistema de Gestión de Riesgos.

7 **Asegurar nivel adecuado de precisión, robustez y ciberseguridad** durante todo su ciclo de vida, que se declarará en la documentación técnica (con especial atención, a la protección contra la manipulación de los datos de entrenamiento).

Riesgo Limitado

Obligaciones de transparencia

1

Sistemas destinados a interactuar directamente con personas físicas (a menos que resulte evidente según circunstancias), excepto para sistemas autorizados por Ley para detectar, prevenir, investigar y enjuiciar delitos.

2

Sistemas que generen contenidos sintéticos de audio, imagen, vídeo o texto: los resultados de salida deben estar marcados en formato legible por máquina y detectable como generado o manipulado artificialmente.

3

Sistemas de reconocimiento de emociones o de categorización biométrica: Informar del funcionamiento a las personas físicas expuestas, excepto en sistemas autorizados por Ley para detectar, prevenir, investigar y enjuiciar infracciones penales.

4

Sistemas que generen contenidos de audio o video que constituyan una ultrasuplantación excepto (i) cuando se autorice su uso para para detectar, prevenir, investigar o enjuiciar delitos o (ii) cuando contenido generado por IA haya sido sometido a un proceso de revisión humana o de control editorial.

SANCIONES

Las sanciones por el incumplimiento del RIA podrán alcanzar, en el peor de los casos, hasta los 35 millones de euros o el 7% del volumen de negocio global del ejercicio anterior.

Grant Thornton

Action Plan

Recomendaciones

1. **Auditoría o fase de "Discovery":** IA propia y de terceros (*check list*).
2. Regulación interna a través de **Protocolo de Uso:** principios rectores y uso de IA prohibida y permitida.
3. Determinación del rol de la empresa (Proveedor, Importador, Distribuidor y/o Responsable del Despliegue).
4. Implementación de **obligaciones/controles** (Gestión de riesgos - ISO 42001).
5. **Formación** (Alfabetización).
6. **Gobernanza de la IA** - AI Officer.

Grant Thornton

NUEVOS RETOS

Tu empresa ante la IA y la ciberseguridad

Cambra de Comerç de Barcelona

Grant Thornton