

APROBACIÓN DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL

01

El Reglamento Europeo de IA, una de las normativas más ambiciosas a nivel mundial, establece principios para el desarrollo ético y la protección de datos. Las organizaciones tendrán hasta el **verano de 2026** para adaptarse a esta normativa, lo que supone un reto significativo para las pequeñas y medianas empresas y los profesionales de la privacidad.

ENTRADA EN VIGOR DE LA DIRECTIVA NIS2

02

Aprobada por la UE en 2022, los Estados miembros tenían hasta el **17 de octubre del 2024** para trasponer la Directiva NIS2 a su legislación nacional. Esta directiva establece nuevos estándares de ciberseguridad para proteger las redes y sistemas de información de sectores claves como energía, salud, transporte y finanzas.

DORA: DIGITAL OPERATIONAL RESILIENCE ACT

03

Aplicable desde el **17 de enero de 2025**, este reglamento asegura que las instituciones financieras sean resilientes frente a riesgos tecnológicos. DORA busca proteger a los usuarios y mantener la estabilidad financiera frente a ciberataques y fallos tecnológicos.

IA GENERATIVA Y LA PRIVACIDAD

04

La democratización de tecnologías como ChatGPT, Copilot o DALL-E plantean **retos sobre la privacidad**. Estos sistemas, que requieren grandes volúmenes de datos para su entrenamiento, pueden generar riesgos relacionados con el consentimiento y la transparencia en los responsables del despliegue que deben analizar y conocer.

RETOS PARA LA APLICACIÓN DEL DERECHO AL ACCESO (CEPD)

05

El Comité Europeo de Protección de Datos señala que es necesaria una mayor **sensibilización sobre las Directrices 01/2022** para ayudar a los responsables del tratamiento a favorecer el derecho de acceso, como elemento principal de la facultad de control del interesado sobre sus datos personales.



CRIPTOACTIVOS Y PRIVACIDAD: REGLAMENTO MICA

06

El reglamento MiCA da a los Estados miembros de la UE hasta el **1 de julio** de 2026 para adaptarse a los cambios. Este reglamento regula el mercado de criptoactivos en la UE, estableciendo medidas para garantizar la privacidad de los usuarios en transacciones digitales y prevenir el uso ilícito de criptomonedas. Además, la **AEPD** ha publicado un documento sobre anonimización en el entorno blockchain.

DIRECTIVA WHISTLEBLOWING

07

Con un plazo de adaptación para las empresas hasta **marzo de 2024**, la Directiva de protección a los informantes que denuncian irregularidades entró en vigor el 1 de diciembre de 2023, estableciendo canales seguros para la comunicación para garantizar la confidencialidad de las fuentes, lo que obliga a implementar protocolos y procesos de información de protección de datos.

INCREMENTO EN BRECHAS DE DATOS

08

Múltiples sectores como la sanidad, finanzas y el comercio electrónico fueron testigos de un aumento de las brechas de seguridad de datos, obligando a las empresas a invertir en mejoras de sus **mecanismos de protección frente a los ciberataques**, así como en contar con sistemas de notificación y apoyo profesional especializado.

CONCIENCIACIÓN PÚBLICA SOBRE LA PRIVACIDAD

09

El Reglamento Europeo de IA, una de las normativas más ambiciosas a nivel El **75% de los ciudadanos españoles** reconoce sentir una mayor preocupación hacia la privacidad y cada vez más usuarios exigen transparencia sobre cómo se usan sus datos personales, lo que supone una presión más para las empresas y organizaciones para adoptar una adecuada cultura de la privacidad.

SANCIONES POR INFRACCIÓN DEL RGPD

10

En el **último trimestre de 2024**, la Agencia Española de Protección de Datos (AEPD) impuso dos multas que se encuentran entre las 10 más altas por infracción del RGPD en España: una sanción de **5 millones de euros** y otra por valor de **3,5 millones a empresas** del sector eléctrico y sector de telecomunicaciones.

