

VER MÁS...

CÓMO ADECUAR TU EMPRESA AL REGLAMENTO DE INTELIGENCIA ARTIFICIAL

PRIMEROS PASOS

La reciente aprobación del Reglamento Europeo de Inteligencia Artificial (RIA) marca el inicio de un periodo de 24 meses en el que las empresas y organismos públicos deben adecuarse a sus obligaciones. La norma, similar en su complejidad y alcance al Reglamento General de Protección de Datos (RGPD), impone sanciones severas de hasta 35 millones de euros o el 7% de la facturación anual, lo que hace imprescindible un cumplimiento oportuno. Las empresas pioneras ya han comenzado este proceso, estableciendo marcos de gobierno interno y de control que aseguren un uso responsable de la inteligencia artificial alineado con los requisitos del RIA.

Para adecuarse al RIA, las empresas deben comenzar con un inventario de las inteligencias artificiales (IAs) que utilizan, determinando su ubicación y propósito. Esto implica desarrollar una metodología de identificación y mantenimiento de registros actualizados. Asimismo, es crucial implementar un modelo de gobierno de IA que, aunque no especificado por el RIA, debe definir roles y competencias clave en el cumplimiento normativo. Aprovechar los mecanismos existentes en privacidad y ciberseguridad, establecer metodologías de riesgos y roles de la organización en cada proyecto de IA, y fomentar la concienciación en todos los niveles de la empresa, son pasos fundamentales para garantizar la adecuación al RIA. Además, es vital verificar que ningún uso actual de IA esté prohibido por la nueva normativa.

¿CÓMO SE PUEDEN PREPARAR LAS EMPRESAS PARA PREVENIR CIBERATAQUES?

VER MÁS...



Las empresas deben adoptar medidas preventivas rigurosas para protegerse contra los ciberataques, que incluyen amenazas como *phishing*, *malware*, *ransomware*, fraude en línea y suplantación de identidad. Estos ataques afectan globalmente, y el sector financiero es un objetivo principal. En Colombia, el Índice de Inteligencia de Amenazas X-Force de IBM 2024 destaca que el país es el segundo más atacado en Latinoamérica, con la explotación de aplicaciones públicas representando el 45% de los incidentes, seguido por phishing y uso de cuentas válidas con un 22%. En 2023, hubo un notable aumento del 266% en el malware destinado al robo de identidades, complicando la detección y elevando los costos de respuesta para las empresas.

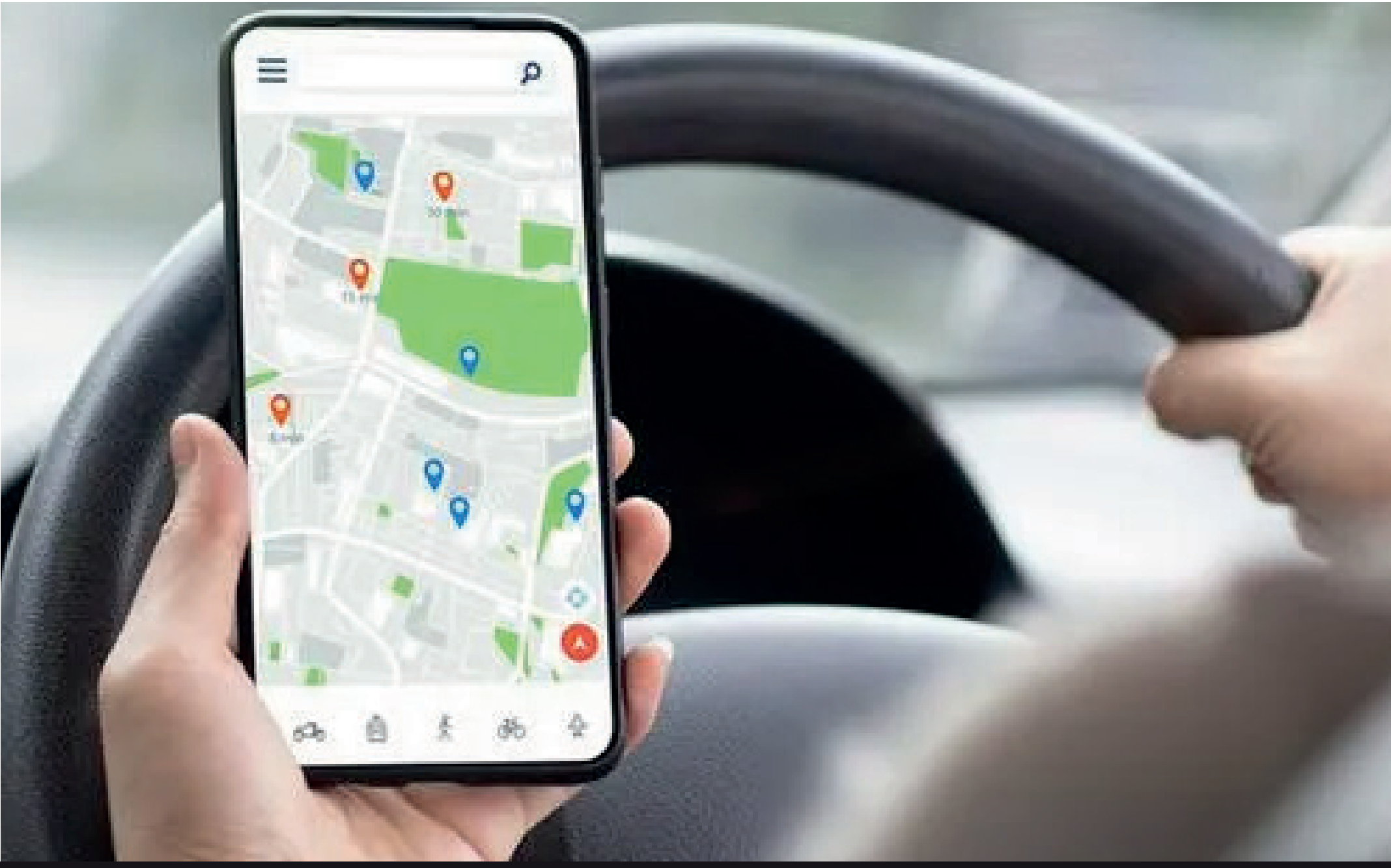
Un ejemplo de cómo las empresas pueden prepararse es uFlow, una empresa de tecnología financiera que ha implementado estándares de seguridad elevados y ha obtenido la certificación ISO/IEC 27001:2013. Esta certificación cubre áreas como Desarrollo, Soporte, Operaciones y su solución SaaS de motor de decisiones. La entidad auditora NYCE validó que uFlow cumple con los requisitos internacionales para un Sistema de Gestión de la Seguridad de la Información. Según Santiago Etchegoyen, CTO de uFlow, esta certificación refleja años de trabajo sistemático en procesos de seguridad que superan los estándares, reduciendo así los riesgos de ciberataques y protegiendo tanto los datos de clientes como la integridad de los sistemas financieros. Adicionalmente, el cumplimiento de normativas legales y regulatorias ayuda a evitar sanciones, destacando la importancia de la seguridad de la información en un mundo cada vez más digitalizado.

META RECIBIÓ REVISIÓN DE LA CORTE SUPREMA EN DEMANDA DE INVERSORES SOBRE RECOLECCIÓN DE DATOS

VER MÁS...

La Corte Suprema de EE. UU. está revisando una demanda multimillonaria contra Meta Platforms Inc. que acusa a la empresa de engañar a los inversores sobre riesgos relacionados con la privacidad de los datos de usuarios, en el contexto del escándalo de Cambridge Analytica. Los jueces evaluarán si un tribunal de apelaciones cometió un error al permitir que la demanda avanzara, considerando que las revelaciones sobre el escándalo afectaron el precio de las acciones de la empresa. Esta revisión podría influir en las reglas legales sobre la divulgación corporativa y tiene implicaciones significativas para las empresas en términos de cómo deben divulgar riesgos pasados que podrían afectar el valor de las acciones.

Los accionistas demandantes argumentan que Facebook (ahora Meta) no reveló adecuadamente el riesgo de que los datos de usuarios fueran mal utilizados, lo que contribuyó a caídas en el precio de las acciones. Por otro lado, Meta sostiene que no tenía razones para anticipar que el escándalo afectaría significativamente a la empresa. La decisión de la Corte Suprema, que se espera en unos nueve meses, podría tener implicaciones financieras considerables para Meta, incluida la posibilidad de enfrentar un acuerdo multimillonario si el caso avanza a juicio.



"ENGAÑAN AL USUARIO": SUPERTRANSPORTE INVESTIGÓ A 'APPS' DE TRANSPORTE Y ALISTA SANCIONES

VER MÁS...

La Superintendencia de Transporte está llevando a cabo investigaciones sobre las aplicaciones de transporte en Colombia debido a prácticas engañosas hacia los usuarios, lo cual podría resultar en sanciones. Estas investigaciones se centran en el transporte ilegal e informal, donde las empresas detrás de las aplicaciones argumentan no prestar el servicio directamente, sino arrendar vehículos, evadiendo así responsabilidades legales. La entidad ha emitido fallos contra estas compañías, destacando que, aunque cambien la denominación del servicio, sigue siendo una prestación de servicio sujeta a multas y sanciones. Además, la Superintendencia está investigando la inducción al error de los usuarios por parte de las aplicaciones, lo que podría resultar en sanciones significativas.

Es importante mencionar que estas acciones de la Superintendencia buscan proteger a los usuarios y garantizar la legalidad en el transporte, enfrentando desafíos como el transporte ilegal y la evasión de normativas de tránsito y transporte por parte de algunas empresas y vehículos en el país.