

Iberoamérica fija criterios para el uso de datos personales en inteligencia artificial

por Iván Martínez, CEO de Intedya

La Red Iberoamericana de Protección de Datos (RIPD) ha publicado en noviembre de 2026 los *Estándares Iberoamericanos sobre el uso de Datos Personales en Sistemas de Inteligencia Artificial*. El documento aborda una cuestión que muchas organizaciones ya tienen sobre la mesa: cómo proteger los datos personales cuando se incorporan a sistemas capaces de aprender de ellos, generar perfiles o influir en decisiones que afectan a las personas. El texto ofrece una referencia común para una región en la que conviven marcos jurídicos distintos. La exigibilidad de cada medida depende de la normativa aplicable, pero contar con criterios compartidos facilita que una empresa con presencia en varios países pueda evaluar sus proyectos y proveedores con una metodología común y ajustar después sus controles a las obligaciones de cada jurisdicción.

A mi juicio, una de las aportaciones más relevantes del documento es que sitúa la protección de datos en todo el ciclo de vida de la inteligencia artificial. La revisión empieza al decidir para qué se utilizará el sistema y con qué información se va a desarrollar o probar. Continúa cuando se incorpora a un proceso real, cuando cambian sus condiciones de uso y cuando la organización tiene que responder por un resultado que ha afectado a una persona.

Para qué se utilizan los datos y cuándo pueden reutilizarse

Imaginemos que una empresa quiere incorporar inteligencia artificial a su servicio de atención al cliente. Puede utilizarla para resumir una conversación y ayudar a un agente a resolver una incidencia. También puede usar esas mismas conversaciones para entrenar un modelo que prediga qué clientes tienen más probabilidades de cancelar su contrato. Los datos de partida son los mismos, pero cambian la finalidad, lo que el cliente podía razonablemente esperar y las consecuencias del tratamiento. Si, además, el proveedor quiere aprovechar esas conversaciones para mejorar un producto que comercializa a otras empresas, aparece otra finalidad que requiere su propio análisis.

Los estándares piden identificar y documentar los tratamientos a lo largo de las distintas fases del sistema, desde el desarrollo y el entrenamiento hasta su evaluación, funcionamiento y mejora. En la práctica, eso obliga a preguntarse de dónde vienen los datos, para qué se obtuvieron, qué base jurídica ampara cada uso y si una reutilización es compatible con la finalidad original. Cuando un proveedor trata información por cuenta de una organización y quiere destinarla a fines propios, como entrenar o mejorar sus modelos, el documento señala que, con carácter general, ese uso constituye una finalidad distinta y requiere una habilitación expresa y una base jurídica que lo ampare.

El mismo razonamiento alcanza a la información accesible en internet. Un perfil profesional, una fotografía o un comentario pueden estar al alcance de cualquiera y, aun así, su uso para entrenar un modelo requiere una justificación. Una persona puede haber publicado su trayectoria para que la contacten y encontrarse después con que esa información se utiliza para construir un sistema de clasificación de candidatos. La organización debe valorar ese nuevo uso teniendo en cuenta el contexto en el que se publicaron los datos, las expectativas de las personas y los efectos que puede producir el tratamiento.

La información que la IA deduce también importa

Uno de los aspectos más interesantes del documento es cómo lleva el principio de minimización a la práctica. La revisión abarca tanto los datos que recibe el sistema como lo que puede deducir a partir de ellos. Un modelo puede combinar horarios, ubicaciones o hábitos de consumo y generar una inferencia sobre la salud o la vulnerabilidad económica de una persona. Esa conclusión puede acabar influyendo en cómo se la trata, incluso cuando es imprecisa o está equivocada.

Por eso, en un proyecto de IA conviene revisar qué variables necesita realmente el sistema, qué perfiles genera y quién puede acceder a ellos o utilizarlos. En un proceso de financiación, por ejemplo, una empresa puede comprobar que el modelo utiliza información pertinente y descubrir después que la combinación de ciertas variables funciona como un indicador indirecto de circunstancias personales que nunca quiso tener en cuenta. La calidad de los datos también debe examinarse en relación con el uso previsto. Un conjunto de datos que funcionó bien en una prueba puede resultar insuficiente para una población distinta o para un contexto en el que las condiciones han cambiado.

Los estándares dedican especial atención a las inferencias sensibles, a las personas en situación de vulnerabilidad y a los neuro datos. También examinan el uso de sistemas que intentan inferir estados cognitivos, emocionales o conductuales. Pensemos en una herramienta que atribuye a un trabajador un determinado estado emocional a partir de su voz o su comportamiento. La evaluación debe considerar para qué necesita la empresa esa inferencia, qué fiabilidad tiene, quién puede verla y qué consecuencias puede tener en una relación en la que el trabajador dispone de un margen limitado para cuestionar su uso.

Cuando existe una intervención humana efectiva

Otra cuestión que veremos cada vez más en las auditorías es cómo distinguir un sistema que ayuda a decidir de un proceso en el que la persona se limita a confirmar lo que el sistema ya ha resuelto. Los estándares establecen que, para excluir el carácter exclusivamente automatizado de una decisión, la intervención humana debe ser previa, real y efectiva. Quien interviene debe poder comprender y valorar el resultado, y contar con autoridad suficiente para confirmarlo, modificarlo o apartarse de él. En un proceso de selección, por ejemplo, el sistema puede ordenar candidaturas y dejar fuera de la lista visible a quienes quedan por debajo de una puntuación. Aunque el equipo de recursos humanos revise todos los perfiles que aparecen en pantalla, el primer filtro ya ha determinado quién llega a esa revisión. En una auditoría, yo preguntaría si el equipo puede recuperar una candidatura descartada, conocer los datos que influyeron en el resultado y reconsiderar la exclusión antes de que produzca efectos. Para que ese control funcione, la persona también necesita tiempo, formación y acceso a información suficiente para ejercer su criterio.

El documento aborda asimismo el riesgo de discriminación. Si un sistema se utiliza para priorizar solicitudes, valorar candidaturas o asignar recursos, las pruebas deberían permitir examinar si determinados grupos reciben sistemáticamente resultados desfavorables y analizar por qué ocurre. En el caso de una herramienta de selección, una comprobación concreta sería revisar si el modelo penaliza las interrupciones de la trayectoria profesional y si ese criterio tiene una justificación relacionada con el puesto.

Transparencia, explicabilidad y ejercicio de derechos

Informar de que una empresa utiliza inteligencia artificial puede ser un primer paso. Para que esa información sirva a la persona afectada, debe permitirle entender con qué finalidad se utiliza el sistema, qué papel tiene en el proceso y cuáles pueden ser las consecuencias. Cuando proceda, también debe poder conocer las vías disponibles para solicitar una intervención humana, impugnar una decisión o ejercer los derechos que le reconozca la normativa aplicable. La explicabilidad adquiere especial importancia cuando hay una reclamación. Si una persona pregunta por qué su solicitud quedó relegada, una descripción general de la tecnología le dirá poco sobre su caso. La organización necesita poder explicar qué información se utilizó, qué factores fueron relevantes y qué margen existía para revisar el resultado. Esto obliga a diseñar el proceso con antelación. Hay que decidir qué información se conserva para reconstruir una decisión, durante cuánto tiempo, con qué controles de acceso y quién puede corregir los datos o reconsiderar el resultado si se detecta un error.

Proveedores, transferencias y seguridad en el uso cotidiano

Muchas organizaciones incorporarán la IA a través de aplicaciones que ya tienen contratadas. Una actualización puede añadir la posibilidad de resumir reuniones, analizar documentos o sugerir respuestas a correos. Para el usuario puede ser una opción más en el menú. Para la empresa, activar esa función puede cambiar quién recibe la información, en qué país se procesa, cuánto tiempo se conserva o si puede reutilizarse para mejorar un servicio. Los estándares examinan la responsabilidad de los actores que intervienen a lo largo de la cadena de valor y las transferencias internacionales de datos. En la práctica, al revisar un proveedor interesa saber qué ocurre con los documentos adjuntos, las instrucciones que introduce el usuario y las respuestas generadas. También importa saber qué proveedores intervienen, qué funciones se pueden configurar y cómo se puede comprobar que las condiciones acordadas se aplican efectivamente al servicio contratado.

El documento presta atención a riesgos propios de estos sistemas, como la posibilidad de que un modelo reproduzca información personal que recibió o de que una herramienta permita acceder a contenidos que deberían estar restringidos. En una aplicación de IA conectada al repositorio documental de una empresa, por ejemplo, una prueba pertinente sería comprobar si respeta los permisos de los documentos originales al generar sus respuestas. Y si se produce una exposición, la organización debería poder identificar la información afectada, contener el incidente y valorar las actuaciones que correspondan.

Qué deberían hacer ahora las empresas

La primera medida que adoptaría sería revisar qué usos de inteligencia artificial existen ya en la organización. Además de los proyectos aprobados formalmente, incluiría las funciones activadas en aplicaciones de uso cotidiano y las herramientas que los equipos han incorporado por su cuenta. Para cada uso, identificaría qué proceso lo utiliza, con qué finalidad, qué datos personales recibe o qué información puede inferir sobre las personas, quién es el proveedor y quién asume la responsabilidad dentro de la empresa.

Con ese inventario, daría prioridad a los usos que manejan información sensible, afectan a personas en situación de vulnerabilidad o influyen en decisiones sobre empleo, financiación o acceso a servicios. En esos casos, revisaría la base jurídica, la necesidad de los datos utilizados, el riesgo de discriminación y la procedencia de una evaluación de impacto. Si el sistema interviene en una decisión, comprobaría con un caso de prueba si la persona responsable dispone de información, tiempo y autoridad para corregir el resultado antes de que produzca efectos, y si la organización puede explicar después qué ocurrió.

También revisaría los contratos y la configuración efectiva de los servicios. Conviene comprobar si el proveedor conserva los documentos y las consultas, si puede reutilizarlos para mejorar sus modelos, qué subproveedores intervienen y dónde se tratan los datos. Con esa información, la empresa puede definir qué herramientas autoriza para cada tipo de información y dar instrucciones concretas a los equipos. Quien necesita resumir un expediente de personal, por ejemplo, debe saber qué herramienta puede utilizar, qué información puede introducir y a quién consultar si el caso plantea dudas.

Por último, incorporaría estas comprobaciones al proceso habitual de aprobación y gestión de cambios. Cada uso debería tener un responsable, unas condiciones de utilización y evidencias de que los controles funcionan. Si cambia el modelo, el proveedor, la finalidad o la influencia del sistema en una decisión, corresponde revisar la autorización. En una auditoría, la prueba más clara será tomar un caso concreto y comprobar quién autorizó ese uso, qué información se trató, cómo se supervisó el resultado y qué respuesta puede dar la empresa si una persona afectada pide una explicación.