

Inteligencia Artificial Responsable

Por *María Luisa Acuña*

No es sorpresa para nadie escuchar de la Inteligencia Artificial generativa. Pueden existir muchas definiciones, pero en términos sencillos, es un tipo de Inteligencia Artificial (IA) que puede generar nuevos contenidos, como texto, imágenes y videos a través de patrones de aprendizaje que se obtienen de datos preexistentes. Asimismo, este tipo de IA también puede incluir varias técnicas de aprendizaje automático.

A menudo escuchamos historias de familiares y colegas que usan Chat GPT (tipo de IA generativa más difundido) para distintas labores que pueden tardar mucho tiempo, o que la persona no tiene conocimiento experto o bien, no nacen naturalmente en ellos. Algunos ejemplos van desde la confección de un discurso de apertura señalando la temática, público objetivo y extensión de tiempo, el envío de un correo electrónico de comunicaciones dentro de la compañía en el que el remitente quiere parecer más cercano y empático cuando esas características no son innatas o con nuestros hijos, creando cuentos a la medida que se pueden hasta ilustrar, indicando características del niño, extensión y gustos particulares. Todos estos casos se tratan justamente del uso de Inteligencia Artificial Generativa.

La cuestión relevante es que en todas estas interacciones con Chat GPT que nos parecen muy lógicas e intuitivas, no hay ningún cuestionamiento en si estoy entregando información sensible, o hacia donde se va toda la información que entrego, o que hacen con la información que envío, o más legalmente, si los entregables de IA generativa están protegidos por derechos de autor. Al final todo se trata de la información y si bien estos riesgos no son propios solamente de este tipo de IA, su uso cada más frecuente, su libre acceso y asombrosa capacidad nos presentan nuevos desafíos para la seguridad de la información y la privacidad de los datos, que es importante tener en consideración aun cuando no exista en nuestro país una regulación específica.

(1) IA de uso libre: Si es de su interés que los colaboradores tengan acceso y puedan usar IA en sus labores diarias, al menos deberá establecer una política en la que incluya cómo usar correctamente IA, que información se debe proteger y las implicancias de una violación a la confidencialidad en esta materia. En este mismo sentido, deberá actualizar las cláusulas contractuales que sean atingentes.

(2) IA como procesos de negocio: Si está evaluando que IA sea parte de sus procesos de negocio, debe evaluar los riesgos de privacidad de los datos a lo largo del ciclo de vida del desarrollo. Para esto, puede ser de utilidad el Framework de la NIST AI 100-1 que entrega elementos específicos de gestión de riesgos para inteligencia artificial (AI RMF 1.0).

(3) IA transparente: El miedo al uso de IA es generalizado principalmente porque representa un conjunto de habilidades que en muchos aspectos puede superar a la inteligencia humana con la ayuda de la tecnología, y por otro, porque es como una caja negra en la que se desconoce lo que pasa con la información. Por ello, las organizaciones que están analizando utilizar IA en sus procesos de negocios o que ya lo han desplegado, deben trabajar en transparentar a su entorno, cuales son sus políticas de privacidad y protección de datos, en cómo sus algoritmos se hacen cargo de cuestiones éticas como la no discriminación, sesgos y equidad, entre otros, y como la IA puede complementar y mejorar ciertas tareas humanas.

Todos estos conceptos se agrupan dentro de lo que hoy comúnmente conocemos como “Inteligencia Artificial Responsable”, que es la corriente destinada a diseñar, desarrollar e implementar IA con una intención de empoderar a los colaboradores y organizaciones, impactando de una manera positiva y justa hacia los clientes y sociedad, para así, contribuir a un entorno de confianza en el uso de esta tecnología que pueda ser utilizada amplia y democráticamente por todos, pero de una manera sana.