trendTIC
Fecha: 30/10/2024 Audiencia: 0 Sección: CIENCIA Y TECNOLOGIA
Vpe: $0 Tirada: 0 Frecuencia: MENSUAL
Vpe pág: $0 Difusión: 0
Vpe portada: $0 Ocupación: 74,12%

Aprovechar la Inteligencia Artificial con procesos seguros en cada etapa

Por Daniel Álvarez Valenzuela
Coordinador Nacional de Ciberseguridad

Chile tiene hoy ventajas comparativas en lo relativo a su marco regulatorio tecnológico. Durante el gobierno del presidente Gabriel Boric se ha avanzado sustancialmente en la regulación de temas digitales, como la protección de datos personales, la ciberseguridad, la inteligencia artificial (IA), la transformación digital y las fintech, entre otros. Todos estos avances son fruto de muchos años de discusión legislativa y de la capacidad de alcanzar acuerdos.

En materia de ciberseguridad e inteligencia artificial existen avances importantes. Chile ya cuenta con una Política de IA como primer paso, va en la segunda versión de la Política Nacional de Ciberseguridad y tiene desde abril la Ley Marco de Ciberseguridad, que establecerá una nueva institucionalidad y campo regulatorio.

Ahora nos toca hacernos cargo de los numerosos desafíos respecto del uso de las tecnologías IA y su relación con la ciberseguridad. En particular, lograr que la implementación de la IA en nuestro país se realice de acuerdo con los lineamientos para un desarrollo seguro de la IA, reglas elaboradas en conjunto por agencias de ciberseguridad de todo el mundo, lideradas por la CISA de EE.UU. y el NCSC del Reino Unido y que incluyeron al CSIRT de Gobierno de Chile y que fueron plasmadas en un documento llamado "Guidelines for Secure AI Develoment".

Sin ciberseguridad, explica el escrito, no podemos usar la IA de forma segura, resiliente, privada, justa, eficaz ni confiable. Más aún, debemos entender que cuando se trata de una tecnología nueva y de alcances desconocidos, las implicancias de no atender debidamente la ciberseguridad son insospechadas.

Dado lo anterior, sus directrices llaman a tener en cuenta la seguridad en cada paso, desde el diseño de los sistemas de IA, pasando por el desarrollo, su implementación, y su operación y mantenimiento. Esto es lo que se denomina "seguridad por diseño" y es una actitud hacia la tecnología que debemos tener en todo orden de cosas, no solo en la IA.

Para lograrla, los desarrolladores y proveedores de sistemas que emplean IA deben asumir una responsabilidad sobre la seguridad de los usuarios de sus sistemas, adoptar una transparencia radical y construir estructuras organizacionales y un liderazgo que tengan a la seguridad por diseño como una prioridad de negocios.

Implementar la seguridad por diseño a los desarrollos basados en IA nos permitirá anticiparnos hoy a casos de uso malicioso de esta tecnología, más allá incluso de los ejemplos que ya hemos observado en otros países, en que actores logran, por ejemplo, convencer a los modelos de IA para que les entreguen información confidencial o que ejecuten acciones no autorizadas.