Javier Puyol
Magistrado y letrado del Tribunal Constitucional en excedencia. Socio director de Puyol Abogados

La IA como aliada de la ciberseguridad

Hoy en día debe tenerse presente que la Inteligencia Artificial (IA) y el aprendizaje automático se está utilizando cada vez más con el propósito de detectar y responder a las ciberamenazas.

En este sentido, tal como señala Mackay, la IA se utiliza en diversos sentidos a los efectos de propiciar un incremento de la ciberseguridad en el ámbito de las organizaciones y de sus sistemas. En este sentido, destaca este autor lo siguiente:

a). Una de las formas en que se utiliza la IA es para detectar vulnerabilidades en el tráfico de red, y ello se produce mediante el análisis de patrones en los datos de tráfico de red, los sistemas de IA pueden identificar amenazas potenciales y alertar a los profesionales de la ciberseguridad.

b). De manera adicional, al mismo tiempo la IA también puede utilizarse para analizar una gran cantidad de datos en busca de posibles amenazas, y ello puede ser especialmente útil para identificar aquellas, que podrían no ser inmediatamente obvias para los analistas humanos.

c). Otra forma en que la IA se utiliza en ciberseguridad es automatizando tareas rutinarias para que consuman menos tiempo. En este sentido, cita un ejemplo consistente en que los sistemas de IA pueden utilizarse para parchear y actualizar automáticamente los sistemas, liberando a los profesionales de la ciberseguridad para que puedan centrarse en tareas más complejas. d). Finalmente, señala que la IA también puede utilizarse para generar informes y alertas, proporcionando información valiosa que ayude a tomar decisiones informadas en materia de ciberseguridad.

Por todo ello, los beneficios potenciales de la IA en la ciberseguridad son significativos, ya que al mejorar la velocidad y la precisión de la detección de amenazas y la respuesta, la IA puede ayudar a reducir el impacto de los ciberataques. En este sentido, destaca que la IA también puede ayudar a mejorar la eficiencia de las operaciones de ciberseguridad, liberando tiempo y recursos valiosos para otras tareasi. En este orden de cosas desde IBM se destaca el papel que juega la IA con relación a la

ciberseguridad en unos escenarios concretos y determinados, destacando una serie de condiciones o interrelaciones entre ambas que son las que se indican a continuación: a). La protección de datos en entornos de nube híbrida

Las soluciones de IA identifican datos ocultos, hacen un seguimiento de las anomalías en el acceso a datos y alertan a los equipos de seguridad sobre posibles actividades de riesgo por parte de cualquiera que acceda a los datos, lo que ahorra un tiempo valioso en la detección y resolución de problemas.

b). La existencia de alertas más precisas y clasificadas por prioridad. El análisis de riesgos basado en IA permite generar resúmenes de incidentes para alertas de alta fidelidad y automatizar las respuestas, lo que a su vez acelera en un promedio del 55 % la investigación y la clasificación de las alertas.

c). La necesidad de la existencia de un equilibrio entre las necesidades de acceso de los usuarios y la seguridad

La IA facilita el equilibrio entre la seguridad y la experiencia del usuario mediante el análisis del riesgo de cada intento de inicio de sesión y la verificación de los usuarios a través de datos de comportamiento, lo cual simplifica el acceso para los usuarios verificados y reduce el coste relacionado con el fraude hasta en un 90 %.

Una de las cuestiones más trascendentes en esta interrelación entre IA y ciber amenazas es la del tiempo de respuesta

Una de las cuestiones más trascendentes en esta interrelación entre la IA y las ciber amenazas es la relativa al tiempo de respuesta ante la producción de estas, que se ha constituido unas de las medidas más trascendentes en la configuración de los sistemas y de los equipos, teniendo presente que la evolución tecnológica afecta indistintamente tanto a los ataques como a las defensas ante los mismos, por ello las pautas de reacción ante este tipo de situaciones no sólo tiene que buscar la eficacia y la eficiencia en los instrumentos de defensa, sino que tiene que llevarse a cabo de una manera sencilla en sus planteamientos, de modo que propicie la celeridad en la toma de decisiones, y ello permita, precisamente, una defensa más adecuada ante dicha situación de riesgo, y en este ámbito la IA, puede jugar un papel esencial a los efectos de poder facilitar adecuadamente dicha defensa, teniendo presente que el autoaprendizaje puede constituir una facto muy importante de mitigación de los daños que puedan inferirse a consecuencia de dichos ataques.

Finalmente, debe tenerse presente que identificación y la predicción de amenazas constituye y representa básicamente otro factor, que influye en los plazos de respuesta a los ataques cibernéticos, y en los que en buena medida, no solo influyen los recursos tecnológicos o incluso de las herramientas de IA de que se disponga, sino también la capacitación y la formación de los profesionales que deben velar por la seguridad de tales equipos y sistemas, y su manejo, donde quedan reflejado la importancia que sigue teniendo el factor humano en los entresijos de este ámbito de actuación.

istock