Datos, ciberseguridad e inteligencia artificial
Fecha: 09-06-2025
Alumno: Taisen Romero Bañuelos.

IA, aprendizaje automático y estadística – Una taxonomía

La exploración del campo de la ciberseguridad bajo el lente de los datos continúa. Se mencionan aspectos clave para poder diferenciar cierta terminología que a menudo se usa uno como sinónimo del otro. Más allá de eso, capta fuertemente mi atención la taxonomía de los algoritmos y modelos mencionados. Algunas cosas que se mencionan (como el aprendizaje por refuerzo y el semi supervisado) me pueden ser sumamente útiles en proyectos fuera de este curso, particularmente aquellos que tienen que ver con datos difíciles de obtener y el PNL.
En cuanto al enfoque de la ciberseguridad, me parece curiosa la relación simbiótica que ha tenido la computación (o ML) con la estadística. Se entiende el ML como las técnicas o metodologías para que la computadora piense, algo así como una máquina de caja negra ya que es la estadística la que se encarga de descubrir cómo se generan esos datos. De hecho, justo a partir de la identificación de los tipos de datos que hay uno puede inferir más fácilmente qué modelo es ideal para trabajar. El tipo de datos (por ejemplo, logs, flujos de red, texto libre en correos o reportes) no solo condicionará el modelo a elegir, sino también el grado de responsabilidad ética que conlleva su uso porque no es lo mismo trabajar con textos de correos electrónicos a trabajar con biométricos. De hecho, siguiendo esta línea quisiera mencionar de nuevo el tema del Reglamento de la UE (2024/1689) que se aplicó en España hace poco. En este nuevo marco legal se clasifican los sistemas de IA en 4 grupos según su nivel de riesgo.

1. **Riesgo Inaceptable (prohibidos):** Manipulación subliminal, clasificación social por gobiernos (al estilo del sistema chino), detección emocional en el entorno laboral o educativo (con excepciones), IA que explote vulnerabilidades de personas (edad, discapacidad).
2. **Riesgo alto:** IA utilizada en infraestructuras críticas (ej. transporte, salud), control de fronteras, sistemas de justicia, evaluación de estudiantes o trabajadores, selección de personal, evaluación de crédito
3. **Riesgo limitado:** Chatbots, asistentes virtuales.
4. **Riesgo mínimo o nulo:** IA de uso general sin impacto relevante en los derechos fundamentales.

Como nos damos cuenta, el nivel de riesgo está estrechamente ligado al tipo de datos que maneja el sistema y a cómo afecta a la sociedad.
A nivel personal, creo que es crucial rescatar la idea de que un modelo no es solo un algoritmo funcionando en segundo plano, sino que es una pieza activa dentro de una estructura mayor que involucra a profesionales encargados y a usuarios finales que sin saberlo podrían verse afectados (aunque siempre me parece más atractivo explorar esos límites fuera del margen legal para dimensionar el verdadero potencial de la tecnología si no se usase con fines maliciosos).