INFLUENCIA DE LA INGENIERÍA SOCIAL PARA LA TOMA DE DECISIONES EN LA INGENIERÍA PORTUARIA Y COSTERA.

M. en C. Etelberto D. Serrano Flores, eserrano@imt.mx, OrcID: 0009-0006-2188-0854., M. en C. María Dolores Servín Lugo, dservin@imt.mx

El conocimiento actual ha permitido un gran espacio para el desarrollo y transformación de la ingeniería y la ciencia. Existen algunas corrientes de pensamiento que califican a la ciencia e ingeniería como algo que ha generado progreso, así como excesos, ha fomentado el control, así como la deshumanización con todas sus repercusiones, no obstante, se asemeja a que en lugares donde no se encuentran estas disciplinas, predominan el hambre, la injusticia, el control inflexible, la violencia y la insalubridad con efectos más graves o considerables.

La ingeniería social sin cualidades académicas y políticas legitimas, parece influir en la vida social al aplicar el principio constructivo de la forma en que se juntan y se dividen los grupos de personas mediante la segmentación, la violencia y la agresividad, generan con ello la evolución y diversificación en distintos escenarios con diversos problemas los cuales trata de resolver un ingeniero social. Galindo C. L. J., (2009).

La ciencia de la comunicación trata de entender cómo es que se articulan las comunidades en función de un común denominador, lo que da lugar de manera integral a una ingeniería de la comunicación social que interactúa en diversos espacios sociales, que a través de la comunicación oral se obtiene información desde varias disciplinas con un perfil científico que actúa desde un nivel individual, grupal y colectivo.

La inteligencia artificial (IA) definida en el Oxford English Dictionary (OED) como la capacidad de una computadora o alguna otra máquina para mostrar o simular un comportamiento inteligente. Nada que no tenga conciencia de sí mismo puede considerarse inteligente. En cambio, es un mecanismo algorítmico para analizar grandes cantidades de datos, pero que tiene grandes imitaciones cognitivas. Finalmente, las predicciones y toma de decisiones no las realiza una computadora por si sola.

Una herramienta Ngram (que muestra patrones de uso de palabras) revela que, hasta la década de 1960, IA e inteligencia artificial eran más o menos sinónimos, pero que a partir pero que desde ese momento se separaron y actualmente la IA se encuentra ampliamente presente en el sector tecnológico, los medios de comunicación, así como en el ámbito académico. ¿Y a qué se debe esto?, bueno pues en parte tiene que ver con la pereza ya que resulta más fácil tipológicamente mencionar o escribir 2 letras en vez de 22. Este aprendizaje automático es una tecnología arcana que en ocasiones es útil para resolver problemas complejos siempre y cuando estén bien definidos. La industria tecnológica está obsesionada con este tipo de tecnología y la razón es porque le permite construir máquinas que aprenden del comportamiento de los usuarios de internet para predecir lo que podrían hacer a continuación, lo que les gusta lo que valoran y lo que podrían comprar. Esta tecnología, es útil también en términos de avances en automatización de procesos, representando con esto, ventajas competitivas o incluso significa el reemplazo de puestos laborales por adopción de estas tecnologías en

sustitución de personal. Sin embargo, esta tecnología tiene grandes desventajas como la gran cantidad de emisiones de carbono que genera por el entrenamiento de grandes sistemas de aprendizaje automático, son sistemas demasiado frágiles y propensos a errores que hacen desconfiar de la misma en términos de seguridad como lo pueden ser los vehículos autónomos, debido a que los datos con los que son alimentados absorben sesgos implícitos que son críticos. Sus creadores la mayor parte del tiempo son incapaces de dar una explicación sobre como estas máquinas realizan determinadas clasificaciones o predicciones por lo que no cumplen con los requisitos democráticos de rendición de cuentas.

De aquí surge una pregunta clave ¿cómo aborda la industria, la sórdida realidad de que se ha jugado el todo por el todo con una tecnología potente pero problemática?, y la respuesta es: evitar llamarla por su nombre real y asignarle un nombre que seduce y romantiza que esta tecnología forma parte de un proyecto grandioso. Dicho de otra manera, es la forma que tiene la industria de mostrar una apariencia de solidez al aire puro mientras se dedica al verdadero negocio de hacer fortunas.

Esta es evidentemente una forma clara en como el lenguaje afecta nuestra percepción de las cosas, en especial ahora que en términos tecnológicos el protagonismo y sobredimensionamiento del fenómeno permite la libertad de su manipulación en forma de ingeniería lingüística abarcando desde lo cotidiano pasando por lo político hasta lo empresarial.

En este sentido se puede llegar a la conclusión de que la inteligencia artificial o máquina inteligente, simplemente ¡no existe!. Una definición más aproximada señala que es un conjunto de programas informáticos que aplican estadística avanzada y que ejecutan operaciones comparables a las que realiza la mente humana como el aprendizaje o el razonamiento lógico, por lo que únicamente son capaces de reproducir patrones que generan un resultado concreto a partir de una serie de datos. Como ejemplo una máquina que “juega” ajedrez, al ser un juego de gestión probabilística de espacios combinatorios únicamente puede hacer eso, con base a las reglas y restricciones con las que se programa. En ningún momento pueden realizar más cosas que aquellas operaciones concretas para las que han sido programadas y mucho menos serán capaces de adquirir una supuesta conciencia.

Un concepto básico que podría ayudar a entender esta terminología es que la inteligencia está relacionada con la capacidad de toma de decisiones, de esta manera se puede afirmar que una máquina no puede generar la inteligencia debido a su falta de habilidad para efectuar una sinapsis neuronal, y mucho menos podrán efectuar la polarización o modulación sinápticas, dado que todo proviene de la biogénesis neuronal.

Al profundizar más sobre el término de las decisiones, desde el año 1966, el profesor Joseph Weizenbaum elaboró un programa de procesamiento de lenguaje (ELIZA) el cual fue capaz de realizar conversaciones con sus pacientes a manera de simular un terapeuta, por lo que fue considerado un promotor de las máquinas pensantes, sin embargo, el consideraba esta interpretación como errónea por lo que en 1976 publicó el libro “*El poder*

informático y la razón humana; del juicio al cálculo", en este libro se distingue perfectamente la capacidad de una computadora y el razonamiento humano por lo que estableció perfectamente la diferencia entre decidir y elegir. El autor aclara que la decisión y control de un proceso industrial se efectúa mediante un circuito o un computador como controlador programado de dicho proceso, decidir es una actividad computacional, algo que puede programarse y, sin embargo, la elección es el producto del juicio, no del cálculo.

Ya para el año 1989 se dio a conocer el libro *"La nueva mente del emperador"*, escrito por Roger Penrose en el cual demuestra que el citoesqueleto de las neuronas en especial los microtúbulos, son lugares específicos para el procesamiento cuántico y, en última instancia, para la conciencia con lo que se concluye que pensamiento humano no es simplemente algorítmico.

Los circuitos artificiales son incapaces de imitar los sistemas nerviosos incluso de los invertebrados más simples. A pesar de utilizar equipos de cómputo más rápidos y sofisticados junto con grandes bases de datos, confiar en que el razonamiento, la inteligencia y la conciencia se generen simplemente al incrementar la complejidad, es un gran error.

Aunque una computadora venza a los ajedrecistas profesionales o sea capaz de presentar un recurso legal al buscar la legislación en su base de datos, no es una máquina pensante. Es importante no banalizar y realizar una correcta diferenciación entre herramientas tecnológicas y seres inteligentes. (Etxebarria E. V., 2022)

En términos de seguridad resulta vital analizar el uso e implementación de estas tecnologías en entornos críticos como lo son los puertos. Los accidentes marítimos representan un desafío significativo en estos términos, así como para el medio ambiente y la economía global. Comprender a profundidad estas causas y los impactos derivados de estos incidentes es esencial para implementar estrategias efectivas de mitigación y prevención. La formación continua, la adopción de tecnologías eficientes, el mantenimiento regular y la cooperación internacional son fundamentales para incrementar la seguridad marítima y minimizar el riesgo de incidencias. Se requiere que tanto las autoridades como todos los involucrados en el comercio marítimo a medida que crece, se adopten estrategias de trabajo conjunto para garantizar un entorno marítimo seguro y sostenible.

La Ley de Seguridad y Responsabilidad para Todos los Puertos (SAFE) de 2007, es un sistema tecnológico impuesto por ley que exigía inicialmente el escaneo del total de contenedores y carga en general destinados a Estados Unidos de América, en busca de riesgos nucleares. Los grandes desafíos logísticos que envuelven a este tipo de detección nuclear han impedido que se cumplan o se lleven a cabo a la fecha, razón por la cual esta normativa ha sido suspendida. (U.S. Citizenship and Immigration Services; https://www.uscis.gov.)

La desconfianza a adoptar un sistema que impida los ataques nucleares es un ejemplo de la presión a la que se resisten los puertos para adoptar nuevas tecnologías pues con cada nueva aplicación también llegan nuevas amenazas de fallo al sistema. En la medida en que aumenta el uso de la tecnología, los puertos se hacen más dependientes

de la misma y por lo tanto más vulnerables a los ciberataques que llegan a inhabilitar las operaciones de las terminales durante mucho tiempo, con consecuencias económicas graves además de que quedan expuestos datos confidenciales.

Los diversos tipos de incidentes derivados de la implementación de tecnologías en los puertos son:

Ciberataques: los sistemas de información portuaria son necesarios para agilizar las operaciones, gestionan información relevante, desde registros de envíos hasta información financiera, pero también se convierten en blancos potenciales para ciberdelincuentes. La amenaza no es solo el robo de información o el espionaje industrial, sino la posibilidad de paralizar completamente un puerto durante tiempo indefinido.

Robo de mercancías: Dentro de las instalaciones portuarias se almacenan y trasladan gran variedad de mercancías que están propensas a la pérdida, el robo o la piratería y que tiene grandes repercusiones económicas, no solo para las empresas portuarias, sino para toda la cadena de suministro a nivel global. Se requiere por lo tanto de sistemas de seguridad física avanzados con capacidad de vigilancia y control de acceso para prevenir este tipo de incidentes.

Colisión de buques: Las colisiones entre buques pueden provocar daños catastróficos, como la rotura del casco, la zozobra o el hundimiento. Estos incidentes pueden atribuirse a fallas de navegación, averías mecánicas, condiciones climáticas desfavorables o fallas humanas. Las lesiones sufridas en las colisiones de buques pueden ir desde pequeños cortes y contusiones hasta lesiones graves o la muerte de miembros de la tripulación y pasajeros.

Figura 1.

El Canal de Suez, bloqueado por el encallamiento de buque.

Fuente: https://www.bbc.com/mundo/noticias-56506254

Accidentes portuarios: Los incidentes en las instalaciones portuarias pueden ocurrir durante el traslado y desecho de bienes, las labores de mantenimiento y reparación, o durante el embarque o desembarque de los barcos. Estos incidentes pueden conllevar caídas de alturas, impactos con maquinaria o cargas en movimiento, o atrapamiento en equipos. Las heridas ocasionadas por accidentes en las vías portuarias pueden ser considerables e involucrar lesiones por aplastamiento, amputaciones o traumas. (Joshua Lee, 2024)

Figura 2.

Accidente de grúa en instalación portuaria.

Fuente: https://www.msn.com/es-us/noticias/other/se-desploma-una-enorme-gr%C3%BAa-portacontenedores-en-un-puerto-de-taiw%C3%A1n/vi-AA1spDED

Ausencia de sistemas de respaldo. La implementación de nuevas tecnologías brinda excelentes oportunidades de mejora, pero también representan grandes debilidades en caso de presentar fallas. Un ejemplo claro fue cuando se inició con la implementación de etiquetas de identificación por radiofrecuencia (RFID) en el ámbito militar el cual formó parte de un procedimiento para realizar un seguimiento más eficaz de los envíos, sin embargo, presentó limitantes ya que, si las etiquetas se colocaban lejos del alcance del lector, no se podían registrar, además si no se afirmaban debidamente, se perdían. Con el paso del tiempo se pierden los conocimientos por parte del personal para realizar las funciones de forma manual y dependen en su totalidad de la tecnología, es decir no cuentan con un sistema alterno o de respaldo con el cual solucionar esta problemática. Una alternativa para poder dar solución a este conflicto es mantener una constante formación y preparación del personal que interactúa en esta cadena logística, así como el resguardo de copias de seguridad que garanticen acortar el tiempo de la puesta en marcha para reestablecer los servicios. Los sistemas de respaldo representan también un ahorro económico sustancial al minimizar las reclamaciones de los seguros.

Con el objeto de mejorar la eficiencia de un puerto en términos de incrementar la velocidad y el rendimiento, reducir retrasos, aumentar el volumen de carga y lograr una mayor eficiencia en los plazos, ha sido notable el aumento en la dependencia tecnológica en puertos y terminales con su consecuente también, mayor exposición a riesgos y amenazas cibernéticas que además de provocar daños físicos que amenazan las operaciones, también ponen en riesgo la seguridad de los empleados y de otras personas que forman parte de la cadena.

Ante esta situación resulta viable la inversión de una estrategia de digitalización "Smart" o inteligente, que ayude a identificar las vulnerabilidades, para proponer alternativas que fomenten la capacidad de resiliencia en la organización.

Debido al incremento de las ciberamenazas, organismos como la Agencia de la Unión Europea para la Ciberseguridad (ENISA), han publicado guías destinadas a mejorar la ciberseguridad. El informe de esta agencia en el 2020 sobre la gestión del Riesgo Cibernético en los puertos propone un enfoque específico para la evaluación de Riesgos Cibernéticos en los puertos:

Figura 3.

Acciones para evaluación de riesgos cibernéticos.

Fuente: https://www.enisa.europa.eu/

A manera de resumen y al considerar una analogía desde el nivel de entendimiento lingüístico podemos concluir que la mal llamada inteligencia artificial no existe, por lo tanto contamos con el apoyo de sistemas de cómputo especializados que mediante algoritmos y datos, programamos y proponemos alternativas para hacer más eficiente nuestro trabajo, sin embargo no podemos delegar la responsabilidad de dejar sin supervisión en todo momento así como establecer límites y criterios de actuación para evitar sorpresas en sitios clave tan importantes como lo es un puerto marítimo. Así entonces, el personal que forma parte de un puerto y las terminales marítimas pueden tomar medidas para ser más resilientes se puede empezar por estos cinco pasos:

1. **Mejorar la formación y la educación.** Los trabajadores del sector marítimo – portuario, tienden a asumir diferentes niveles de conciencia cibernética con base a diferentes experiencias y capacidades por lo que es necesario recibir capacitación adecuada en formación tecnológica y digital a todos los niveles, así como un entrenamiento para la gestión de los riesgos cibernéticos a los que se enfrenta este sector que está cada vez más digitalizado, con esto se buscará la manera de reducir y minimizar los errores humanos que son parte crucial para mantener la seguridad de los puertos y terminales, así como para aumentar la resiliencia cibernética de toda la cadena de suministro. (https://www.ibm.com/mx-es/topics/cyber-resilience)

2. **Invertir en personal especializado en ciberseguridad.** Al tener en cuenta los riesgos potenciales asociados a la creciente digitalización, los puertos y terminales, en función del el tamaño y la complejidad de su empresa, deberían considerar la posibilidad de invertir en personal con una sólida formación en procesos de ciberseguridad que ayuden a minimizar los riesgos.

3. **Identificar los riesgos de terceros.** La compleja interacción de proveedores, usuarios y clientes en los puertos y terminales representa una variedad de diversos puntos fuertes y débiles en materia de ciberseguridad, por lo que se debe de identificar y realizar una detallada descripción de los puntos de contacto y del tipo de conexión de las operaciones, lo cual ayudará a vislumbrar en qué medida contribuye cada integrante de la cadena con las vulnerabilidades y riesgos a la ciberseguridad. Es importante mantener un canal de comunicación con todos los integrantes, así como una restricción rigurosa a los accesos innecesarios a los sistemas informáticos.

4. **Atacar los puntos débiles del sistema.** En algunas ocasiones en las instalaciones portuarias se opera con sistemas informáticos o de comunicación anticuados o sin actualizaciones de seguridad requeridas por lo que esta falta podría representar grandes riesgos de seguridad, y tal vez con la inversión adecuada de personal calificado en materia de seguridad se pueda llegar a identificar los puntos débiles del sistema en la empresa, y de esta manera recomendar acciones para mantener actualizado los sistemas de seguridad y comunicaciones.

5. **Mantener una actualización permanente en materia de normatividad.** Constantemente, las autoridades competentes actualizan reglamentos y normas de ciberseguridad. En este caso la Organización Marítima Internacional (OMI) y su Comité de Seguridad Marítima, han establecido algunas recomendaciones sobre la gestión de riesgos cibernéticos marítimos, cabe destacar que algunos países adoptan sus propios requisitos y sanciones por incumplimiento. Las entidades portuarias pueden operar acorde a más de un régimen normativo, lo que exige compromiso para garantizar que sus operaciones cumplen todos los requisitos. Cuando los riesgos asociados a los eventos cibernéticos se entienden, se cuantifican y se gestionan correctamente, las oportunidades en la digitalización los superan y tienen un gran alcance.

Referencias.

Etxebarria E. V. (2022). Qué es y qué no es inteligencia artificial. The Conversation. Academic rigour, journalistic flair. Australia. **Qué es y qué no es inteligencia artificial**

Galindo C. J. L. (2009). Métodos, técnicas Ingeniería Social, Comunicología e Historia Oral. Estudios sobre las Culturas Contemporaneas. ISSN (Versión impresa): 1405-2210. Universidad de Colima. México.

Joshua Lee, (2024). Types of Maritime Accidents and Injuries. Armstrong Lee & Baker LLP – Houston Office TX. EEUU.(Types of Maritime Accidents and Injuries - ALB Lawyers)

Penrose, R. (1989) La mente nueva del emperador. En torno a la cibernética, la mente y las leyes de la física. Consejo Nacional de Ciencia y Tecnología. Fondo de Cultura Económica. México.