PERRY CENTER OCCASIONAL PAPER
SEPTIEMBRE 2024

Infraestructuras críticas

Amenazas, retos y oportunidades de la Inteligencia Artificial y el Aprendizaje Automático

Boris Saavedra, Ph.D.

CENTRO DE ESTUDIOS
DE DEFENSA HEMISFÉRICA
WILLIAM J. PERRY

National Defense University

Foto de portada: La Inteligencia Artificial (AI) y Aprendizaje Automático (machine learning en inglés) están transformando los negocios, la industria, y la sociedad en América Latina.
Crédito: Fintech

Editor-en-jefe: Patrick Paterson, Ph.D.
Diseño: Gabrielli Raya Lebrón

Infraestructuras críticas

Amenazas, retos y oportunidades de la Inteligencia Artificial y el Aprendizaje Automático

Boris Saavedra, Ph.D.

CENTRO DE ESTUDIOS
DE DEFENSA HEMISFÉRICA
WILLIAM J. PERRY

PERRY CENTER OCCASIONAL PAPER
SEPTIEMBRE 2024

Infraestructuras críticas
Amenazas, retos y oportunidades de la Inteligencia Artificial y el Aprendizaje Automático

Boris Saavedra, Ph.D.

Introducción

En la actualidad, la evolución de tecnologías aceleradas, exponenciales y convergentes, tales como la Inteligencia Artificial generativa (IA), el Aprendizaje Automático o Machine Learning (ML, por sus siglas en Inglés) y la Analítica de Meta Data (Big Data Analytics, por su denominación en inglés), han cambiado en forma disruptiva la operatividad de las infraestructuras críticas. Los ciberdelincuentes y los estados nacionales malintencionados están poniendo cada vez más su mirada en las infraestructuras críticas. Los resultados pueden ser dañinos, de largo alcance y duraderos. En mayo de 2021, DarkSide, un grupo criminal cibernético ruso, llevó a cabo un ataque de *ransomware* (ciber secuestro de datos) contra un gran operador de oleoductos en la costa este de los Estados Unidos, que interrumpió el suministro de combustible y provocó compras de pánico y escasez generalizada de gasolina en toda esa zona.

En el año 2016, publicamos un artículo sobre las infraestructuras críticas, en el cual exploramos el presente y el futuro de los beneficios de la tecnología emergente, pero también su cara ominosa. Las Tecnologías de la Información y la Comunicación (TIC, por sus siglas en inglés) basadas en computadoras, son las fuerzas impulsoras que se han creado y pueden ser pirateadas. Esto constituye un hecho aleccionador dada nuestra dependencia radical, conectividad y vulnerabilidad en estas máquinas para todo, desde nuestras necesidades individuales hasta los servicios financieros y de producción de la red eléctrica de una nación.[1]

En ese artículo se llamó la atención de los funcionarios gubernamentales y del sector privado de Latinoamérica y el Caribe sobre las amenazas y desafíos de la ciberseguridad, para proteger las infraestructuras críticas en el ciberespacio y su implicancia en el día a día de la interacción y supervivencia humanas. En este informe, analizaremos a nivel político y estratégico, el ambiente tecnológico actual, caracterizado por los ya mencionados procesos acelerados, exponenciales y convergentes, que han generado innovaciones disruptivas. Todo este conjunto de hechos impacta a la humanidad en general y las infraestructuras críticas, factor fundamental para la vida en el planeta. En este orden de ideas, el objetivo es analizar, política y estratégicamente, las infraestructuras críticas en Latinoamérica y el Caribe, a la luz de la IA generativa, la Analítica de Meta Data y el ML, que han impactado su funcionamiento en forma significativa.

Incidentes Recientes

En mayo de 2021, Conti, otro grupo de *ransomware* ruso, emprendió un ataque contra el servicio de

[1] David E. Sanger, Clifford Krauss and Nicole Perlroth, "Cyberattack forces a shutdown of a top U.S. pipeline." The New York Times. May 13, 2021. Link: https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html, accessed 19 July 2024.

salud Irish Health, afectando la atención de pacientes durante meses, lo que obligó a los proveedores de atención médica a cancelar citas, posponer cirugías electivas y retrasar tratamientos. Un par de semanas después, REvil, un tercer grupo criminal ruso de *ransomware*, atacó a un gran productor de carne, lo que obligó a la empresa a cerrar plantas en los Estados Unidos, Canadá y Australia, afectando los suministros nacionales de alimentos y los precios de la carne.

Varias agencias gubernamentales en América Latina han sido objeto de ataques de *ransomware* en el año 2022. Algunas de las víctimas han sido Costa Rica, Chile y República Dominicana y en septiembre de 2023 de acuerdo con el índice global de ciberseguridad la región más vulnerable del mundo es Latinoamérica donde el ataque perpetrado a Colombia, Chile y Argentina confirma la intensa actividad de los grupos de hackers especializados en ataques a infraestructuras críticas.[2]

Concepto: Las naciones de América Latina y el Caribe han sido atacadas cibernéticamente en múltiples ocasiones, incluidos incidentes recientes en Costa Rica, Chile y la República Dominicana. ***Crédito:*** Adobe Stock

Por ejemplo, Costa Rica se convirtió en víctima de ataques de *ransomware* a gran escala, iniciados por el ya mencionado grupo criminal Conti, en abril de 2022. Comenzando en el Ministerio de Hacienda de Costa Rica, la actividad criminal cibernética finalmente involucró a 27 ministerios diferentes en una serie de irrupciones interrelacionadas.

A su vez, el Ministerio del Interior de Chile informó en agosto 2022, que los sistemas y servicios en línea de una agencia gubernamental, fueron interrumpidos por un *ransomware* que tenía como objetivo los servidores Windows y VMware ESXi. Este ciberataque cifró archivos en sistemas comprometidos y

[2] Jimmy Pepinosa, "Cuáles son los ataques cibernéticos más comunes en Argentina, Colombia y Chile," Infobae, 23 de octubre 2023. Link: https://www.infobae.com/tecno/2023/10/18/cuales-son-los-ataques-ciberneticos-mas-utilizado-en-argentina-colombia-y-chile/, accessed 19 July 2024.

los renombró con la extensión crypt.

En el caso de la República Dominicana, una organización gubernamental también fue atacada por *ransomware*. El centro nacional de ciberseguridad del país dijo, el 24 de agosto de 2022, que el Instituto Agrario Dominicano (IAD) del Ministerio de Agricultura fue atacado, pero destacó que el gobierno no planeaba pagar un rescate, para evitar alentar a los actores de amenazas a realizar este tipo de operaciones. Bleeping Computer informó que el *ransomware* denominado Quantum estuvo involucrado en este ataque. Los ciberdelincuentes afirmaron haber robado más de un Terabyte (TB) de datos lo cual representa 728.177 disquetes o 1.498 CD, de información de archivos y exigieron un rescate de 650.000 dólares.[3]

El proceso acelerado de digitalización y modernización de las infraestructuras críticas en Latinoamérica y el Caribe, es producto de dos acontecimientos principales: la situación de digitalización acelerada en la post pandemia del COVID-19 y la evolución de la tecnología digital emergente a escala mundial. También se observa un crecimiento importante de los ataques, que se ubica en 1,130 ataques por semana, lo cual representa un 28 por ciento de incremento, si se considera el total acumulado durante los dos años anteriores.[4]

Términos y definiciones

A fin de lograr un mejor entendimiento de cada una de estas tecnologías, es necesario conceptualizarlas. La Analítica de Meta Data o Analítica de Meta Data es un término que se aplica a toda aquella información que no puede ser procesada o analizada utilizando medios o herramientas tradicionales. Dentro del sector de tecnología de la información y la comunicación, Big Data es una referencia a los sistemas que manipulan grandes conjuntos de datos. Con el avance tecnológico se ha incorporado la analítica, la cual permite superar las dificultades más habituales en estos casos, centrándose en la captura, almacenamiento, búsqueda, intercambio, análisis y visualización de los datos. Hay cuatro características claves que definen la información relativa a esta técnica:

1. Volumen: los datos relativos a la Big Data se producen en cantidades mucho más grandes que los datos tradicionales.

2. Velocidad: los flujos de datos de medios sociales, aunque no es tan masivo como los datos generados por máquinas, producen una gran afluencia de opiniones y valiosas relaciones para la gestión de clientes.

3. Variedad: los formatos de datos tradicionales tienden a ser relativamente bien definidos por un esquema de datos. En contraste, los formatos de datos no tradicionales exhiben un ritmo vertiginoso de cambio.

[3] Eduard Kovacs, "Ransomware Attacks Target Government Agencies in Latin America," Security Week, 01 de septiembre 2022. https://www.securityweek.com/*ransomware*-attacks-target-government-agencies-latin-america/, accessed 19 July 2024.

[4] Check Point. Cyber security report 2022. Check Point Research third quarter of 2022 revels an increase in attacks and unexpected developments. Link: https://resources.checkpoint.com/cyber-security-resources/2022-cyber-security-report

4. Valor: el valor económico de los diferentes datos varía significativamente. El desafío esencial es identificar la información valiosa, transformarla y extraer los datos para su análisis.[5]

La Analítica de Meta Data es una tecnología que recopila, inspecciona, purifica y transforma datos, con la finalidad de destacar toda la información que sea de gran utilidad para elaborar conclusiones que sirvan para la toma de decisiones y permita mejorar los procesos de gestión. Todo ello se realiza en convergencia con las comunicaciones inalámbricas 5G, de gran velocidad y volumen de datos. Por tal razón, se requiere comprender el papel persistente de los datos en la reorganización del poder en general y particularmente en los Sistemas de Control y Adquisición de Data (SCADA, por sus siglas en inglés) y el Sistema de Control de Procesos Industriales (ICS, por sus siglas en inglés), para el funcionamiento de las infraestructuras críticas. Esto, a su vez, exige la comprensión actualizada de los avances tecnológicos y su impacto a nivel de funcionamiento, para la protección optimizada de tan importante sector.[6]

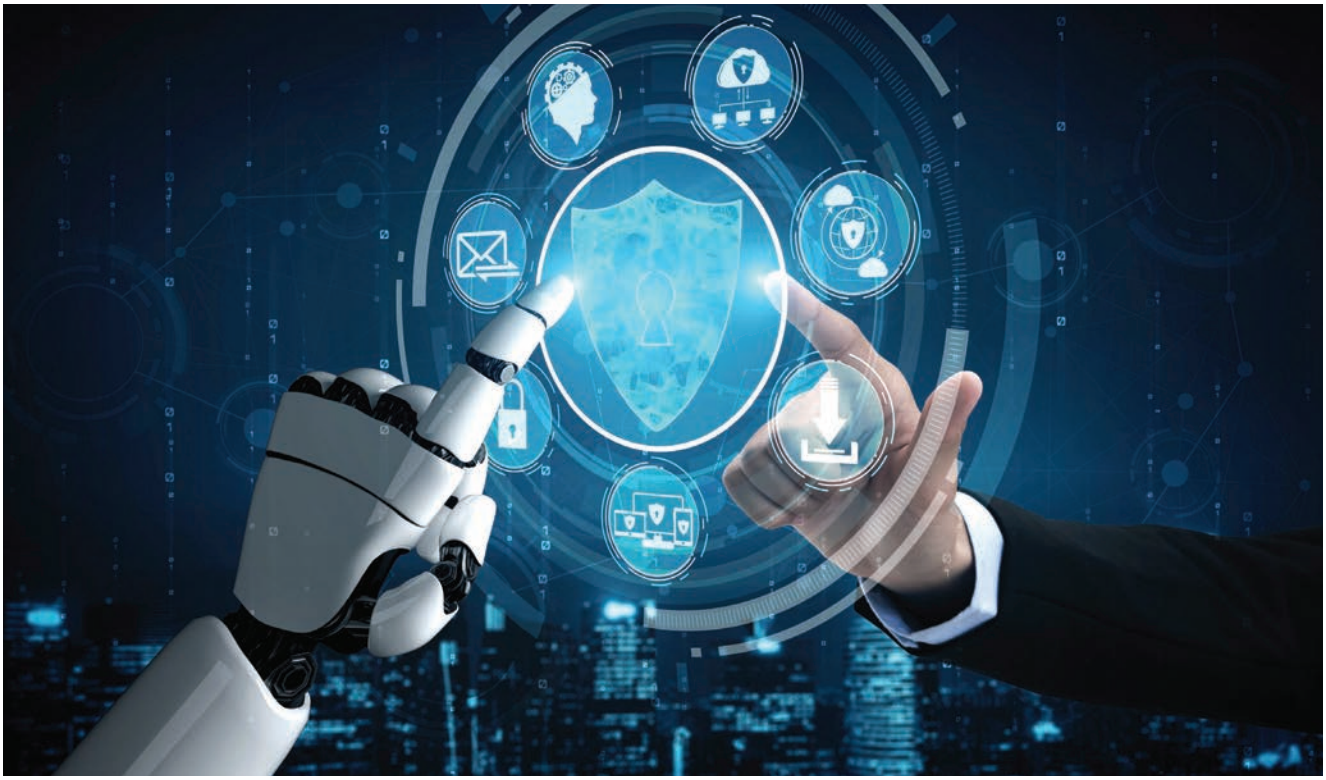
Aprendizaje Automático o Machine Learning (ML)

El surgimiento de la Industria 4.0 ha visto un aumento rápido de los ataques cibernéticos a los sistemas y procesos industriales, particularmente a los ICS y SCADA. Estos sistemas constituyen los objetivos principales tanto para los ciberdelincuentes como para los estados-nación que buscan extorsionar grandes rescates o causar interrupciones gracias a su capacidad para causar un impacto devastador, dejándolos sin funcionamiento o funcionando en forma limitada. Aunque los sistemas actuales de detección pueden ayudar, todavía enfrentan muchos desafíos que no pueden superar con sus capacidades tradicionales. Debido a la necesidad de comprender mejor estos retos, es necesario (1) comprender el panorama de vulnerabilidad actual en ICS y SCADA y (2) estudiar los avances actuales de los métodos basados en ML. Con respecto al uso de ML, los clasificadores básicos brindan información sobre los beneficios y las limitaciones de los avances recientes con respecto a dos vectores de rendimiento: precisión de detección y variedad de ataque.[7]

[5] María Perez Marques, *Big Data: Técnicas, Herramientas y Aplicaciones.* Madrid, España: RC Libros, julio 2015. ISBN: 978-84-943055-5-9.

[6] "La importancia de la Data Analytics y el Business Intelligence en la digitalización," 03 de septiembre 2020. Link: https://www.atrebo.com/es/la-importancia-del-data-analytics-y-el-business-intelligence-en-la-digitalizacion/, accessed 19 July 2024.

[7] Mohammad Shahin, et al, "Classification and Detection of Malicious Attacks in Industrial IoT Devices via Machine Learning," 13 October 2022, in *Flexible Automation and Intelligent Manufacturing: The Human-Data-Technology Nexus.* Link https://link.springer.com/chapter/10.1007/978-3-031-18326-3_10, accessed 19 July 2024.



Concepto: Big Data permite el rápido acceso e intercambio de información. ***Crédito:*** Shutterstock

Los avances tecnológicos del ML, un pariente de la IA, que ha llegado en estos últimos años a ser uno de los mayores éxitos, hasta el punto de que a partir del 2013 ha desplazado algunos de los objetivos más ambiciosos de la IA tradicional. De hecho, en algún momento los términos se han usado en forma indistinta, de acuerdo con Michael Jordan y Tom Michel expertos investigadores de IA, quienes expresaron que hoy día resulta más fácil tener un modelo aprendido de los datos que una codificación estricta de reglas dominada por IA. El poder de adaptabilidad de los algoritmos de ML pueden verse como una búsqueda a través de un gran espacio de programas, guiados por la experiencia de capacitación para encontrar un programa que optimice las métricas de rendimiento.

Inteligencia Artificial Generativa (IA)

La IA es una de las tecnologías que ha hecho los avances más impactantes a nivel global en los últimos dos años. Sin embargo, el empleo de este término en algunos casos ha sido mal utilizado, generando confusión en el público en general. Lo mismo sucede con el empleo del término "infraestructura crítica". Por tal razón, proporcionaremos una definición de ambos conceptos, a fin de lograr un mejor entendimiento del análisis.

1. Inteligencia Artificial: La Real Academia Española de la Lengua la define como: "Disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje, o el razonamiento lógico".

2. Infraestructura Crítica: La agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA, por sus siglas en inglés) la define de la siguiente manera: La infraestructura crítica son aquellos

activos, sistemas y redes que proporcionan funciones necesarias para nuestra forma de vida.

Ambas definiciones las encontramos fáciles de entender, sin embargo, la pregunta sería ¿Cómo es el uso práctico, a nivel política y estrategia? Para contestarla comenzaríamos por decir que los servicios que hay detrás de las infraestructuras han cambiado y se han transformado, haciéndolas inteligentes. Esto quiere decir que, con nuevas herramientas digitales, se integra la gestión mediante la recopilación y análisis de los datos de manera inteligente, lo cual permite la corrección automática de actividades, buscando siempre la optimización del producto o servicio.[8]

Además, la información obtenida de una infraestructura inteligente se podría transmitir a otra similar, mediante el Internet de las Cosas (IoT, por sus siglas en inglés). Esto permite que tales infraestructuras intercambien la información y experiencia en forma automática, lo cual nos lleva a estandarización de procesos, para la mejor toma de decisiones de la gestión. De hecho, en la actualidad el sistema de infraestructuras de las ciudades inteligentes busca, a través de la conectividad e integración de la alineación de todas las infraestructuras, una mejora continua del rendimiento, que al final se traduce en retorno de inversión y un servicio optimizado y seguro.[9]

En la actualidad, la IA se utiliza mucho en otras actividades importantes, como la eficiencia energética, predicción de fallas y mantenimiento de infraestructuras y también en aspectos de ciberseguridad. Todo ello se logra mediante la recopilación de datos y transformación en información, para una perfecta distribución de energía y la anticipación a cualquier tipo de fallas o el adelanto a posibles ciberataques.

El 21 de abril de 2023, el secretario de Seguridad Nacional de los Estados Unidos de Norteamérica, Alejandro N. Mayorkas, anunció durante su primer discurso sobre el Estado de la Seguridad Nacional dos nuevas iniciativas innovadoras para combatir las amenazas en evolución. En su alocución se centró en dos tendencias que darán forma a lo que el presidente Biden ha llamado una "década decisiva" para el mundo: la revolución creada por la inteligencia artificial generativa (IA) y la amenaza multifacética que plantea la República Popular China (RPC).

Concepto: En 2023, el secretario de Seguridad Nacional de los Estados Unidos de Norteamérica, Alejandro N. Mayorkas, anunció nuevas iniciativas para combatir la evolución de las amenazas en línea. ***Crédito:*** The Rio Times

[8] Chris Wiggins and Matthew L. Jones, *How Data Happened: A History from the Age of Reason to the Age of Algorithms.* W.W. Norton & Company. New York. 2023.

[9] La inteligencia artificial en la gestión de infraestructuras críticas," Atrebo, 08 April 2021. Link: https://www.atrebo.com/es/la-inteligencia-artificial-en-la-gestion-de-infraestructuras-criticas/, access 19 July 2024.

Esta es la primera vez que el Departamento de Seguridad Nacional (DHS por sus siglas en inglés) anuncia la creación de un grupo de trabajo dedicado a la IA. Dicho grupo impulsará aplicaciones específicas de esta materia para avanzar en misiones críticas de seguridad nacional, lo que incluye trabajar con socios en el gobierno, la industria y la academia, para evaluar el impacto de la IA en nuestra capacidad para proteger la infraestructura crítica.

Con todos los ojos puestos en los posibles beneficios y amenazas que plantean los productos emergentes impulsados por IA, como GPT-4, ChatGPT, AlphaCode, GitHub Copilot y otros, no es de extrañar que el gobierno federal está considerando cómo podría aprovechar esta tecnología para la seguridad nacional. El DHS se centrará en el uso de la IA para el logro de 4 objetivos principales, a fin de avanzar en las misiones críticas de seguridad nacional:[10]

1. Uso de la IA para proteger la cadena de suministro y los entornos comerciales. Una de las principales aplicaciones de esta tecnología dentro del DHS, será mejorar la integridad de las cadenas de suministro y el entorno comercial más amplio. Al integrar la IA en sus operaciones, el DHS tiene como objetivo controlar la carga de manera más efectiva, identificar los bienes producidos con trabajo forzoso y gestionar el riesgo asociado con el comercio.

2. Uso de la IA para detectar actividad criminal de drogas y sustancias químicas. y para contrarrestar el flujo de fentanilo hacia los Estados Unidos. El DHS planea aprovechar esta tecnología para mejorar la detección de envíos de dicha sustancia, identificar e interceptar el flujo de precursores químicos a nivel mundial e interrumpir nodos clave en las redes criminales involucradas en el tráfico de este letal opioide.

3. Uso de la IA como herramienta forense digital para interceptar y prevenir la explotación cibernética de menores. El grupo de trabajo de IA también desempeñará un papel crucial colaborando con otras agencias del gobierno en la lucha contra la explotación y el abuso sexual infantil en línea. Al aplicar esta tecnología a las herramientas forenses digitales, el DHS tiene como objetivo identificar, localizar y rescatar a las víctimas de estos crímenes atroces, así como detener a los perpetradores.

4. Uso de la IA para proteger la infraestructura crítica. La cooperación con socios en el gobierno, la industria y la academia será esencial para evaluar el impacto de la IA en la protección de la infraestructura crítica. El grupo de trabajo operará en estrecha colaboración con estas partes interesadas para evaluar cómo estas técnicas pueden fortalecer la protección de los sistemas e instalaciones vitales.

El uso de la IA en la ciberseguridad es cada vez más importante, para que las organizaciones prevengan los ciberataques. Esta tecnología es capaz de analizar enormes cantidades de datos, cientos y miles de veces más rápido que los humanos, lo que permite una detección eficaz de amenazas. Los sistemas de IA, en combinación con procesamiento automático o ML, pueden aprender de experiencias

[10] Department of Homeland Security (DHS). "Secretary Mayorkas Announces New Measures to Tackle A.I., PRC Challenges at First State of Homeland Security Address," 21 April 2023. Link: https://www.dhs.gov/news/2023/04/21/secretary-mayorkas-announces-new-measures-tackle-ai-prc-challenges-first-state, accessed 19 July 2024.

anteriores y reconocer patrones que conducen a predicciones más precisas, con menos falsos positivos para los equipos de seguridad.

La Inteligencia Artificial está en constante evolución, presentándose continuos desafíos, los cuales debemos atender para mejorar los procesos productivos y de control industrial. En la competitividad actual de las empresas que buscan mejorar su desempeño año tras año, la tecnología adquiere un papel primordial y, muy particularmente, la IA.

El GPT-4 es la última versión de transformadores pre entrenados generativos, un tipo de modelo de aprendizaje profundo, que se utiliza para el procesamiento del lenguaje natural y la generación de texto. Marca un hito significativo en el campo de la inteligencia artificial, especialmente en el procesamiento del lenguaje natural.

Este avance, muy acelerado y disruptivo, ha generado preocupaciones en el gobierno de EE. UU, particularmente en CISA, sobre la creciente popularidad de los sistemas ICS y SCADA, por los ataques a las tecnologías operativas (OT). En una nota relacionada con la infraestructura crítica, los miembros del Senado de los Estados Unidos piden elevar el estatus del rol principal de seguridad cibernética dentro del Departamento de Energía.[11]

La IA generativa representa una transformación tecnológica muy importante y disruptiva con oportunidades para el crecimiento económico, industrial, de educación superior, con impactos positivos en la salud, también surgen preocupaciones de orden ético, legal, y de medio ambiente que requieren una atención cuidadosa para su debida solución. Adicionalmente, tomando en consideración que los países en vías de desarrollo no cuentan con el acceso equitativo a este tipo de tecnología para beneficiarse de sus bondades sería recomendable que los países desarrollados faciliten un apoyo amplio en infraestructura y el marco adecuado para el diseño de la política y la implementación de la estrategia para los países en vías de desarrollo que les permita contar con una respuesta integral para la adopción de la IA generativa que requiere un cuidadosa consideración de sus implicaciones en diferentes dominios.

Finalmente, debemos entender que el gran potencial de la IA generativa en convergencia con aprendizaje automático ML podríamos considerarlo como el centro de gravedad de los cambios disruptivos en la actualidad en este sentido se requiere incentivar la colaboración que priorice las consideraciones éticas, inclusividad, y desarrollo sostenible a escala global en forma responsable con la finalidad de contar con las posibilidades de prosperidad que nos ofrece estas tecnologías. Sin embargo, existe el riesgo de que algunos países queden atrapados en la competencia de las grandes potencias como campos de prueba indirectos de estas tecnologías como clientes que respeten a la nación proveedora y/o como campo de batalla (caso de Ucrania) donde las potencias se prueban entre sí y los riesgos que esto representa para esos países en particular.

[11] AI Offers Potential to Enhance the U.S. Department of Homeland Security," 06 June 2023, Link: https://mixmode.ai/blog/ai-offers-potential-to-enhance-the-u-s-department-of-homeland-security/, accessed 19 July 2024.

Concepto: La inteligencia artificial ofrece muchas ventajas: protección de las cadenas de suministro, detención de delincuentes, análisis forense y protección de infraestructuras críticas. ***Crédito:*** Adobe Stock

Convergencia de tecnologías digitales

La convergencia de la IA, el ML y la Analítica de Meta Data es importante, porque guardan una estrecha relación. Primero, la IA puede utilizarse para mejorar la ciberseguridad y maximizar la resiliencia de productos, servicios y sistemas, de las instituciones públicas y privadas del Estado. Segundo, la IA está empezando a ser utilizada por cibercriminales y *hacktivistas* para poner en riesgo la ciberseguridad y perpetrar diferentes tipos de ataques a las infraestructuras críticas con *ransomware* altamente sofisticados o la generación de noticias falsas en campañas de desinformación. La convergencia de estas tecnologías podría mejorar los niveles de ciber defensa proactiva y así disminuir la susceptibilidad a los ciberataques. La organización, categorización, y priorización de las infraestructuras críticas y los beneficios de esa convergencia tecnológica en la actualidad, permitirán perfeccionar la funcionalidad, disponibilidad e integridad, de todos estos recursos, por lo cual se deben desarrollar sistemas de IA seguros, que preserven la privacidad y la identidad, a fin de generar la confianza de sus usuarios. Dada la convergencia tecnológica, es necesario que las estrategias de ciberseguridad, estén coordinadas en forma integral para crear técnicas, métodos y herramientas que faciliten el diseño, desarrollo, validación y despliegue de sistemas basados en estas tecnologías de punta con especial énfasis en la IA, con un enfoque multicriterio que considere la ciberseguridad de la información, del modelo y del resultado.

Conclusiones

Como se señaló precedentemente, las tecnologías aceleradas, exponenciales y convergentes, particularmente la IA generativa, ML y la Analítica de Meta Data, han impactado en forma significativa el funcionamiento de las infraestructuras críticas, haciéndolas más eficientes y eficaces operativamente. Sin embargo, al mismo tiempo, más vulnerables a ataques más sofisticados por parte de los cibercriminales y *hacktivistas*.

En los últimos años, las mejoras en materia de ciberseguridad de infraestructuras críticas en general se han manifestado en estrategias y políticas declarativas. Sin embargo, en la práctica, la implementación

es muy escasa, con lo cual se pone en peligro, entre otras cosas, la necesaria recuperación económica post pandémica que requiere la región.

Si se prolonga la transformación digital en medio del proceso de evolución tecnológica descrito a lo largo del presente trabajo, Latinoamérica y el Caribe estarán expuestas a una brecha digital que crecería exponencialmente y que colocaría a la región en una desventajosa condición irreversible para su recuperación a nivel de los países desarrollados.

Esta zona requiere, con carácter de urgencia, implementar marcos normativos y regulatorios basados en estándares internacionales, que ayuden a fortalecer la ciberseguridad de las infraestructuras críticas. Una posible alternativa, podría ser el modelo de gobernanza planteado por el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés),[12] dependiente del Departamento de Comercio de los Estados Unidos.

La región requiere diseñar políticas e implementar estrategias que fomenten la asociación público-privada, en materia de protección de infraestructuras críticas, con capacidades de interoperabilidad digital, empleo de *soft robotics* de protección, y cooperación institucional, que generen la resiliencia operativa necesaria y suficiente.

El gobierno, juntamente con el sector privado, debería implementar mecanismos para analizar el grado de madurez en seguridad cibernética y fijar parámetros, a partir de los resultados, mediante un proceso de mejora continua, que minimice el riesgo y funcione como herramienta para generar confianza de la integridad de la cadena de suministro y distribución digital.

Las mayores amenazas para las infraestructuras críticas son los ataques de *ransomware*. Para evitar convertirse en una víctima de estos ataques, se requiere desarrollar estrategias de acción preventiva como primera opción y no el pago de rescates. Si la única elección fuese recurrir al pago, se recomienda asesoramiento externo y conducir el proceso con personal especializado en recuperación de *ransomware*.

La Inteligencia Artificial generativa, al analizar el código existente (GPT-4), podría detectar actividades sospechosas y alertar al personal correspondiente. Esto podría ayudar a las organizaciones a prevenir ciberataques y mantener sus datos seguros. Aunque GPT-4 tiene el potencial de mejorar las soluciones de ciberseguridad, todavía quedan muchos desafíos por abordar.

El análisis de la ciberseguridad es un componente crítico de la infraestructura crítica digital actual. A medida que el panorama de amenazas evoluciona, también deben hacerlo las herramientas y técnicas utilizadas por los profesionales de la seguridad. GPT-4, un potente sistema de procesamiento del lenguaje natural (NLP, por sus siglas en inglés), es una herramienta innovadora que se puede utilizar para identificar y analizar amenazas que facilitan la descripción general completa de sus capacidades y desarrollar la estrategia preventiva adecuada.

La analítica de meta data constituye una herramienta indispensable para poder tener un eficiente control de la huella digital de una organización. Este sistema informático ha aumentado exponencialmente

[12] Artificial Intelligence Risk Management Framework. Link: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

en los últimos años debido a la introducción de dispositivos IoT, una mayor adopción de la computación en la nube y la creciente prevalencia de prácticas de trabajo remoto.

Un número creciente de organizaciones están migrando una parte importante de sus datos y aplicaciones a la nube, implementando entornos de tecnología de la Información (TI) híbridos. Si bien la computación en la nube ofrece varios beneficios, como escalabilidad, ahorro de costos y flexibilidad, viene con su propio conjunto de desafíos y amenazas de seguridad. El perímetro de seguridad tradicional para la mayoría de las organizaciones, particularmente de infraestructuras críticas, ha ido desapareciendo gradualmente y aumentando significativamente la complejidad general de la TI, creando numerosos vectores de ataque nuevos, que los actores de amenazas pueden explotar. En consecuencia, se requieren políticas y estrategias que consideren el desarrollo de capacidades de inspección de la capa de aplicaciones para la prevención de amenazas y capacidades críticas de visibilidad y control.

Los métodos y recursos para la protección de infraestructuras críticas disuaden o mitigan los ataques en su contra, causados por personas (terroristas, piratas informáticos), por la naturaleza (huracanes, inundaciones) y por accidentes ocasionados por materiales peligrosos (HazMat, por sus siglas en inglés), que involucran sustancias nucleares, biológicas o químicas. La convergencia de la IA y el ML son capaces de analizar grandes cantidades de datos para identificar patrones y detectar anomalías que puedan indicar un ciberataque. Estas tecnologías también pueden automatizar las respuestas a las amenazas, aumentando la velocidad y la eficiencia de la respuesta.

La convergencia de la IA generativa, la ML y la Analítica de Meta Data, facilita la organización, categorización, y priorización de las infraestructuras críticas. En la actualidad, permitirá perfeccionar la funcionalidad, disponibilidad, e integridad de estos procesos tecnológicos, lo cual requiere voluntad política para desarrollar la normativa legal y las políticas y estrategias necesarias y suficientes que la región demanda con carácter de urgencia.

CENTRO DE ESTUDIOS DE DEFENSA HEMISFÉRICA
WILLIAM J. PERRY
National Defense University
Abraham Lincoln Hall
260 5th Ave. Bldg. 64
Washington, DC 20319-5066