ESPECIAL 2024

Ciberseguridad & Inteligencia Artificial

Ciberseguridad e Inteligencia Artificial: retos y oportunidades

En inglés, se utiliza la palabra buzzword para referirse a un término o expresión que se vuelve popular y se usa con frecuencia, a veces sin un entendimiento profundo de su significado. Una frase de su uso como ejemplo es, "Artificial intelligence has become a buzzword in recent years", que en español significa "La inteligencia artificial se ha convertido en una palabra de moda en los últimos años".

El término buzzword refleja dos aspectos al mismo tiempo: por un lado, un concepto que está entre los trending topics, no solo en redes sociales, sino también en empresas, organizaciones, noticieros, cafeterías y prácticamente en cualquier lugar. Por otro lado, implica que no solo es un concepto de moda, sino que también puede ser algo que no necesariamente comprendemos a profundidad.

Quizás un fenómeno de este tipo lo vivíamos hace unos años en el mundo de las tecnologías de la información con el término "Transformación Digital", un concepto que tenía tantas definiciones como especialistas había. Aunque en la actualidad varios de esos especialistas ahora se han transformado en expertos en inteligencia artificial, pero eso es tema para otro artículo.

Según el estudio Talent Trends 2024 desarrollado por PageGroup, el 75% de los líderes empresariales prevé que la IA generará cambios significativos en los próximos tres años[1] . Lo cierto es que el reciente boom que ha tenido la IA y la aceleración de su adopción tanto para uso personal como corporativo, ha traído consigo desafíos complejos, especialmente porque los mismos avances tecnológicos que ayudan a proteger sistemas también pueden ser usados por actores maliciosos para realizar ataques más sofisticados.

Un informe del National Cyber Security Center (NCSC) del Reino Unido, publicado a inicios del 2024 , señala que todos los tipos de actores de amenazas cibernéticas (estatales y no estatales, capacitados y menos capacitados) ya están utilizando IA, en distintos grados. Entre sus conclusiones indica que casi con toda seguridad la IA aumentará el volumen y aumentará el impacto de los ciberataques en los próximos dos años

En este contexto, conversamos con Francesca Gatica, Magíster en seguridad de información y ciberseguridad, líder y moderadora del foro nacional de ciberseguridad Chile, Head of information cybersecurity SAAM S.A., José Lagos, socio principal de Cybertrust Latam, Rocío Ortiz, Subdirectora de Industrias del Futuro del Centro de Innovación UC y Directora Ejecutiva del Laboratorio de Ciberdefensa para Protección de Infraestructuras Críticas Ciberlab, Matías Allende encargado de ciberseguridad de la Municipalidad de Peñalolén, Instructor del Programa de Ciberseguridad del Institute Risk & Security Information y Magíster en Ciberseguridad, Mauricio Ramírez, Country Manager de Palo Alto Networks y Catherine Muñoz, Socia y directora legal de idónea consultores, quienes entregan sus perspectivas sobre cómo la IA está moldeando el panorama de la ciberseguridad y el papel que juegan la regulación y las políticas públicas en esta materia.

Los riesgos de la IA en manos de ciberatacantes

Un informe del National Cyber Security Center (NCSC) del Reino Unido, publicado a inicios del 2024[2] , señala que todos los tipos de actores de amenazas cibernéticas (estatales y no estatales, capacitados y menos capa-

Francesca Gatica
Magíster en seguridad de información y ciberseguridad
Líder y moderadora del foro nacional de ciberseguridad Chile
Head of information cybersecurity SAAM S.A

citados) ya están utilizando IA, en distintos grados. Entre sus conclusiones indica que casi con toda seguridad la IA aumentará el volumen y aumentará el impacto de los ciberataques en los próximos dos años, siendo una de las razones la reducción de las barreras para que los ciberdelincuentes novatos o los hackers a sueldo lleven a cabo operaciones de acceso y recopilación de información más eficaces con IA.

El FBI en mayo de este año advirtió a las personas y empresas que tengan cuidado con la creciente amenaza que representan los cibercriminales que utilizan herramientas de inteligencia artificial (IA) para llevar a cabo sofisticados ataques de phishing e ingeniería social y estafas de clonación de voz y video[3].

"Los ciberatacantes pueden usar la IA para crear ataques de phishing más realistas y generar deepfakes que logran evadir sistemas de seguridad"

"Los ciberatacantes pueden usar la IA para crear ataques de phishing más realistas y generar deepfakes que logran evadir sistemas de seguridad", destaca Francesca Gatica, lo que ha llevado a un aumento de ataques sofisticados que emplean técnicas de ingeniería social para engañar a las víctimas y acceder a información sensible.

En este contexto, Rocío Ortiz enfatiza que "el uso de la IA impacta a distintos niveles. La IA permite y facilita que se generen ataques con mayor alcance y escala, especialmente por medio de la automatización de intentos de ataques maliciosos". Un ejemplo de esto, es el uso de la IA para personalizar campañas de phishing, lo que aumenta su efectividad al adaptarse al perfil de las víctimas. Además, la IA generativa ha facilitado la creación de deepfakes y otros tipos de engaños visuales, que pueden utilizarse para suplantar identidades y manipular la percepción de los usuarios.

Mauricio Ramírez menciona que "la IA es una herramienta que se está utilizando para la generación de ataques a toda la industria, como el robo de credenciales, malware avanzado y suplantación de identidades". Esto representa un reto importante para las organizaciones, que deben desarrollar nuevas formas de protección que puedan anticipar y mitigar estos riesgos antes de que se conviertan en problemas serios. En este sentido, la ciberseguridad se ha convertido en una competencia constante entre la innovación defensiva y la creatividad ofensiva.

Por su parte José Lagos destaca que, aunque la IA ha sido un gran aliado para la defensa, su uso por parte de ciberdelincuentes plantea un escenario complicado: "Si bien es cierto que hoy se utiliza para mejorar los ataques de phishing, o Spearphishing, avanzando a entornos que hoy son impensados y la aceleración de los mismos, generará un batalla de ciberseguridad ofensiva vs defensiva, utilizando herramientas de IA ". Esto implica que las empresas deben estar en un estado de preparación constante, desarrollando modelos predictivos que les permitan anticipar las tácticas de los atacantes y ajustando sus defensas de manera proactiva.

En resumen, la facilidad con la que los atacantes pueden acceder a tecnologías avanzadas ha permitido la proliferación de ciberamenazas que combinan la automatización y el análisis de grandes volúmenes de datos con fines maliciosos. Entre los riesgos más relevantes asociados al uso de la IA en manos de actores maliciosos, se encuentran:

"Destacar la falta de talento especializado y más aún la diferencia de género, hoy en día sólo existe un 15% efectivo de mujeres que nos desempeñamos en ciberseguridad a nivel técnico y estratégico"

1. Phishing Personalizado y Automatizado

Uno de los riesgos más significativos es el uso de la inteligencia artificial para personalizar y automatizar campañas de phishing. Tradicionalmente, el phishing consistía en el envío masivo de correos electrónicos con contenido engañoso para robar credenciales. Sin embargo, con el uso de la IA, estas campañas se han vuelto mucho más sofisticadas.

2. Deepfakes y Suplantación de Identidad

Los deepfakes son una de las manifestaciones más visibles del uso de la inteligencia artificial para crear contenido falso y engañoso. A través de redes generativas adversarias (GAN), los ciberatacantes pueden crear videos, imágenes o audios que simulan de manera convincente la apariencia o voz de una persona real.

Estos deepfakes pueden ser utilizados para múltiples fines maliciosos, como la difusión de desinformación, el desprestigio de figuras públicas o la realización de fraudes financieros. Por ejemplo, un deepfake podría ser utilizado para crear un video de un eje-

cutivo de una empresa anunciando un cambio importante, lo que podría manipular el mercado de valores o causar pánico entre los empleados. Además, los deepfakes también son usados para generar contenido de chantaje, como videos falsos que comprometen a una persona y que luego son utilizados para extorsionarla.

3. Desarrollo de Malware Avanzado

La inteligencia artificial también se ha utilizado para crear malware más eficiente y adaptable. Tradicionalmente, el malware operaba con patrones fijos y predecibles, lo que permitía a los programas antivirus detectar y eliminar amenazas conocidas. Sin embargo, con la introducción de la IA, ha surgido una nueva generación de malware que puede aprender de su entorno y modificar su comportamiento para evadir la detección.

Por ejemplo, el malware basado en IA puede analizar el comportamiento de un sistema específico y ajustar su forma de actuar para evitar ser detectado por soluciones de ciberseguridad. Esto incluye técnicas de polimorfismo, donde el malware cambia su código cada vez que se replica, y técnicas de aprendizaje por refuerzo, donde el software malicioso aprende a través de la interacción con el entorno y ajusta sus estrategias para maximizar su capacidad de daño.

4. Automatización de Ataques de Fuerza Bruta y escaneo de vulnerabilidades

Los ataques de fuerza bruta y el escaneo de vulnerabilidades no son nuevos en el ámbito de la ciberseguridad, pero la IA ha permitido que estas técnicas se vuelvan mucho más efectivas. Con algoritmos de machine learning, los atacantes pueden analizar miles de combinaciones de contraseñas y ajustarlas en tiempo real para mejorar sus intentos de acceso no autorizado a cuentas de usuarios.

Además, los ciberatacantes pueden emplear inteligencia artificial para analizar grandes volúmenes de datos de redes y encontrar vulnerabilidades no parcheadas en servidores y aplicaciones web. La IA les permite identificar patrones de comportamiento que podrían indicar la presencia de una vulnerabilidad específica, lo que acelera el proceso de encontrar puntos de entrada en los sistemas de la organización.

5. Ataques de Denegación de Servicio (DDoS) Automatizados

La inteligencia artificial ha facilitado la creación de botnets más poderosas y eficientes. Una botnet es una red de dispositivos infectados que, bajo el control de un atacante, pueden ser utilizados para lanzar ataques masivos de denegación de servicio (DDoS). Con la ayuda de la IA, estas redes pueden ser gestionadas de forma más inteligente, lo que les permite cambiar dinámicamente sus objetivos y ajustar la intensidad de los ataques para eludir las contramedidas de seguridad implementadas por las víctimas.

Un estudio de la Universidad de Stanford denominado, Do Users Write More Insecure Code with AI Assistants? muestra que solo el 3 % de los desarrolladores que utilizan asistentes de IA producen productos seguros, frente al 21 % de aquellos que no tienen acceso a estas herramientas; el 36 % de quienes emplean IA presentan vulnerabilidades en sus productos, como inyecciones SQL, comparado con el 7 % de quienes no utilizan IA

Los ataques DDoS basados en IA pueden ser más impredecibles y difíciles de mitigar porque son capaces de cambiar sus patrones de tráfico de manera automática para evitar ser bloqueados por las soluciones tradicionales de mitigación de DDoS. Esto los hace más persistentes y efectivos, pudiendo interrumpir los servicios de una empresa durante períodos prolongados y causando pérdidas económicas significativas.

Por otro lado, el uso de herramientas de inteligencia artificial en el desarrollo de software está cada vez más extendido. Una encuesta de GitHub[4] revela que el 92 % de los desarrolladores en EE. UU. ya emplean herramientas de codificación de IA tanto en su trabajo como fuera de él. Los desarrolladores destacan que estas tecnologías les ayudan a mejorar sus habilidades (57 %), aumentar su productividad (53 %), enfocarse en tareas creativas en lugar de actividades repetitivas (51 %) y prevenir el agotamiento (41 %).

Para los encargados de ciberseguridad en las organizaciones, esta tendencia plantea nuevos desafíos, ya que deben establecer medidas de seguridad que orienten a los desarrolladores en el uso adecuado de las herramientas de IA. Además, un estudio de la Universidad de Stanford denominado, Do Users Write More Insecure Code with AI Assistants?[5] , muestra que solo el 3 % de los desarrolladores que utilizan asistentes de IA producen productos seguros, frente al 21 % de aquellos que no tienen acceso a estas herramientas; el 36 % de quienes emplean IA presentan vulnerabilidades en sus productos, como inyecciones SQL, comparado con el 7 % de quienes no utilizan IA. Por lo que, los CISOs tienen la responsabilidad de facilitar una transición desde una IA en la sombras a un entorno conocido como Bring Your Own AI (BYOAI), que permita un control más efectivo.

Los desafíos de Integrar IA en las estrategias de ciberseguridad

La implementación de la IA en productos de ciberseguridad ha mostrado resultados positivos, pero también ha revelado desafíos importantes. Según José Lagos, "la utilización de IA, especialmente en herramientas de ciberseguridad defensiva como la detección de phishing o la detección de malware, es algo que se utiliza desde hace varios años". Sin embargo, advierte que el verdadero reto no radica solo en adoptar estas tecnologías, sino en hacerlo de manera estratégica. "El desafío actual es poder definir un plan de transformación digital orientado a la ciberseguridad, en donde el CISO debiera ser el gran articulador de este propósito".

"la inteligencia artificial ha sido un elemento clave en nuestra industria desde hace varios años, permitiéndonos detectar y responder a amenazas de forma rápida y eficiente"

Este plan, según Lagos de Cybertrust Latam, debe cumplir con varios objetivos clave: asegurar el cumplimiento de la estrategia de negocio, disminuir el tiempo de detección de un ataque y acelerar la recuperación de la empresa en caso de un incidente. "En este nuevo propósito, la función de ciberseguridad debe desarrollar capacidades adaptativas, analíticas y predictivas", afirma. Esto significa que no basta con tener herramientas tecnológicas avanzadas; es crucial que las empresas se adapten continuamente a las nuevas formas de ataque y ajusten sus estrategias a la rapidez con la que evoluciona el panorama de amenazas.

Mauricio Ramírez
Country Manager de Palo Alto Networks

Rocío Ortiz
Subdirectora de Industrias del Futuro del Centro de Innovación UC
Directora Ejecutiva del Laboratorio de Ciberdefensa para Protección de Infraestructuras Críticas (Ciberlab)

Por otro lado, Gatica de SAAM, señala que "la IA generativa ha mejorado significativamente la detección de anomalías y tráficos maliciosos, permitiendo identificar comportamientos sospechosos de manera mucho más rápida". Sin embargo, advierte que la misma tecnología que ayuda a proteger también puede ser utilizada en contra: "La IA facilita el desarrollo de ciberataques más sofisticados, como el phishing personalizado y los ataques de denegación de servicio". Este es uno de los grandes desafíos de la ciberseguridad moderna: encontrar un equilibrio entre el uso de la IA para la defensa y la necesidad de protegerse contra los ataques que se valen de las mismas herramientas.

"La clave está en generar espacios neutrales para compartir conocimiento y testear casos de uso de tecnologías como la IA"

Ramírez de Palo Alto Networks comparte esta visión, destacando que "la inteligencia artificial ha sido un elemento clave en nuestra industria desde hace varios años, permitiéndonos detectar y responder a amenazas de forma rápida y eficiente". Según el ejecutivo, los tiempos de detección, que antes podían extenderse por días o incluso horas, "ahora son cuestión de minutos gracias a la capacidad de la IA para analizar grandes volúmenes de datos y proporcionar alertas automáticas".

La capacidad de la IA para procesar datos a una velocidad sin precedentes permite a las organizaciones identificar patrones de comportamiento sospechosos y responder a ellos antes de que se conviertan en amenazas críticas. Ramírez menciona que, en su experiencia, "esto ha mejorado la protección de plataformas a nivel global, permitiendo una detección más temprana y precisa de ataques que antes pasaban desapercibidos". Sin embargo, el uso de la IA en ciberseguridad no se limita únicamente a la detección temprana de amenazas.

La evolución de la ciberseguridad impulsada por la inteligencia artificial no muestra signos de desaceleración. De hecho, se espera que la integración de la IA en productos de ciberseguridad continúe siendo una prioridad para muchas organizaciones. "En el pasado, era suficiente utilizar firewalls y agentes antimalware para proteger los activos", menciona Matías Allende de la Municipalidad de Peñalolén, quien ha trabajado en el desarrollo de tecnologías avanzadas para proteger sistemas críticos. Sin embargo, con la creciente sofisticación de las amenazas, "la IA se ha convertido en un elemento clave en la ciberseguridad, mejorando y aportando más precisión y rapidez en la detección y análisis de amenazas en tiempo real".

Allende destaca la importancia de estas tecnologías para proteger sectores críticos como la banca y la salud. "En la Municipalidad de Peñalolén, después de un ataque del ransomware Locky en 2017, vimos la oportunidad de implementar tecnología XEDR, que extiende las capacidades de EDR mediante modelos de machine learning". Gracias a esta implementación, lograron "detectar amenazas como WannaCry y Zepto antes de que infectaran nuestros sistemas". Esta experiencia subraya el valor de la IA para prevenir amenazas antes de que se materialicen y causen daños significativos.

La colaboración como pilar de la ciberseguridad

El carácter global de las amenazas cibernéticas hace que la cooperación tanto a nivel nacional como internacional sea un componente esencial para la ciberseguridad. Rocío Ortiz destaca que " los cibercriminales cuentan con gobernanzas y modelos de colaboración y de compartir conocimiento de forma ágil y altamente sofisticada, eso les permite moverse a mayor velocidad ". En contraste, muchas organizaciones y gobiernos aún trabajan de forma aislada, lo que dificulta la creación de una respuesta coordinada frente a las amenazas globales.

"es crucial desarrollar modelos de formación de competencias aplicadas especializados y ágiles, que logren conjugar tecnologías y dominios como la ciberseguridad y la IA en contextos industriales y procesos de específicos, requeridos para la operación"

Para Ortiz, "la clave está en generar espacios neutrales para compartir conocimiento y testear casos de uso de tecnologías como la IA". Esto puede incluir la creación de laboratorios de ciberseguridad donde los sectores público, privado y académico puedan colaborar en la investigación de nuevas amenazas y en el desarrollo de soluciones innovadoras. Estas iniciativas permiten a los participantes intercambiar experiencias, compartir buenas prácticas y desarrollar estándares que puedan ser adoptados de manera amplia.

Catherine Muñoz, también resalta la importancia de este tipo de colabora-

ciones. "La colaboración entre la academia, la industria y el gobierno es fundamental, especialmente en áreas tan dinámicas y complejas como la ciberseguridad impulsada por inteligencia artificial", afirma. Muñoz considera que la academia debe liderar la investigación de nuevas soluciones mientras que la industria tiene el rol de aplicarlas en entornos reales. "El gran desafío es sincronizar estos esfuerzos para que sean complementarios, evitando que cada sector trabaje de forma aislada", subraya, destacando la necesidad de una cooperación efectiva para enfrentar los desafíos de la IA en ciberseguridad.

"El desafío actual es poder definir un plan de transformación digital orientado a la ciberseguridad, en donde el CISO debiera ser el gran articulador de este propósitos"

La creación de redes internacionales de colaboración que ha generado por ejemplo el CSIRT de Gobierno, espacios como el recientemente inaugurado Laboratorio de Ciberdefensa para Protección de Infraestructuras Críticas (Ciberlab) o el Foro Nacional de Ciberseguridad, son ejemplos de cómo se pueden unir esfuerzos para enfrentar estas amenazas.

Cabe señalar que el foro impulsado por el Senador Kenneth Pugh ha convocado a académicos, profesionales, empresas y organizaciones interesadas en la ciberseguridad a unirse con el objetivos de generar políticas públicas que permitan fortalecer la seguridad en línea, proteger los derechos digitales y promover un ciberespacio confiable y generar soluciones a través del debate de las siguientes cinco dimensiones: Política y estrategia de seguridad cibernética; Cultura cibernética y sociedad; Formación, capacitación y habilidades de seguridad cibernética; Marcos legales y regulatorios; y estándares, organizaciones y tecnologías.

Formación de Talento

Es vox populi la escases de expertos en ciberseguridad, que a nivel global llega a 3.4 millones de profesionales el año pasado, según estudio del Consorcio de Certificación de Seguridad de Sistemas de Información (ISC2). Mientras que en Chile según un estudio del CSIRT de Gobierno[6], en nuestro país existe una brecha de 28.000 expertos en ciberseguridad.

Por esta razón, Francesca Gatica, resalta la importancia de destacar la falta de talento especializado y más aún la diferencia de género, "hoy en día sólo existe un 15% efectivo de mujeres que nos desempeñamos en ciberseguridad a nivel técnico y estratégico?". Agregando que "si bien es cierto, existen iniciativas que están potenciando este punto, se debe esperar algunos años en que pueda ser efectivo".

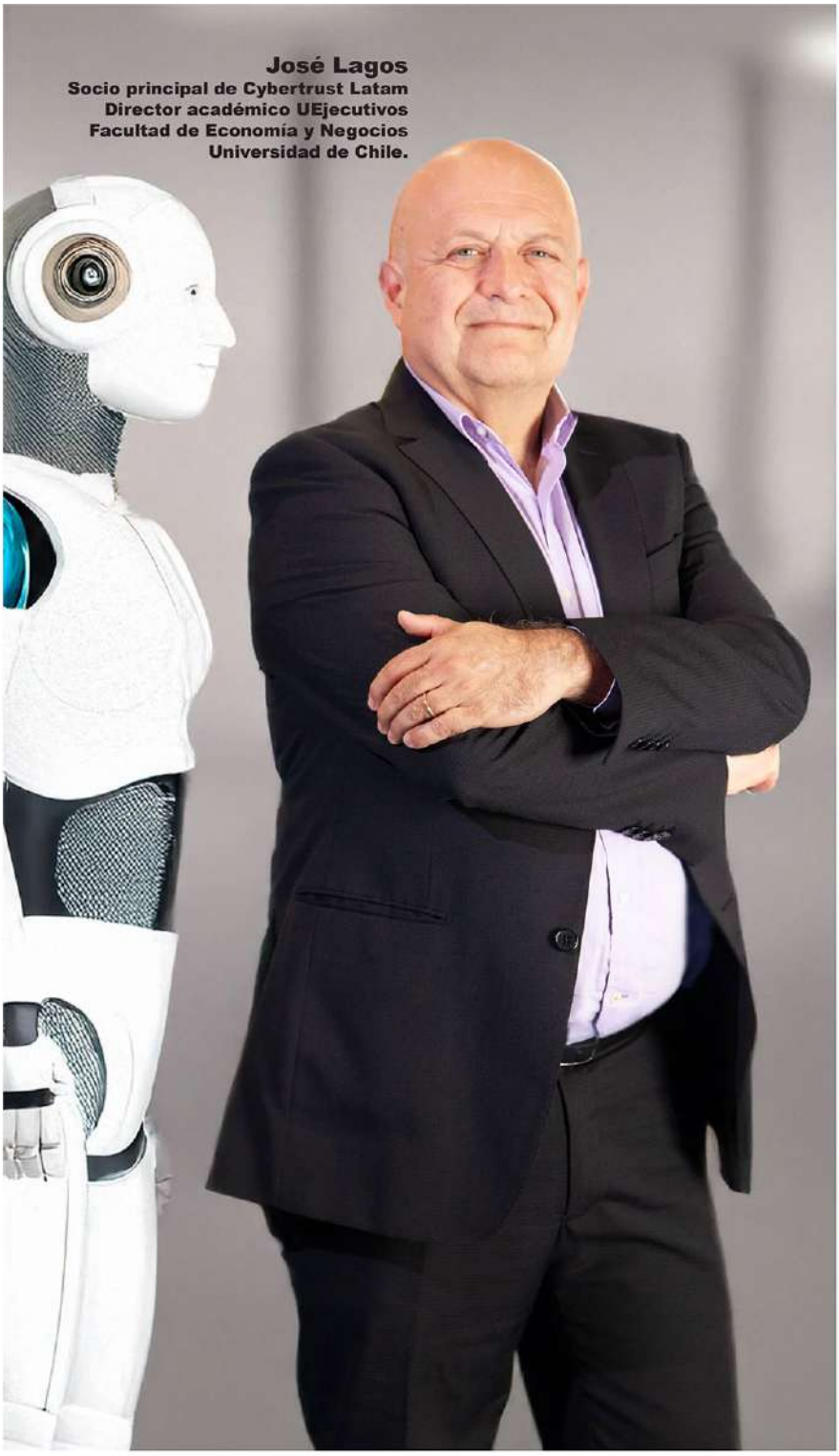
La falta de expertos es uno de los "principales desafíos están asociados a la escasez de talento especializado, principalmente dado el déficit de especialistas en áreas como la ciberseguridad", para Rocío Ortiz del Centro de Innovación UC, quien además señala que es crucial desarrollar "modelos de formación de competencias aplicadas especializados y ágiles, que logren conjugar tecnologías y dominios como la ciberseguridad y la IA en contextos industriales y procesos de específicos, requeridos para la operación". Este enfoque es fundamental para mantener a las organizaciones a la vanguardia de las nuevas amenazas.

La demanda de profesionales en ciberseguridad ha superado la oferta, lo que ha llevado a un aumento de los salarios y a una competencia feroz entre las empresas para atraer y retener talento. Esto también ha provocado que muchas organizaciones enfrenten dificultades para implementar estrategias de ciberseguridad efectivas, ya que carecen de los recursos humanos necesarios para gestionar y analizar de manera adecuada las herramientas avanzadas de IA.

Para Matías Allende, "los laboratorios de investigación y las instituciones académicas desempeñan un rol crucial al invertir en el desarrollo de nuevos modelos de IA y formar especialistas que impulsarán futuros avances. Hoy parece difícil de creer, pero la IA existe desde los años 50 y ha ido evolucionando, en técnicas y aplicaciones, hasta el uso actual del machine learning, deep learning y la IA generativa. La tecnología ha evolucionado rápidamente, creando tanto oportunidades como desafíos en múltiples sectores, incluido el cibercrimen". Agregando que es "fundamental formar profesionales no solo en lo técnico, sino también en la gestión ética de la IA para evitar situaciones distópicas como las mostradas en películas como Terminator o I, Robot, aunque suene a ficción varios expertos y líderes han declarado que "la mitigación del riesgo de extinción de la IA debería ser una prioridad mundial", declaración publicada en el Center for AI Safety".

"La función de ciberseguridad debiera tener capacidades adaptativas, analíticas y predictivas, en donde los aspectos de innovación incremental, innovación radical o disruptiva es esencial para el desarrollo de nuevas barreras de defensa utilizando inteligencia artificial, en cualquiera de sus disciplinas"

En instituciones como IRSI (Information Risk and Security Institute), señala Allende, "he observado de primera fuente cómo la educación está impulsando la capacitación continua (upskilling) y la reconversión profesional (reskilling), permitiendo a las personas mejorar sus competencias en ciberseguridad. Debemos proporcionar los recursos adecuados para que las nuevas generaciones puedan gestionar los riesgos técnicos y éticos aso-



ciados al avance de la IA".

Por su lado, José Lagos enfatiza la necesidad de desarrollar una "cultura organizacional que valore la innovación y la agilidad". Esto implica no solo invertir en la formación de especialistas, sino también fomentar una mentalidad de adaptación y mejora continua en todos los niveles de la organización. "La función de ciberseguridad debiera tener capacidades adaptativas, analíticas y predictivas, en donde los aspectos de innovación incremental, innovación radical o disruptiva es esencial para el desarrollo de nuevas barreras de defensa utilizando inteligencia artificial, en cualquiera de sus disciplinas, como machine Learning, deep Learning o IA generativa".

Desafíos regulatorios y normativas internacionales

La nueva Ley Marco de Ciberseguridad en Chile es gran avance en la modernización de la regulación del país para enfrentar los desafíos que presenta la era digital. Sin embargo, Catherine Muñoz advierte que, "regular la inteligencia artificial en un contexto de ciberseguridad plantea desafíos significativos debido al carácter emergente y evolutivo de ambas áreas. Uno de los principales desafíos es la dificultad para prever todas las implicancias futuras del desarrollo de la IA. Las regulaciones no pueden ser tan restrictivas como para frenar la innovación, pero al mismo deben ser lo suficientemente robustas como para proteger a los ciudadanos. Otro reto es la adaptación rápida ante nuevas amenazas: la IA no solo

se utiliza para defender sistemas, sino que también puede ser explotada por actores malintencionados, generando ciberataques más sofisticados. Además, es complejo coordinar las regulaciones nacionales con las normativas internacionales y asegurar la protección de datos personales en un entorno globalizado".

"Es fundamental formar profesionales no solo en lo técnico, sino también en la gestión ética de la IA para evitar situaciones distópicas"

Muñoz menciona que "Chile, en su calidad de líder regional en IA, tiene la oportunidad de participar activamente en la definición de estas normativas, colaborando con otros países y organismos internacionales para asegurar que nuestras regulaciones no solo respondan a las necesidades locales, sino que también se alineen con los estándares internacionales". Esto es crucial para países que buscan posicionarse como líderes en innovación tecnológica y que desean atraer inversión extranjera. Sin un marco regulatorio claro y adaptado a los tiempos, las empresas pueden enfrentar incertidumbre legal, lo que podría desalentar la adopción de tecnologías avanzadas como la IA.

Por último, la ejecutiva de idónea consultores advierte que "Las regulaciones no pueden ser tan restrictivas como para

frenar la innovación, pero al mismo deben ser lo suficientemente robustas como para proteger a los ciudadanos". Esto es especialmente relevante en un entorno donde la inteligencia artificial y las tecnologías digitales están en constante evolución.

Conclusiones: un futuro artificial que demandará inteligencia para enfrentar las nuevas amenazas

La inteligencia artificial ha traído enormes beneficios para la ciberseguridad, transformando la manera en que las organizaciones protegen sus sistemas, detectan amenazas y responden a incidentes. Sin embargo, esta misma tecnología, cuando es utilizada con fines maliciosos, plantea una amenaza de gran magnitud que sigue creciendo y evolucionando. La velocidad a la que se desarrollan nuevas técnicas de ataque y defensa impulsadas por IA es un desafío para empresas, gobiernos y ciudadanos, quienes deben prepararse para un futuro en el que las amenazas digitales serán cada vez más complejas y sofisticadas.

"Los laboratorios de investigación y las instituciones académicas desempeñan un rol crucial al invertir en el desarrollo de nuevos modelos de IA y formar especialistas que impulsarán futuros avances"

El uso de IA para desarrollar ataques más personalizados, como el phishing de voz o la suplantación de identidad mediante deepfakes, es solo la punta del iceberg. Estas amenazas demuestran cómo la tecnología permite a los ciberdelincuentes realizar ataques dirigidos con un nivel de precisión y personalización sin precedentes, incrementando sus posibilidades de éxito y dificultando la identificación de los ataques. A medida que la inteligencia artificial avanza, los ataques basados en IA pueden llegar a ser tan creíbles que incluso los sistemas de seguridad más avanzados tendrán dificultades para detectarlos. En este sentido, la preparación para enfrentar estas nuevas amenazas no es solo una opción; es una necesidad urgente.

Para enfrentar este complejo panorama, es fundamental que las organizaciones adopten un enfoque de ciberseguridad que sea proactivo, adaptable y colaborativo. La implementación de herramientas avanzadas de IA para la defensa es solo una pieza del rompecabezas. También es crucial fomentar una cultura de ciberseguridad dentro de las organizaciones, donde todos los empleados, desde la alta dirección hasta el personal operativo, estén informados y capacitados para identificar y responder ante amenazas. La concientización y educación en ciberseguridad son esenciales, ya que los seres humanos siguen siendo uno de los eslabones más débiles en la cadena de defensa. Las campañas de formación y concientización deben ser continuas y adaptarse a las amenazas emergentes.

Además, la preparación para un futuro con nuevas amenazas requiere una colaboración efectiva entre el sector público y privado. Los gobiernos, las empresas y las instituciones académicas deben trabajar juntos para investigar y desarrollar soluciones innovadoras, compartir información sobre amenazas en tiempo real y establecer estándares comunes que fortalezcan la ciberseguridad global. La cooperación internacional es especialmente relevante, dado que las amenazas cibernéticas no conocen fronteras. La creación de marcos de colaboración y la participación en foros internacionales, como el Foro Mundial de Ciberseguridad o la Alianza Internacional para la Ciberseguridad, son esenciales para enfrentar amenazas de alcance global.

El ámbito legislativo también tiene un papel clave en esta preparación. Los marcos regulatorios deben evolucionar para establecer normativas que guíen el uso ético de la inteligencia artificial en ciberseguridad y prohíban su utilización con fines maliciosos. Sin embargo, la regulación en esta área debe ser flexible para adaptarse rápidamente a las innovaciones tecnológicas y equilibrada para no obstaculizar el desarrollo de IA en el ámbito de la defensa. La creación de leyes de ciberseguridad que incluyan sanciones para los actores maliciosos, así como incentivos para que las organizaciones adopten prácticas de seguridad más robustas, es crucial para mantener un entorno seguro y estable.

"Chile, en su calidad de líder regional en IA, tiene la oportunidad de participar activamente en la definición de estas normativas, colaborando con otros países y organismos internacionales para asegurar que nuestras regulaciones no solo respondan a las necesidades locales, sino que también se alineen con los estándares internacionales"

Otra área de enfoque importante es la inversión en la formación de talento especializado. La falta de profesionales en ciberseguridad es una preocupación creciente, y a medida que la inteligencia artificial se convierte en un componente integral de las estrategias de defensa y ataque, es esencial

Catherine Muñoz
Socia y directora legal de Idónea consultores

que exista un grupo de expertos capacitados en el uso de estas tecnologías. Los programas de educación y capacitación en IA y ciberseguridad, tanto en instituciones académicas como dentro de las empresas, ayudarán a crear una generación de especialistas que puedan enfrentar los desafíos del futuro. Esta inversión en talento debe ser continua, y los programas de formación deben actualizarse constantemente para mantenerse al día con las nuevas técnicas y herramientas.

"La colaboración entre la academia, la industria y el gobierno es fundamental, especialmente en áreas tan dinámicas y complejas como la ciberseguridad impulsada por inteligencia artificial"

Por último, es importante que las organizaciones adopten un enfoque de ciberseguridad basado en la resiliencia. La mentalidad tradicional de "evitar el ataque a toda costa" ya no es suficiente. En un entorno donde los ataques son inevitables, la clave está en desarrollar la capacidad de recuperación rápida y efectiva. Esto implica no solo contar con sistemas de respuesta a incidentes bien diseñados, sino también realizar pruebas regulares de resiliencia, como simulaciones de ataques, para evaluar la capacidad de respuesta de la organización. La resilien-

cia implica que, aun si un ataque tiene éxito, la organización sea capaz de minimizar el daño, recuperar la operatividad en el menor tiempo posible y aprender de la experiencia para reforzar sus defensas.

En conclusión, el futuro de la ciberseguridad en la era de la inteligencia artificial exige una combinación de tecnología avanzada, regulación adecuada, educación y colaboración. Solo con una estrategia integral y adaptativa se podrá hacer frente a las amenazas cada vez más sofisticadas que plantea el uso de la IA en manos de ciberatacantes. La clave para las organizaciones y gobiernos radica en estar un paso adelante, adoptando una actitud de anticipación y respuesta proactiva, y fomentando un ecosistema global de cooperación que permita enfrentar estas amenazas de manera unida y efectiva. El desafío es grande, pero con el enfoque correcto, es posible construir un futuro digital más seguro y resiliente.

1 https://www.trendtic.cl/2024/10/nuevas-tendencias-en-captacion-y-retencion-de-talento-el-bienestar-y-la-flexibilidad-superan-a-la-renta-como-prioridades/

2 https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat#section_5

3 https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence

4https://github.blog/news-insights/research/survey-reveals-ais-impact-on-the-developer-experience/

5 https://arxiv.org/abs/2211.03622

6 https://www.trendtic.cl/2024/06/estudio-csirt-de-gobierno-calcula-en-28-mil-la-brecha-de-especialistas-en-ciberseguridad/

7 Fuente: Foro Nacional de Ciberseguridad Chile

Fotos de voceros, editadas con IA.