Vol. Nº 9
Abril/2021
www.csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS

Investigación, Tendencia y Concientización

LAS DOS CARAS DE LA INTELIGENCIA ARTIFICIAL PARA LA CIBERSEGURIDAD

Cooperación Internacional
Reino Unido

Tendencias
Deepfakes

Comunidades Nacionales
El desarrollo de la **IA** en el Bío-Bío

Legal
La Intéligencia Artificial se toma la agenda Pública

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT es el Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile. Su misión es reducir los riesgos de la ciberseguridad en las redes del Gobierno de Chile, asesorando a las diferentes organizaciones que lo componen, actuando como socio estratégico en la defensa de las amenazas y colaborando para brindar mayor seguridad y robustez a las infraestructuras del Estado.

¿Cómo lo **hacemos?**

Contamos con un equipo multidisciplinario de profesionales y las tecnologías para proveer de asistencia técnica y logística a nuestros beneficiarios, así como prevenir la explotación de vulnerabilidades y actuar oportunamente frente a amenazas y ciberataques.

- MONITOREO DE LAS PLATAFORMAS DE INTERNET DE ORGANISMOS PÚBLICOS Y PRIVADOS **24/7**
- INVESTIGACIÓN Y CAPACITACIÓN PARA ENFRENTAR LAS AMENAZAS DEL FUTURO
- DETECCIÓN DE VULNERABILIDADES DE SITIOS Y SISTEMAS WEB DEL ESTADO
- GESTIÓN DE INCIDENTES Y DIFUSIÓN DE MEDIDAS PREVENTIVAS
- INCORPORACIÓN DE NUEVAS TECNOLOGÍAS Y HERRAMIENTAS DE SEGURIDAD INFORMÁTICA
- MEJORA CONTINUA DE LOS ESTÁNDARES DE CIBERSEGURIDAD DEL PAÍS

145 8712 7864
096 4321 5541

Alianza del Pacífico · FIRST · CSIRTamericas.org · MERIDIAN Connecting and Protecting

INDICE

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS

Investigación, Tendencia y Concientización

cibersucesos@interior.gob.cl

Director: Carlos Landeros Cartes

Jefa de contenidos y edición:
Katherina Canales Madrid

Colaboradores equipo CSIRT:
Ramón Rivera, Hernán Espinoza,
Cristobal Hammersley

Diseño y diagramación: Jaime Millán

EDITORIAL

Carlos Landeros Cartes
Director Nacional
CSIRT de Gobierno

Una de las herramientas tecnológicas de las que más se habla hoy en día, a veces con incertidumbre y otras veces con desconocimiento, es de la inteligencia artificial, a la que decidimos dedicar el presente número de CiberSucesos.
Como ha sido el caso de la gran mayoría de las nuevas herramientas que ha ido desarrollando la humanidad a lo largo de su historia, la inteligencia artificial representa un enorme potencial tanto como para usos benéficos como para otros maliciosos, y esta dualidad es también patente cuando hablamos de sus efectos para la ciberseguridad.
Es así como el tema central de nuestro presente número son los beneficios y peligros que suponen el uso de la inteligencia artificial (y técnicas como el machine learning) para la defensa de nuestras redes, incluyendo formas en que hacen más fácil y eficiente la ciberseguridad, identificando, por ejemplo, nuevas amenazas a través del análisis de patrones de comportamiento, hasta la dificultad que suponen al prestarse igualmente para mejorar las amenazas digitales con malware cada día más inteligente y silencioso.
En la misma línea, profundizando en usos maliciosos de las técnicas de inteligencia artificial, tenemos un artículo dedicado a los deepfakes, que se han vuelto mucho más fáciles de hacer en el último par de años. Qué son, cómo funcionan y qué se puede hacer para evitar caer en sus engaños, son también parte de esta edición.
En Comunidades Nacionales destacamos el avance de la Universidad de Concepción en numerosos proyectos que avanzan en el uso de la inteligencia artificial en ámbitos como la medicina, la educación y la industria forestal. Y como ejemplo internacional, nos adentramos en la experiencia británica con el desarrollo de una estrategia de inteligencia artificial, la cual combina un foco en el desarrollo de una industria con esa tecnología con la creación de una instancia especializada en su desarrollo ético.
Finalmente, la columna legal se adentra precisamente en los detalles de nuestra propia Política Nacional de Inteligencia Artificial, desarrollada para Chile bajo el liderazgo del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, y pronta a ser publicada. La política toma en cuenta el desarrollo de la necesaria infraestructura, del capital humano necesario y de las medidas indispensables para garantizar el uso ético y responsable de los datos de las personas.

LAS DOS CARAS

DE LA INTELIGENCIA ARTIFICIAL PARA LA CIBERSEGURIDAD

Como toda tecnología que ha desarrollado la humanidad a lo largo de la historia, el uso de las distintas formas de la inteligencia artificial significa tanto una promesa para el reforzamiento de la ciberseguridad, como un factor de riesgo que facilitará a los delincuentes desarrollar ataques más inteligentes y a gran escala, llevándonos a plantearnos dilemas que están, incluso, al borde de las fronteras de la ética y la moral.

Ventajas de la IA **para la ciberseguridad**

Técnicas de inteligencia artificial como el machine learning y el deep learning están siendo cada día más usadas para advertir de forma automática la presencia de amenazas digitales, sobre la base del aprendizaje dinámico de conductas y comportamientos normales versus anormales, pues el malware actual se adaptó a la búsqueda de firmas estáticas, realizada por los antivirus tradicionales, y aprendió a ocultar esas y otras señales para evitar su detección.

Además, a medida que la transformación digital se hace más profunda y las operaciones cibernéticas de las compañías aumentan, necesariamente la superficie de ataque que necesita ser protegida también se expande. Más aún, para muchos negocios hoy en día, la captura y análisis de enormes cantidades de datos es crucial para sus estrategias de mercado, subsistencia presente y posicionamiento futuro.
Por todo lo anterior, resulta muchas veces imposible para los equipos mantener una vigilancia adecuada de tanta información sin la ayuda de programas que puedan supervisar los sistemas, entender los contextos sobre referencias históricas y comprensión del presente de los datos sobre la base de sus comportamientos, mejorando sus capacidades de forma autónoma a través del machine learning.

Por eso, la utilidad más mencionada de la inteligencia artificial para la ciberseguridad es la detección de intrusiones. Con técnicas de IA se pueden analizar grandes cantidades de datos muy rápidamente, buscando patrones de comportamiento identificados como sospechosos, con lo que pueden incluso descubrir tipos nuevos de malware (ataques de día cero) o códigos que esconden sus componentes maliciosos para dificultar su detección.
Un beneficio es que, para estos programas, el analizar mayores cantidades de datos va mejorando sus habilidades de detección (aunque al principio deben contar con datos elegidos por humanos para entender los patrones que deben reconocer).Complemento perfecto para la creciente importancia del denominado “big data”.
Otros usos similares en funciones de ciberseguridad son el inventario automatizado de los activos digitales de una organización, la búsqueda de debilidades en los programas de seguridad de una red (o sea, dónde es más probable que se produzca una brecha), o la recolección de información sobre los ataques que están “de moda” entre los ciberdelincuentes, un ejemplo de ciberinteligencia, para priorizar decisiones de monitoreo sobre las formas en que es más probable que la empresa sea atacada.

La detección automatizada de patrones también es usada para sistemas de identificación de usuarios, como parte de las medidas para evitar la suplantación de humanos por parte de bots, o para detectar intrusiones no autorizadas a una red por parte de usuarios no autorizados.
La adopción de sistemas automatizados puede facilitar una respuesta a incidentes de seguridad informática más rápida y eficiente. Y tal como los tradicionales filtros de spam, los servicios de correo incorporan herramientas de aprendizaje de máquinas para la detección de phishing, para ponerlos en cuarentena y eliminarlos, reduciendo la efectividad del principal vector de malware en el mundo de la ciberseguridad actual.

Es decir, la IA puede llegar a proporcionarnos un CiberInvestigador-IA que pueda automatizar el análisis de gran cantidad de datos y encontrar en ellos las anomalías que identifiquen un ataque que haya ocurrido, que esté ocurriendo, y lo más interesando aún que este por ocurrir (predecir). Este último aspecto, que parece futurista, ya presenta avances y pueden observarse en el siguiente link: https://twitter.com/BforeAi en donde esta empresa, utilizando IA, señala que puede predecir la aparición de dominios maliciosos antes de que estén activos.

Inteligencia artificial (IA): Los sistemas de inteligencia artificial (IA) son software (y posiblemente también hardware) diseñados por humanos que, dado una objetivo complejo, como actuar en la dimensión física o digital, al percibir su entorno a través de la adquisición de datos, interpretando los datos recopilados, los datos estructurados o no estructurados, razonando sobre el conocimiento, o procesamiento de la información, derivada de estos datos y decide la(s) mejor(es) acción(es) a tomar para lograr la meta dada. Los sistemas de IA pueden usar reglas simbólicas o aprender un modelo numérico, y también pueden adaptar su comportamiento, analizando cómo el medio ambiente se ve afectado por sus acciones anteriores.

Machine learning (ML): El aprendizaje automático (ML) es un subconjunto de la IA, donde los algoritmos están entrenados para inferir ciertos patrones basados en un conjunto de datos con el fin de determinar las acciones necesarias para lograr un objetivo dado.

Deep learning (DL): El deep learning es un tipo de machine learning que entrena a una computadora para que realice tareas como las hacemos los seres humanos, como el reconocimiento del habla, la identificación de imágenes o hacer predicciones..

Riesgos de la IA **para la ciberseguridad**

Por contrapartida, la IA, como cualquier herramienta, también está disponible para los cibercriminales, y en consecuencia, la automatización también facilitará a los ciberdelincuentes multiplicar sus ataques y al mismo tiempo, hacerlos más sofisticados. Esto acrecienta el actual proceso de masificación del malware, que ha puesto cada día los códigos maliciosos al alcance de más ciberdelincuentes y bandas criminales, quienes ni siquiera necesitan saber de tecnología, solo les basta comprar los programas en mercados ilícitos llegando a los extremos de consumir IAaS (IA como servicio en la nube).

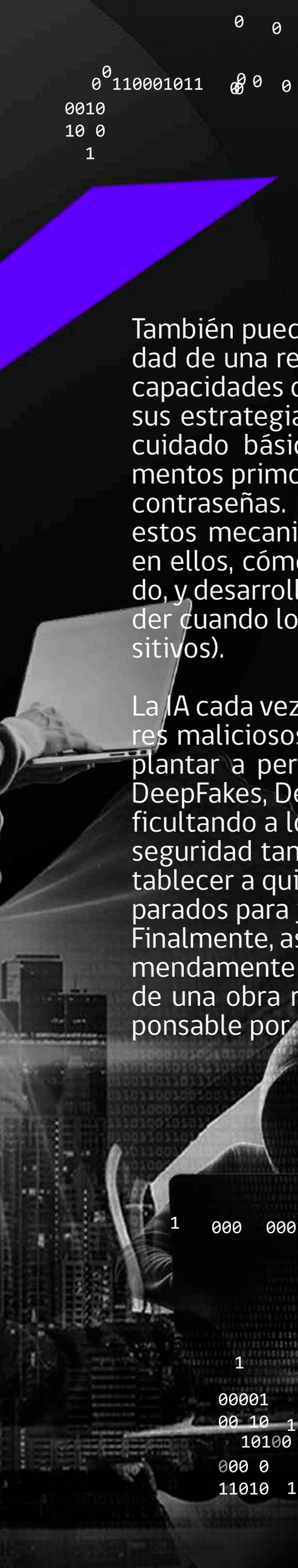
Es así como existen ejemplos de malware que aprovechan el machine learning para adaptarse a las defensas que enfrentan. Ya en 2018, IBM diseñó el código que bautizó como DeepLocker, que usa IA para esconderse y pasar desapercibido hasta definir que ha encontrado una víctima en específico, a la que identifica gracias a elementos como el reconocimiento facial y de voz y la geolocalización (¡otro recordatorio de que debemos tener cuidado con lo que compartimos en las redes sociales!).

Del mismo modo, los mecanismos usados por las compañías para protegerse, automatizando la ciberinteligencia, serán usados por los delincuentes para buscar brechas y objetivos más fáciles de penetrar. Técnicas de aprendizaje automatizado ya están siendo utilizadas para recolectar información de redes sociales con el fin de refinar y hacer más personalizados los ataques de phishing, por ejemplo, como en el famoso caso de la suplantación de la voz de un CEO para robar a su empresa. Un tema similar es la forma en que la IA ya está facilitando el desarrollo y propagación de noticias falsas a través de los denominados deepfakes, cuyo empleo para realizar ciberestafas analizamos en otro artículo de este mismo número de CiberSucesos.

La IA definitivamente esta ayudando a que los malware (soportados por IA o mejorados por IA) sean mucho más eficaces y difíciles de detectar por parte de las herramientas tradicionales, pues incorporan capacidades que les permiten actuar adaptivamente y evadir los controles con mayor facilidad.

El presente de los “asistentes inteligentes” ha ido ganando espacio de manera importante en los hogares de las personas, pero estos dispositivos basados en IA también pueden volverse contra nosotros al ser manipulados por terceras partes permitiéndoles por ejemplo escuchar nuestras conversaciones o tomar el control de la domótica de nuestro hogar (luces, temperatura, cierres o apertura de puertas y ventanas entre otros muchos).
Otra manera en la que la IA puede terminar afectando nuestra ciberseguridad es que puede potenciar enormemente las herramientas para adivinar contraseñas, amplificando exponencialmente el poder de los actores maliciosos que buscan acceder de manera no autorizada a nuestros datos, a nuestras empresas, a nuestras instituciones.

La utilización de IA puede llegar a impactar el devenir político de un país, mediante la facilitación a empresas o estados a acceder a enormes fuentes de datos que permiten modelar estrategias de intervención en las sociedades mediante bots (debidamente entrenados con el sesgo malicioso) que coordinados bajo una estrategia hostil pueden moldear conductas, resaltar miedos, despertar odios y en consecuencia orientar una conducta ante los procesos sociales y democráticos de una nación.



También puede ser un problema para la ciberseguridad de una red, poner una confianza excesiva en las capacidades de la IA, que desvíe a la organización de sus estrategias de ciberseguridad, o de medidas de cuidado básicas como la concientización en elementos primordiales, como la generación de buenas contraseñas. Asimismo, las empresas que adopten estos mecanismos deberán calibrar cuánto confiar en ellos, cómo verificar que no se estén equivocando, y desarrollar protocolos para saber cómo responder cuando lo hagan (por ejemplo, con los falsos positivos).

La IA cada vez más, desde la perspectiva de los actores maliciosos, será utilizada para impersonar o suplantar a personas reales combinando técnicas de DeepFakes, DeepBots, DeepHacks y DeepExploits dificultando a los investigadores y auditores en ciberseguridad tanto la atribución del delito como el establecer a quien se lleva ante un juez. ¿Estamos preparados para juzgar a una IA?.
Finalmente, así como nos preguntamos aspectos tremendamente fundamentales como quien es el autor de una obra realizada por una IA o quien es el responsable por un accidente causado por un automóvil conducido autónomamente por una IA, también nos hemos de preguntar quién es el autor de un hackeo cuando este sea llevado cabo por una IA. Si la atribución de un hackeo en las condiciones actuales es tremendamente difícil, esta nueva dimensión viene a hacerlo aún más complejo y difícil de establecer; teniendo en cuenta que la atribución conlleva decisiones jurídicas importantes según las consecuencias de los actos maliciosos (muerte de una persona por ejemplo), llegando incluso a decisiones en la que dos países pueden definir entrar en guerra.

Los desafíos que nos plantean las IA para la ciberseguridad van desde los más simples usándola para elaborar IA-malware, pasando por la construcción de entidades virtuales que suplanten a seres humanos o conglomerados de estos afectando decisiones de una nación, hasta los complejos dilemas de atribución y justicia para castigar a los culpables.
En síntesis la misma herramienta, que le otorga a la ciberseguridad increíbles avances y progresos en automatización y capacidad de procesamiento de información, le plantea enormes desafíos para enfrentar las amenazas que ella misma representa en la medida que es utilizada para fines maliciosos.

LA ESTRATEGIA DEL REINO UNIDO PARA POTENCIAR EL USO DE LA INTELIGENCIA ARTIFICIAL

El gobierno británico ha definido una estrategia para convertirse en líder mundial en esta nueva tecnología, impulsando su utilización con elementos como el aumento en su inversión en investigación y desarrollo, la generación de instancias para la compartición responsable de datos entre instituciones privadas, y la creación de un Centro para la Ética de Datos e Innovación.

El pasado mes de marzo el Reino Unido presentó su nueva estrategia de inteligencia artificial (IA), una de las diez prioridades tecnológicas del gobierno británico. Como explicó durante su presentación el secretario general Oliver Dowden, la estrategia de IA tiene tres ejes:

- El crecimiento de la economía a través del uso extendido de las tecnologías de IA.
- El desarrollo ético, seguro y confiable de IA esponsable.
- Conseguir resiliencia de cara a los cambios poniendo énfasis en el desarrollo de talento e investigación y desarrollo.

Esta estrategia británica fue elaborada en acuerdo con el sector de IA y con recomendaciones del denominado AI Council (Concejo IA, que publicó su Hoja de Ruta IA en enero), industria, academia y sociedad civil y se plasma en el documento de política denominado IA Sector Deal.

El aspecto económico ha sido clave en la formulación de la estrategia IA del Reino Unido. De hecho, el desarrollo de esta tecnología, junto a la economía de los datos, es uno de cuatro "Grandes Desafíos" planteados por Whitehall para poner al Reino Unido a la vanguardia de las industrias del futuro.

Entre las numerosas medidas industriales británicas para aumentar su productividad y poder adquisitivo se encuentran:

1. Elevar la inversión en investigación y desarrollo hasta el 2,4% del PIB para 2027
2. Invertir 725 millones de libras en un nuevo fondo para fomentar la innovación.
3. Generar más de 1.000 millones de libras en inversión pública para mejorar la infraestructura digital.
4. Reunir más de 20 mil millones de libras en inversión en negocios innovadores y de alto potencial, incluyendo el establecimiento de un nuevo fondo de inversión de 2.500 millones de libras en el British Business Bank.

Y en lo respectivo específicamente a la IA, se comprometen hasta 950 millones de libras en apoyo al sector, incluyendo aportes del gobierno, la industria y la academia, lo que se suma a 250 millones de libras para generar tecnología de vehículos conectados y autónomos.

El objetivo británico es liderar la industria de IA, y no esperar a que se desarrolle y dejar la iniciativa a otras naciones. Para ello, las propuestas también su ponen mejorar las instituciones que apoyan la IA, constituir una fuerza laboral capacitada y estimular el acceso a los datos, todos factores elementales para el desarrollo de esta tecnología.

INFRAESTRUCTURA E IDEAS

De los 1000 millones de libras que el Reino Unido está invirtiendo en mejorar su infraestructura digital, como un paso crucial para conseguir su ambición de liderar al mundo en IA, la mayor parte está siendo usada en extender sus redes 5G y de fibra óptica. Pero también se desarrollarán otras iniciativas clave, como la generación de esquemas para la compartción de datos en el sector privado, a través de Data Trusts, mecanismos en los cuales los partícipes tienen claros sus derechos y deberes respecto de los datos contenidos, para facilitar el acceso a la información protegiendo los datos sensibles y asegurando la responsabilidad.
Más aún, para fomentar el surgimiento de mayor innovación, la inversióny desarrollo (que buscan hacer crecer a 2,4% en 2027 y a 3% para el largoplazo) incorpora iniciativas como competiciones para llevar al mercado ideas con potencial, con 725 millones de libras con este fin, a cargo del Industrial Strategy Challenge Fund (ISCF). Por ejemplo, se contempla un desafío para mejorar la de tección temprana de enfermedades crónicas, con una inversión sustancial en técnicas de diagnóstico de IA, para lo que el gobierno británico compromete 210 millones de libras.

El ISCF invertirá asimismo 93 millones de libras para un programa de robótica e IA en ambientes extremos, para el uso de estas tecnologías en rubros como la energía nuclear y la generación de energía en alta mar, la minería profunda y la minería en el espacio, para generar mejores prácticas laborales y aumentar la productividad.
También se dispondrá de programas para aplicar la IA a la reducción de enfermedades que afectan a la industria agrícola, y para la provisión de más servicios de forma digital en el sector público. Así, se compromete la inversión de hasta 20 millones de libras por parte del GovTech Fund para la aplicación de IA en el sector servicios, desarrollando nuevas aplicaciones y tecnologías en sectores como la justicia y los seguros.

DESARROLLO CON ÉTICA

Pero en relación con su segundo eje rector, esta política de IA también consideró la creación de un Centro para la Ética de Datos e Innovación (CDEI), que asesora al gobierno británico para el uso ético de la información a través desde la coordinación entre políticos, industria y la sociedad civil. Ya se encuentra en funciones, publicando durante 2020 distintos reportes, incluyendo uno sobre el uso de datos para personalizar los mensajes, contenidos y servicios a los que se enfrentan las personas, y la primera edición de su AI Barometer, que resume las principales oportunidades, riesgos y desafíos asociados al uso de datos y la IA en cinco sectores: justicia criminal, servicios financieros, salud y cuidado social, redes sociales y digitales y energía y servicios básicos.

Tendencia Digital

DEEPFAKES

“El río de la verdad va por cauces de mentiras”

Con la llegada de las redes sociales y su masificación en escalas astronómicas, se ha puesto la información en prácticamente cada hogar y en cada persona a través de sus dispositivos móviles y el acceso a la información que consumimos de esas fuentes hacen para la cibercriminalidad que esta técnica constituya una poderosa herramienta útil a sus fines de engaño y fraude a personas, las empresas o a los países.
El DeepFake es una técnica de inteligencia artificial en la que se emplean modernos recursos técnicos, para falsear vídeos, haciendo que parezcan reales. El término proviene del inglés, utilizando una combinación de las palabras deep learning (aprendizaje profundo) y fake (falso). Así, se le cambia el rostro a una persona, resultando en una imagen en tiempo real con el rostro superpuesto de otra persona y audio o narrativas diferentes.

El DeepFake, va más allá de ser una información malintencionada, pues incorpora vídeos y audios, con montajes que aparentan ser reales, con la capacidad de engañar fácilmente al receptor de esos mensajes
En la industria del cine, ha sido posible alterar el metraje de video durante décadas, pero hacerlo tomaba tiempo, artistas altamente calificados y mucho dinero. La tecnología DeepFake está cambiando el juego. A medida que se desarrolla y prolifera, cual quier persona podría tener la capacidad de hacer un video falso convincente. La primera exposición a DeepFake para la mayoría del público en general ocurrió en 2017. Esto fue cuando un usuario anónimo de Reddit publicó videos que mostraban a celebridades como Scarlett Johansson en situaciones sexuales comprometedoras.

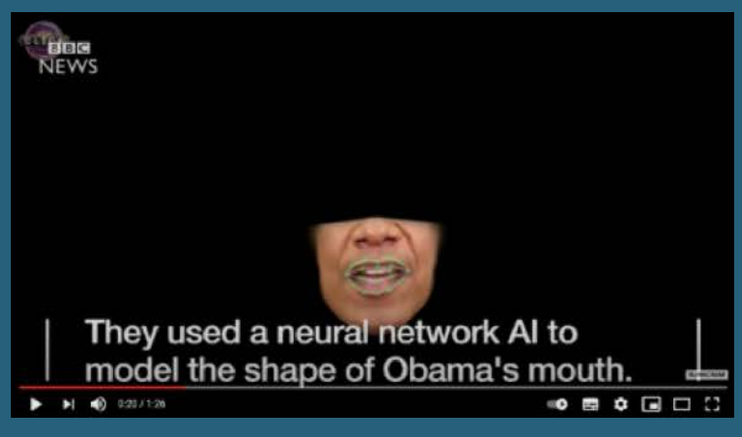
Pero, no era una situación de la vida real, era la combinación del rostro de la celebridad y el cuerpo de una actris porno fusionados usando tecnología DeepFake para hacer parecer que algo sucedió en la vida real a pesar de que era falso. Las celebridades y las figuras públicas fueron originalmente las más susceptibles a la farsa, ya que los algoritmos requerían un amplio metraje de video para poder crear un DeepFake, y eso estaba disponible para celebridades y políticos.

Cuando los investigadores de la Universidad de Washington publicaron un DeepFake del presidente Barack Obama y luego lo hicieron circular en Internet, quedó claro cómo se podía abusar de esa tecnología. Los investigadores pudieron hacer que el video del presidente Obama dijera lo que quisieran que dijera. Imagínese lo que podría suceder si cualquier inescrupuloso presentaran un DeepFake de un líder msndial como una comunicación real. Podría ser una amenaza para la seguridad mundial o los procesos

¿Cómo se **detectan**?

Al alimentar a las computadoras con ejemplos de videos reales, así como videos DeepFake, los investigadores están entrenando computadoras para detectar videos DeepFake, es decir, la misma tecnología que se utiliza para su creación, la inteligencia artificial, puede utilizarse para detectar los videos y audios falsos, pero es un trabajo en desarrollo.

Microsoft ha desarrollado una herramienta para detectar DeepFake: imágenes manipuladas por computadora en las que la imagen de una persona se ha utilizado para reemplazar la de otra.
El software analiza fotos y videos para dar una puntuación de confianza sobre si es probable que el material haya sido creado artificialmente.



Recomendaciones

Ten siempre en cuenta los siguientes aspectos:

1. **Contexto:** observe el contexto del artículo, video o audio. ¿Cuándo fue escrito o publicado? ¿De dónde viene? ¿Han cambiado los eventos desde entonces? ¿Existe alguna información nueva que pueda cambiar su perspectiva?

2. **Credibilidad:** compruebe la credibilidad de la fuente. ¿Tiene el sitio reputación de integridad periodística? ¿El autor cita fuentes creíbles? ¿O es satírico? ¿Está en una lista de sitios de noticias falsos? ¿Es realmente un anuncio que se hace pasar por una noticia real?

3. **Construcción:** Analice la construcción del artículo, video o audio. ¿Cuál es el sesgo? ¿Hay palabras cargadas? ¿Alguna técnica de propaganda? ¿Alguna omisión que deba tener en cuenta? ¿Puedes distinguir entre los hechos y las opiniones? ¿O es simplemente especulación?

4. **Corroboración:** corrobore la información con otras fuentes de noticias creíbles. Asegúrese de que no sea la única fuente que hable de la noticia. Si es así, es muy probable que no sea cierto.

Aplique **Criterio:**

Comparar y contrastar fuentes de información. Una sola fuente puede equivocarse fácilmente, por lo que es aconsejable ver si varios medios de comunicación de renombre informan lo mismo.

No comparta sin verificar. Una regla útil es verificar tres veces antes de difundir lo que cree que son noticias.

Si publica información errónea, corríjala rápidamente.

Sea escéptico.

Utilice el pensamiento crítico.

Universidad de Concepción

EL DESARROLLO DE LA **IA** EN EL BÍO-BÍO

Múltiples desarrollos de esta tecnología llevan a cabo investigadores de la Universidad de Concepción, con potencial aplicación en áreas como la salud, la astronomía y la educación, explica Julio Godoy, académico de dicha casa de estudios.

Julio Godoy
Ingeniero Civil Informático
Universidad de Concepción

"En nuestra Facultad de Ingeniería estamos realizando varias acciones relacionadas con la inteligencia artificial (IA)", explica Julio Godoy, ingeniero civil informático, Ph.D. en Ciencias de la Computación de la Universidad de Minnesota y académico de la Universidad de Concepción. Él mismo está trabajando en esta disciplina, comenta, con la aplicación y desarrollo de métodos de IA "para hacer robots más inteligentes, y que puedan interactuar de manera natural con las personas".

Las principales áreas de investigación en IA, detalla el ingeniero, son el procesamiento de señales, la salud, la energía y los procesos industriales. "Hemos formado un grupo de interés en Inteligencia Artificial (ia.udec.cl), en el cual los académicos que realizan investigación fundamental o aplicada con IA estamos desarrollando colaboraciones que nos permitan ampliar el rango de aplicaciones de técnicas de IA en problemas que impactan tanto a la industria como a la sociedad en general", explica Godoy.

Los beneficios ya se están viendo, cuenta el experto, con la aplicación de proyectos desarrollados por docentes de la universidad y los ingenieros de su Unidad de Data Science, en empresas como Arauco y CMPC, las cuales han logrado hacer más eficientes sus procesos. "En algunos casos, esto implica que hay drones haciendo tareas que antes hacían personas, dando lugar a que se puedan aprovechar mejor los recursos humanos para tareas más complejas pero más seguras", indica.

FALTA DE RECURSOS HUMANOS PARA LA **IA** EN CHILE

De acuerdo con Julio Godoy, uno de los desafíos más importantes que enfrenta la IA en nuestro país es una escasez de personas capacitadas en ella, lo que, señala, ya ha sido notado por consultoras como Accenture. De hecho, el académico indica que incluso para alumnos recién titulados de la Universidad de Concepción con conocimientos de IA no es difícil encontrar trabajo en esa área.

Entre los desarrollos, el académico desglosa numerosos casos en distintos departamentos de la Universidad de Concepción. Por ejemplo, en el departamento de Ciencias de la Computación, destaca el trabajo del Dr. Guillermo Cabrera, quien desarrolla nuevos algoritmos de aprendizaje automático y visión por computadora para su aplicación en la próxima generación de telescopios, como también la investigación realizada por el Dr. Roberto Asín, quien usa la IA para solucionar problemas de Optimización Combinatoria, "computacionalmente desafiantes", explica.

IA PARA LA SALUD Y LA EDUCACIÓN

"Creo que en dos áreas donde se verán más pronto los beneficios de algunos de nuestros proyectos es en la salud y la educación", añade Godoy. Así, en salud, la Dra. Pamela Guevara usa métodos de IA para el análisis de imágenes médicas, "en particular de resonancia magnética de difusión, para el estudio de la conectividad cerebral", detalla. Y en la misma línea, comenta que el Dr. Sebastián Godoy aplica la IA para apoyar la detección no invasiva de enfermedades cutáneas, "mediante el procesamiento multimodal de videos de cámaras visibles e infrarrojas".

Está asimismo el trabajo del Dr. Esteban Pino, quien desarrolla algoritmos de apoyo a las decisiones médicas, los que a partir de señales fisiológicas mono o multimodales, "emulan las decisiones que realizaría un experto". Y también el Dr. Jorge Pezoa, quien utiliza técnicas de machine learning para optimizar recursos y la resiliencia en redes de datos.
Godoy estima que gracias a trabajos como estos, tendremos "la capacidad de predecir, en base a un análisis de exámenes médicos, qué tan propensos estamos a enfermar por diversas patologías, lo que nos permitirá implementar tratamientos preventivos que mejoren nuestra esperanza y calidad de vida", especialmente gracias a la evolución de dispositivos sensores que formen parte del denominado internet de las cosas, que con IA adviertan en tiempo real de síntomas y condiciones de salud peligrosas, por ejemplo.

REEMPLAZAR LAS TAREAS RIESGOSAS Y REPETITIVAS

El profesor Godoy estima que el mayor potencial de la IA, en términos generales, es ayudar a las personas a concentrar su trabajo en labores de mayor creatividad y valor, dejando las tareas más tediosas y de riesgo en manos de las máquinas. “Uno de los objetivos centrales de los métodos de IA que se desarrollan hoy es que puedan ayudar a las personas a realizar sus mejor sus trabajos, en lugar de sencillamente reemplazarlos”, asegura, aunque inmediatamente agrega que de todas formas existe el riesgo de que la adopción de estas técnicas conlleve la pérdida de sus empleos para muchas personas.

Y por el lado de la educación, Godoy nombra a los investigadores María Angélica Pinninghoff, Ricardo Contreras y el Dr. Pedro Salcedo, quienes han trabajado con los llamados “algoritmos evolutivos” para “atacar el problema del bullying en las salas de clases”. El ingeniero civil informático explica que la IA entrega además ventajas en la forma de “tutores inteligentes”, los cuales apoyarán a los profesores con la ventaja de poder adaptar la presentación de contenidos y su evaluación a las necesidades y capacidades de cada estudiante.

Legal

LA INTELIGENCIA ARTIFICIAL **SE TOMA LA AGENDA PÚBLICA**

La Transformación Digital avanza a pasos agigantados, al igual que la tecnología que la soporta. Es así y tal como pudimos abordar en números pasados de esta revista, que cada vez son más los organismos e instituciones de distintos sectores los que abrazando las nuevas capacidades de cómputo y almacenamiento migran áreas completas de su operación del mundo físico al digital.

La Digitalización, tiene una cuestión que es transversal y esto es la gran cantidad de datos que a través de ella se generan o se digitalizan. Es esta gran cantidad de datos, la que sumada a nuevos algoritmos y capacidades de procesamiento han hecho que el concepto de Inteligencia Artificial, que comenzó a ser desarrollado en la década de 1950 se vuelva una realidad. Es así como hoy en día ella ya se encuentra presente en nuestros teléfonos, autos e incluso en el mismo programa a través del cual estoy escribiendo. Como se puede apreciar, la Inteligencia Artificial o IA es una tecnología de propósito general debido a que está inmersa en distintos sectores de la economía. Esta transversalidad y su capacidad de generar cambios disruptivos en distintos rubros le han hecho ganar un rol protagónico durante los últimos años. Rol del cual el Estado no puede estar ajeno. Es por ello que, durante el año 2019, un grupo de ministerios liderados por el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación presentaron un diagnóstico sobre la necesidad de elaborar una Política Nacional de IA que permitiera capturar los beneficios de la tecnología, posicionando a Chile no solo como un importador, sino que, participando de su investigación y desarrollo, a la vez de abordar riesgos e impactos sociales asociados a su desarrollo. Bajo dichas premisas, es que durante ese mismo año se comenzó a desarrollar la mencionada política, destacando una gran participación ciudadana en dicho proceso.

Hoy y luego de casi dos años de desarrollo, la Política Nacional de Inteligencia Artificial se encuentra ad-portas de ser oficialmente publicada. ¿Pero en qué consiste?. En líneas generales, la política tiene por objeto empoderar a chilenos y chilenas en el uso y desarrollo de sistemas de Inteligencia Artificial, propiciando el debate sobre sus dilemas éticos y sus consecuencias regulatorias, sociales y económicas. Para ello, la política se estructura en base a tres ejes interrelacionados:

1 FACTORES HABILITANTES: Está referido a los elementos necesarios para el desarrollo de la inteligencia artificial, tales como datos, capital humano y la infraestructura tecnológica.

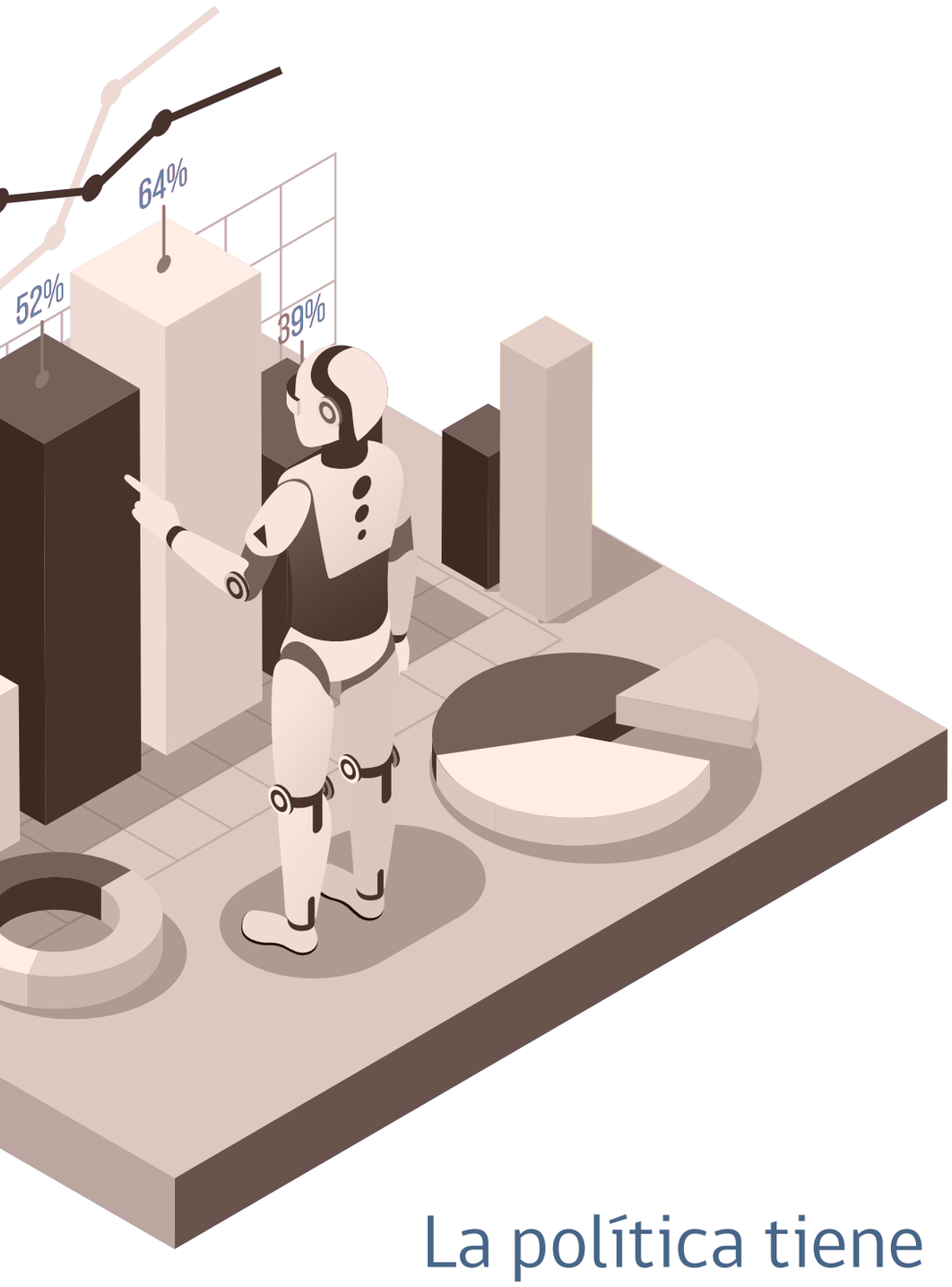
2 DESARROLLO Y ADOPCIÓN: Está referido al espacio en donde se desarrolla y despliega la IA, tales como la academia, el Estado y el sector privado.

3 ÉTICA, ASPECTOS REGULATORIOS E IMPACTOS SOCIALES Y ECONÓMICOS: Es en este último eje en el que se encuentran incluidos algunos de los aspectos normativos más relevantes de acuerdo con la discusión ciudadana y a la experiencia nacional e internacional, como la IA en la protección al consumidor, en la privacidad, en el sistema de propiedad intelectual y en la ciberseguridad.

Junto a los 3 ejes, la política también fija principios orientadores transversales para el desarrollo de esta tecnología:

Principios orientadores de la **IA**

- **IA** con centro en las personas
- **IA** segura
- **IA** inclusiva y con perspectiva de género
- **IA** al servicio del Ambiente
- **IA** con foco en niñas, niños y adolescentes
- **IA** multidisciplinaria
- **IA** con perspectiva territorial y descentralización
- **IA** desde la deliberación y la participación



La política tiene muchos objetivos, **pero ninguno de ellos es realizable sin:**

UNA ADECUADA INFRAESTRUCTURA TECNOLÓGICA

Es por ello, que este es el primer factor habilitante, ya que, sin altas velocidades de conectividad, tecnología de nube, data-centers y otros, es imposible impulsar el uso y desarrollo de la IA. En dicho contexto el principal habilitador dentro del Gobierno de Chile llamado a implementar esa infraestructura es la Subsecretaría de Telecomunicaciones. En esa lógica, la Política tiene como objetivo impulsar el desarrollo del sistema de conectividad nacional, avanzando en el despliegue de redes 5g y solucionando los problemas de provisión de conectividad de la última milla.

CAPITAL HUMANO CON LAS COMPETENCIAS NECESARIAS

La política no desconoce la gran escasez de habilidades en IA y otras tecnologías en Chile, por lo que dentro de las líneas de trabajo, se propone la formación de una mesa de trabajo para incorporar la IA en la formación técnico profesional, iniciativas público privadas como la de Talento Digital que busca desarrollar ese tipo de capacidades con énfasis en la empleabilidad, cursos de IA liderados por CORFO para que emprendedores, pequeñas y medianas empresas integren esta tecnología y el desarrollo de habilidades complejas en la etapa preescolar. Junto con impulsar el desarrollo de nuevo capital humano, también se debe recapacitar a gran parte de la fuerza laboral actual, para que pueda adaptarse y enfrentar las constantes y complejas transformaciones que el uso de la IA traerá al mercado laboral. Para acabar con esas carencias, propone desarrollar instrumentos que permitan incentivar la especialización en esta área del conocimiento, fortaleciendo fuertemente los programas de Becas del Ministerio de educación, fondos CORFO, el fortalecimiento de magister y doctorados, así como la reformulación del curriculum escolar para incorporar el pensamiento computacional.

DATOS GENERADOS PRINCIPALMENTE COMO CONSECUENCIA DE LA DIGITALIZACIÓN.

Los datos de calidad y en grandes cantidades son fundamentales para el desarrollo de herramientas de IA, es por ello que la política también busca incentivar la existencia de repositorios públicos de datos que sean accesibles a los desarrolladores. En ese sentido, la Agencia Nacional de Investigación y desarrollo está trabajando en una política de acceso abierto a la información científica, de manera de asegurar el acceso a los datos científicos generados con recursos del Estado.

La política, junto con incentivar el desarrollo de la infraestructura y el capital humano necesarios, así como también el incentivar las herramientas de IA dentro del Estado y la generación de diversos indicadores de avance en la adopción de estas tecnologías, también se hace cargo de sus aspectos éticos.
En ese sentido, debemos tener claro que la IA ofrece grandes beneficios, pero también tiene riesgos asociados, tales como los relativos a los derechos fundamentales, como la dignidad, la privacidad, la libertad de expresión y la no discriminación arbitraria. Siendo uno de los más reconocidos la generación de sesgos discriminatorios no deseados en su funcionamiento.
Para hacer frente a estos desafíos, la política propone desarrollar una agenda de análisis sobre los aspectos éticos y normativos de la IA, con el fin de determinar si las normas vigentes son suficientes para dar cumplimiento a los principios que deben regir la IA, así como también el desarrollar una institucionalidad que sea capaz de velar tanto por el desarrollo y uso de la IA como por el respeto de los derechos fundamentales que puedan ser afectados.
Para cumplir con dichas premisas, el contar con una IA cibersegura es fundamental. La transversalidad sectorial de la IA hace que los efectos negativos de la

explotación de una vulnerabilidad, el mal uso o una falla en su operación debido a un incidente de ciberseguridad sean de extrema gravedad. Es por eso que la política establece que la ciberseguridad debe ser un componente central de la IA. Por otra parte, la IA puede ser utilizada en aplicaciones ofensivas y defensivas de ciberseguridad, en ese sentido la política busca impulsar un trabajo conjunto con CSIRT GOB para fomentar el uso de herramientas defensivas de IA y generar instancias de cooperación para conocer los beneficios y riesgos de esta tecnología en materia de ciberseguridad. Trabajo que ya se ha iniciado mediante la planificación de un ciber ejercicio y conferencia de alcance internacional que abordará dichas temáticas.
Finalmente, y para su ejecución, la política establece una gobernanza compuesta por un Consejo de Ministros y un Consejo Nacional de Inteligencia Artificial además de una Secretaría Ejecutiva quien estará a cargo de hacerle seguimiento al plan de acción de la política.
El plan, enumera las acciones propuestas, confirmadas, en implementación y completadas que abarcan los años 2020 y 2022, debiendo actualizarse este último año para el periodo 2023 al 2025.

Entre algunas de las acciones en ejecución encontramos:

1. Desarrollo de un puente digital Asia-Sudamérica
2. Desarrollo del Sistema de Conectividad Nacional
3. Despliegue de infraestructura 5G
4. Generación de Demanda desde los Laboratorios Naturales
5. Plan Nacional de Lenguas Digitales
6. Plan piloto para instituciones de educación técnico profesional en IA
7. Curso de IA para emprendedores y PYMES
8. Focalización de becas Chile de PhD en IA
9. Data Observatory para facilitar acceso a datos públicos

La política será la hoja de ruta para el desarrollo y la adopción responsable de la IA en el país, constituyendo en sí misma, un avance importante, en la medida en que sitúa a la IA en un lugar relevante de la agenda pública, destacando la preocupación gubernamental por un tema que ya no corresponde a un futuro lejano sino a un presente inmediato.

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile

CONTÁCTANOS

+(562) 2486 3850

registra un incidente

Síguenos

Twitter de CSIRT
https://twitter.com/csirtgob/

LinkedIn
https://www.linkedin.com/company/csirt-gob/

Youtube
https://www.youtube.com/channel/UCua0E5J29V1Rn-VtLHPP4Nw/

Instagram
https://www.instagram.com/csirtgobcl

Equipo de Respuesta ante Incidentes
de Seguridad Informática

Teatinos 92 piso 6
Santiago, Chile
www.csirt.gob.cl