



PONTIFICIA
UNIVERSIDAD
CATÓLICA
DE CHILE

Reflexionando sobre la humanidad y la IA

Manuel Espinoza Quintero

IIC2613 — Inteligencia Artificial
Profesor Jorge Baier Aranda
Marzo de 2024

1. Trabajo a futuro:

(a) Personalmente considero que destaco sobre el promedio en las siguientes habilidades o talentos:

1) **Buena reacción frente a situaciones adversas:**

Me percibo como una persona que tiene la habilidad sobre el promedio para el manejo del estrés o enojo frente a situaciones contrarias, esto debido a que he notado la capacidad que tengo de manejar situaciones de frustración y perseverar, por ejemplo, en trabajos o interrogaciones para la universidad, proyectos personales, entre otros.

2) **Investigación e innovación:**

Otra habilidad que considero tener sobre el promedio es el uso de la creatividad, y llevado a un ámbito más cercano a la ingeniería, la innovación. He percibido que abordo problemas desde una perspectiva más innovadora, y me encuentro varias veces cuestionando algo establecido. Además, siempre me ha gustado saber como funcionan las cosas, incluso las que al promedio de la gente no les interesan.

(b) Las siguientes actividades me hacen entrar en estado de Flow:

1) **Programar:**

Cuando programo, especialmente al enfrentarme a desafíos que requieren soluciones creativas y técnicas, me concentro completamente en el proceso. Además, me da mucha satisfacción hacer funcionar un código. A esto muchas veces lo acompaño con escuchar música, que me aísla de lo exterior, y ayuda a la inmersión del estado de Flow.

2) **Jugar fútbol:**

Jugar fútbol, y cualquier deporte, induce muy fácilmente al estado de Flow mediante la concentración intensa y la respuesta física. La conexión profunda con el juego, me genera una inmersión de este estado.

(c) Como futuro Ingeniero Civil de Software, imagino múltiples problemáticas donde mis habilidades pueden tener un impacto significativo. Las de mayor relevancia que se me ocurren son las siguientes:

1) **Ciberseguridad y protección de la privacidad:**

La seguridad y la protección de la información siguen siendo las dos bases de la privacidad en un mundo cada vez más digital. Mi capacidad de reacción ante las situaciones adversas y mi inclinación por la investigación y la innovación me permitirían aportar nuevas soluciones de seguridad.

2) **Acceso equitativo a la educación tecnológica:**

El problema de la equidad en la educación tecnológica sigue siendo el de las regiones y los grupos socioeconómicos. Construir plataformas educativas modernas basadas en la innovación me permitirá participar en su accesibilidad masiva y personalizada.

3) **Sostenibilidad y tecnologías ecológicas:**

La crisis climática ha requerido manejar muchas innovaciones, y el campo de la tecnología no es una excepción. Esto significa que podría aplicar mis conocimientos de software para idear nuevas herramientas que sean útiles para optimizar el uso de los recursos, mejorar la eficiencia energética y promover la sostenibilidad.

Elección y desarrollo detallado: **Ciberseguridad y protección de la privacidad:**

La ciberseguridad y la protección de la privacidad es un tema cada vez más crítico en la sociedad actual. Los datos personales se han convertido en una “moneda” valiosa, tanto para las empresas que buscan personalizar servicios y/o poner publicidades como también para las personas maliciosas que buscan explotar esa información con objetivos fraudulentos. [1]

Los crecientes incidentes de ciberataques, violaciones de datos y prácticas de vigilancia invasiva han aumentado la preocupación pública y la demanda de soluciones eficaces. Se trata, por tanto, de una cuestión de importancia para cuidar las infraestructuras críticas de nuestros países, que dependen, en gran medida, de sistemas guiados por la seguridad informática, con el fin de no generar una falta de confianza en las instituciones financieras, las redes energéticas y otros sistemas.

Además, la protección de la privacidad también forma parte del mantenimiento de los derechos individuales y la libertad. Un ejemplo actual es la tecnología de escaneo de iris de WorldCoin, realizado en Chile. [4]

Este es un proyecto que busca garantizar el acceso universal a la economía global utilizando una criptomoneda y, al hacerlo, plantea varias preguntas importantes con respecto a cuestiones de consentimiento informado y, lo más importante, la seguridad de los datos biométricos. La empresa WorldCoin, por su parte, asegura que después de todo el proceso de determinación de la unicidad y humanidad de los usuarios, las imágenes de Iris se eliminan”. Al mismo tiempo, es motivo de preocupación la total falta de claridad en relación con los propósitos y la ubicación exacta del uso de los datos recopilados en los registros biométricos. [5]

El presidente de la Comisión de Defensa del Senado y los expertos en ciberseguridad han advertido que los datos deben seguir un proceso escrupuloso, ya que los datos podrían proteger a las personas de estar expuestas a fraudes, estafas o riesgos discriminatorios derivados del uso de datos para la inferencia de inteligencia artificial, por ejemplo, información médica u otra información sensible. La preparación y la respuesta ante cualquier eventual violación de la seguridad serían esenciales; más aún, los datos podrían ser de naturaleza sensible, como los del iris. Por último, sería muy necesario seguir innovando para seguir produciendo tecnologías y protocolos de seguridad más nuevos que ofrezcan una mejor protección de la privacidad del usuario sin comprometer la funcionalidad o el acceso a servicios digitales innovadores como WorldCoin.

Trabajar en la resolución de estos problemas, especialmente en el desarrollo de software de seguridad, me permitirá entrar con frecuencia en el estado de Flow. Las tareas dentro de esta problemática son principalmente la programación o el desarrollo de soluciones de seguridad inventivas en situaciones que requieren adaptación rápida e imaginación. Esto mejoraría no sólo mi productividad sino también la calidad del trabajo realizado y haría que toda la experiencia fuera bastante satisfactoria y personalmente enriquecedora.

- (d) La pregunta que se encuentra en Anexos fue realizada a ChatGPT, modelo GPT-3.5, siendo esta la respuesta:

¡Por supuesto! Aquí tienes ejemplos de cómo podrías aplicar tus habilidades para abordar cada una de las problemáticas mencionadas:

1. Problemas de ciberseguridad y protección de la privacidad:

- Buena reacción frente a situaciones adversas: Ante una brecha de seguridad en una empresa, podrías utilizar tu capacidad de reacción para coordinar un equipo de respuesta, minimizar el impacto y tomar medidas correctivas rápidamente.
- Investigación e innovación: Podrías investigar y desarrollar nuevas técnicas de cifrado o sistemas de detección de intrusiones más avanzados para proteger la información y la privacidad de los usuarios en línea.

2. Falta de acceso equitativo a la educación tecnológica:

- Buena reacción frente a situaciones adversas: Ante la falta de recursos en ciertas comunidades para acceder a la educación tecnológica, podrías colaborar con organizaciones sin fines de lucro para proporcionar programas de capacitación en línea o crear iniciativas locales para enseñar habilidades tecnológicas básicas.

- Investigación e innovación: Podrías investigar métodos innovadores de enseñanza en línea que sean accesibles y adaptables a diferentes entornos socioeconómicos, como el uso de tecnologías de realidad virtual o plataformas de aprendizaje adaptativo.

3. Falta de sostenibilidad y tecnologías ecológicas:

- Buena reacción frente a situaciones adversas: Frente a la creciente preocupación por el impacto ambiental de la tecnología, podrías colaborar con empresas para implementar prácticas más sostenibles en el desarrollo de software, como la optimización de recursos en la infraestructura de servidores o el diseño de algoritmos energéticamente eficientes.
- Investigación e innovación: Podrías investigar y desarrollar tecnologías ecológicas, como sistemas de energía renovable para centros de datos o algoritmos de optimización de rutas para reducir las emisiones de carbono en la logística de entrega de productos.

Con tu formación como Ingeniero Civil de Software y tus habilidades de reacción frente a adversidades, investigación e innovación, tienes el potencial para abordar estas problemáticas de manera efectiva y contribuir positivamente al mundo en el que vivimos.

- (e) La respuesta de ChatGPT me parece muy bien estructurada y aborda de manera directa cómo las habilidades de reacción ante situaciones adversas e investigación e innovación pueden aplicarse específicamente a cada una de las problemáticas presentadas. Es especialmente útil cómo vincula cada habilidad con acciones concretas que se pueden tomar en cada una.

Estoy de acuerdo en gran parte con la respuesta que dio ChatGPT, especialmente en la importancia de la reacción rápida y efectiva ante problemas y la constante búsqueda de innovaciones como motores de cambio. Sin embargo, creo que hay espacio para profundizar o ajustar algunos aspectos para alinearlos aún más conmigo.

Para la ciberseguridad y protección de la privacidad, más allá de reaccionar ante brechas de seguridad y desarrollar nuevas tecnologías de protección, podría ser útil enfatizar también la educación del usuario y la concienciación como parte de la estrategia. Muchas brechas de seguridad ocurren debido a errores humanos o falta de conocimiento sobre prácticas seguras. Por tanto, parte de la innovación podría dirigirse a crear programas de formación para usuarios de distintos niveles técnicos, o incentivar leyes de protección de datos. En el ejemplo dado de WorldCoin, se ve que las personas chilenas buscan una recompensa rápida y tienen ignorancia de que se puede hacer con sus datos.

En cuanto a la falta de acceso equitativo a la educación tecnológica, me gustaría añadir la importancia de personalizar el aprendizaje para adaptarse a las necesidades individuales de los estudiantes. Esto implica no solo investigar métodos innovadores de enseñanza, sino también desarrollar herramientas que permitan personalizar el contenido educativo. Así se podría maximizar el impacto de los recursos disponibles, especialmente en comunidades con limitado acceso a la tecnología.

Por último, respecto a la falta de sostenibilidad y tecnologías ecológicas, me parece lo suficientemente completa la respuesta, considerando mis habilidades personales frente a esta problemática.

2. Rol de la Inteligencia Artificial en tu futuro:

- (a) El papel de la Inteligencia Artificial en los problemas de ciberseguridad y privacidad es de doble filo, ya que sirve como herramienta para defenderse y como una fuente de amenazas. Por un lado, la IA se convierte en una parte esencial de la capacidad de defensa de la ciberseguridad para detectarlos, prevenirlos y responder a ellos de manera mucho más efectiva que los métodos tradicionales del pasado. Por ejemplo, en este caso, el análisis en tiempo real de volúmenes masivos de datos, donde una IA podría identificar patrones de comportamiento que son anormales y proporciona una predicción de amenazas a la seguridad incluso antes de que causen daño, como identificar accesos no autorizados. [3] [2]

Por otro lado, la propia capacidad de la IA para procesar y analizar grandes conjuntos de datos plantea importantes preocupaciones sobre la privacidad. La recopilación, el almacenamiento y el análisis de datos personales sin una gestión adecuada es peligroso para el usuario y puede exponerlo a riesgos tales como identificación inadecuada o elaboración de perfiles sin consentimiento. Ejemplos de ello incluyen el proyecto WorldCoin, donde se aplica el escaneo del iris para construir una identidad digital especial. Sin embargo, dejando de lado la seguridad y la privacidad, surgen dudas sobre la transparencia en el uso y la protección de los datos biométricos recopilados.

Siguiendo la misma línea, la IA también se utiliza para hacer actos fraudulentos, por ejemplo, para crear software de phishing o material audiovisual falso para engañar. Esto agregará un nivel adicional de complejidad a la ciberseguridad, ya que los defensores deben ser innovadores todo el tiempo para dejar atrás a los atacantes.

En conclusión, la inteligencia artificial tiene un gran potencial para ser una herramienta eficaz para impulsar la ciberseguridad y la privacidad, pero también proporciona nuevas fuentes de complejidad y vulnerabilidad. Se debe garantizar la consideración adecuada de estos aspectos durante el desarrollo e implementación de cualquier solución de IA en esta área para equilibrar la seguridad y los derechos individuales.

- (b) Las áreas de la inteligencia artificial, mencionadas en clase, involucradas en soluciones para el problema de la ciberseguridad y la protección de la privacidad son:

1. Planificación y Búsqueda Heurística:

Esta área se puede relacionar bastante, ya que sirve para desarrollar estrategias de defensa en ciberseguridad. Esta permite a los sistemas anticipar acciones de atacantes, optimizando las respuestas defensivas. Por ejemplo, pueden usarse para automatizar la asignación de recursos de seguridad en una red y predecir ataques futuros basándose en patrones identificados.

2. Representación Lógica del Conocimiento y Razonamiento:

Esta área también se puede relacionar para modelar y entender las tácticas y técnicas, así como para automatizar el razonamiento sobre las políticas de seguridad y privacidad. Por ejemplo, un sistema podría utilizar reglas lógicas para inferir que una serie de intentos de inicio de sesión fallidos desde una ubicación geográfica extraña, seguidos de un patrón de tráfico de red sospechoso, indican un posible ataque de fuerza bruta.

3. Procesamiento de Lenguaje Natural:

El Procesamiento de Lenguaje Natural tiene un papel importante en la monitorización de comunicaciones y en la detección de phishing o software malicioso que utiliza lenguaje para engañar a los usuarios. Por lo tanto, también se relaciona.

4. Visión por Computador:

La visión por computador puede tener aplicaciones específicas, como en la autenticación biométrica. Sin embargo, su relación directa con la ciberseguridad y protección de la privacidad es más limitada en comparación con las otras áreas.

5. Aprendizaje Automático:

Es una de las áreas más fundamentales y relacionadas con la ciberseguridad y la protección de la privacidad. Este se utiliza para detectar patrones de ataques, identificar incoherencias en el tráfico de red, análisis de malware, entre otros.

En resumen, casi todas estas áreas de la IA tienen aplicaciones importantes en la ciberseguridad y la protección de la privacidad, con excepción de la visión por computador, cuyo uso es más específico.

(c) Para resolver este problema se requiere tanto del Sistema 1 como del Sistema 2, por lo siguiente:

- Sistema 1: Este sistema es importante para la detección inmediata de amenazas. Deben existir algoritmos que sean similares a aquellas conclusiones que nuestro cerebro parece hacer en forma automática, para que se identifiquen patrones de comportamiento sospechoso sin intervención humana.
- Sistema 2: La participación del sistema 2 es más evidente si consideramos el análisis profundo a amenazas de ciberseguridad, que deben interpretarse mediante un esfuerzo consciente y del razonamiento lógico. Por otro lado, en cuanto a la privacidad y resguardo de datos, se exige un pensamiento crítico, ya sea por temas éticos o legales.

Referencias

- [1] IBM. (2024). *Ciberseguridad*. Recuperado de <https://www.ibm.com/mx-es/topics/cybersecurity>. Último acceso: 2024-03-23.
- [2] IBM. (2024). *IA y Ciberseguridad*. Recuperado de <https://www.ibm.com/mx-es/ai-cybersecurity>. Último acceso: 2024-03-23.
- [3] Kaspersky. (2024). *IA y Ciberseguridad*. Recuperado de <https://www.kaspersky.es/resource-center/definitions/ai-cybersecurity>. Último acceso: 2024-03-23.
- [4] AS Chile. (2024). *Escaneo de iris en Chile por Worldcoin: Cuánto pagan, riesgos, por qué lo hacen y en qué se usa la información*. Recuperado de <https://chile.as.com/actualidad/escaneo-de-iris-en-chile-por-worldcoin-cuanto-pagan-riesgos-por-que-lo-hacen-y-en-que-se-usa-la-informacion-n/>.
- [5] MegaNoticias. (2024). *Worldcoin: Qué es, peligros de vender iris, criptomonedas*. Recuperado de <https://www.meganoticias.cl/nacional/442188-worldcoin-que-es-peligros-de-vender-iris-criptomonedas-12-03-2024.html>.

Anexo:

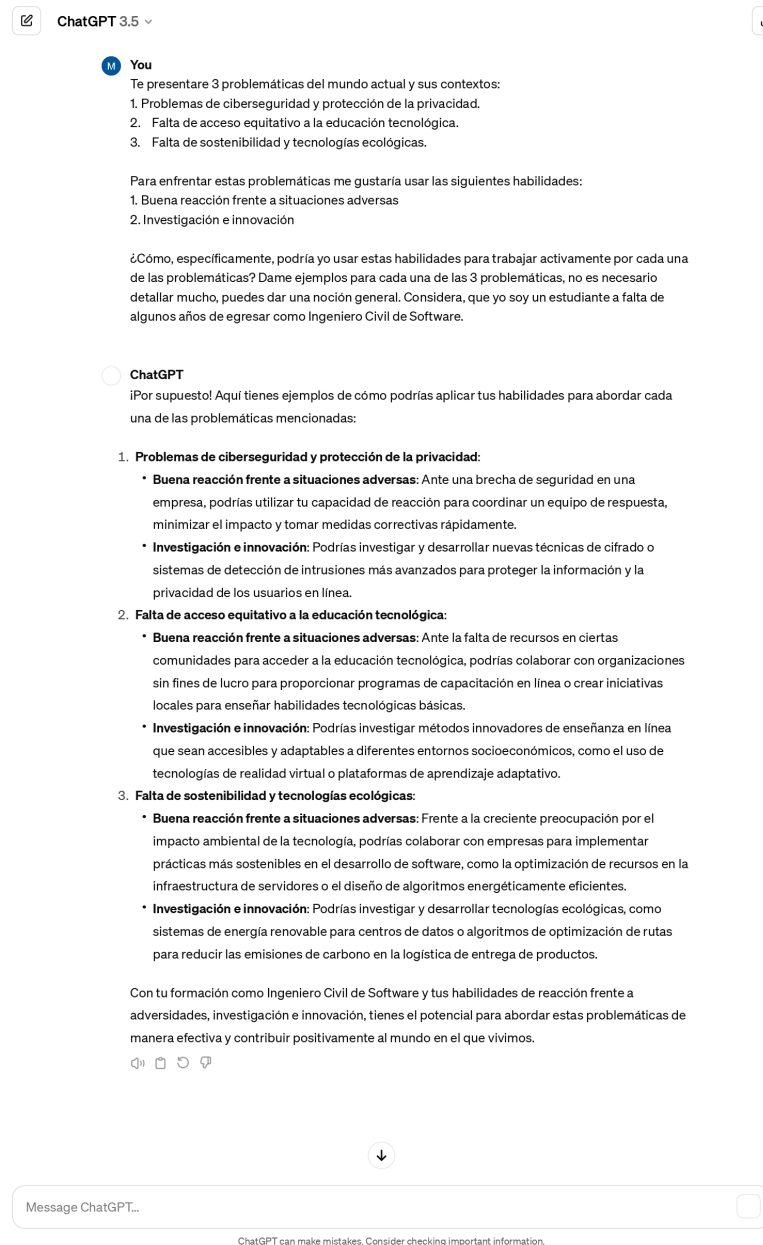


Figura 1: Conversación con ChatGPT