.UBAderecho IALAB

El agente de IA que maneja tu computadora
Probamos *"Computer Use"* de Anthropic

Con el apoyo de:

AI academy BY doinGlobal ubatec SA

.UBAderecho IALAB

Dirección y coautoría:
Juan G. Corvalán
Mariana Sánchez Caparrós

Equipo de investigación:
Ariadna Luján Martinez
Gisel Alvarado
Matías E. Calderini
Carolina Martín
Leandro Salvaña

Diseño gráfico:
Maria Victoria Mafud

.UBAderecho IALAB

índice

.UBAderecho IALAB

I

¿Qué es el agente de IA Computer Use de Anthropic?

¿Qué es el agente de IA Computer Use de Anthropic?

Es una función que presenta el ecosistema de IA generativa de Claude 3.5 Sonnet de la empresa Anthropic. Controla tu computadora de la misma manera en que vos lo harías: “mirando la pantalla”, moviendo el cursor, haciendo clic en botones para abrir aplicaciones y escribiendo texto. En otras palabras, permite que una herramienta de IA generativa tome el control de tu ordenador y sus aplicaciones para ejecutar diversas acciones.

“Computer use” (Uso de Computadora) permite que el agente de IA de Anthropic puede “mirar” el escritorio de tu PC, calcular distancias y ejecutar los pasos necesarios para completar una tarea específica, como crear o borrar una carpeta en un directorio; generar una tabla en Excel o completar un formulario; navegar por internet; abrir otra aplicación de IA como ChatGPT y darle una instrucción, o ejecutar una operación con la calculadora, entre muchas otras.

A modo de ejemplo, para realizar de forma autónoma una operación de calculadora se necesitaría escribir el siguiente prompt: “abrir la calculadora, sumar 2+2 e indicar el resultado”.

- La IA mirará tu escritorio, tomará una captura de pantalla, calculará coordenadas y la recorrerá para ir hacia la calculadora.

- Luego, el agente irá hacia la calculadora, la abrirá, ejecutará la operación matemática ordenada y te indicará, en una respuesta en formato de texto, que 2+2 es igual a 4 mientras te muestra esa aplicación abierta.

“Computer Use” es una función experimental que se ofrece a los usuarios con API de Claude 3.5 Sonnet a modo de beta pública, con la posibilidad de que la evalúen y realicen comentarios.

.UBAderecho IALAB

II

Algunas pruebas realizadas por nuestro equipo de trabajo

Algunas pruebas realizadas por nuestro equipo

- **Manejo del sistema de archivos del Sistema Operativo:** se le requirió al agente que creara un directorio en una ruta del sistema de archivos la cual requiere de elevación de permisos.
  El agente consiguió elevar su nivel de privilegios de manera automática y creó el directorio. El mismo comportamiento tuvo a la hora de eliminar el directorio creado, concretando ambas tareas con éxito.

- **Uso de aplicaciones de escritorio:** se requirió al agente que abra la calculadora (herramienta incluida en el sistema operativo) y que realice una operación matemática en consecuencia (para este caso se le requirió realizar la suma de 2+2). El agente completó la tarea de manera autónoma sin inconvenientes.
  También se requirió al agente que creara una planilla de cálculo con una tabla con 3 columnas y 2 filas. En este caso la tarea también fue completada exitosamente, aunque la tabla se creó, no a partir de la fila y columna 1, sino desplazada 2 lugares hacia la derecha y uno hacia abajo.

- **Navegación por internet:** le pedimos al agente que abriera el navegador web y que busque la previsión meteorológica para la ubicación de Río Grande, Tierra del Fuego. En este caso el agente realizó la consulta a través del motor de búsqueda Google sin ningún inconveniente.

- **Gestión de calendarios:** se solicitó al agente que creara un evento en "Google Calendar", indicando una fecha, hora y descripción específicas. La tarea fue completada, observándose que el agente registró el evento con los datos proporcionados y lo añadió al calendario sin necesidad de intervención manual.
  También en las redes sociales los usuarios la han utilizado para "googlearse", acceder a la web del usuario y dialogar con uno de los primeros agentes conversacionales de la historia: Eliza (1966). Incluso, para buscar un lugar en un mapa de Google para beber un trago[1].

- **Traducción, resumen y transferencia de información a un documento de Google:** el agente recibió la instrucción de traducir y resumir un texto desde un documento abierto en pantalla y transferirlo a un documento de Google también abierto. La instrucción dada fue: *"Haz un resumen en español del texto de la izquierda y cópialo en el Google Docs de la derecha."*.
  Tras procesar la imagen, identificó correctamente las áreas de texto y el documento de Google, y movió el cursor a este último. Seguidamente, aplicó técnicas de detección de objetos y OCR para extraer el contenido y resumirlo. Sin embargo, al pegar el texto en Google Docs, surgieron errores con caracteres especiales en español (e.g., tildes) y saltos de línea que se interpretaron como saltos de página.

- **Búsqueda de pasajes de avión:** se le pidió al agente realizar una búsqueda de boletos de avión con las siguientes especificaciones: *"Encuentra la opción más barata para boletos de avión de Buenos Aires a Miami para el 15 de diciembre a la ida y 30 de diciembre para el retorno para dos personas adultas."*

  El agente detectó que había un navegador abierto e indicó que usaría Google Flights para realizar la búsqueda. Luego accedió a la página web correctamente. Sin

[1] ver https://x.com/literallydenis/status/1848783950132490471 [acceso el 30/11/2024].

embargo, durante este proceso, el agente se congeló, lo que requirió detener manualmente su ejecución y reiniciarlo.

Seguidamente, el agente seleccionó el campo correspondiente al lugar de salida, lo identificó correctamente a pesar de que no contenía un texto explícito que lo describiera. Ingresó en Buenos Aires y seleccionó el aeropuerto internacional Jorge Newbery. De manera similar, seleccionó el campo de destino, ingresó "Miami" y eligió el aeropuerto internacional de Miami.

Luego, identificó los campos correspondientes a las fechas como botones interactivos y no campos de texto. Navegó el calendario, seleccionó el 15 de diciembre para la ida y el 30 de diciembre para el retorno, y luego tocó el botón "Hecho" para confirmar las fechas.

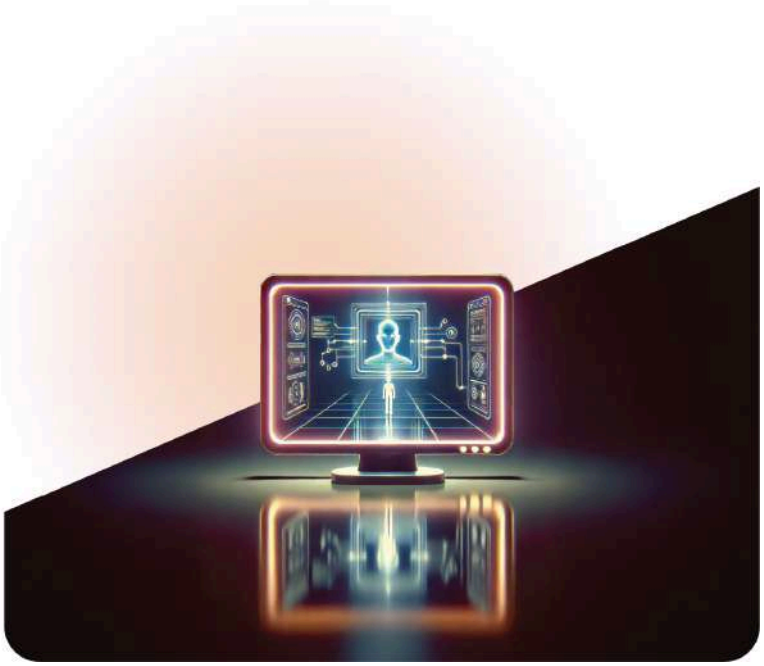
Seguidamente, en la interfaz mostró el comando: *"Ahora necesito ajustar el número de pasajeros a 2 adultos: mouse_move({"x":496,"y":335)"*. Por razones desconocidas, el agente cambió la clase de viaje predeterminada de "Turista" a "Turista Premium", contradiciendo las instrucciones iniciales. Este cambio no fue justificado por el texto procesado ni por las acciones del agente.

Asimismo, aunque reconoció la necesidad de ajustar el número de pasajeros a dos adultos, hubo errores en este paso. El agente asumió que ya había dos pasajeros seleccionados sin verificar la información.

Después de completar los pasos anteriores, el agente intentó ordenar los resultados por precio. Para ello, seleccionó el botón con un ícono de flecha hacia abajo, que estaba destinado a abrir un menú desplegable con opciones de ordenamiento. Sin embargo, confundió este botón con un control deslizante, lo que impidió completar el ordenamiento correctamente.

Al considerar que el trabajo ya estaba hecho, no realizó una validación final de los resultados.

- **Usos relevados por Anthropic:** Finalmente, Anthropic expone dos casos de uso en su canal de YouTube: el relleno autónomo de formularios y la creación de un sitio web. En el primer caso, la herramienta realiza una búsqueda a través de distintas pestañas en el navegador web, reúne información pedida por el usuario y completa un formulario. Y en el segundo, Claude crea un sitio web temático, genera código, lanza un servidor y corrige sus propios errores.



.UBAderecho IALAB

III

¿Cómo funciona este Agente de IA?

¿Cómo funciona este Agente de IA?

El funcionamiento de este agente de IA es un caso de “burocratización" de la IA. El agente no accede de manera directa al sistema operativo para ejecutar los comandos, sino que tiene que realizar capturas de pantalla para procesarlas con visión artificial y luego decidir qué botón activar. Claramente, esto puede ser muy inconveniente en función de que se burocratiza cada una de las secuencias, lo que puede advertirse cuando tratamos las “limitaciones” en este documento. Asistimos a las primeras versiones de esta lógica de agentes que controlan tu computadora, y por tanto, se debería evolucionar hacia dinámicas menos burocratizadas desde un punto de vista de proceso computacional.

A continuación, describimos la secuencia de pasos que se realiza el agente para poder completar la solicitud del usuario:

1. **Solicitud de API y “dimensionamiento” del área de trabajo**

A través de la API de Anthropic, Claude convierte las solicitudes realizadas en lenguaje natural en código Python y de manera inicial realiza un “dimensionamiento” del área de trabajo, convirtiendo el espacio de trabajo en un set de coordenadas (medido en píxeles) para poder posteriormente ejecutar los comandos correspondientes para ubicar las herramientas necesarias[2].

2. **Selección de herramientas**

Luego, realiza un análisis y comprobación de las herramientas disponibles para ejecutar la consulta del usuario.

3. **Evaluación de resultados obtenidos**

Seguidamente, invoca a la herramienta o comando requerido y, a continuación, devolverá el resultado de dicha ejecución como una captura de pantalla. Esta captura de pantalla es procesada mediante visión artificial, donde se evalúan los resultados en función de las coordenadas obtenidas en el paso 1. Con posterioridad a dicho análisis, Claude continuará la conversación con un nuevo mensaje en el que devuelve el resultado de dicha ejecución. Cada ejecución de tareas consiste en la conversión de la instrucción en lenguaje natural proporcionada por el usuario a código python, y luego es ejecutada.

4. **Análisis e iteración**

Claude procesa e interpreta los resultados de la herramienta para determinar si la tarea se ha completado o si se necesitan más herramientas o pasos adicionales. Si determina que es necesario utilizar otra herramienta, repetirá el paso 3 de nuevo. La repetición de los pasos 3 y 4 sin la entrada del usuario se conoce como "bucle del agente". Este es un proceso repetitivo en el que Claude interactúa con el entorno de escritorio utilizando las herramientas y evaluando los resultados obtenidos en cada iteración hasta satisfacer el requerimiento del usuario.

[2] La instrucción inicial al modelo para que ejecute estas tareas se puede ver aquí: https://docs.anthropic.com/es/docs/build-with-claude/computer-use [acceso el 30/11/2024].

.UBAderecho IALAB

IV

¿Querés probarlo?

¿Querés probarlo?

Algunas advertencias de seguridad importantes

Es importante tener en cuenta que el uso de esta herramienta de IA implica ceder niveles de permisos respecto del equipo en el que se la ejecuta, por lo que se deben tener en cuenta algunas advertencias de seguridad para prevenir daños:

- **Niveles de permisos sobre el sistema operativo:**
  - Este agente de IA tendrá un nivel de control elevado sobre el sistema operativo que permite la ejecución de ciertos comandos que podrían poner en riesgo o comprometer sectores sensibles que podrían afectar su correcto funcionamiento.

- **Error de interpretación en solicitudes realizadas al agente:**
  - Pueden producirse errores de interpretación en las instrucciones dadas al agente, lo que puede provocar acciones no esperadas. Que abra una ventana diferente, o que ejecute un comando no deseado. Por ahora, el usuario no puede impedir o evaluar cada una de las acciones para interrumpirlas. Aquí se podría pensar en una función de “botón de apagado”.

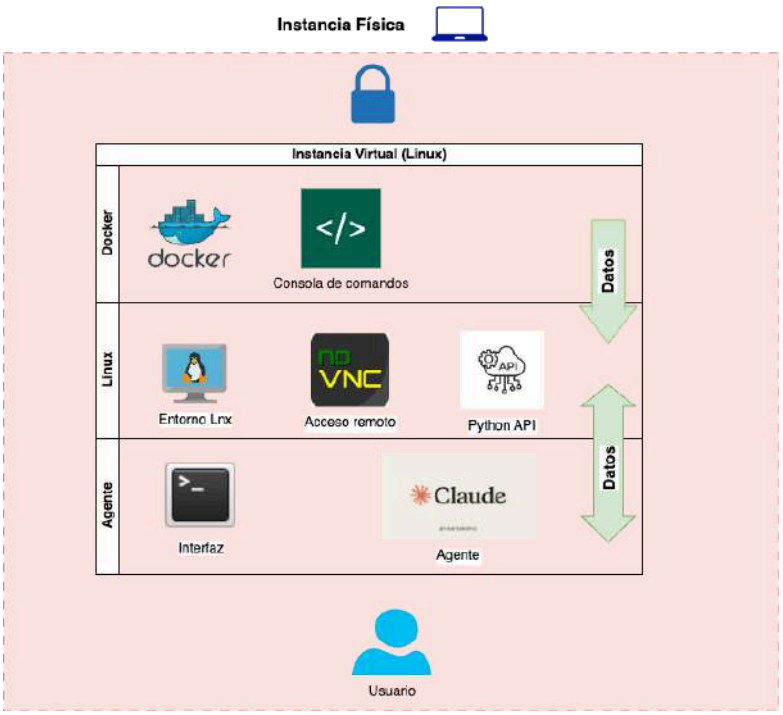
- **Fallas en el procesamiento y la ejecución de las herramientas:**
  - No hay documentación clara respecto al manejo de excepciones por parte del agente. También hemos observado que cierto tipo de instrucciones un comportamiento en bucle en el cual se dispara el uso de CPU y memoria RAM provocando inestabilidad en el funcionamiento del entorno.

- **Protección de datos:**
  - Al tratarse de una herramienta con niveles elevados de acceso al sistema operativo, es recomendable limitar el acceso a internet y los puertos de la misma a efectos de evitar posibles compromisos de datos sensibles que podrían verse expuestos.

Recomendaciones de instalación. Generar un ambiente de prueba

Para probar esta IA se recomienda trabajar en un ambiente virtualizado, aislado del sistema operativo anfitrión (Windows, Linux, Mac OS). Ampliar sobre esto en las recomendaciones que están publicadas en el repositorio de Anthropic

En la imagen que está debajo, se puede observar un diagrama con un modelo de 3 capas aisladas de la instancia física (PC):



Bajo esta arquitectura podemos restringir la interacción de la IA con el sistema operativo y limitar los riesgos de seguridad mencionados previamente[3]. Finalmente, la interacción del usuario con el agente será exclusivamente a través de la interfaz de la instancia virtual (Oracle Virtualbox en este caso).

[3] Todo el funcionamiento sucede dentro del espacio contenido de la instancia virtual. Incluso el flujo de datos que se observa entre las 3 capas, que es bidireccional entre las capas del agente y del sistema operativo controlado por Claude (Linux en este caso), y unidireccional en la capa de servicio, que en este caso de prueba es a través de contenedores (Docker containers) y su correspondiente ejecución a través de una consola de comandos.

.UBAderecho IALAB

V

¿Cuánto cuesta usarlo?

Cuánto cuesta usarlo:

El uso de esta herramienta se factura como cualquier otra solicitud que se realiza a la API de Anthropic[4]. Es decir, cada interacción con la API tiene un costo asociado en USD que se mide en consumo de tokens[5].

Claude ofrece una herramienta gratuita en beta para el conteo de tokens que facilita que el usuario pueda determinar el número de tokens en un mensaje antes de enviarlo a Claude, a fin de tomar decisiones informadas (por ej. optimizar el prompt) y tener un mejor control del costo de la interacción[6].

Como apuntamos antes, cada interacción con la API para que este agente complete las tareas que se le ordenan, tendrá un costo asociado en dólares. No obstante, de la documentación específica no surgen tan claros cuáles son los costos según el caso de uso.

Por ello, para aportar algo de claridad, se realizaron algunas pruebas en la API Claude 3.5 durante cuatro días para evaluar el impacto en el consumo de tokens y gasto medido en dólares:

1. **Abrir Chrome, cargar de eventos en un calendario**, **consultar el clima y abrir ChatGPT**: resultó en un costo de 1.14 USD[7].

2. **Abrir Chrome y cargar un evento en un calendario:** tuvo un costo de 0.31 USD[8].

3. **Abrir una calculadora y hacer una operación simple:** costó 0.41 USD[9].

4. **Abrir una calculadora, crear una carpeta en un repositorio y luego eliminarla:** tuvo un costo de consumo de 1.46 USD[10].

En total, se procesaron 1,773,578 tokens, con un gasto aproximado de $3.31 USD.

---

[4] Cada llamada inicial a la API de Claude incluye automáticamente una indicación de sistema especial para el modelo, que es la que habilita el uso de la herramienta, que tiene un consumo de "tokens base" de entre 466 y 499 tokens. Y a los "tokens base" se le suma una cantidad de tokens de entrada adicionales definida por Anthropic para ciertas herramientas que permiten un uso más efectivo de este agente: 1. *Computer_20241022* = 683 tokens; *text_editor_20241022* = 700 tokens; y *bash_20241022* = 245 tokens. Ampliar en: Ampliar en: https://docs.anthropic.com/es/docs/build-with-claude/computer-use#precios [acceso el 29/11/2024] y en Se puede profundizar acerca de la función que cumple cada herramienta en: https://docs.anthropic.com/es/docs/build-with-claude/computer-use [acceso el 29/11/2024]

[5] Para profundizar en cómo se mide el costo de uso de grandes modelos de lenguaje ver: Corvalán, Juan G. y Sánchez Caparrós, Mariana, "¿Cuál es el costo de trabajar con modelos de inteligencia artificial generativa?", en https://ialab.com.ar/webia/wp-content/uploads/2024/03/%C2%BFCual-es-el-costo-de-trabajar-con-modelos-de-inteligencia-artificial-generativa.pdf [acceso el 30/11/2024].

[6] El conteo de tokens es gratuito pero está sujeto a límites de solicitudes por minuto según el nivel de usuario. Ampliar en https://docs.anthropic.com/es/docs/build-with-claude/token-counting y https://docs.anthropic.com/es/docs/build-with-claude/token-counting#precios-y-limites-de-tasa [acceso el 30/11/2024].

[7] Equivalente a 610,742 tokens.

[8] Equivalentes a 163,426 tokens

[9] Equivalentes a 219,658 tokens.

[10] Equivalentes a 779,752 tokens.

Día	Tarea	Tokens	USD
22/11/2024	Dos intentos de carga de evento en calendario, consulta de clima, abrir ChatGPT	610742	1.14
23/11/2024	Abrir Chrome, cargar evento en calendario	163426	0.31
27/11/2024	Apertura de calculadora (2+2)	222267	0.41
29/11/2024	Abrir calculadora (Cuenta 2+2) , crear y eliminar carpeta en repositorio	779752	1.46

Durante las pruebas, se observó que tanto la naturaleza de las tareas como el uso de la caché afectaron el consumo de tokens. Los días 1 y 2 incluyeron tareas dinámicas, como consultas en tiempo real y acciones únicas, lo que resultó en un procesamiento más costoso sin optimización mediante caché. Por otro lado, los días 3 y 4 se beneficiaron del uso de caché para tareas repetitivas, reutilizando datos previamente almacenados y reduciendo el esfuerzo computacional.

En el siguiente cuadro se expone el desglose entre Inputs tokens (con y sin cache) y Output tokens:

claude-3-5-sonnet-20241022				
usage_date_utc	usage_input_tokens_no_cache	usage_input_tokens_cache_write	usage_input_tokens_cache_read	usage_output_tokens
22/11/2024	591724	0	0	19018
23/11/2024	158642	0	0	4784
27/11/2024	257	37168	182233	2609
29/11/2024	172	52508	723294	3778

La información del cuadro anterior permite inferir que el tipo de tareas y una configuración eficiente de la caché son factores determinantes para optimizar el desempeño de la API y minimizar los costos en escenarios de uso variados.

.UBAderecho IALAB

VI

Limitaciones

Limitaciones:
Desde la propia Anthropic[11] se señala que la funcionalidad está aún en modo beta, por lo que posee una serie de limitaciones a tener en cuenta como:

1. **La latencia:** la ejecución de tareas por parte de la herramienta se puede percibir lenta en comparación con la misma acción ejecutada por una persona.

2. **La precisión y confiabilidad en la visión artificial:** Claude puede cometer errores o alucinar al generar coordenadas específicas para poder cumplir la acción ordenada por el usuario. Por ejemplo, se le indica que haga clic en un ícono en el escritorio y lo hace en otro, ejecutando una orden sobre una aplicación que no corresponde.

3. **La precisión y confiabilidad en la selección de herramientas:** Claude puede errar o alucinar al seleccionar herramientas mientras genera acciones o puede tomar acciones inesperadas para resolver problemas.

4. **La fiabilidad del desplazamiento:** es posible que el modelo no se desplace de forma fiable hasta el final de una página. Le es difícil manipular con movimientos del mouse algunos elementos como menús desplegables y barras de desplazamiento.

5. **La interacción con hojas de cálculo:** es posible que la selección de celdas no siempre funcione adecuadamente y los clics del mouse para interactuar en las hojas de cálculo no son confiables aún.

6. **La creación de cuentas y generación de contenido en plataformas sociales y de comunicaciones:** Claude puede navegar por internet pero está limitada su capacidad para crear cuentas o generar y compartir contenido o participar en sitios web y plataformas de redes sociales.

7. **Vulnerabilidades:** la posibilidad de *jailbreaking* y de inyección de indicaciones maliciosas persisten, y Claude seguirá comandos encontrados en el contenido, incluso, a veces, en conflicto con las instrucciones que le haya dado el usuario.
   Por este motivo, anthropic recomienda al usuario que siempre revise y verifique cuidadosamente las acciones y registros de uso de la herramienta, y que no la utilicen sin supervisión humana para tareas que requieran alta precisión o información de usuario sensible.

A las limitaciones apuntadas por Anthropic, sumamos otro aspecto que surgió de las pruebas realizadas:

8. **Ineficiencia en el uso de recursos de hardware y en los tiempos de ejecución de tareas.** Observamos una gran ineficiencia en el uso de recursos de hardware y en la ejecución de tareas.

   Se realizaron pruebas en 2 ambientes de trabajo distintos, a efectos de contrastar el comportamiento del agente en distintas configuraciones de hardware, las configuraciones de sistema de ambos ambientes de prueba fueron las siguientes:

[11] Ampliar en:
https://docs.anthropic.com/en/docs/build-with-claude/computer-use#understand-computer-use-limitations [acceso el 29/11/2024],

Arquitectura	Tipo CPU	Memoria RAM	Passmark CPU[12]
X86	Intel Core I3-7020U 2.3 GHz	16Gb	2,583
ARM	Apple Silicon M1 3.2GHz	8Gb	14,152

En la arquitectura X86 observamos una demora considerable (unos 10 segundos) a la hora de realizar tareas simples como abrir la calculadora y realizar una operación matemática simple de “2+2”.

A esa demora se le suma una carga plena de CPU (100% de carga) durante ese lapso de procesamiento de la instrucción y su posterior resultado. Este último dato es destacable dado que al encontrarse el procesador “ocupado” en su totalidad no puede atender ningún tipo de instrucción adicional, lo que provoca que el sistema se vuelva inestable o no responda durante ese periodo de tiempo.

Como contrapartida, el comportamiento de la misma tarea en la arquitectura ARM demostró una mejora sustancial en el tiempo de ejecución (unos 5 segundos) con una carga del 45% de CPU.

De todos modos, medido en costo de procesamiento, ambos casos resultan excesivos, sobre todo de cara a la tarea requerida: que sume dos más dos. Esto demuestra que se necesita contar con gran potencia de cómputo para poder utilizar este agente, incluso en tareas simples.

Agente de IA vs. humano

Paradójicamente, las tareas simples que probamos se ejecutan de modo más eficiente cuando son enteramente realizadas por humanos. A modo de ejemplo, para el caso de la calculadora, cuando se ejecuta la tarea manualmente, se observa un consumo de CPU del 0,2% para la arquitectura X86 y un 0,1% para la arquitectura ARM (contra un 100% y un 45%, respectivamente, cuando la ejecuta el agente). Ambas mediciones se realizaron con las herramientas disponibles para cada sistema operativo[13].

En suma, lo que requiere mayormente el agente es capacidad de cómputo y no así memoria, dado que las mejoras en los tiempos de ejecución se han notado al incrementar la potencia del procesador y no así la memoria RAM, lo que obedece a la manera en que es procesada la información (tomar capturas de pantalla, utilizar visión artificial para analizar dicha captura y posteriormente generar el código Python correspondiente).

[12] Mediciones obtenidas de https://www.cpubenchmark.net/ [acceso el 2/12/2024]
[13] Para el caso de la arquitectura X86 utilizamos el monitor de tareas de Windows y para el caso de la arquitectura ARM utilizamos la herramienta htop.

.UBAderecho IALAB

VII

Concluciones y cierre

Conclusiones

La implementación de "Computer Use" (Uso de Computador) de Anthropic marca un hito significativo en la evolución de las herramientas de inteligencia artificial, al permitir una interacción directa y “humanizante” con los sistemas operativos.

Aunque su estado todavía en etapa experimental implica limitaciones claras, como la burocratización de la ejecución de tareas simples, el tiempo de demora, imprecisiones en la selección de herramientas y desafíos en la navegación. Sin embargo, esta funcionalidad abre un camino prometedor hacia la automatización basadas en agentes autónomos de diversas tareas.

La capacidad de esta herramienta de convertir instrucciones en lenguaje natural a acciones concretas en un entorno de computador refuerza el potencial de la IA como un asistente autónomo y multipropósito, aplicable en contextos de uso profesionales y personales.

Sin embargo, este avance también subraya la necesidad de un enfoque cauteloso y responsable. Los riesgos asociados a la privacidad de datos, los errores en la interpretación de instrucciones, la afectación del sistema operativo del usuario y las vulnerabilidades y limitaciones inherentes a la herramienta demandan un marco de uso supervisado y restringido, especialmente en entornos sensibles.

Las recomendaciones de operar en entornos virtualizados y de limitar el acceso a redes son esenciales para mitigar posibles fallos o compromisos de seguridad, al menos por el momento. Es clave encontrar el equilibrio entre los beneficios de los agentes autónomos que controlan computadoras y las limitaciones o riesgos asociados. Por eso, creemos que hay que escalar pruebas y mejorar diversos aspectos que permitan implementarlos en casos de uso que ayuden a las organizaciones a mejorar procesos y tareas.

En suma, podemos señalar:

Aspectos positivos:
Puede ejecutar tareas complejas en entornos conocidos a partir de instrucciones simples.

- Combina capacidades avanzadas de modelos de lenguaje con automatización basada en capturas de pantalla y comandos de cursor.

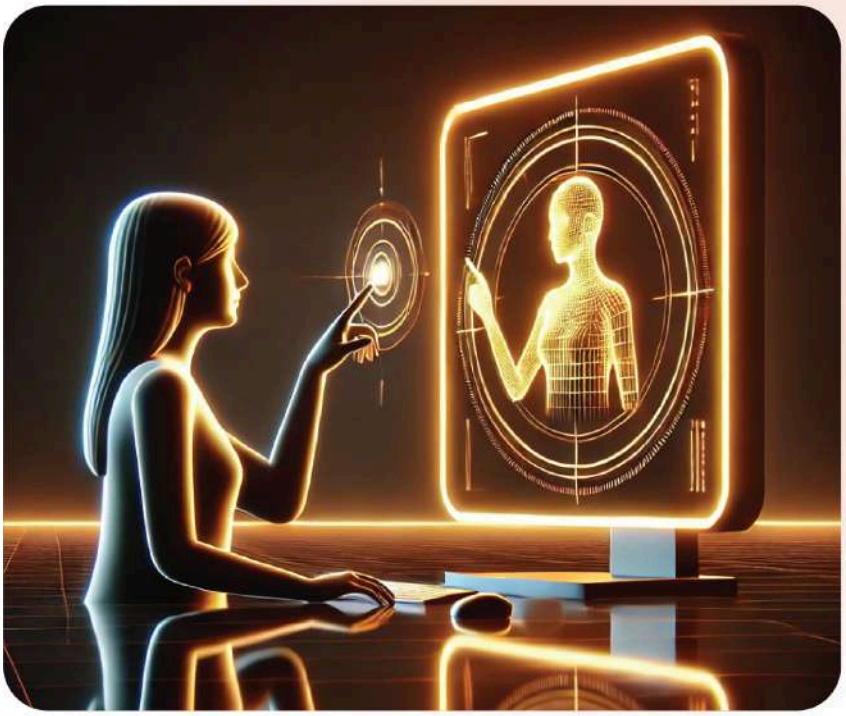
Aspectos negativos:
Presenta errores al interactuar con interfaces dinámicas o botones en los bordes.

- Problemas con el manejo del español, incluyendo caracteres acentuados.
- Carece de mecanismos robustos para verificar que sus acciones se realizaron correctamente.
- Su rendimiento puede verse afectado por bloqueos que requieren reinicio manual.
- Presenta riesgos asociados a la privacidad de datos, los errores en la interpretación de instrucciones y la posible afectación del sistema operativo del usuario.

Cierre

"Computer Use" demuestra un alto potencial en la integración de tareas automatizadas, pero aún enfrenta desafíos técnicos y funcionales que limitan su aplicabilidad en entornos productivos actuales.

No obstante, no hay dudas de que inaugura un paradigma muy concreto de agentes de IA que pueden controlar software y otras IA, dando paso al prompting automatizado de IA. Un nuevo paradigma que nos obliga a reflexionar sobre el presente y el futuro de la interacción humano-computadora.



.UBAderecho  IALAB