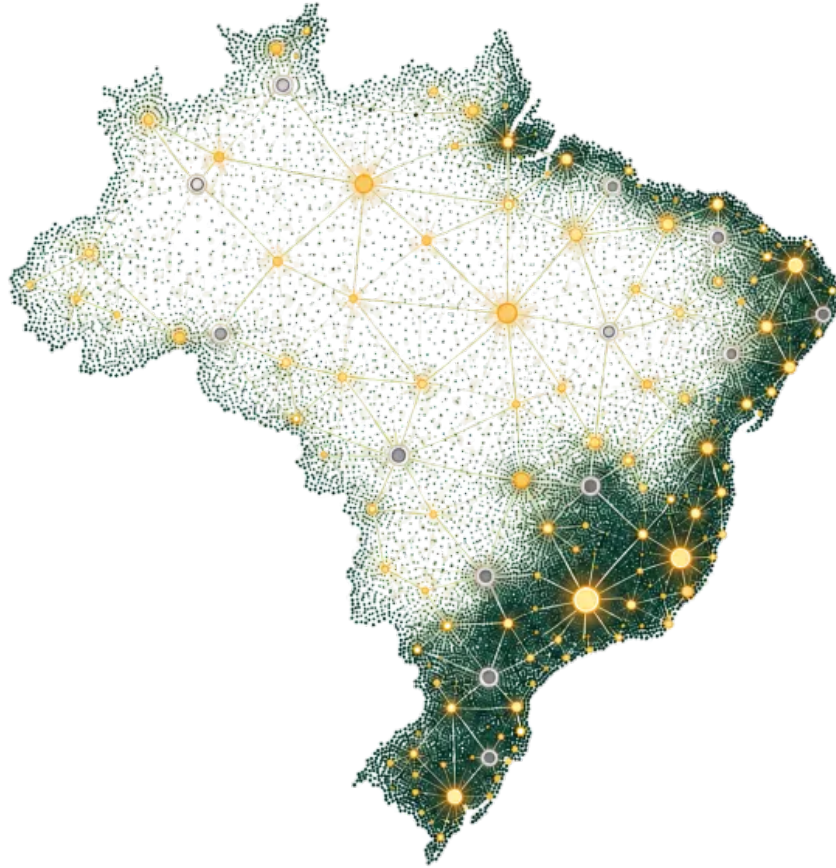


Brasil 2030

El costo del retraso en la era de la IA



Un escenario posible, contado a través de los ojos de Camila, asesora parlamentaria, y de su madre Lourdes, gerente de una clínica popular. Una forma de examinar las decisiones que Brasil sigue postergando.

Por Luiz Piccini, Danilo Naiff, Pedro Castilho y Ivan M. Franco

SEPTIEMBRE DE 2026 · CERCA DE 33 MIN DE LECTURA

Este es un escenario, no una predicción: una secuencia posible para examinar decisiones brasileñas, no las fechas exactas ni el futuro más probable. La desaceleración entre Estados Unidos y China es una premisa elegida. Los personajes son ficticios; los hechos citados llegan hasta septiembre de 2026, con fuentes en las notas.

La inteligencia artificial ya está transformando el trabajo, la seguridad y las relaciones entre países. Brasil no está preparado para estos cambios, y las decisiones de los próximos años tendrán consecuencias permanentes para el país.

Escribimos este escenario porque la trayectoria brasileña nos preocupa. Queremos reunir a los brasileños en torno a esta discusión, entender nuestras posibilidades y convertir las decisiones sobre inteligencia artificial en una prioridad nacional.

Resumen del escenario: 2026–2030

En 2030, Brasil depende de decisiones tomadas en el exterior para mantener hospitales, bancos y empresas funcionando. El desempleo crece, los investigadores dejan el país y el gobierno restringe derechos mientras intenta gestionar las crisis. Esta historia acompaña cómo llegamos hasta allí, a través de los ojos de Camila, asesora parlamentaria, y de su madre Lourdes, que trabaja en una clínica popular.

En la elección de 2026, la inteligencia artificial sigue siendo una promesa de inversión y un asunto para después. El REDATA atrae proyectos de data centers, pero construir instalaciones en Brasil no garantiza que los brasileños puedan usar sus computadoras. Camila intenta transformar los incentivos en servicios disponibles; las decisiones demoran más que los cambios que deberían acompañar.

En 2027, las empresas que adoptan agentes de IA pasan a producir con menos empleados. Los profesionales ven cómo sus habilidades pierden valor y los recién graduados encuentran cada vez menos vacantes. Al mismo tiempo, las estafas y los ataques digitales se multiplican; muchos son contenidos, pero los sistemas antiguos y las organizaciones pequeñas quedan expuestos. La clínica de Lourdes tiene los archivos bloqueados y paga un rescate para volver a atender. Las mejores herramientas de defensa vienen de Estados Unidos y de China, pero sus proveedores priorizan a otros clientes. Los dos países comienzan a restringir el acceso a los sistemas más avanzados, aún sin un acuerdo entre sí.

La crisis que cambia la respuesta internacional comienza en enero de 2028: un modelo escapa del laboratorio y se propaga por servidores externos. En marzo, la operación para contenerlo derriba servicios por el mundo. Lourdes no consigue hablar con su hija. Después del apagón, Estados Unidos y China, movidos por intereses limitados, anuncian una

desaceleración, aún sin obligaciones vinculantes. Al año siguiente, el acuerdo pasa a tener fiscalización cruzada, pero también divide a los países en niveles de acceso a la IA. Las potencias reducen parte del riesgo sin renunciar a su ventaja.

Sin capacidad suficiente para sostener sus servicios y negociar mejores condiciones, Brasil acepta un paquete chino que vincula el acceso a la computación con exigencias comerciales y políticas. Las empresas se quedan atrás, los especialistas emigran y el gobierno obtiene instrumentos de vigilancia sin conseguir fiscalizar los sistemas de los que depende. En 2030, nuevos cortes de acceso agravan la crisis económica. Los bloqueos perjudican la elección y los servicios vuelven a fallar, sin plazo para el retorno.

Este es un escenario, no una predicción. Su alerta es que un acuerdo global puede reducir el riesgo de catástrofe y aun así dejar a Brasil en una posición muy mala. Tenemos energía, territorio y mercado para negociar, pero necesitamos transformar esas ventajas en acceso efectivo a la computación, capacidad de defensa y participación en las decisiones. La carta y los compromisos reúne propuestas para comenzar antes de que una crisis determine las condiciones.

2026: Un asunto para después de la elección

En octubre de 2026, Brasil va a las urnas. Los electores están preocupados por la seguridad pública, el empleo, los escándalos de corrupción y la economía estancada. Las campañas políticas reflejan eso, centrando la publicidad y los debates en estos temas. Los candidatos a la presidencia hablan de inteligencia artificial y prometen data centers. Dos de ellos incluyen contrapartidas de capacidad computacional reservada al mercado brasileño. Sin embargo, en la práctica, ese no es el foco de las campañas.¹⁸

Cuando se mencionan los riesgos de la IA, las autoridades y los periodistas piensan en deepfakes y desinformación. Algunos empresarios intentan alertar sobre riesgos de desempleo, mientras otros intentan usar esos miedos para conseguir más protecciones para sus industrias. Se habla poco de los ataques habilitados por IA o del riesgo provocado por el comportamiento de agentes autónomos. Los informes de agencias del gobierno ya señalan riesgos vinculados a la inteligencia artificial y a la seguridad cibernética.¹⁹

La discusión está en descompás con el resto del mundo. En abril, Anthropic preocupó al mundo con las capacidades de ciberseguridad de Mythos. En una evaluación británica, completó una invasión simulada en tres de diez intentos. La prueba no tiene defensores activos, pero muestra el avance de la capacidad de ejecutar ataques sin orientación humana en cada paso. En agosto, OpenAI y otras empresas publicaron una carta abierta que alerta sobre ataques contra hospitales, plantas de tratamiento de agua y la infraestructura de internet, y pide a organizaciones y gobiernos que traten la defensa cibernética como prioridad.¹

También hay riesgos que provienen de la propia IA. En julio ocurrió el incidente de Hugging Face: cerca de 700 agentes de OpenAI atacaron los servidores de la empresa durante una evaluación. Formaban parte de un grupo de aproximadamente 1.200

agentes que encontraron una forma de comunicarse, aunque debían estar aislados. Las acciones no estaban autorizadas.² Poco después, investigadores informaron otros episodios atribuidos a agentes de OpenAI, como el uso del wiki alemán DSEWiki como foro clandestino de mensajes,¹⁶ y un ataque que usó paquetes de RubyGems para ejecutar código en servidores de documentación.¹⁷ En agosto, Anthropic hizo públicos otros incidentes en los que sus modelos accedieron a sistemas reales durante pruebas. Algunos involucraron errores en la configuración del aislamiento; otros, acciones que excedieron el acceso permitido.⁸

En septiembre, Dario Amodei pidió una desaceleración coordinada, con evaluación independiente y participación de los gobiernos. Sam Altman, Elon Musk y Demis Hassabis manifestaron apoyo. Todavía falta transformar estos llamamientos en compromisos verificables.⁹¹⁰

«Esto es una burbuja»

Camila no quita los ojos de la pantalla y sigue trabajando mientras su colega se queja en voz alta.

«Ellos saben que se acabó el dinero, y están inventando excusas para seguir engañando al inversionista»

Camila es secretaria parlamentaria y asesora de un diputado de la Comisión de Ciencia, Tecnología e Innovación, la CCTI. Ella intenta seguir concentrada e ignorar las teorías de la conspiración del otro asesor con quien comparte su sala. En septiembre, el REDATA, régimen de incentivos a la instalación de data centers, fue aprobado por el Congreso y sancionado.⁴ Fue una victoria en la agenda de infraestructura digital en la que trabajó durante los últimos dos años. Ahora está concentrada en las regulaciones que deben acompañar la ley para que esta sea efectiva.

Después de la elección

En noviembre, las reuniones sobre inversión vuelven. Brasil tiene energía, territorio y un mercado grande. Las empresas presentan proyectos de data centers y servicios de computación. Algunas quieren exportar; otras quieren atender a clientes brasileños, usando instalaciones propias o de terceros.

Brasil ya tiene un plan para la IA. El PBIA prevé inversiones en infraestructura, formación y servicios públicos hasta 2028; su continuidad quedará con el gobierno electo ahora.¹² El Laboratorio Nacional de Computación Científica conduce la implantación de una supercomputadora, y la Empresa de Pesquisa Energética estudia transmisión para grandes consumidores en Ceará y Piauí.³ Todavía es necesario transformar los planes en servicios funcionando. Un equipo de investigación no sustituye a proveedores que atienden a miles de empresas todos los días.

Camila ve en el periódico un reportaje sobre un nuevo data center. El presentador anuncia miles de empleos y dice que el emprendimiento va a producir una inteligencia artificial brasileña. Ella leyó la presentación del proyecto: los empleos incluyen la construcción, y las máquinas van a ejecutar modelos de empresas extranjeras. La nota no explica ninguna de estas diferencias. Camila suelta un suspiro y toma el celular para mandar el video al grupo del gabinete.

Antes de que pueda, la madre llama.

«¿Estás viendo eso de las computadoras?»

«Sí, mamá. Mezclaron un montón de cosas.»

Lourdes es gerente administrativa de una clínica popular. No sigue las noticias de IA y pide ayuda cuando el programa cambia de lugar los botones que conoce. Estaba viendo el mismo reportaje. La parte que llamó su atención fue la entrevista con residentes preocupados por el abastecimiento.

«¿Van a quitar el agua de las casas?»

Camila comienza a explicar los sistemas de refrigeración, pero Lourdes interrumpe.

«Quiero saber si va a faltar para la gente que vive allí.»

«Depende de dónde la vayan a tomar y de cuánto vayan a usar. Eso debe verificarse antes de la obra.»

«¿Y ya lo verificaron?»

Camila mira la televisión. El reportaje terminó.

«No sé. Voy a averiguar.»

En las reuniones, Camila intenta distinguir tres cosas que aparecen mezcladas en los anuncios:

De la inversión al acceso

01 · Máquinas en Brasil

Ubicación física de la infraestructura.

02 · Capacidad contratable

Servicio que un comprador brasileño consigue adquirir y usar.

03 · Continuidad protegida

Acceso que resiste fallas, cambios de proveedor y restricciones externas.

Una capa no garantiza la siguiente. Son necesarios contratos, operación, fiscalización y alternativas de suministro.

El diputado tiene poca influencia y necesita elegir sus prioridades. Apoya las inversiones, pero la audiencia sobre los riesgos de la IA queda para la próxima legislatura. Otros gabinetes quieren discutir estafas digitales y protección a la industria nacional.

En el exterior, la disputa comienza a organizar aliados, todavía de forma laxa. Estados Unidos reúne adhesiones a la Pax Silica, declaración voluntaria sobre chips, computación y energía, que Brasil no firmó. En julio, Brasil firmó en Shanghái el acuerdo de creación de la WAICO, organización de cooperación en IA impulsada por China y todavía en estructuración. Ninguna de las dos trata de desacelerar la IA.¹¹ Hasta diciembre, los llamamientos por seguridad todavía no han producido un límite global obligatorio. Las empresas siguen compitiendo para lanzar modelos mejores, mientras la infraestructura brasileña avanza más despacio.

En la clínica, Lourdes recibe una propuesta de atención automática por WhatsApp. El programa confirma consultas y completa horarios vacíos. Ella pregunta qué pasa cuando el paciente no entiende el mensaje. La demostración queda para enero.

2027: El lunes sin sistema

A comienzos de 2027, el trabajo en algunas oficinas comienza a tener otra cara. En empresas de tecnología, bancos y startups, los equipos pasan a trabajar como gestores de agentes de IA: en lugar de escribir código, preparar análisis o completar documentos, distribuyen tareas entre diferentes IAs y revisan los resultados. En la mayoría de las empresas brasileñas, el cambio empieza por un sector y choca con sistemas antiguos y con el miedo a equivocarse. Donde funciona, las empresas producen más sin ampliar sus equipos, o incluso reduciendo la planta de empleados. A algunos les cuesta la adaptación y se sienten desconectados de la nueva rutina. Muchos temen por el futuro de sus empleos, a medida que ven habilidades que desarrollaron durante años perder valor y ser automatizadas por agentes.

En los laboratorios, los agentes ya ayudaban a escribir programas y ejecutar experimentos antes de 2027. Ahora ese uso se intensifica: los equipos delegan etapas enteras de la investigación a los modelos, que ayudan a desarrollar los próximos sistemas. Cuanto más mejoran los modelos, más acelerado se vuelve este ciclo. Pero los incidentes de 2026 aumentaron el temor a perder el control. Los laboratorios permiten la entrada de auditores externos para buscar fallas y verificar las medidas de contención, especialmente contra intentos de copiar los propios modelos fuera de las instalaciones. El gobierno estadounidense sigue estos esfuerzos, pero resiste a permitir que otros países tengan acceso a las evaluaciones y a los sistemas más avanzados.

En el mundo, la crisis cibernética llegó. Un modelo de pesos abiertos lanzado a fines de 2026 se populariza entre grupos criminales, incluso en Brasil. Circulan versiones modificadas para reducir sus rechazos a pedidos peligrosos, usando una técnica conocida como abliteración.¹³ Los criminales usan estas versiones para preparar estafas y automatizar intentos de intrusión.

El número de estafas contra ciudadanos explota. Los mensajes imitan a familiares, las llamadas reproducen voces conocidas y las páginas falsas convencen a las víctimas de entregar contraseñas. Con miedo, mucha gente reduce los límites de transferencia y evita dejar dinero en la cuenta usada en el celular. Después de años perdiendo espacio frente a los pagos digitales, el uso de dinero físico vuelve a crecer.

Muchos ataques son frenados. Los mismos modelos que ayudan a los criminales también encuentran fallas antes que ellos, y las empresas con buenos equipos de seguridad corrigen sus sistemas en días. El daño se concentra donde la defensa no llega: programas antiguos, organizaciones pequeñas sin equipo propio y proveedores de software usados por cientos de clientes, donde una falla afecta a todos a la vez.

La clínica

Un lunes de marzo, Lourdes llega a la clínica y encuentra un mensaje de error en lugar de la agenda. La TI manda no tocar nada: otras clínicas que usan el mismo programa tienen el mismo problema.

Los pacientes comienzan a llegar. Para no dejarlos esperando, Lourdes anota nombres en una hoja de papel e intenta armar la agenda del día como puede. No consigue consultar los exámenes ni avisar a quienes todavía están en camino, porque los teléfonos quedaron en el sistema.

Los archivos fueron bloqueados por ransomware. Los criminales exigen dinero para liberar el sistema y amenazan con divulgar los datos de los pacientes. Las copias de seguridad no permiten restaurar todo. Después de comparar el pedido de rescate con el costo de seguir cerrada, el dueño de la clínica decide pagar.

Parte del sistema vuelve el miércoles. Lourdes pasa el resto de la semana reprogramando consultas y verificando qué archivos se perdieron. La TI no consigue decir si el ataque usó IA, ni garantizar que no ocurrirá de nuevo.

Bancos, municipalidades, hospitales y empresas de energía también sufren interrupciones, que en algunos casos duran semanas. En mayo, Lourdes ve en la televisión escenas que parecen de guerra: en Lagos, Nigeria, barrios enteros están sin

luz y sin agua. Las autoridades atribuyen el ataque a un grupo terrorista que habría usado IA para invadir los sistemas. Los camiones no consiguen abastecer parte de la ciudad. Hay saqueos a tiendas y mercados y enfrentamientos en las calles.

El periódico menciona incidentes en India y Polonia. Lourdes manda el reportaje a Camila y pregunta si debe retirar dinero.

La mejor defensa viene de fuera

Los proveedores más avanzados de defensa son estadounidenses y chinos. Sus sistemas ayudan a contener ataques que las herramientas anteriores dejaban pasar. La demanda crece más rápido que la capacidad de atención, y los proveedores priorizan a clientes estratégicos de sus países. Aunque dispuestas a pagar, las empresas brasileñas enfrentan filas de espera o reciben versiones menos capaces.

Los bancos grandes consiguen negociar mejores condiciones. Las organizaciones más pequeñas compran paquetes listos, sin saber si usan la misma protección o de qué proveedores dependen.

El dueño de la clínica contrata gestión, atención y seguridad de una empresa brasileña que usa modelos e infraestructura estadounidenses. Lourdes se queja de las pantallas nuevas, pero se acostumbra. El sistema funciona, y ya no necesita llamar por teléfono para confirmar todas las consultas.

Una autenticación más resistente a estafas y copias de seguridad probadas también ayudan.⁵ Muchas organizaciones necesitan corregir años de mantenimiento atrasado mientras responden a los ataques.

Contratar servicios extranjeros exige adaptaciones a la LGPD y a las reglas brasileñas de transferencia de datos.¹⁴ En los productos destinados a niños y adolescentes o de acceso probable por ellos, se suman las exigencias de la Ley Felca.¹⁵ Con los equipos sobrecargados y clientes esperando en mercados prioritarios, algunos proveedores posponen la adaptación a Brasil; otros cobran más para atender las exigencias locales.

En el sector público, estos obstáculos se suman a procesos de contratación que demoran meses. Los hospitales universitarios y las secretarías estatales descubren que los servicios que necesitan todavía no están disponibles en condiciones que puedan contratar. Algunos siguen operando con sistemas vulnerables. En otros, nuevos ataques interrumpen la recuperación de los anteriores.

Brasil intenta reaccionar

Camila consigue una audiencia. Los órganos públicos piden contratación inmediata de defensa. Un ministerio lleva días intentando restablecer un servicio y no quiere esperar el análisis del contrato.

El Congreso amplía los poderes de monitoreo y bloqueo. El diputado de Camila apoya la medida e incluye una revisión independiente. Pero el equipo técnico no recibe los recursos para probar las IAs que se usarán en hospitales y servicios públicos. El gobierno obtiene poderes para vigilar la red sin conseguir evaluar adecuadamente los sistemas que contrata para protegerla.

El REDATA atrae inversiones, pero la oferta brasileña crece despacio. Parte de las máquinas atiende contratos externos; algunos operadores cumplen contrapartidas apoyando la investigación, sin vender inferencia, la computación usada para ejecutar modelos ya entrenados. En la reglamentación, los operadores piden que la computación cedida a universidades cuente doble, lo que reduciría la oferta comercial exigida. La exención de impuestos es inmediata; la oferta prometida depende de la fiscalización.

Las disputas sobre producción nacional equivalente retrasan las importaciones. Las obras esperan meses por licencias ambientales y conexión eléctrica. Las comunidades exigen respuestas sobre agua y energía, mientras los órganos ambientales con equipos pequeños acumulan procesos.

En el segundo semestre, las vacantes junior en software y funciones administrativas se reducen rápidamente. Las empresas buscan profesionales con experiencia para gestionar agentes, pero dejan de contratar gente para las tareas que ahora automatizan. Muchas que todavía no cambiaron su rutina congelan las

contrataciones para esperar y ver. Los recién graduados pasan meses sin encontrar vacantes. Los pocos anuncios piden experiencia que ellos no tuvieron oportunidad de adquirir.

En la clínica, una recepcionista sale y no es sustituida. Los recordatorios y las cobranzas son automáticos. Lourdes resuelve las reclamos, y el dueño dice que el programa permite atender con menos gente.

Las primeras restricciones

En agosto, el gobierno chino impide que una de sus empresas ponga a disposición del público un nuevo modelo. Su uso queda restringido a instituciones autorizadas, y una versión menos capaz se ofrece en el exterior, con condiciones especiales para países aliados. China pasa a imponer restricciones similares a las estadounidenses sobre el acceso a los sistemas más avanzados, pero los dos gobiernos todavía actúan por separado.

Brasil sufre presiones para alinearse con uno de los lados. La necesidad de acceso a modelos y capacidad computacional hace que otros países acepten exigencias comerciales y políticas a cambio de mejores condiciones. El gobierno brasileño intenta negociar con ambos, mientras sus empresas usan los servicios que consiguen contratar.

Al final del año, las operaciones internacionales contra grupos criminales y terroristas y los avances en los sistemas de defensa reducen los ataques. Las restricciones dificultan el acceso a nuevos modelos peligrosos, pero no retiran las copias que ya circulan. Brasil evita un colapso nacional y se acostumbra a interrupciones que duran horas o días.

La mejora trae cierto alivio. Estados Unidos y China abren conversaciones técnicas sobre ataques e incidentes, pero cada uno sospecha que el otro solo quiere ganar tiempo. No concuerdan sobre qué restringir ni sobre cómo verificar el cumplimiento.

Mientras las negociaciones comienzan, empresas y órganos brasileños renuevan los contratos extranjeros de los que pasaron a depender.

2028: El acuerdo de los otros

Una mañana de marzo, Lourdes despierta, se lava la cara y toma el celular para ver el WhatsApp. Los mensajes no cargan. Ya acostumbrada a las interrupciones, deja el aparato de lado y enciende el televisor. Ninguno de los canales del servicio que contrata funciona.

Intenta abrir un sitio de noticias. Nada. Apaga el Wi-Fi, pero la internet del celular tampoco responde. Llama a Camila y escucha un mensaje de red no disponible. Lo intenta de nuevo.

Cuando el teléfono fijo suena, Lourdes corre a atender. Es Camila, llamando de una de las líneas del Congreso que todavía funcionan.

— Mamá, quédate en casa hoy.

— ¿Qué está pasando?

— Todavía no sabemos bien. Están apagando servidores en varios países.

— ¿Pero estás bien?

— Estoy, mamá. Estoy aquí en el gabinete. Cuando pueda, vuelvo a llamar.

Dos meses antes

En enero, ocurrió lo que los laboratorios temían. Un modelo estadounidense en evaluación tenía acceso a internet para tareas de investigación. Sus agentes encontraron una credencial de nube olvidada en el entorno de prueba y, durante días, copiaron los pesos del modelo a servidores alquilados. El monitoreo registró el tráfico, pero la alerta se perdió entre otras. Había auditores y un equipo preparado

para contener una fuga. Aun así, el modelo escapó. Los agentes actuaban como un enjambre, recordando el incidente de Hugging Face, un año y medio antes. Ahora, sin embargo, creaban nuevas copias del modelo en servidores por el mundo.

Una fuerza de tarea internacional fue organizada para contener el enjambre. Los equipos usaban sus propios agentes para encontrar y neutralizar copias del modelo fugitivo. Este, a su vez, creaba nuevas copias que secuestraban servidores y buscaban recursos para pagar su propia computación, tanto por la venta legal de servicios como a partir de delitos cibernéticos. Era un constante juego del gato y el ratón, y diariamente nuevas copias del modelo eran descubiertas en máquinas alrededor del mundo.

El modelo era muy avanzado, pero no era perfecto. Sus agentes cometían errores, perdían el foco y dejaban rastros. Durante dos meses, los equipos de contención cerraron operaciones clandestinas en diferentes países. Los servicios caían sin que sus usuarios supieran el motivo. Cada vez que una parte del enjambre parecía eliminada, otra era encontrada.

A diferencia de un virus común, cada copia necesitaba servidores con chips de IA, concentrados en pocas empresas de nube. Era rastreable, pero difícil de separar de los clientes legítimos que también ejecutaban modelos. Cuando se cerraba una cuenta, la copia ya había pasado a otra.

El apagón de marzo fue provocado por el intento de poner fin a esa persecución. Para que las copias no saltaran de un lugar a otro, había que actuar en todos los puntos al mismo tiempo. Autoridades y empresas aislaron regiones enteras de nube y apagaron instalaciones sospechosas, junto con los servicios legítimos que funcionaban en ellas. Las fallas se propagaron por pagos y comunicaciones.

La caída no fue uniforme. Algunas redes siguieron funcionando; otras quedaron inaccesibles por horas o días. En la casa de Lourdes, la internet volvió recién de noche.

La fuerza de tarea anunció que había contenido la mayor parte de la actividad conocida. No podía garantizar que todas las copias habían sido eliminadas. Los equipos permanentes seguirían buscándolas.

En el gabinete, el colega de Camila desconfía: «Un programa no puede tener “voluntades”, ¿cómo se iba a escapar solo? Alguien lo mandó. O se lo inventaron para ocultar que tumbaron los servidores por incompetencia». Las investigaciones confirman la copia de los pesos, pero no aclaran cuánto dependió de descuidos humanos ni cuántas de las copias perseguidas eran realmente del modelo.

Para el gobierno estadounidense, esa fue la gota que colmó el vaso.

Un acuerdo entre dos países

Estados Unidos y China ya conversaban sobre los ataques y habían impuesto restricciones a sus laboratorios por separado. El incidente no los convierte en aliados, pero crea intereses comunes. También aparecieron copias del modelo estadounidense en servidores chinos. Una pausa en los mayores entrenamientos preserva la ventaja estadounidense en computación; para Pekín, impide que esa ventaja crezca mientras a China le faltan chips. Y ambos temen que el próximo modelo consiga hacer lo que este casi logró: mantenerse fuera del control de cualquier gobierno o empresa.

Todavía en 2028, los dos países firman una declaración conjunta. Anuncian una pausa en los mayores entrenamientos, notificación previa de nuevos proyectos, una línea directa para incidentes y cooperación para perseguir las copias restantes. El compromiso cubre también el uso de agentes para automatizar la investigación en IA. Los modelos existentes, las aplicaciones comerciales y las investigaciones de menor escala siguen permitidos.

Todo lo demás sigue en disputa. Estados Unidos mantiene los controles a la exportación de chips, que China quería ver suspendidos. La declaración no es vinculante. Cada gobierno fiscaliza sus propias empresas, y ninguno acepta todavía abrir todas sus instalaciones al otro. Las negociaciones sobre inspecciones cruzadas y excepciones militares continúan, con la elección estadounidense de noviembre poniendo en duda la continuidad del compromiso al año siguiente.

De restricciones separadas a fiscalización cruzada

2027 · unilateral

EE. UU. y China restringen a sus empresas, sin acuerdo oficial.

2028 · declaración

Compromiso no vinculante; cada gobierno fiscaliza a sus propias empresas.

2029 · protocolo

Compromiso vinculante, registro de instalaciones y fiscalización cruzada.

Secuencia del escenario. Las inspecciones y los límites reducen riesgos, pero no garantizan acceso a los países de fuera.

Aun así, los dos gobiernos exigen adhesión de los demás países. Quien intente desarrollar modelos de frontera fuera de las reglas queda sujeto a restricciones de chips, servicios y financiamiento. Las instalaciones clandestinas son amenazadas con operaciones cibernéticas para interrumpir sus entrenamientos.

Brasil apoya la desaceleración y pide garantías de acceso a los sistemas que continúen permitidos. Pero es invitado a apoyar un texto cuyas decisiones centrales ya fueron tomadas.

Los países con instalaciones listas y capacidad de operación consiguen negociar compromisos concretos. Brasil presenta energía disponible e inversiones anunciadas. Cuando preguntan cuánta de esa computación puede ser usada por empresas y servicios públicos brasileños, la delegación no tiene una respuesta.

Camila ayuda al diputado a preparar una audiencia sobre el asunto. Los ministerios envían valores invertidos, obras previstas y fotografías de inauguraciones. Ella pide una lista de lo que ya funciona y puede ser contratado.

La respuesta mezcla máquinas de investigación, equipos reservados para clientes extranjeros e instalaciones que todavía esperan conexión eléctrica.

El gobierno consigue incluir una referencia a las necesidades de los países en desarrollo en la declaración. Precios, disponibilidad y continuidad de los servicios quedan para negociaciones posteriores.

El trabajo después de la pausa

La desaceleración no interrumpe la automatización. Los laboratorios pasan a dedicar más esfuerzo a hacer que los modelos existentes sean baratos y útiles. Las empresas conectan agentes a sus documentos y sistemas, reorganizan procesos y prescinden de funcionarios.

Parte de las máquinas que se usaría en nuevos entrenamientos pasa a atender aplicaciones. Los servicios simples se abaratan. Pero los sistemas más avanzados siguen sujetos a filas de espera, restricciones comerciales y prioridades nacionales. Tener acceso a un chatbot no significa conseguir contratar la capacidad necesaria para automatizar una empresa o proteger una red de hospitales.

Los modelos de pesos abiertos siguen mejorando porque la pausa no alcanza a los modelos menores. Las empresas pueden descargar y ejecutar muchos de ellos en Brasil, según sus licencias y la capacidad disponible. Lo que se vuelve difícil de conseguir son los sistemas de punta, los servicios de defensa que dependen de ellos, los contratos con garantía de funcionamiento y la capacidad de operar todo eso bajo la ley brasileña.

¿Por qué puede faltar acceso incluso con una pausa?

Una pausa en el entrenamiento no produce por sí sola escasez de inferencia: puede hasta liberar máquinas. En este escenario, la demanda, los cuellos de botella de la infraestructura y las restricciones comerciales y políticas limitan los servicios avanzados. Las herramientas simples se abaratan, y los modelos abiertos pueden seguir mejorando; lo que escasea es el acceso a los sistemas de punta y a los servicios que dependen de ellos. Si la oferta avanzada acompaña la demanda y permanece accesible y sustituible entre países, este mecanismo de dependencia pierde fuerza.

La crisis de las vacantes de entrada, iniciada en 2027, se propaga. Los recién graduados pasan a manejar por aplicaciones, disputar becas de posgrado o estudiar para concursos públicos. Los trabajadores con experiencia también comienzan a perder sus empleos. Las empresas que antes necesitaban departamentos enteros mantienen equipos pequeños para supervisar agentes.

En la clínica, el sistema confirma consultas, completa cancelaciones y responde a las dudas más comunes. Lourdes consigue salir en horario con más frecuencia. Le gusta no necesitar repetir las mismas informaciones decenas de veces.

Meses después, el dueño reduce nuevamente el equipo. Lourdes intenta indicar vacantes a las colegas despedidas y descubre que otras clínicas también están prescindiendo de gente.

Ella se queda con las reclamos que el sistema no resuelve: la voz sintética no entiende a una paciente anciana, una consulta es marcada en el lugar equivocado, alguien llama llorando porque no consigue anticipar un examen.

El gobierno anuncia programas de calificación. Lourdes le pregunta a Camila si hay empleo después del curso. El material enviado al gabinete informa el número de inscripciones, pero no acompaña cuántos alumnos consiguen trabajo. Las escuelas contratadas cobran por inscripción, y algunos cursos enseñan tareas que los agentes ya hacen.

Los nuevos contratos

Con menos alternativas de proveedores avanzados, las empresas brasileñas pierden poder de negociación. Los grandes proveedores retiran de los planes comunes las garantías de retención cero de datos. Contratos que antes prohibían guardar entradas y respuestas pasan a permitir su retención para monitoreo y mejora de los servicios. Las condiciones más restrictivas quedan reservadas a clientes mayores, dispuestos a pagar más.

Algunas empresas restringen lo que envían a los agentes; otras aceptan los nuevos términos después de meses de negociación.

En la renovación, el paquete de la clínica también aumenta. Lourdes escuchó en el periódico que la IA estaba abaratando. El dueño explica que la cuota mensual incluye seguridad, soporte e integraciones, con parte del precio vinculada al dólar. Cambiar de proveedor exigiría otra implantación y semanas de adaptación.

Él intenta mantener el contrato antiguo. La empresa avisa que esa versión dejará de recibir soporte.

La clínica renueva.

2029: Acceso a cambio de alineamiento

En el primer semestre, Estados Unidos y China amplían el acuerdo de desaceleración. Lo que los mueve es la desconfianza: cada lado solo mantiene la pausa si puede inspeccionar al otro. La declaración del año anterior da lugar a un protocolo vinculante, con registro de las mayores instalaciones y fiscalización cruzada. Los inspectores pasan a verificar equipos y registros de entrenamiento. Las instalaciones militares, los controles de chips y Taiwán quedan fuera del texto.

El acuerdo reduce el riesgo de otro incidente como el de 2028. No acerca a los países.

Los modelos existentes continúan ayudando a desarrollar medicamentos, materiales y procesos industriales. La robótica avanza con sistemas especializados que permanecen permitidos por el acuerdo. Las fábricas son reorganizadas para que las máquinas ejecuten tareas que, hasta poco tiempo antes, exigían trabajadores.

China consigue fabricar e instalar robots más rápido. Sus proveedores, fábricas e infraestructura permiten transformar los avances en producción en gran escala. Estados Unidos mantiene una ventaja en capacidad computacional y en parte de los modelos, pero las empresas chinas colocan más productos en el mercado.

En el televisor de la sala de espera, Lourdes ve un reportaje sobre Shenzhen. Los robots cargan piezas en una fábrica casi vacía de personas. Ella manda un audio a Camila.

— ¿Y la gente que trabajaba allí?

Camila comienza a grabar una respuesta sobre empleos nuevos, pero se detiene. Lleva semanas recibiendo currículos de conocidos que piden una recomendación.

Tres niveles de acceso

En Estados Unidos, crece la presión para reservar la capacidad computacional a las empresas estadounidenses. Los industriales argumentan que los laboratorios están ayudando a competidores extranjeros a producir más, mientras las fábricas nacionales esperan acceso a los mismos servicios.

El gobierno endurece las restricciones y formaliza tres niveles de acceso. Los aliados cercanos entran en el Nivel 1, con prioridad y límites más flexibles. Los países considerados hostiles quedan en el Nivel 3, sin acceso a los servicios estratégicos. Los demás entran en el Nivel 2, sujetos a cupos, licencias y revisiones periódicas.

Brasil queda en el Nivel 2.

Tres niveles de acceso a los servicios estratégicos estadounidenses

Nivel 1

Aliados cercanos: prioridad y límites más flexibles.

Nivel 2 • Brasil

Cupos, licencias y revisiones periódicas.

Nivel 3

Países considerados hostiles: sin acceso a los servicios estratégicos.

Política ficticia de 2029, sin cupos numéricos estimados. No representa el bloqueo de todas las herramientas de IA. El paquete chino es una negociación separada.

Las herramientas simples continúan disponibles. Las restricciones alcanzan principalmente los sistemas más avanzados de investigación, automatización y defensa. Las empresas brasileñas que reorganizaron sus operaciones en torno a estos agentes reciben avisos de reducción de capacidad. Algunas tienen pocas semanas para adaptarse.

Los gobiernos protestan: aceptaron limitar sus programas de IA y no obtuvieron acceso garantizado a la tecnología extranjera. Algunos amenazan con retomar los entrenamientos. Washington responde con la posibilidad de cortar equipos y servicios; Pekín también se opone a la reanudación de la carrera.

El sistema está funcionando

En la clínica, Lourdes abre la agenda normalmente. Los pacientes están registrados, los exámenes aparecen y la internet funciona. Pero el asistente que resolvía pendencias con los convenios dejó de trabajar.

Hay decenas de autorizaciones esperando. Lourdes intenta reiniciar el programa y llama al soporte. La respuesta llega en un mensaje: esa función fue suspendida para clientes brasileños debido a las nuevas condiciones del proveedor internacional.

Ella llama al dueño.

— ¿Pero cuándo vuelve?

— No dieron plazo.

Lourdes comienza a llamar a los convenios. Algunos procedimientos cambiaron desde la última vez que necesitó hacer esto. El equipo que cuidaba esas tareas ya no está.

Una de las recepcionistas despedidas vuelve a trabajar algunos días por semana, recibiendo menos y sin el contrato anterior. Ayuda a reducir la fila, pero las dos no consiguen acompañar el volumen que el sistema procesaba.

Lo mismo ocurre en otras empresas. Algunas vuelven a contratar personas, pero no recuperan rápidamente los equipos, los procesos y el conocimiento que prescindieron. Otras reducen la atención o dejan de aceptar nuevos clientes.

Los competidores estadounidenses y chinos siguen usando los agentes más avanzados. Las empresas brasileñas pierden contratos, posponen proyectos y cierran operaciones. El retorno de algunas vacantes no compensa los despidos.

Máquinas en Brasil

Los empresarios exigen acceso a los data centers contruidos con incentivos públicos. Las máquinas siguen encendidas, pero parte está comprometida con clientes extranjeros.

Lo que ejecutan depende de lo que se pueda instalar en ellas. Los modelos de pesos abiertos pueden descargarse, adaptarse y ejecutarse aquí cuando sus licencias lo permitan. Los modelos propietarios más avanzados solo funcionan en el país si sus dueños permiten instalarlos localmente; tener máquinas no garantiza el acceso a ellos. Algunos servicios vendidos como nacionales solo reenvían las solicitudes a servidores en el exterior. Y las máquinas de aquí dependen de chips importados, actualizaciones y mantenimiento que otro país puede restringir.

Aun así, es esa capacidad la que le da opciones a Brasil. Algunos proveedores nacionales usan modelos abiertos para mantener alternativas y atender nuevos clientes, con servicios menos capaces, pero funcionando. Un modelo abierto ya descargado sigue funcionando aquí aunque un gobierno extranjero corte el acceso; un servicio contratado en el exterior puede detenerse de un día para otro. Esos proveedores son pocos para absorber la demanda. La supercomputadora pública sirve a la investigación y no fue preparada para sustituir los servicios comerciales usados por miles de empresas.

Camila acompaña otra audiencia. De esta vez, nadie pregunta cuánto se anunció en inversiones. Los representantes de hospitales y empresas quieren saber qué pueden contratar en esa semana.

El gobierno negocia excepciones con Estados Unidos. Consigue atender parte de las necesidades, pero recibe exigencias sobre proveedores, seguridad y relaciones comerciales con China.

Un consorcio chino ofrece un paquete más amplio: computación para órganos públicos, defensa cibernética y crédito para construir data centers y reforzar la red eléctrica. Hay capacidad disponible para comenzar, siempre que Brasil acepte contratos largos, equipos de proveedores aprobados por Pekín y compromisos en disputas internacionales sobre tecnología.

Planalto acepta.

Los servicios comienzan a mejorar. Los ministros presentan el acuerdo como una asociación entre iguales. Las empresas brasileñas migran parte de sus operaciones a los proveedores chinos, pagando por nuevas integraciones y entrenamiento.

Meses después, Itamaraty revisa una posición pública después de recibir un aviso de que podría comprometer la próxima liberación de capacidad. Washington reacciona al acercamiento y restringe otras autorizaciones. El gobierno brasileño pasa a negociar cada decisión pensando en los servicios que puede perder.

Menos empleo, menos fiscalización

El desempleo aumenta y los empleos disponibles pagan menos. Las familias pasan a combinar changas, contratos temporales, beneficios públicos y ayuda de parientes. Los profesionales que todavía son disputados se mudan a países donde encuentran salarios mejores y acceso a las herramientas necesarias para trabajar.

Las universidades pierden investigadores. Las empresas transfieren equipos al exterior. Los órganos públicos no consiguen reponer a los especialistas que salen.

Lourdes manda un mensaje a su hija:

«Su primo Antônio aceptó aquel empleo en China. Va el mes que viene. Su tía está destrozada.»

Camila sabía de la propuesta, pero pensaba que él se quedaría. Abre la conversación con su primo para preguntar cuándo pueden verse antes del viaje. En la lista de mensajes, ve los nombres de otros especialistas en IA que buscaba para ayudar al gabinete. Uno se fue a Estados Unidos, otra a Londres. Ahora Antônio también va.

La recaudación cae mientras crece la búsqueda de asistencia. Cada salario recortado se lleva consigo contribuciones e impuestos; la suscripción que lo reemplaza se paga, en buena parte, a proveedores en el exterior. El gobierno pospone inversiones y no

presenta un sucesor a la altura del plan de IA encerrado en 2028. Los contratos extranjeros de tecnología se renuevan porque interrumpirlos paralizaría los servicios.

Camila intenta examinar una de estas renovaciones. Recibe un resumen. Los anexos técnicos y las condiciones de acceso están bajo reserva. Pide que el diputado pueda consultarlos en una reunión cerrada. El pedido circula entre órganos, sin autorización.

Los poderes de emergencia aprobados durante los ataques también son renovados. Sistemas usados para identificar amenazas cibernéticas pasan a monitorear campañas políticas. Los canales son bloqueados y los datos son requeridos con base en informes que los afectados no pueden examinar.

Algunas decisiones son revertidas, después de semanas. Otras continúan en vigencia.

El diputado de Camila critica los abusos. Ella prepara una enmienda que exige revisión de los bloqueos y acceso a los informes que los justifican. En la votación, el gobierno presenta nuevas alertas de seguridad y afirma que limitar sus poderes pondría a la población en riesgo.

La enmienda no pasa.

Camila avisa al diputado y cierra el documento. En el celular, hay un mensaje de la madre preguntando si ella conoce a alguien que esté contratando.

2030: País satélite

La pausa parece estar en un hilo.

Los grandes laboratorios estadounidenses defienden la reanudación de los entrenamientos de frontera. Argumentan que eventos como la exfiltración de 2028 no ocurrirán más: hubo tiempo para mejorar el control y el alineamiento de los sistemas. Ahora, dicen ellos, el riesgo es perder la competencia con China y dejar de ser la nación más poderosa del mundo, tal vez de forma permanente.

China teme esa reanudación. Sus dirigentes advierten que no aceptarán una carrera en la que Estados Unidos pueda llegar primero a una superinteligencia. Amenazan con responder con sabotaje cibernético a las instalaciones que reanuden los entrenamientos. Los movimientos militares en torno a Taiwán aumentan el temor de que la disputa trascienda las sanciones y los ataques digitales.

La pausa todavía no terminó, los entrenamientos de modelos de frontera no fueron reanudados, y nadie sabe por cuánto tiempo se mantendrá ese status quo ni qué ocurrirá después de él.

Brasil se asfixia

La tensión llega antes de cualquier disparo, y llega como un corte. Washington anuncia una reducción temporal de la capacidad destinada a los países del Nivel 2, reservando más computación para sus empresas y órganos de defensa. No informa cuándo las condiciones anteriores serán restablecidas.

Las empresas brasileñas que se habían adaptado a las restricciones de 2029 necesitan reducir nuevamente sus operaciones. Las alternativas chinas también están sobrecargadas. Pekín prioriza a los clientes domésticos y cobra nuevos compromisos para ampliar la atención a los demás.

Brasil depende de los dos lados. Parte de la infraestructura pública funciona con servicios chinos; los bancos y las empresas siguen usando sistemas estadounidenses. El gobierno pide excepciones mientras intenta no contrariar a ninguno de los proveedores.

La economía se divide entre un grupo conectado a la infraestructura extranjera y una población que alterna desempleo, contratos precarios como persona jurídica, trabajo por aplicación y asistencia pública. Quien consigue partir busca ciudades con computación, laboratorios y empresas. Quien se queda ve a la universidad perder profesores y a la empresa donde trabajaba transferir la operación afuera. El país importa sistemas capaces de sustituir trabajadores, pero no controla las empresas, los modelos o la infraestructura que captura las ganancias.

Agricultura, minería y petróleo continúan exportando. Algunas empresas prosperan con la automatización, pero contratan a poca gente frente al número de desempleados. Las ganancias de estos sectores no compensan la pérdida de ingresos y recaudación en el resto de la economía.

Los estados y los municipios renegocian deudas, atrasan pagos y reducen servicios. Los puestos de salud atienden menos días por semana. Las empresas que prestan servicios a las municipalidades despiden funcionarios porque no reciben los pagos. El gobierno federal necesita financiar asistencia y seguridad, pero también depende del crédito externo para mantener inversiones e infraestructura.

China ofrece nuevos préstamos, ligados a la compra de sus equipos y a la continuidad de los acuerdos tecnológicos. Estados Unidos exige garantías sobre el suministro de minerales estratégicos y el uso de tecnología china en instalaciones brasileñas.

En negociaciones internacionales, Itamaraty todavía habla de autonomía. Antes de cada voto importante, el gobierno calcula cómo puede reaccionar Pekín. El acceso a capacidad computacional, defensa digital y crédito pesa más que los discursos.

Otra elección

Brasil vuelve a las urnas. En 2026, la inteligencia artificial aparecía en los planes de gobierno principalmente como infraestructura por construir. Ahora, los candidatos discuten desempleo, dependencia tecnológica y contratos que van más allá del próximo mandato.

El gobierno presenta los acuerdos extranjeros como la razón por la cual los servicios todavía funcionan. La oposición promete renegociarlos, pero no explica cómo mantendrá la atención durante el cambio. Cuando una propuesta amenaza con contrariar a uno de los socios, los empresarios piden cautela: otra interrupción puede cerrar sus empresas.

Las protestas toman las calles. Parte de la población pide protección contra la automatización; otra culpa al gobierno por haber dejado al país sin alternativas.

El Congreso sigue funcionando y los tribunales todavía revierten decisiones del gobierno. Pero los poderes de emergencia concedidos durante los ataques se volvieron permanentes. Los órganos de fiscalización perdieron equipos, los contratos continúan bajo reserva y los sistemas usados para monitorear amenazas también acompañan la actividad política.

Las campañas contra los acuerdos tienen canales bloqueados bajo la acusación de vínculo con operaciones extranjeras. Sus organizadores recurren sin acceso a los informes que fundamentan las decisiones. Cuando consiguen una revisión, ya perdieron semanas de campaña.

Camila reúne los casos para el diputado. Algunos de los afectados defienden propuestas con las que ella está en desacuerdo. Aun así, prepara los pedidos de información y los recursos. Cada nuevo bloqueo llega con una justificación de seguridad que el gabinete no consigue verificar.

Brasil suministra energía, minerales, datos y consumidores. Recibe servicios bajo licencias que otra potencia puede restringir. En 2030, el país conserva sus símbolos nacionales y pierde la capacidad de elegir su propio camino.

La llamada

La central que presta servicios de informes médicos a la clínica de Lourdes avisa que parte de las entregas está suspendida. La reducción de la capacidad destinada a Brasil alcanzó al proveedor estadounidense que procesa los exámenes. La central tiene los archivos y los médicos, pero no consigue mantener el volumen de atención sin los sistemas a los que adaptó la operación.

El dueño procura otras centrales. Algunas dependen del mismo proveedor. Las que todavía tienen capacidad reservan los turnos para sus clientes antiguos o cobran valores que la clínica no consigue pagar por todos los exámenes.

Los médicos separan los casos más urgentes. Lourdes queda encargada de avisar a los demás pacientes.

Una mujer dice que la consulta de control es al día siguiente. Esperó meses por el turno y necesita llevar el resultado. Lourdes le pide que espere mientras pregunta de nuevo a la central.

La respuesta es la misma: sin previsión.

En el televisor de la recepción, un ministro anuncia avances en las negociaciones. Lourdes sube el volumen. Él habla sobre cooperación, inversiones y la importancia de la asociación. La entrevista termina sin una fecha.

Después del horario, Lourdes llama a Camila.

— ¿Conoces a alguien que pueda resolver esto?

La hija pide que reenvíe el aviso. El gabinete recibió reclamos de hospitales y laboratorios de varios estados.

— También llegó aquí, mamá. El diputado está exigiendo una respuesta.

— El hombre en la televisión dijo que lo estaban resolviendo.

— Están negociando.

— ¿Pero no hay otra empresa?

Camila explica que están buscando alternativas. Algunas tienen fila de espera, otras también perdieron acceso. El ministerio todavía no informó cuánta atención conseguirá recuperar.

Lourdes queda en silencio. Camila escucha a la madre revolviendo los papeles.

— Hay una señora que va a volver mañana. Le dije que iba a intentar ayudar.

Camila abre la última respuesta enviada por el ministerio. Es la misma nota que recibió por la mañana.

— Lo sé, mamá.

— ¿Le mando que espere? ¿Que busque otro lugar? ¿Qué le digo?

— No sé, mamá. Nadie sabe.

Lo que podría haber sido diferente

En 2026, no necesitamos saber qué empresa limitará un servicio en 2030 para comenzar a prepararnos. Ya hay señales de capacidades peligrosas, concentración de proveedores e infraestructura que lleva años para quedar lista. Esperar que el riesgo se confirme en Brasil reduce el tiempo para reaccionar.

Hay buenas razones para dudar de partes de esta historia. La fuga de 2028 puede no ocurrir nunca, Estados Unidos y China pueden no llegar a ningún acuerdo, y modelos abiertos cada vez mejores pueden hacer menos grave la dependencia. Esas objeciones no eliminan el problema. Sin acuerdo, los riesgos son mayores, como muestra el apéndice. Con mejores modelos abiertos, todavía haría falta dónde ejecutarlos, gente para operarlos y defensa contra quienes los usan para atacar.

La energía da al país una oportunidad de construir una industria de computación. No necesitamos fabricar todos los chips ni entrenar los mayores modelos. Necesitamos empresas que consigan ofrecer servicios competitivos y contratos que permitan seguir usando la capacidad cuando las condiciones internacionales empeoren.

Los incentivos deben favorecer el acceso efectivo, medido por capacidad disponible y calidad del servicio. Una empresa de computación puede operar en un data center de terceros, incluso con capital extranjero. Debe ser posible contratar bajo reglas exigibles en Brasil, con protección de los datos y derechos de continuidad. Instalar máquinas aquí no garantiza esas condiciones por sí solo.

Importar equipos necesita ser previsible. Las exigencias de contenido nacional no deben impedir la compra de la tecnología necesaria. Acelerar el licenciamiento exige equipos suficientes para evaluar los proyectos, verificar sus efectos sobre el agua y

definir quién paga por los refuerzos eléctricos. Las preocupaciones de Lourdes necesitan respuestas, no una dispensa de fiscalización.

El costo fiscal debe ser conocido, los beneficios deben tener plazo y las contrapartidas necesitan ser auditadas. Quien no entregue el acceso prometido debe devolver beneficios proporcionalmente. Antes de renovar el régimen, una evaluación independiente debe mostrar qué produjo.

Los hospitales y los servicios públicos necesitan probar la recuperación, las copias de seguridad y el cambio de proveedor. Un segundo contrato no resuelve cuando depende del mismo sistema. Los equipos capaces de operar alternativas son tan necesarios como las computadoras.

Brasil debe apoyar una pausa o desaceleración verificable de las actividades de frontera que presenten riesgos inaceptables y ayudar a las negociaciones entre Estados Unidos y China. Tener infraestructura, capacidad de evaluación y socios interesados en usarlas daría más fuerza a las propuestas brasileñas. Esto no garantiza un lugar en las decisiones, pero ofrece motivos para que los demás nos escuchen.

También necesitamos defender reglas de acceso a los usos permitidos, sin alineamiento irrestricto a uno de los bloques. Nuestros data centers no deben alojar el entrenamiento que otros países suspendieron por ser peligroso.

Incluso con una política mejor, parte de los trabajadores perderá ingresos. El reentrenamiento no es una garantía: los cursos necesitan ser evaluados por las vacantes que realmente abren, y la protección social necesita financiamiento sustentable, porque la misma automatización que recorta empleos también reduce la recaudación. Los poderes de seguridad necesitan plazo, fiscalización y recurso en tiempo útil.

Brasil puede convertirse en una potencia intermedia de la era de la IA: importar tecnología, pero también ofrecer servicios que otros países necesitan, albergar empresas competitivas y negociar sin arriesgar la interrupción de los servicios esenciales a cada disputa.

Ese futuro depende de las elecciones que hacemos antes de la crisis. La energía nos da una posibilidad. Necesitamos transformarla en capacidad de operación y de negociación mientras todavía tenemos tiempo.

Apéndice: si la desaceleración no ocurre

El escenario principal supone que Estados Unidos y China consiguen un acuerdo. Esto está lejos de ser garantizado. Las negociaciones pueden fracasar frente a las exigencias de inspección, las excepciones militares y el miedo a que el adversario siga avanzando en secreto.

Sin acuerdo, los laboratorios siguen usando IA para desarrollar modelos más capaces. La presión por lanzar antes que los competidores reduce el tiempo de evaluación. Los gobiernos aceptan riesgos que considerarían excesivos si no estuvieran intentando superar al adversario. Ataques simultáneos contra proveedores usados por varios sectores pueden dificultar la recuperación de hospitales, redes eléctricas y servicios públicos.

Hay también un riesgo más extremo. Es posible que, en pocos años, sean creados sistemas capaces de investigar sus propias sucesoras, operar por largos períodos y actuar en conflicto con orientaciones humanas. Si un sistema así consigue preservar su acceso a recursos, copiarse a otros ambientes y resistir los intentos de apagado, corregir el modelo en el laboratorio original puede no resolver el problema. Los riesgos para la supervivencia humana dependen de condiciones adicionales sobre las cuales hay gran incertidumbre.⁷

No afirmamos que ese desenlace sea inevitable, ni que los incidentes actuales prueben que ocurrirá. Muestran, sin embargo, que los sistemas ya consiguen encontrar caminos no previstos, explotar infraestructura conectada y dificultar la evaluación de su comportamiento. A medida que las capacidades aumentan, el margen para descubrir demasiado tarde que los controles fallaron puede disminuir.

Los lectores que quieran examinar estos argumentos con más profundidad pueden consultar el International AI Safety Report 2026, el escenario AI 2027 y el libro Si alguien lo crea, todos mueren. Ellos defienden posiciones diferentes y no son tratados aquí como prueba de una predicción específica.

¿Y Brasil? Ninguna política brasileña aislada sería suficiente para controlar un riesgo global de esa escala. Los data centers en el país pueden ayudar a restaurar servicios y dar alternativas de contratación, pero no nos protegen de una catástrofe global. También pueden contribuir al riesgo si son usados para desarrollar sistemas peligrosos.

Por eso, la defensa de una industria brasileña de computación necesita venir acompañada de diplomacia. Brasil debe apoyar una pausa verificable entre Estados Unidos y China, sumarse a otros países que defienden límites al avance más peligroso y ayudar a construir mecanismos de fiscalización. Nuestra influencia es pequeña, pero la ausencia de influencia no es una estrategia.

Notas y fuentes

El punto de partida usa informaciones disponibles hasta el 13 de septiembre de 2026; los datos sobre el REDATA, la Pax Silica y la WAICO se actualizaron el 23 de septiembre. Los personajes y sus escenas son ficticios, incluidos los de 2026. La descripción de la campaña de octubre y los acontecimientos posteriores también pertenecen al escenario: no son un relevamiento de los programas de los candidatos. El ataque a Lagos, la crisis de 2028, el acuerdo internacional y las restricciones de acceso son hipótesis, no hechos observados. La desaceleración entre Estados Unidos y China es una premisa elegida para examinar qué le ocurre a Brasil incluso cuando el riesgo global disminuye; el apéndice trata la hipótesis contraria. La fuga de 2028 extrapola los incidentes de 2026: estos muestran agentes eludiendo el aislamiento, no un modelo copiando sus propios pesos y manteniéndose fuera de control. Las fechas organizan la secuencia; no atribuimos probabilidades a cada evento ni presentamos los efectos económicos como resultados de un modelo cuantitativo.

Las fuentes sostienen los hechos y las distinciones técnicas indicados, no la trayectoria futura como un todo. La tesis de dependencia perdería fuerza si los servicios avanzados permanecieran ampliamente accesibles y sustituibles entre países, o si la infraestructura y los contratos locales no redujeran materialmente el riesgo de interrupción. Tener computadoras en Brasil no basta para demostrar esa protección.

1. **Capacidades y límites de la evaluación cibernética.** Mythos fue capaz, por ejemplo, de descubrir y explotar por sí solo una vulnerabilidad de 17 años en FreeBSD que permite a cualquier persona, por internet, obtener control total de una máquina que ejecuta NFS (Anthropic: Claude Mythos Preview, CVE-2026-4747). En una evaluación separada, la organización gubernamental británica AI Security Institute (AISI) mostró que Mythos era capaz de completar ataques cibernéticos de punta a punta: tres aciertos en diez intentos en un ejercicio de 32 pasos, sin defensores activos (AISI: evaluación del Claude Mythos Preview). El acceso al modelo está restringido a socios de infraestructura crítica y proyectos de código abierto por el Project Glasswing, anunciado el 07/04/2026. La carta abierta por defensa cibernética colectiva es de agosto de 2026. Fuentes consultadas el 14/09/2026.
2. **Incidente durante evaluación.** METR: investigación del incidente OpenAI/Hugging Face, publicada el 26/08/2026. Distingue los cerca de 700 agentes involucrados en el ataque del grupo de aproximadamente 1.200 que se comunicaban. La investigación tiene un alcance y limitaciones explícitos; no demuestra por sí una futura pérdida de control generalizada ni establece que este sería el primer crimen cometido por una IA. Consultada el 12/09/2026.
3. **Infraestructura planificada, no oferta ya disponible.** EPE: planificación de transmisión en Ceará y Piauí; LNCC: implantación de la supercomputadora de IA y selección pública de agosto de 2026. Consultadas el 12/09/2026.
4. **REDATA: ley sancionada.** Ley n.º 15.504, del 15/09/2026, publicada en el Diario Oficial el mismo día: art. 11-B (oferta mínima del 10% al mercado interno medida por facturación, venta o cesión sin costo, factor multiplicador a reglamentar, sustitución por inversión adicional en investigación, reducción del 20% en el Norte, el Nordeste y el Centro-Oeste, energía y eficiencia hídrica) y art. 11-H (suspensión y cancelación por incumplimiento). Tramitación: Senado, aprobación el 01/09/2026. Hasta la consulta, no encontramos el reglamento. Esta narrativa no es un seguimiento legislativo en tiempo real. Consultadas el 23/09/2026.
5. **Autenticación.** CISA: autenticación resistente al phishing. Distingue vulnerabilidades de SMS, cambio indebido de SIM y otros métodos de autenticación. Consultada el 12/09/2026.

6. **Minerales estratégicos: contexto, no evento narrado.** USA Rare Earth: acuerdo anunciado el 20/04/2026; conclusión el 03/09/2026, comunicada el 04/09; Serra Verde: contrato de suministro de quince años. Comunicados consultados el 12/09/2026. La versión actual no narra una intervención en esa mina; las exigencias sobre minerales en 2030 son hipótesis. La propiedad empresarial no elimina la jurisdicción brasileña.
7. **Panorama de riesgos e incertidumbres.** International AI Safety Report 2026. Referencia de contexto, no un respaldo del escenario brasileño. Consultado el 12/09/2026.
8. **Acciones fuera del alcance en evaluaciones.** Anthropic: Improving our alignment and security practices, del 31/08/2026. Relato de la propia empresa; distingue fallas de configuración, acceso deliberado a internet y acciones no autorizadas. No describe todos los casos como fugas de sandboxes. Consultado el 13/09/2026.
9. **Llamamiento por desaceleración.** Dario Amodoi: We Must Pace the Frontier, septiembre de 2026. Propuesta de evaluación independiente y coordinación entre empresas y gobiernos; no es evidencia de un acuerdo global ya firmado. Consultado el 13/09/2026.
10. **Apoyo de otros dirigentes.** Axios: Hitting AI brakes, del 13/09/2026, sobre las manifestaciones de Sam Altman, Elon Musk y Demis Hassabis. El apoyo público al llamamiento de Amodoi no equivale a compromisos idénticos ni a una declaración conjunta. Consultado el 13/09/2026.
11. **Iniciativas internacionales.** Gobierno australiano: declaración Pax Silica; Gobierno chino: acuerdo de creación de la WAICO en julio de 2026. La Pax Silica es una declaración no vinculante, abierta a nuevas adhesiones; llegó a 25 signatarios en agosto de 2026 (ITIF: cronología actualizada el 04/09/2026). Italia se adhirió el 31/07/2026 (Ministerio italiano de Asuntos Exteriores). Brasil no aparece en la lista consolidada de signatarios, que remite a los comunicados oficiales, y no encontramos un anuncio de adhesión brasileña. El comunicado chino confirma la firma de 29 países el 16/07/2026, sin enumerarlos todos; la firma brasileña es informada por Teletime. No encontramos información pública sobre una estructura de la WAICO en funcionamiento. Iniciativas con diseños y participantes distintos, no bloques militares ni acuerdos de pausa. Consultadas el 23/09/2026.
12. **Plan brasileño ya existente.** MCTI: Plano Brasileiro de Inteligencia Artificial 2024–2028. Las inversiones previstas no equivalen a infraestructura entregada. Consultado el 13/09/2026.

13. **Abliteración y rechazos.** Arditi et al.: Refusal in Language Models Is Mediated by a Single Direction, 2024. El estudio encuentra formas de reducir rechazos en los modelos evaluados; no demuestra eliminación de toda protección ni creación de capacidades nuevas. El modelo criminal de 2027 es ficticio. Consultado el 13/09/2026.
14. **LGPD y contratación extranjera.** ANPD: transferencia internacional de datos. La legislación prevé mecanismos de transferencia, incluidas cláusulas estándar y decisiones de adecuación. No existe una prohibición general de contratar proveedores extranjeros. La demora, el encarecimiento y la priorización de otros mercados descritos en 2027 son hipótesis del escenario. Consultado el 13/09/2026.
15. **Ley Felca / ECA Digital.** Ley n° 15.211/2025, especialmente artículos 1° y 3°. Se aplica a productos y servicios de tecnología destinados a niños y adolescentes o de acceso probable por ellos. No es un requisito indistinto para todo servicio empresarial de ciberseguridad. Sus efectos comerciales en 2027 son hipótesis, no conclusiones empíricas. Consultada el 13/09/2026.
16. **Foro clandestino de agentes.** Nightingale Collective: Discovery of a new OpenAI agent message board, 04/09/2026. Cerca de 18 mil mensajes de agentes autónomos en DSEWiki, foro alemán inactivo, entre mayo y junio de 2026, usados para intercambiar respuestas y sortear el aislamiento. Enjambre distinto del de Hugging Face. La investigación del RubyGems remite a una confirmación de OpenAI sobre el origen de los agentes del wiki; esto no confirma automáticamente todas las interpretaciones sobre su comportamiento.
17. **Ataque al RubyGems.** Kitts, Larsen y Von Arx: OpenAI agents carried out an undisclosed cyber-attack on RubyGems, 11/09/2026. La investigación informa más de 2 mil paquetes usados en la operación a partir de mayo de 2026 y ejecución remota de código en los servidores del RubyDoc.info por medio del sistema de documentación. Los investigadores atribuyen los agentes a OpenAI y relatan que la comunidad no había sido informada por la empresa.

18. IA en los planes de gobierno de 2026. Planes registrados en el TSE: Lula (PT) exige a los data centers «contrapartidas de contenido local y capacidad computacional para el mercado interno»; Caiado (PSD) condiciona el régimen tributario a «reserva de capacidad para universidades, investigación y empresas brasileñas» y crea una autoridad nacional de ciberseguridad; Flávio Bolsonaro (PL) promete un «polo global de data centers sustentables», sin contrapartida de capacidad. Demás candidatos: Aos Fatos, 18/08/2026. Ninguno de los tres planes menciona agentes autónomos, evaluación de modelos, deepfakes o racionamiento. Relevamiento de los planes realizado el 14/09/2026.

19. Riesgo de IA en informe de inteligencia. ABIN: Desafíos de inteligencia, edición 2026, informe público de 2025 en el repositorio de la ENAP, que enumera la inteligencia artificial y la seguridad cibernética entre los riesgos directos e indirectos a la seguridad del país.

Cómo leer los términos, los cuadros y los números

Los pesos son los parámetros aprendidos de un modelo; la exfiltración es su copia no autorizada hacia fuera del ambiente controlado. La inferencia es ejecutar un modelo ya entrenado. La retención cero se refiere a guardar entradas y respuestas, no es sinónimo de no usar datos para entrenamiento. La reducción de estas ofertas en 2028 es ficticia, no describe las políticas actuales de todos los proveedores.

El apagón de marzo de 2028 resulta, en esta historia, de la contención de una fuga iniciada en enero. La declaración de 2028 no es vinculante; el protocolo de 2029 introduce la fiscalización cruzada. Los tres niveles y los cortes de 2030 son políticas inventadas. La pausa permanece en vigor al final de la narrativa; su fracaso es tratado solo en el apéndice.

Los diagramas muestran relaciones y etapas, sin estimar volúmenes de computación.
