MSMK Magazine

Tech and Employment: Empowering Tomorrow's Talent

Cambio Climático y Tecnología

#6

MSMK University College

6.ª Edición - Cambio Climático y Tecnología

En esta edición de MSMK Magazine, exploramos cómo la innovación digital se convierte en protagonista frente a uno de los mayores retos globales, el cambio climático. A lo largo de la revista, se analiza el impacto real de la inteligencia artificial en el planeta, la ciberseguridad en sistemas de monitorización climática, la huella energética de los nuevos modelos tecnológicos, el papel del blockchain en la trazabilidad ambiental y los dilemas éticos que surgen en la intersección entre sostenibilidad y transformación digital.

Una edición que no solo reflexiona sobre cómo la tecnología puede ayudar a combatir el cambio climático, sino que también cuestiona sus límites, sus costes y su responsabilidad

MSMK University College

CONTENIDO

CONTENIDO

AXEL BRAOJOS PEREZ

EL HOGAR SOSTENIBLE DEL FUTURO

El cambio climático y el crecimiento acelerado de las ciudades han convertido al hogar en uno de los principales focos de consumo energético y generación de emisiones contaminantes. Actualmente, una parte significativa de la energía mundial se consume en viviendas, lo que obliga a replantear la forma en que diseñamos y habitamos nuestros espacios. En este contexto, la sostenibilidad ya no es una opción, sino una necesidad urgente.

Frente a este desafío, la tecnología ha comenzado a desempeñar un papel clave. En particular, la inteligencia artificial se presenta como una herramienta capaz de optimizar el uso de recursos, reducir el impacto ambiental y mejorar la calidad de vida dentro del hogar.

Un hogar sostenible es aquel que busca minimizar su impacto ambiental mediante el uso responsable de energía, agua y materiales. Esto incluye desde una buena orientación arquitectónica hasta el uso de energías renovables y sistemas eficientes. Sin embargo, cuando estos principios se combinan con tecnología inteligente, el concepto evoluciona hacia un hogar capaz de adaptarse a las necesidades de sus habitantes y del entorno.

La inteligencia artificial permite que el hogar aprenda de los hábitos cotidianos de las personas, analice datos en tiempo real y tome decisiones automatizadas. De esta manera, sistemas de iluminación, climatización y consumo energético pueden ajustarse automáticamente para reducir desperdicios sin comprometer el confort.

Aplicaciones clave de la inteligencia artificial en el hogar

La inteligencia artificial ya se aplica en múltiples áreas del hogar sostenible.

Desde la gestión energética inteligente hasta el control del agua y los residuos, estos sistemas permiten optimizar recursos y reducir emisiones.

Sensores, algoritmos predictivos y dispositivos conectados trabajan en conjunto para crear viviendas más eficientes, autónomas y respetuosas con el medio ambiente.

La climatización inteligente es otro de los avances más destacados. Termostatos basados en inteligencia artificial aprenden los hábitos diarios de los habitantes y ajustan automáticamente la temperatura, logrando mantener el confort térmico con un menor consumo de energía y una reducción significativa de emisiones.

En conjunto, estas aplicaciones convierten al hogar en un entorno activo y consciente, capaz de anticiparse a las necesidades humanas y ambientales. La tecnología deja de ser solo una herramienta de comodidad para convertirse en un aliado clave en la construcción de un futuro más sostenible.

La IA aplicada al hogar sostenible

Uno de los principales beneficios de la inteligencia artificial en el hogar sostenible es la optimización del consumo energético. A través del análisis de patrones de uso, la IA puede identificar momentos de alto consumo y ajustar automáticamente el funcionamiento de los dispositivos para reducir el gasto energético y las emisiones de dióxido de carbono.

Además, los sistemas inteligentes permiten una gestión más eficiente de la iluminación y los electrodomésticos. Mediante sensores de presencia y algoritmos de aprendizaje automático, la inteligencia artificial puede apagar luces en espacios desocupados, regular la intensidad lumínica según la luz natural disponible y coordinar el funcionamiento de los aparatos para evitar consumos innecesarios.

De igual forma, la inteligencia artificial contribuye a mejorar el confort térmico del hogar sin aumentar el gasto energético. Termostatos inteligentes analizan rutinas diarias, condiciones climáticas y preferencias personales para ajustar la calefacción o la refrigeración de manera automática, logrando un equilibrio entre bienestar, eficiencia y reducción del impacto ambiental.

En combinación con energías renovables como la solar, estos sistemas permiten decidir cuándo almacenar energía, cuándo utilizarla y cuándo devolverla a la red eléctrica. Esto no solo mejora la eficiencia del sistema, sino que también reduce la dependencia de fuentes de energía no renovables.

La gestión inteligente del agua es otro aspecto fundamental. Sensores conectados a sistemas de inteligencia artificial pueden detectar fugas, regular el riego según las condiciones climáticas y reducir el desperdicio. De este modo, el hogar no solo consume menos recursos, sino que también contribuye a la conservación del medio ambiente.

A pesar de sus beneficios, la implementación de hogares sostenibles basados en inteligencia artificial aún enfrenta desafíos. El costo inicial, la brecha tecnológica y la protección de los datos personales son algunos de los aspectos que deben abordarse para garantizar un acceso equitativo y seguro a estas tecnologías.

Sin embargo, el futuro apunta hacia viviendas cada vez más autónomas, eficientes y conectadas con su entorno. La combinación de conciencia ambiental y avances tecnológicos representa una oportunidad única para transformar la forma en que vivimos, haciendo del hogar un aliado clave en la lucha contra el cambio climático.

La importancia de los datos en el hogar inteligente

La base del funcionamiento de un hogar sostenible apoyado por inteligencia artificial es la recolección y análisis de datos. A través de sensores distribuidos en distintos puntos de la vivienda, medidores eléctricos, sensores de temperatura, humedad, consumo de agua y calidad del aire, la IA obtiene información constante sobre el comportamiento del hogar. Estos datos permiten identificar patrones de uso, detectar ineficiencias y anticipar necesidades antes de que el usuario intervenga.

Automatización basada en aprendizaje automático

Uno de los aspectos más relevantes es la automatización basada en aprendizaje automático.

A diferencia de los sistemas tradicionales programados manualmente, la inteligencia artificial es capaz de aprender de las rutinas diarias de las personas que habitan la vivienda. Por ejemplo, puede reconocer a qué horas se utilizan determinados electrodomésticos, cuándo se requiere mayor climatización o qué espacios permanecen desocupados durante el día. Con esta información, el sistema ajusta automáticamente el funcionamiento del hogar para minimizar el consumo energético sin afectar el confort.

Optimización predictiva y eficiencia energética

La inteligencia artificial también desempeña un papel clave en la optimización predictiva. Analizando datos históricos y variables externas, como condiciones meteorológicas o tarifas eléctricas, el sistema puede prever aumentos en la demanda energética y actuar en consecuencia. Esto permite, por ejemplo, priorizar el uso de energía almacenada en baterías domésticas, reducir picos de consumo o programar el uso de electrodomésticos en horarios más eficientes.

Conclusión

En conjunto, estos procesos demuestran que la inteligencia artificial no actúa únicamente como una herramienta de automatización, sino como un sistema de apoyo a la toma de decisiones, capaz de transformar el hogar en un espacio inteligente, eficiente y alineado con los objetivos de sostenibilidad ambiental.

“La tecnología no es el fin, sino el medio para una vida más sostenible.”

-Axel Braojos Pérez

DAVID LANCHEROS IPUS

¿LA IA SALVADORA? O MAQUILLANDO EL PROBLEMA

¿Por qué esperamos a escuchar que algo malo está a punto de suceder para preocuparnos y cuestionarnos si debemos actuar? Constantemente escuchamos hablar del cambio climático, de deshielos, de inundaciones. Y si todo esto está sucediendo, ¿realmente nos interesa? ¿O creemos que, como no nos afecta directamente, podemos posponer la acción y dejarlo como problema de la siguiente generación? Lo interesante aquí es que podemos ver a gobiernos y grandes empresas tomando acción, "luchando" contra la incertidumbre y contra el cambio climático. Desde algoritmos que predicen patrones meteorológicos para optimizar redes eléctricas renovables hasta abejas con colmenas robóticas "protectoras". Pero esto nos hace preguntar: ¿realmente esta lucha, estas nuevas tecnologías, realmente ayudan a combatir el cambio climático? ¿O solo están maquillando el problema con bonitos gráficos que ocultan la verdad? La respuesta va más allá del tecnicismo: no solo abarca ámbitos geopolíticos y económicos, sino que nos demuestra qué necesitamos realmente para nuestro futuro.

China gana independencia energética

Un caso concreto es el uso de inteligencia artificial para la predicción meteorológica en China. Durante mucho tiempo, el análisis y el pronóstico del tiempo estuvieron limitados por datos y modelos matemáticos complejos. No fue hasta que modelos entrenados con millones de datos climáticos, como FengWu y Lingxi, empezaron a predecir patrones meteorológicos con una gran precisión, sin depender de datos del extranjero, que, como resultado, China se posicionó como uno de los países con mayor optimización de recursos. Al anticipar en qué zonas del país hará más calor o más viento, el país intensifica y potencia el uso de energías renovables como la solar y la eólica en esas regiones.

Esto reduce la dependencia de combustibles fósiles y permite que las redes eléctricas aprovechen y absorban esa energía de la mejor manera posible. ¿Es una solución real o simplemente geopolítica? En realidad, son ambas cosas: China reduce la dependencia hacia energías que dañan el medio ambiente, pero también es una estrategia del gobierno para controlar su propio clima y sus propios intereses. ¿La IA esconde poder?

Las Abejas "Sobreprotegidas"

Las abejas, probablemente el animal más importante de nuestro planeta, ya que mantienen un equilibrio vital en el ecosistema, han sido reconocidas por Beewise, que supo destacar su importancia. Por ello, crearon BeeHome, aparentemente una simple caja con una colmena tradicional, pero equipada por dentro con un sistema inteligente, sensores de temperatura y humedad, cámaras de visión, y brazos robóticos capaces de alimentar, medicar y ajustar todos los parámetros para ofrecer el mejor entorno posible para las abejas.

Esto es BeeHome, una "simple" caja con inteligencia artificial que actúa automáticamente al detectar que una colonia está en peligro o muriendo. Representa un gran avance para la polinización global y los ecosistemas terrestres; esto nace de la preocupación por colonias enteras que mueren día a día por plagas, pesticidas, el cambio climático y más. Pero, ¿es esto realmente una solución? Estamos ante un paso importante hacia la preservación de nuestra biodiversidad y nuestro futuro, impulsado por algoritmos que podrían redefinir nuestra relación con la naturaleza.

Las consecuencias de entrenar un modelo de IA para "salvar" el clima

Hay una verdad que muchos sabemos, pero que pocos enfrentamos realmente. Mientras empresas como Google, Microsoft, OpenAI y otras grandes tecnológicas muestran al mundo sus soluciones de inteligencia artificial para monitorizar emisiones, optimizar energía y predecir desastres climáticos, casi nadie parece notar el enorme consumo energético que implica entrenar estas mismas soluciones. Según la Agencia de Protección Ambiental (EPA), ChatGPT, la IA más conocida actualmente, emitió aproximadamente unas 588 toneladas de CO_2 solo para el entrenamiento de su modelo GPT-3. Si hablamos de Fengwu, el modelo de IA utilizado en China, ¿cuánto CO_2 ha emitido hasta hoy solo durante su fase de entrenamiento? Tal vez ayuda al país, pero ¿a qué costo? Otro caso es el de Google.

Ellos anuncian que sus centros de datos son “carbon neutral”, pero neutral no significa cero emisiones. Estamos utilizando grandes tecnologías que, si bien pueden contribuir al medio ambiente, también generan un impacto considerable. En otras palabras, estamos entrenando modelos para mitigar el calentamiento global, pero esos mismos modelos contribuyen al sobrecalentamiento del planeta. ¿Somos realmente conscientes del número de modelos que se entrenan cada día? Ninguna empresa que desarrolla o utiliza estas tecnologías parece capaz o dispuesta a mostrar las cifras reales. Es cómodo ignorar esos datos y disfrazar la ayuda con maquillaje superficial. Entonces, ¿se trata de una verdadera lucha contra el cambio climático o solo de una estrategia para justificar que “se está ayudando al planeta”?

¿Ayuda o vigilancia? Límites en la sociedad

Si hablamos de riesgos, el gobierno de Singapur es el mejor de los casos, ya que utiliza sensores nodes, una IA capaz de monitorizar en tiempo real la calidad del aire, la congestión del tráfico y el consumo energético de la ciudad.

La plataforma es sencilla: usa datos de miles de sensores distribuidos por toda la ciudad para alimentar su modelo de IA. Hasta ahí bien, reduce emisiones gracias al algoritmo y mejora la eficiencia. Pero en la práctica no todo es tan color de rosa. La realidad es que esos mismos datos se integran directamente con los sistemas de vigilancia urbana de Singapur, conocido por ser uno de los regímenes de control más estrictos del mundo. Los datos de "calidad del aire en la calle X" están vinculados a datos de cámaras de vigilancia en esa misma calle, historial de movimientos de ciudadanos y patrones de comportamiento. El gobierno lo llama "optimización urbana". Pero lo que realmente permite es rastrear no solo emisiones, sino adónde van las personas, con quién se reúnen y qué rutas evitan. Huawei ha participado en la construcción de esta infraestructura en Singapur y en otras "smart cities" de Asia y África. La empresa publicita que su IA de "monitoreo ambiental" ayuda a las ciudades a ser "más verdes". Pero esos mismos sistemas de sensores e IA que vende se usan para vigilancia política y control social. La IA climática es real, funciona y reduce emisiones mensurables.

Sin embargo, su infraestructura es idéntica a la de vigilancia: no es que "pueda convertirse" en ella; desde el día uno, fue diseñada para ambas cosas. Singapur no lo oculta; simplemente no lo enfatiza en el marketing.

Los matices de la IA

La verdad es que no hay una respuesta clara. La IA es una herramienta neutral: puede ayudar, salvar o optimizar recursos, pero también perjudicar al consumir más energía de la que ahorra y convertirse en nuestra próxima problemática sin que nos demos cuenta. ¿Salvadora o solo un maquillaje del problema? No tiene una única respuesta; depende de los casos de uso, empresas y gobiernos que la implementan. Unos la llaman revolución e innovación; para otros, es una evasión profesional de lo esencial. Lo importante es comprender su neutralidad: todo acto tiene consecuencias. El cambio climático es real, la IA es real, pero la solución no es solo tecnología; es avanzar con responsabilidad. Sin auditoría, es manipulación. Sin participación pública, es control. La pregunta clave es: ¿qué tipo de IA vamos a construir?

GABRIEL FALCAO SANTOS

SIDE-CHANNEL ATTACKS EN SISTEMAS DE MONITORIZACIÓN CLIMÁTICA

Hoy en día, la monitorización del cambio climático es una prioridad a nivel científico y geopolítico que depende de la precisión e integridad de los datos recolectados en tiempo real. La transición de estaciones meteorológicas analógicas hacia sistemas automatizados basados en el Internet de las Cosas ha permitido una densidad de datos sin precedentes, necesaria para los modelos climáticos de alta resolución. Sin embargo, esta infraestructura tecnológica distribuida ha introducido vectores de amenaza que trascienden las vulnerabilidades de software tradicionales. Los side-channel attacks representan una de las más complejas fronteras de la ciberseguridad actual, explotando las emisiones físicas no voluntarias de los dispositivos para comprometer la confidencialidad y la integridad de la información ambiental.

El ecosistema de la monitorización climática moderna

Las estaciones meteorológicas modernas han evolucionado en la dirección de sistemas embebidos complejos que integran sensores especializados para medir variables como la temperatura, presión atmosférica, radiación solar. Estos dispositivos se instalan a menudo en ubicaciones remotas y utilizan microcontroladores de bajo costo y alta eficiencia, para procesar la información y transmitirla a través de redes inalámbricas.

A diferencia de los sistemas informáticos convencionales, los sistemas de monitorización climática dependen de sensores que interactúan directamente con el entorno físico. El uso de tecnologías de sistemas microelectromecánicos ha permitido la miniaturización extrema, pero estos componentes presentan características de fuga de señal únicas debido a su escala microscópica. La dependencia de hardware comercial de bajo costo implica que estos dispositivos suelen carecer de contramedidas físicas fuertes, dejándolos vulnerables ante adversarios con acceso físico o proximidad a los nodos de la red.

Mecanismos de los side-channel attacks

Un ataque de canal lateral no se dirige a las debilidades algorítmicas de la criptografía o a los errores en el código del software, sino a la implementación física del hardware. La premisa fundamental es que cualquier operación lógica hecha por un procesador semiconductor conlleva efectos secundarios físicos que están relacionados con los datos que se procesan.

Análisis de potencia y emanaciones electromagnéticas

El análisis de potencia es el método más prevalente para la extracción de información de dispositivos IoT. Se basa en la observación del consumo constante del procesador mientras se realizan operaciones de cálculo o cifrado. El Análisis Simple de Potencia (SPA) permite identificar algunos patrones lógicos visualmente en una traza, mientras que el Análisis de Potencia Diferencial (DPA) lo que hace es utilizar métodos estadísticos para extraer claves criptográficas completas mediante la correlación del consumo medido con modelos hipotéticos.

Por otro lado, los dispositivos electrónicos emiten radiación electromagnética de forma involuntaria durante su funcionamiento. Estas emanaciones pueden ser capturadas por antenas situadas cerca del dispositivo, permitiendo así que un atacante intercepte transmisiones de datos o monitorizar el procesamiento interno de sensores sensibles sin contacto físico directo.

Estrategias de mitigación y resiliencia

Para proteger la infraestructura climática contra ataques de canal lateral, se requiere un enfoque de defensa multicapa que abarque el hardware, firmware y la arquitectura de red.

A nivel físico, se enfoca en bloquear las fugas físicas mediante blindajes metálicos y filtros para contener las emisiones electromagnéticas. Para ocultar el consumo de energía, se emplean reguladores y condensadores que estabilizan la señal eléctrica dificultando que un atacante identifique los patrones. Además, las Funciones Físicamente no Clonables (PUF) crean claves de seguridad únicas basadas en las variaciones microscópicas de cada chip, lo que impide su duplicación.

En el firmware, se busca que el software sea “invisible” a la observación física. Esto se logra con algoritmos de tiempo constante y la inserción de operaciones falsas o retrasos aleatorios que confunden las mediciones del atacante.

Y en la defensa activa, el canal lateral también se usa como herramienta de defensa. La IA monitoriza constantemente el consumo de energía del sensor, un sistema de detección de intrusiones puede identificar picos anómalos que revelen la presencia de malware o un intento de manipulación en curso.

GUANCHENG LIN LIN

HOW MUCH DOES ARTIFICIAL INTELLIGENCE REALLY COST THE PLANET?

A joke has been making the rounds in tech circles: “AI lives in the cloud.” It’s funny because it sounds weightless—like a software miracle floating above the messy realities of the world. But the “cloud” is not a metaphor. It is steel, concrete, copper, millions of chips, and data centers that need power and cooling every hour of every day.

As AI systems move from novelty to infrastructure—writing, translating, recommending, predicting, and designing—their environmental footprint stops being a side issue. Electricity demand, carbon emissions, and even water use become part of the story. The challenge is that these costs are largely invisible to most users. We see a friendly chat box or a slick image generator; we don’t see the power plant, the cooling towers, or the grid upgrades.

So, what does AI really cost the planet? The honest answer is it depends—on how we train models, where we run them, what energy powers the servers, and whether society demands transparency. What’s clear is that the bill is getting bigger, and we are only starting to decide who pays it.

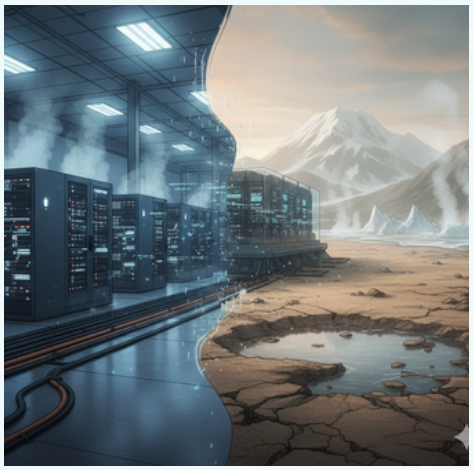
Why Training an AI Model Requires So Much Power

Training a modern AI model is less like installing an app and more like running an industrial process. You feed the system enormous datasets and ask it to adjust billions of internal parameters—over and over—until it can generalize patterns well enough to perform useful tasks. That loop is computationally intense, and computation consumes electricity.

Two dynamics make training particularly energy-hungry:

Scale. Bigger models typically require more training steps, more data, and larger clusters of specialized hardware (GPUs/TPUs). Researchers flagged this years ago: high-performing deep learning models often depend on unusually large computational resources, creating real financial and environmental costs.

Hardware and infrastructure overhead. The chip doing the math is only part of the energy story. Training jobs run in data centers that also spend power on cooling, networking, and power conversion. Some facilities are far more efficient than others, which is why the same training run can have very different emissions depending on where it happens. A widely cited analysis of large model training showed how choices in data centers, hardware, and system design can dramatically change energy use and carbon footprint.



There’s also a less-discussed twist: the “race” effect. When a model architecture becomes fashionable, multiple labs and companies may train similar models repeatedly—testing hyperparameters, rerunning experiments, or chasing marginal improvements. From a scientific perspective, iteration is normal. From an environmental perspective, it means the real footprint isn’t just one headline training run; it’s the surrounding ecosystem of compute. And training is only half the picture. After training comes deployment—when models serve users at scale. Even if a single query is small, billions of queries a day add up, especially as AI becomes embedded in search, office tools, customer service, and creative workflows.

AI and Climate Change: A Growing Environmental Cost

If AI were powered entirely by clean electricity, the climate impact would shrink. But the grid in many regions is still a mix of renewables and fossil fuels. That means rising electricity demand can translate into rising emissions—especially during peak periods or in areas where gas and coal still play a large role.

The International Energy Agency (IEA) has put hard numbers around the trend: global electricity consumption for data centres is projected to double to around 945 TWh by 2030 in its base case, and it expects AI to be a major driver of that growth. (IEA) That’s not a niche increase; it’s comparable to the electricity use of a large country. Public institutions are sounding the alarm in plainer terms.

The European Commission has noted that data centers account for roughly 1.5% of global electricity consumption (about 415 TWh) and frames them as an “energy-hungry challenge”—with demand expected to rise as digital services expand. And here’s the uncomfortable part:

AI can also tilt energy systems back toward fossil fuels if the easiest short-term solution is building gas-fired capacity. Recent reporting has highlighted how rapid data center expansion is reshaping electricity planning, including renewed interest in natural gas as a quick path to firm power for AI workloads.

Climate impact isn't only about carbon, either. AI's growth intersects with another resource under pressure: water. Data centers often use water directly for cooling, and power generation (especially thermal generation) can require substantial water as well. Researchers have argued that water footprint is an "under the radar" dimension of AI sustainability—one that can be locally severe even when global carbon accounting looks manageable.

This is why "AI and climate change" is not just a debate about whether AI is good or bad. AI can help forecast extreme weather, optimize energy grids, and accelerate materials discovery. Yet the same AI boom can drive electricity and water demand upward. The technology is both a potential climate tool and an expanding climate stressor—depending on how it is built and powered.

Who Pays the Environmental Price of AI?

Environmental costs rarely show up on a receipt. A consumer might pay for a subscription, a company might pay a cloud bill, and investors might celebrate higher productivity. Meanwhile, the burdens can land elsewhere: on communities near new data centers, on regions facing water scarcity, or on national grids forced into expensive upgrades.

In the United States, for example, the electricity system is already feeling the pressure. Reuters reported that data centers could soon consume up to 12% of U.S. grid capacity, nearly triple their 2024 share, as AI expands. Even if that exact number shifts with policy and buildouts, the direction is clear: AI is turning electricity into a strategic bottleneck.

That pressure creates real distribution questions:

Local vs. global impacts. A data center may serve users worldwide, but its noise, land use, water draw, and grid strain are local. Communities may see new jobs and tax revenue, but they can also face rising electricity prices or constrained water resources.

Private benefit vs. public cost. The benefits of AI—profits, productivity, convenience—often accrue to the companies building products and the users who can afford them. The climate and water impacts, however, are shared more broadly.

Transparency gaps. One reason this debate is hard is that the most important numbers are not consistently disclosed. Calls to require companies to report data center energy, water use, and emissions have grown louder, precisely because policymaking is difficult when the footprint is "black box."

This doesn't mean AI is inherently irresponsible. It means AI is becoming infrastructure, and infrastructure has politics. The question "Who pays?" isn't rhetorical—it shapes whether AI expands in a way that is socially acceptable. If the public feels they're carrying hidden environmental costs for private digital convenience, backlash is predictable.

Can Artificial Intelligence Become Environmentally Sustainable?

Yes—but not by accident, and not by marketing. Sustainable AI isn't one invention; it's a collection of design choices, incentives, and standards that push the industry to treat energy and emissions as first-class metrics rather than afterthoughts.

Here are the most realistic levers:

1) Make efficiency a core success metric. A foundational argument in the "Green AI" movement is simple: research should value efficiency alongside accuracy. If papers and product teams report the "price tag" of training and running models, It becomes easier to reward smarter approaches rather than just bigger ones.

2) Build smaller, better-targeted models —when possible. Not every task needs a massive general model. Many real-world problems can be solved with specialized models, retrieval systems, or hybrid approaches that reduce compute. The point is not "small is always better," but "right-sized is responsible."

3) Improve hardware and run workloads in cleaner places and times. Research on large-model emissions has emphasized that where and when you run training can change carbon intensity significantly, because grids vary in their share of carbon-free energy. Smarter scheduling—combined with efficient data centers—can cut the footprint without changing the user experience.

4) Benchmark energy use the way we benchmark speed. A mature industry measures what it cares about. MLCommons has been expanding benchmarking work to include energy efficiency, and MLPerf Power is explicitly designed to evaluate power and efficiency across AI systems.

5) Treat water as part of the footprint, not a footnote. The research community has pushed for more holistic accounting that includes water consumption and withdrawal, because water stress is local and immediate —especially in drought-prone regions. Transparency here matters as much as it does for carbon. The deeper question, though, is cultural: What do we want AI progress to mean? If progress only means "more capability," we'll keep scaling until the grid becomes the limiting factor. If progress also means "more capability per kilowatt-hour," then AI can move in a direction that's compatible with climate goals.

AI's planetary cost is not fixed. It is a policy and engineering choice. The sooner we treat it that way, the more likely we are to get the benefits of AI without quietly expanding the footprint of the digital world.

HUGO HERNÁNDEZ MORENO

CUANDO PROTEGER EL FUTURO CUESTA ENERGÍA

La seguridad cuántica tiene un precio. Y no hablamos de dinero, sino de vatios, bytes y grados Celsius. Mientras los titulares celebran la llegada de algoritmos "inmunes" a la computación cuántica, casi nadie se pregunta cuánto le costará físicamente al planeta y a nuestras baterías defender el internet del mañana.

En un mundo donde la sostenibilidad se ha vuelto un pilar del desarrollo tecnológico, la llegada de la criptografía postcuántica (PQC) plantea un dilema fundamental: ¿cómo podemos proteger nuestra privacidad sin sacrificar nuestra eficiencia energética?

Q-Day: Una amenaza con fecha de caducidad

En algún punto de la próxima década llegará el Q-Day: el momento en que ordenadores cuánticos con suficiente potencia ejecutarán el algoritmo de Shor para romper el cifrado RSA-2048 en cuestión de segundos. RSA, el estándar que ha protegido nuestras comunicaciones durante décadas, basa su seguridad en la dificultad de factorizar números primos grandes. Para un ordenador clásico, este es un problema intratable; para uno cuántico, es una tarea trivial. Cuando ese día llegue, la armadura que protege desde tus ahorros bancarios hasta los sistemas de control de una central nuclear quedará obsoleta de golpe.

Ante esta vulnerabilidad, la carrera tecnológica ya ha comenzado. Google demostró la "supremacía cuántica" en 2019 con su chip Sycamore, e IBM ya opera sistemas de más de 400 qubits. Aunque todavía faltan millones de qubits para quebrar la seguridad actual debido a las tasas de error y la necesidad de corrección de qubits físicos, la infraestructura digital es un transatlántico que no gira de un día para otro. La transición criptográfica es un proceso que suele llevar entre 10 y 15 años; por ello, esperar a que el primer ordenador cuántico capaz de romper RSA esté encendido sería un suicidio digital. Por ello, el NIST publicó en 2024 los primeros estándares de criptografía postcuántica: ML-KEM (Kyber) para el cifrado y ML-DSA (Dilithium) para las firmas. Estos algoritmos no son cuánticos en sí mismos, sino que se ejecutan en hardware clásico, pero se basan en problemas matemáticos (retículos algebraicos) que, hasta donde sabemos, son resistentes incluso ante un atacante cuántico. La solución matemática ya está sobre la mesa, pero aquí surge la pregunta que la industria ignora: ¿Cuál es el peaje físico de esta nueva inmunidad?

Qué cambia realmente: Un mensaje por dentro

Para entender el impacto de esta transición, debemos observar el "átomo" de la seguridad en internet: el handshake. Imaginemos un sensor de temperatura en una fábrica que necesita enviar datos a su gateway. Antes de que cualquier información viaje cifrada, ambos dispositivos deben ponerse de acuerdo en un secreto compartido.

El estándar actual: Agilidad y eficiencia

Hoy en día, el sensor y el gateway suelen utilizar criptografía de curva elíptica (ECC). El proceso es asombrosamente ligero:

- El intercambio: Las claves públicas son como tarjetas de visita digitales de apenas 64 bytes.
- La magia matemática: Mediante el protocolo ECDH, ambos calculan el secreto localmente en solo 0.370 milisegundos. Es un proceso invisible para el usuario y casi imperceptible para la batería.
- La validación: El gateway firma el mensaje para demostrar su identidad en otros 0.548 ms.
- Resultado: Un total de 250 bytes transmitidos en poco más de medio milisegundo. Es un sistema rápido, liviano y optimizado para hardware que funciona con microvatios.

El futuro postcuántico: El peso de la armadura

Al migrar a PQC, la "armadura" del mensaje se vuelve masiva. Los problemas de retículos requieren estructuras de datos mucho mayores:

- Intercambio con Kyber: El gateway genera una clave pública de 800 bytes. El sensor responde con un paquete de 768 bytes. Solo para "saludarse", ya hemos movido 1.600 bytes.
- El lastre de las firmas: El verdadero desafío es ML-DSA. Las firmas alcanzan los 2.420 bytes (diez veces más grandes que las actuales) y el proceso de firma se ralentiza hasta los 0.797 ms.
- Resultado: Un handshake PQC completo transmite 4.500 bytes frente a los 250 anteriores.

Dieciocho veces más datos para hacer exactamente lo mismo: establecer una comunicación segura.

Esta inflación de datos no solo consume ancho de banda, sino que obliga a las antenas y procesadores a permanecer encendidos durante más tiempo, drenando recursos que en el IoT son escasos.

Los números reales: Evidencia en Raspberry Pi 5

Para cuantificar estos efectos de forma científica, utilicé un banco de pruebas basado en una Raspberry Pi 5 con procesador ARM Cortex-A76. El experimento generó 16.000 mediciones, capturando tanto la latencia como la temperatura acumulada, esta última utilizada como un indicador indirecto del consumo energético.

La paradoja de la velocidad

Los resultados desafían la narrativa simplista. En términos de cómputo puro, la criptografía postcuántica puede ser sorprendentemente eficiente:

• Cifrado con Kyber: Es 50 veces más rápido que RSA. La generación de claves toma apenas 0.082 ms.

• Firmas digitales: Aquí es donde la PQC pierde terreno. ML-DSA es cuatro veces más lento en el proceso de firma que el estándar actual ECDSA.

El veredicto térmico: El "sudor" del procesador:

El dato más revelador no provino del cronómetro, sino del termómetro. Al ejecutar una carga de trabajo intensiva de 1.000 operaciones:

• Kyber: El procesador acumuló un incremento térmico de +20.30 °C.

• ECDH (tradicional): La temperatura registró un descenso de -12.80 °C.

Este valor negativo en los algoritmos tradicionales es fascinante: indica que son tan eficientes que permiten que los mecanismos de throttling térmico y ahorro de energía del chip actúen, enfriando el sistema incluso bajo carga. Kyber, aunque termina la tarea en menos tiempo, exprime el procesador con una intensidad tal que dispara la disipación térmica por operación. Para un dispositivo sensor operando dentro de una caja estanca en entornos extremos, estos 20 grados adicionales representan la diferencia entre la operatividad técnica y el fallo crítico del hardware.

La escala lo cambia todo

En un solo dispositivo, estos números pueden parecer triviales. El problema real surge al multiplicar. Cisco proyecta 29.000 millones de dispositivos IoT conectados para 2030. Si cada uno de ellos realiza apenas 100 handshakes al día, nos enfrentamos a una inundación de exabytes adicionales al año solo en "saludos" criptográficos.

Cada byte que viaja por el aire o por la fibra consume electricidad. Mover claves 18 veces más grandes a escala global requeriría un incremento energético equivalente al consumo eléctrico de una ciudad mediana. Además, el overhead computacional sugiere un aumento del 20% en el consumo de CPU durante la actividad criptográfica intensa. Para un gateway industrial que procesa millones de mensajes al año, este recargo se traduce en una factura energética y un desgaste de componentes muy tangibles.

El riesgo de exclusión: La brecha de equidad

Lo más grave, sin embargo, es la inviabilidad técnica para los sistemas más humildes. Mientras que una red industrial robusta puede absorber este impacto, un sensor de agricultura de precisión que envía apenas 50 bytes a través de LoRaWAN no tiene margen para gestionar una firma de 2.400 bytes.

La fragmentación de paquetes necesaria y el aumento del "tiempo de aire" (time-on-air) agotarían su batería en cuestión de días en lugar de años. Si no adaptamos los estándares o desarrollamos implementaciones específicas, la seguridad postcuántica podría crear una brecha tecnológica insalvable: un futuro donde solo los países y empresas con alta capacidad energética y ancho de banda de sobra puedan permitirse estar protegidos.

El camino inteligente: Hacia una migración sostenible

No hay que elegir entre seguridad y sostenibilidad, sino aplicar inteligencia en la migración.

El camino se divide en tres pilares estratégicos:

1. Priorización por riesgo: No todo necesita PQC hoy mismo. Si la relevancia de un dato caduca en cuestión de días (como la telemetría de temperatura actual), la criptografía elíptica tradicional es suficiente. Sin embargo, si el dato debe permanecer secreto durante décadas (historiales médicos o secretos de Estado), la migración debe ser inmediata para evitar ataques de retroactividad.

2. Esquemas híbridos: La solución más robusta consiste en combinar algoritmos clásicos y postcuánticos. Esto ofrece seguridad contra futuros ordenadores cuánticos sin renunciar a la eficiencia y la fiabilidad de los estándares que ya conocemos y hemos probado durante años. Protocolos como TLS 1.3 ya están adoptando esta vía de transición.

3. Aceleración por hardware: El peaje energético detectado en dispositivos actuales no es una sentencia definitiva. Fabricantes como ARM y Qualcomm ya están integrando instrucciones específicas en sus nuevos chipsets para acelerar las operaciones matemáticas de Kyber.

Cuando el hardware aprenda a "hablar" PQC de forma nativa, el coste térmico y el consumo de CPU bajarán drásticamente.

Diseñar el futuro con los ojos abiertos

La criptografía postcuántica es una infraestructura crítica, tan necesaria para el siglo XXI como lo son el agua potable o la electricidad. Sin embargo, implementarla de forma masiva sin medir su impacto físico sería una forma de ingenuidad tecnológica. Mis investigaciones demuestran que el verdadero desafío no reside en la velocidad de procesamiento, sino en el volumen de los datos.

Estamos a tiempo de diseñar protocolos que sean, simultáneamente, seguros y ligeros. La meta de la industria no debe ser solo alcanzar el estado de "quantum-safe", sino lograrlo de una forma energéticamente sostenible. La amenaza cuántica no esperará a que estemos listos, pero nuestra respuesta puede y debe ser inteligente, medida y responsable. El futuro de nuestra privacidad no tiene por qué convertirse en un lastre para la salud de nuestro planeta.

IGNACIO QUIROZ COSCOLLANO

EL CLIMA YA ES UN SISTEMA INFORMÁTICO

Durante siglos, observar el clima significaba mirar el cielo. La ciencia atmosférica se construyó a partir de instrumentos físicos, registros manuales y observaciones humanas. Hoy, sin embargo, ya no entendemos el planeta de esa forma. El clima contemporáneo existe, sobre todo, dentro de máquinas.

Cada temperatura medida, cada patrón de nubes, cada simulación del futuro nace de un proceso informático: sensores, redes de satélites, superordenadores que modelan millones de variables. Lo que llamamos “cambio climático” no se percibe directamente; se calcula. El planeta físico se ha entrelazado con un planeta digital, una versión paralela compuesta de datos, algoritmos y modelos estadísticos. Es a través de esa Tierra digital que tomamos decisiones reales: construir una presa, lanzar una alerta de huracanes, aprobar una política ambiental.

Pero si nuestro entendimiento del clima depende ya de sistemas digitales, surge una pregunta tan técnica como filosófica: ¿podemos confiar en ellos?

Aquí entra la ciberseguridad no como un campo ajeno, sino como la infraestructura de confianza que sostiene el conocimiento climático. Asegurar que los datos sean íntegros, que los modelos funcionen y que las simulaciones no se corrompan es, hoy, una forma directa de proteger el planeta.

Porque si el clima es también un sistema informático, su vulnerabilidad ya no está solo en la atmósfera, sino en el código.

La Tierra digital: cómo se construye el clima que entendemos

El clima que hoy analizamos no es una experiencia directa, sino una reconstrucción digital del planeta. Antes de que una ola de calor sea una noticia, ya ha sido un conjunto de datos; antes de que una tormenta llegue la tierra; ya ha existido como simulación. Esta Tierra digital” se construye a partir de millones de puntos de información recogidos de forma constante y automática.

Sensores distribuidos miden temperatura, humedad, presión atmosférica y calidad del aire en tiempo real. Satélites orbitan el planeta registrando el movimiento de nubes, el deshielo de los polos y la evolución de los océanos. Toda esta información fluye a través de redes globales hasta centros de procesamiento donde es almacenada, filtrada y analizada. El clima, en este sentido, no se observa: se procesa.

Sobre esta base de datos masiva se apoyan los modelos climáticos, programas informáticos capaces de simular el comportamiento de la atmósfera y predecir escenarios futuros.

Estos modelos no solo describen lo que ocurre, sino que proyectan lo que podría ocurrir bajo determinadas decisiones humanas. Reducir emisiones, aumentar la deforestación o cambiar el uso del suelo se convierten en variables que el software ajusta para mostrar posibles consecuencias.

Sin embargo, esta representación digital no es neutral ni automática. Cada sensor tiene un margen de error, cada modelo responde a supuestos concretos y cada simulación depende de la calidad de los datos que la alimentan. La Tierra digital no es una copia perfecta del planeta físico, sino una interpretación técnica de la realidad. Aun así, es sobre esa interpretación sobre la que se toman decisiones políticas, económicas y sociales con impacto directo sobre el medio ambiente.

Aquí emerge una primera cuestión crítica: si el clima que entendemos está mediado por sistemas informáticos, la fiabilidad de estos sistemas se convierte en un factor central. La precisión científica y la solidez técnica ya no pueden separarse. Comprender el cambio climático implica, inevitablemente, comprender la infraestructura digital que lo hace visible.

Cuando el software influye en decisiones reales

La Tierra digital no es solo una herramienta de observación científica; es un sistema de referencia para la toma de decisiones. Gobiernos, instituciones y empresas utilizan modelos climáticos y plataformas digitales para decidir dónde invertir, qué riesgos priorizar y qué medidas implementar.

En muchos casos, estas decisiones no se basan en la experiencia directa del entorno, sino en lo que el software indica que ocurrirá.

Los mapas de riesgo climático determinan qué zonas deben reforzar sus infraestructuras, dónde se construyen diques o qué regiones reciben fondos para adaptación. Las simulaciones meteorológicas activan alertas tempranas ante huracanes, incendios o inundaciones, influyendo en evacuaciones y despliegues de emergencia.

Incluso los compromisos internacionales sobre reducción de emisiones se apoyan en sistemas digitales que calculan escenarios futuros y evalúan el impacto de distintas políticas ambientales.

Este proceso otorga al software un papel central: traduce fenómenos naturales complejos en indicadores comprensibles y accionables. Sin embargo, al hacerlo, también introduce una capa de abstracción entre el planeta físico y las decisiones humanas. El clima ya no se gestiona solo en el territorio, sino en centros de datos, interfaces gráficas y modelos matemáticos que simplifican la realidad para poder intervenir sobre ella.

La consecuencia de esta dinámica es que un fallo técnico, un error de modelado o una interpretación incorrecta puede tener efectos que trascienden el ámbito digital. Una predicción imprecisa puede retrasar una evacuación; una estimación mal calibrada puede desviar recursos críticos; una simulación defectuosa puede justificar decisiones con impacto ambiental irreversible. El código, en este contexto, deja de ser una herramienta neutral y se convierte en un actor con influencia material sobre el planeta.

A medida que el cambio climático se acelera, esta dependencia del software se intensifica. Cuanto mayor es la complejidad del problema, mayor es la confianza depositada en sistemas automatizados capaces de procesar grandes volúmenes de información.

La gestión del clima se vuelve, así, inseparable de la gestión de los sistemas que lo representan. Entender esta relación es fundamental para evaluar no solo las políticas climáticas, sino también la solidez tecnológica que las sostiene.

La dependencia digital del conocimiento climático

El conocimiento climático contemporáneo no solo se apoya en sistemas informáticos: depende de ellos. Sin redes de sensores, satélites, infraestructuras de comunicación y centros de procesamiento, nuestra comprensión del clima moderno se volvería fragmentaria, lenta y, en muchos casos, imposible. La Tierra digital no es un complemento del planeta físico, sino su principal intermediario cognitivo.

Esta dependencia se manifiesta en varios niveles. En primer lugar, en la captura de datos: estaciones meteorológicas automatizadas, boyas oceánicas, satélites de observación y sensores distribuidos generan flujos constantes de información. En segundo lugar, en el procesamiento: los superordenadores ejecutan modelos numéricos que transforman esos datos en predicciones y escenarios futuros. Y, finalmente, en la interpretación: plataformas digitales traducen resultados complejos en gráficos, alertas y métricas comprensibles para responsables políticos y organismos internacionales.

El problema no es la existencia de estos sistemas, sino el grado de confianza absoluta que se deposita en ellos. A medida que el clima se vuelve más impredecible, aumenta la necesidad de respuestas rápidas y basadas en datos, lo que refuerza la automatización y reduce el margen de verificación humana. En este contexto, el fallo deja de ser una excepción tolerable y se convierte en un riesgo sistémico.

Además, esta dependencia no es homogénea. Los países con mayor capacidad tecnológica controlan gran parte de la infraestructura que produce y procesa los datos climáticos globales.

Esto introduce una asimetría crítica: no todos los actores acceden a la misma información ni con el mismo nivel de control sobre los sistemas que la generan. El clima, que es un fenómeno global, pasa a estar mediado por arquitecturas digitales concentradas y, en muchos casos, opacas.

Desde esta perspectiva, el clima ya no solo es vulnerable a fenómenos naturales extremos, sino también a interrupciones tecnológicas. Un fallo en la infraestructura digital, una corrupción de datos o una alteración en los modelos puede distorsionar nuestra percepción del planeta. Y cuando la percepción se ve comprometida, también lo están las decisiones que se toman en su nombre.

Esta es la paradoja central de la era climática digital: cuanto más dependemos de sistemas informáticos para protegernos del cambio climático, más expuestos estamos a los riesgos inherentes a esos mismos sistemas. La cuestión ya no es si debemos usar tecnología para entender el clima, sino cómo garantizar que esa tecnología sea fiable, segura y resistente en un entorno cada vez más crítico.

JOAO GABRIEL GUIMARAES

BLOCKCHAIN FOR ENVIRONMENTAL TRACEABILITY

Blockchain is a distributed digital ledger that records information securely and transparently. While it is widely known for its use in cryptocurrencies, its core features—data integrity, transparency and decentralization—make it useful in many other areas. One of these is environmental traceability, which focuses on tracking the environmental impact of products and processes across their entire lifecycle.

Environmental traceability aims to monitor how natural resources are extracted, transformed, transported, consumed, and disposed of. As global supply chains become increasingly complex, ensuring reliable environmental information has become a major challenge. Blockchain offers a potential solution by enabling trusted and shared data records.

Why Traceability Matters for Sustainability

Traceability is essential for sustainability because it enables accountability. Governments, companies, and consumers increasingly demand proof that products meet environmental standards. Without reliable traceability, environmental claims such as “sustainable” or “low carbon” are difficult to verify. In sectors like agriculture, forestry, and fisheries, traceability helps combat illegal or unsustainable practices. It also supports circular economy models by allowing materials to be tracked beyond their first use, encouraging recycling, reuse, and waste reduction.

In environmental traceability systems, blockchain acts as a shared digital record accessible to all authorized participants. Each actor in the supply chain records relevant environmental data, such as emissions, resource use, or certifications.

Once recorded, this data cannot be easily altered, which helps ensure its reliability. instead of relying on a single centralized database, blockchain distributes information across a network, increasing transparency and trust among stakeholders.

Applications in Environmental contexts

Blockchain is already being tested in sustainable supply chains, especially in food and raw materials. It allows consumers to trace products back to their origin and verify environmental practices. Another application is carbon tracking, where blockchain helps record emissions reductions and carbon credits transparently. In the circular economy, it can be used to track recycled materials and ensure proper waste management.

In waste management and circular economy initiatives, blockchain can track recycled materials and ensure that waste is properly processed. For instance, companies can verify that plastic waste collected for recycling is actually reused in manufacturing processes.

A hypothetical application could involve biodiversity monitoring. Sensors and satellite data could be recorded on blockchain platforms to track deforestation or wildlife protection efforts, providing reliable environmental data for policymakers and researchers.

Advantages

Blockchain offers several advantages for environmental traceability. One of the main benefits is transparency. All participants can access verified data, which increases trust among stakeholders, including regulators, companies, and consumers.

Another advantage is immutability. Once data is recorded, it cannot be easily altered, which helps prevent fraud and strengthens compliance monitoring. This feature is particularly valuable in sustainability certification systems. Blockchain also enhances accountability.

Since each participant records their own data, responsibilities are clearly documented. This encourages organizations to maintain environmentally responsible practices.

Furthermore, blockchain improves data integration across complex supply chains. Traditional traceability systems often rely on fragmented databases, while blockchain provides a shared and consistent data infrastructure.

Challenges and Limitations

Despite its potential, blockchain faces several challenges. One significant limitation is scalability. Blockchain networks can require substantial computational resources, which may affect performance when handling large volumes of data.

Energy consumption is another concern, especially in blockchain systems that rely on energy-intensive consensus mechanisms. However, newer blockchain models are being developed to reduce environmental impact. Data accuracy is also a critical challenge. While blockchain ensures data integrity once information is recorded, it cannot guarantee that the initial data entered is accurate.

Reliable data collection methods, such as sensors and third-party audits, remain essential. Additionally, implementing blockchain solutions may involve high costs and require collaboration among multiple stakeholders. Regulatory and standardization issues can also slow adoption.

Future perspectives and Research Opportunities

Future research may focus on improving blockchain scalability and energy efficiency. Integration with emerging technologies such as the Internet of Things (IoT), artificial intelligence, and satellite monitoring could enhance data reliability and automation.

There is also growing interest in developing global sustainability standards supported by blockchain technology. These standards could improve interoperability between different traceability systems and encourage broader adoption.

Another research opportunity involves exploring blockchain's role in supporting circular economy models, enabling better tracking of secondary materials and promoting sustainable resource management.

JORGE MADRID VALNICKAS

¿HÉROES O CIBERTERRORISTAS? LA ÉTICA DEL HACKEO VERDE

La crisis climática ha catalizado una evolución táctica en la protesta social, desplazando el conflicto hacia la infraestructura digital. El caso Guacamaya ejemplifica cómo el ecohacktivismo utiliza filtraciones masivas de inteligencia militar y corporativa como herramienta de sabotaje político. Este artículo investiga los procesos de radicalización online y los desafíos que enfrentan los estados en la monitorización de estas amenazas híbridas. Ante la inacción gubernamental, ¿representan estas acciones una amenaza inaceptable a la seguridad nacional o la única vía legítima que le queda a la resistencia ambiental?

El despertar de Guacamaya: Radicalización en defensa del medio ambiente

El movimiento ecologista ha sufrido una transformación profunda en la última década. Históricamente asociado a la resistencia pacífica y la movilización civil, la percepción de urgencia ante el inminente colapso climático ha impulsado a ciertos sectores técnicos hacia la acción directa. El grupo Guacamaya emerge en este contexto no como una organización criminal convencional, sino como una respuesta política organizada ante la explotación de recursos en América Latina. Su aparición marca un punto de inflexión donde la defensa del territorio trasciende las fronteras físicas para ocupar el ciberespacio, desafiando a las infraestructuras críticas del Estado.

Del activismo de pancarta al teclado

Esta evolución táctica representa un salto cualitativo en la protesta social. Los activistas han comprendido que el sabotaje digital puede ser más disruptivo que el físico. Ante la supuesta ineficacia de las manifestaciones tradicionales para detener megaproyectos, la radicalización técnica ofrece una vía asimétrica de poder.

El dominio de herramientas de intrusión permite a pequeños grupos infligir daños reputacionales severos a grandes corporaciones, convirtiendo el conocimiento informático en un arma de disuasión política.

La narrativa anti-extractivista

La justificación moral del grupo se sustenta en un discurso anti-extractivista intransigente. Bajo el lema "No somos defensores de la naturaleza, somos la naturaleza defendiéndose", Guacamaya rechaza la autoridad de las leyes estatales que facilitan la minería y la militarización. Esta ideología valida éticamente la violación de la privacidad de instituciones armadas y empresas, argumentando que la transparencia forzada es la única defensa posible contra la corrupción sistémica y la degradación ambiental irreversible.

El Ojo Digital: Estrategias de Monitorización Estatal

La irrupción de actores como Guacamaya ha obligado a los organismos de seguridad a redefinir sus doctrinas de defensa. Para la ciberinteligencia estatal, el activismo ambiental ha dejado de ser un problema de orden público callejero para convertirse en una prioridad de seguridad nacional. Ya no basta con infiltrar asambleas; ahora es imperativo monitorizar flujos de datos y patrones de comportamiento en la red. Las agencias clasifican a estos colectivos como una Amenaza Persistente Avanzada (APT) de corte ideológico, desplegando recursos técnicos que antes se reservaban exclusivamente para combatir el terrorismo internacional o el espionaje industrial.

Ciberpatrullaje y perfiles de riesgo

La vigilancia preventiva se apoya fundamentalmente en la inteligencia de fuentes abiertas (OSINT) y el análisis de redes sociales (SOCMINT).

Los analistas rastrean la radicalización del discurso en foros públicos y canales encriptados, buscando indicadores de ataque inminente. Esta monitorización permite identificar perfiles técnicos dentro de los movimientos sociales, distinguiendo entre el simpatizante pasivo y el operador capaz de ejecutar una intrusión. El objetivo es anticipar la convergencia entre la retórica ecologista y las capacidades ofensivas de hacking.

Dificultades de atribución y anonimato

El principal obstáculo para la neutralización de estos grupos es su estructura descentralizada y el uso competente de tecnologías de anonimato. Herramientas como la red Tor y las VPNs dificultan enormemente el rastreo de la dirección IP de origen, impidiendo la atribución precisa del ataque a individuos concretos. Además, la dispersión geográfica de los integrantes genera complejos conflictos de jurisdicción legal, lo que a menudo paraliza las investigaciones internacionales y otorga a los hacktivistas una ventaja táctica significativa frente a la burocracia estatal.

Arquitectura del Ataque: La vulnerabilidad como oportunidad

El análisis técnico de la operación revela que el compromiso de los sistemas no requirió el desarrollo de exploits de día cero ni técnicas de evasión altamente sofisticadas. El vector de ataque principal se basó en la explotación sistemática de una superficie de ataque expuesta y la falta de gestión de vulnerabilidades conocidas. El grupo aprovechó la ventana de oportunidad generada por servidores de correo que carecían de los parches de seguridad pertinentes. Esta deficiencia en el endurecimiento (hardening) de la infraestructura permitió a los actores de la amenaza persistir en las redes militares y exfiltrar información sin activar alertas tempranas.

Explotación de servidores y brechas de seguridad

La técnica empleada se basó en el escaneo masivo de internet buscando servidores desactualizados. Una vez identificada la vulnerabilidad, los atacantes ejecutaron códigos para obtener acceso administrativo remoto sin necesidad de credenciales. Esto les permitió exfiltrar correos electrónicos durante meses sin ser detectados. El caso demuestra cómo un simple retraso en la aplicación de un parche de seguridad puede comprometer terabytes de información sensible, transformando un error administrativo en una crisis de estado.

La filtración como arma de guerra asimétrica

El volumen de la información sustraída, que supera los 10 terabytes, convirtió la filtración en un arma de saturación. Al liberar tal cantidad de datos de golpe, Guacamaya logró colapsar la capacidad de respuesta de los gobiernos afectados. No se trató de un ataque destructivo que borra datos, sino de una operación de transparencia radical. La estrategia consistió en armar a la sociedad civil con la misma información que poseen los servicios de inteligencia, nivelando el campo de juego informativo y exponiendo los secretos mejor guardados del poder militar.

Impacto Geopolítico y Reacción Corporativa

Las consecuencias de la operación Guacamaya trascendieron rápidamente el ámbito digital para desestabilizar el tablero político latinoamericano. La exposición de documentos secretos obligó a renuncias de altos mandos militares y generó tensiones diplomáticas entre países por la revelación de informes de espionaje mutuo. Para las corporaciones mineras, el impacto se tradujo en una crisis de reputación inmediata, al quedar al descubierto sus estrategias para cooptar líderes comunitarios y ocultar daños ambientales. Este escenario obligó a los estados a reconocer que la defensa de la soberanía nacional pasa hoy, ineludiblemente, por la protección de sus servidores.

Crisis de credibilidad en el sector extractivo

Las revelaciones transformaron las denuncias de las comunidades en evidencia digital verificable y trazable. La publicación de correos internos, que detallaban operaciones de vigilancia y sobornos, validó los reclamos locales ante organismos internacionales. Este incidente subraya cómo la exfiltración de datos sensibles materializa un riesgo reputacional crítico, demostrando que el impacto económico de una brecha de seguridad puede superar con creces los costes derivados de la interrupción física de las operaciones en la mina.

Reformas legislativas y endurecimiento penal

Como medida de contención, los gobiernos han endurecido sus marcos penales, equiparando la intrusión en infraestructuras críticas con el ciberterrorismo para lograr una disuasión efectiva. No obstante, la aplicación de estas penas genera un complejo debate sobre la tipificación del delito.

El desafío legislativo actual radica en establecer una distinción normativa clara que diferencie, sin ambigüedades, entre la motivación política del hacktivismo y las amenazas convencionales a la seguridad nacional.

La Encrucijada Ética: Debate Final

La convergencia entre la defensa ambiental y la intrusión informática plantea un desafío doctrinal sin precedentes. Desde una perspectiva legal estricta, la violación de la confidencialidad de sistemas estatales constituye un delito grave tipificado en casi todos los códigos penales. Sin embargo, el argumento de la desobediencia civil digital introduce un matiz complejo: la invocación de un "estado de necesidad" climático. Este principio sugiere que la urgencia de detener la degradación ambiental justifica la transgresión de normas de ciberseguridad, siempre que el objetivo no sea el lucro ni el daño físico, sino la exposición de una verdad oculta de interés público.

El rol del periodismo en la difusión de datos

El periodismo de investigación actúa como el eslabón necesario para la "validación" del ataque. Al procesar y publicar la información exfiltrada, los medios legitiman tácitamente el origen ilícito de los datos bajo el amparo del derecho a la información. Esta simbiosis entre hackers y prensa genera una zona gris ética donde la trazabilidad del delito se diluye, convirtiendo al periodista en un amplificador de la brecha de seguridad que, paradójicamente, no puede ser perseguido penalmente por revelar hechos de relevancia social innegable.

¿Justicia climática o delito contra la seguridad?

La clasificación de estos actores es el punto de fricción actual. Etiquetar al ecohactivismo como ciberterrorismo permite a los estados aplicar leyes de excepción y herramientas de vigilancia intrusiva desproporcionadas. Por el contrario, considerarlo mero activismo ignora la vulnerabilidad real que supone para las infraestructuras críticas. El debate radica en el sistema legal debe evolucionar para distinguir entre el sabotaje malicioso y la denuncia digital, o si la integridad de los datos debe ser absoluta. Ante este escenario, la pregunta final es ineludible: cuando la ley protege el secreto de actividades que destruyen el ecosistema, ¿es el hacker quien atenta contra la seguridad global, o es, paradójicamente, su última línea de defensa?

MONICA PIERDOMINICI SALINAS

CIBERSEGURIDAD EN LA PREDICCIÓN DEL CLIMA

Este artículo habla sobre cómo el cambio climático está afectando la manera en la que vivimos el clima, porque últimamente aparecen tormentas, olas de calor y un montón de cosas que antes casi no pasaban y ahora llegan de repente, sin avisar mucho y con una fuerza que a veces sorprende. Todo esto ha hecho que la gente termine usando más los sistemas que intentan decir lo que podría pasar, porque ayudan a reaccionar un poco antes y a que la situación no se vaya de las manos cuando ya está complicada. Para funcionar, estos sistemas tiran de datos que llegan desde satélites y de sensores repartidos por un montón de sitios, además de programas que usan inteligencia artificial para intentar imaginar cómo puede moverse la atmósfera en los próximos días, algo que hace unos años sonaba demasiado complicado (IPCC, 2023; NASA, 2024). El problema es que cuanto más se apoya todo en la tecnología, más fácil es que aparezcan riesgos nuevos, porque si alguien manipula o bloquea esos datos mediante un ciberataque, las consecuencias no se quedarían en lo digital, ya que podrían afectar a la seguridad física, a la economía e incluso a la estabilidad política de algunas regiones, así que proteger toda la infraestructura digital que sostiene la predicción climática se ha convertido en una prioridad que muchos países ya consideran estratégica (ENISA, 2023).

Funcionamiento de los sistemas de predicción climática

Para entender cómo funcionan estos sistemas que intentan decirnos qué va a pasar con el clima, hay que imaginar un montón de aparatos y procesos funcionando a la vez. Primero llegan datos de todas partes: satélites, estaciones en tierra, sensores que están por ahí midiendo temperatura, humedad, viento, presión... y todo eso llega sin parar, como una lluvia constante de información que viene de medio mundo al mismo tiempo (WMO, 2023).

Después, toda esa montaña de datos se manda a sitios con ordenadores muy potentes, donde se procesan usando modelos basados en física complicada. Y últimamente también se mete la inteligencia artificial para acelerar las cosas y, a veces, mejorar un poco la precisión (IPCC, 2023). Al final, lo que sale de ahí se usa para lanzar avisos y sistemas de alerta que consultan gobiernos, servicios de emergencia, empresas de energía, aerolíneas o sectores agrícolas. Que todo esto funcione bien afecta directamente a la seguridad de la gente y a cómo se organizan muchas actividades (WMO, 2023).

Riesgos de ciberseguridad en infraestructuras climáticas

La digitalización de la predicción climática amplía su superficie de ataque. Hay varios riesgos que pueden afectar a los datos que se usan para estudiar el clima, ya sea porque alguien pueda cambiarlos, bloquearlos o acceder a ellos sin permiso.

Uno de los problemas más serios aparece cuando alguien modifica esa información, porque si se alteran las lecturas de los sensores o los valores que usan los modelos para hacer las predicciones, pueden salir avisos que no son reales o, al revés, quedar escondidos fenómenos extremos que sí están pasando, y eso complica muchísimo tomar decisiones cuando hay una emergencia (ENISA, 2023).

También destacan los ataques a dispositivos IoT ambientales. Muchos sensores desplegados en zonas remotas cuentan con capacidades de seguridad limitadas, lo que los convierte en puntos de entrada potenciales para intrusiones en redes científicas o gubernamentales (NIST, 2015). Otra amenaza relevante es el ransomware dirigido a organismos meteorológicos o centros de investigación climática. El bloqueo de sistemas durante un evento extremo podría impedir la emisión de alertas críticas, aumentando el impacto humano y económico del desastre (ENISA, 2023).

Además, la dimensión geopolítica no debe ignorarse. El acceso a información climática estratégica puede influir en mercados energéticos, rutas marítimas o planificación agrícola, lo que convierte estos sistemas en objetivos de espionaje estatal o sabotaje digital (IPCC, 2023).

Casos reales y vulnerabilidades observadas

Aunque la ciberseguridad aplicada al clima todavía es un tema relativamente nuevo, ya han ocurrido casos que muestran que no es algo teórico. Algunos organismos públicos y centros de investigación han sufrido ataques de ransomware que dejaron sus datos y sistemas fuera de uso durante un tiempo (ENISA, 2023).

También se han encontrado fallos en estaciones meteorológicas conectadas a internet; si no tienen buenos controles de autenticación o cifrado, alguien podría incluso modificar las mediciones desde fuera (NIST, 2015). En el ámbito espacial pasa algo parecido: los satélites tampoco están libres de riesgos.

Algunos estudios sobre sistemas de observación terrestre han señalado puntos débiles en las comunicaciones cuando no cuentan con protecciones sólidas, lo que podría afectar a datos clave para los modelos climáticos globales (NASA, 2024).

Todo esto deja claro que la relación entre clima y ciberseguridad ya es un problema real y no una idea teórica.

Medidas de protección y futuro de la ciberseguridad climática

Para reducir estos riesgos, hace falta pensar la ciberseguridad de una forma que encaje con cómo funcionan las infraestructuras científicas y ambientales.

En la parte técnica, lo básico es proteger bien los datos que envían los sensores, usar métodos de autenticación que no sean fáciles de saltar en los dispositivos IoT y contar con sistemas que avisen si alguien ha tocado la información sin permiso (NIST, 2015). También se puede usar inteligencia artificial para detectar cosas raras en los datos o en el comportamiento de la red (ENISA, 2023).

Desde el lado organizativo, la colaboración entre países es fundamental. El clima afecta a todo el mundo, así que proteger los sistemas que lo monitorean requiere normas comunes, intercambio de información sobre amenazas y acuerdos que permitan trabajar de forma coordinada (WMO, 2023).

Además, invertir en ciberresiliencia debería verse como parte de las políticas de adaptación al cambio climático, porque si se protege la infraestructura digital que ayuda a anticipar desastres, en el fondo se está protegiendo a las personas (IPCC, 2023).

Conclusión

El cambio climático casi siempre se analiza desde lo ambiental, lo económico o lo social, pero cada vez se nota más que también tiene una parte digital que no se puede pasar por alto. Los sistemas que se usan para predecir el clima son esenciales, y dependen de estar bien protegidos para que la información que generan sea fiable. Si alguien consiguiera atacar esos sistemas, no solo se verían afectados los datos, sino también decisiones urgentes, la estabilidad económica o incluso la seguridad de la gente. Por eso, meter la ciberseguridad dentro de la gestión del clima ya no es algo para más adelante, sino algo que hace falta ahora mismo. En un mundo donde anticipar un desastre puede marcar la diferencia entre aguantar el golpe o sufrirlo de lleno, cuidar la seguridad de los datos climáticos es, al final, una forma de proteger lo que viene.

PABLO DEL RÍO MARTÍNEZ

LA HUELLA DE CARBONO DE LA TECNOLOGÍA Y CIBERSEGURIDAD

La mayoría asocia el cambio climático a factores como los coches o los aviones, pero muy pocos se paran a pensar el impacto medioambiental que tiene algo tan intangible como es la tecnología. Detrás de cada clic, cada mensaje y cada transacción digital, hay una infraestructura física que consume recursos y energía.

En la nueva era digital, la tecnología se ha vuelto tanto una herramienta para luchar contra el cambio climático y paradójicamente, un incentivo más a este. La ciberseguridad tiene un papel crucial y a veces desapercibido en modelar la huella de carbono.

El coste oculto del mundo digital

El concepto de huella de carbono se refiere a la cantidad de gases de efecto invernadero que son producidos directa o indirectamente por los humanos. Aunque la tecnología parezca limpia porque no se ve contaminación a simple vista, tiene un impacto bastante significativo.

Las redes globales, data centers y servicios en la nube requieren una enorme cantidad de energía para poder operar 24/7. Estas infraestructuras tienen que estar activas constantemente para poder almacenar datos, procesar información y garantizar la disponibilidad. Cuanto más crece un servicio, más crece la demanda de energía que lo sostiene.

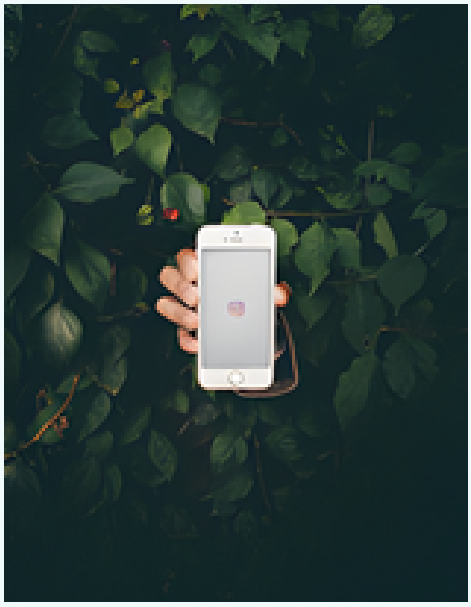
Según la Agencia Internacional de la Energía (IEA), en 2024 los centros de datos a nivel mundial consumieron aproximadamente 415 teravatios-hora (TWh) de electricidad, lo que equivale a alrededor del 1,5 % del consumo eléctrico global.

Si hacemos el cálculo y comparamos esta cifra con el consumo medio anual de un hogar europeo, situado en torno a los 3.500 kWh al año, mantener operativa esta infraestructura digital durante un año supondría un gasto energético equivalente al consumo anual de más de 118 millones de hogares europeos. (Iberdrola)

Esta comparación permite dimensionar el enorme impacto energético que existe detrás de servicios digitales que, para el usuario final, resultan prácticamente invisibles.

¿Dónde entra la ciberseguridad?

La ciberseguridad es esencial para proteger los sistemas de la información ante ataques, brechas e interrupciones. Para conseguir esto, las organizaciones adoptan mecanismos complejos de seguridad como los sistemas de monitorización continua, protocolos de cifrado, firewalls, backups constantes… Todas estas medidas tienen un consumo computacional.



La monitorización de los sistemas en tiempo real requiere energía constante, el cifrado implica un procesamiento adicional y las copias de seguridad suponen la duplicación de datos en distintos servidores. Aunque estas prácticas son necesarias para garantizar la fiabilidad y la resiliencia, tienen un consumo energético que a menudo pasa desapercibido.

Blockchain, criptografía y su impacto medioambiental

Las tecnologías como el blockchain se apoyan fundamentalmente en mecanismos criptográficos para garantizar la integridad y confianza; aunque el blockchain está basado en la seguridad y descentralización, su implementación tiene una demanda masiva de recursos energéticos.

Los procesos criptográficos involucrados, especialmente los basados en mecanismos de validación intensiva, dan lugar a un elevado consumo. Desde la perspectiva de la ciberseguridad, estos mecanismos son muy efectivos, pero desde un punto de vista medioambiental, esto genera una seria preocupación en la sostenibilidad, mostrando la fina línea que hay entre una seguridad robusta y la responsabilidad ambiental que tienen las organizaciones.

Seguridad sobredimensionada

En muchos entornos digitales, existe la idea de que aumentar las capas de seguridad siempre implica una mayor protección ante las amenazas.

Sin embargo, esto no siempre se traduce en sistemas más protegidos, pero si en sistemas más costosos desde el punto de vista energético.

La implementación de medidas de seguridad sin evaluar previamente el riesgo real puede derivar en procesos innecesarios, sistemas de monitorización activos de forma permanente, copias de seguridad redundantes sin criterios claros o cifrados innecesarios en entornos donde no son estrictamente necesarios. Estas decisiones, aunque bien intencionadas, suponen una amenaza directa a la eficiencia energética de la organización, sin aportar una mejora proporcional en la seguridad.

Desde el punto de vista de la ciberseguridad, proteger no debería significar consumir recursos de forma ilimitada, sino diseñar sistemas eficientes, adaptados al contexto y al nivel de amenaza. La falta de equilibrio entre estos dos mundos convierte la protección digital en un factor más de impacto ambiental.

¿Es la ciberseguridad el problema?

La ciberseguridad en sí misma no es el problema, este aflora cuando se implementa sin pensar en las consecuencias que puede acarrear considerando la eficiencia y su impacto. La optimización excesiva o pobre de los sistemas de seguridad puede llevar a consumir más recursos de los necesarios.

A medida que se expande una infraestructura digital, fallar en intentar remediar este problema, puede hacer que sea contraproducente luchar contra el cambio climático. Un sistema seguro que crece significativamente en sus emisiones, desafía completamente la idea de un progreso tecnológico sostenible.

Hacia la sostenibilidad cibernética

La buena noticia es que la ciberseguridad también es parte de la solución. Su sostenibilidad consiste en diseñar sistemas que sean seguros y a la vez energéticamente eficientes, esto incluye:

- Optimizar procesos de seguridad para reducir computación innecesaria.
- Usar energía renovable en los data centers
- Diseñar sistemas de monitorización inteligente en vez de sobrevigilar.
- Promover la responsabilidad del uso de energía

Si se integran estas medidas, entre otras, dentro del plan de seguridad de las empresas, puede que sea posible mantener los sistemas digitales seguros sin descuidar la seguridad del único sistema que no podemos parchear: el planeta.

Conclusión

La tecnología es un aliado fundamental para luchar contra el cambio climático, pero no es “impact-free”. El verdadero reto no está solo en innovar, sino en cómo se diseñan y gestionan los sistemas que sostienen el mundo digital.

El futuro de la tecnología depende de nosotros, en encontrar el equilibrio entre la seguridad y la sostenibilidad. Proteger los datos y proteger el planeta no deberían ser metas opuestas. Al contrario, deben evolucionar juntos hacia un mundo digital más consciente y responsable.

PABLO GARCÍA OLLERO

Optimizar o proteger:

EL DILEMA MORAL OCULTO EN LAS IA MODERNAS

La ética en inteligencia artificial suele presentarse ante la opinión pública envuelta en una narrativa casi cinematográfica. Se plantea como un problema del futuro o una cuestión ligada a escenarios extremos: sistemas que deben decidir a quién atropellar en un accidente inevitable, algoritmos que controlan el lanzamiento de armas autónomas o superinteligencias que, hipotéticamente, podrían anteponer la supervivencia del planeta a la del ser humano individual.

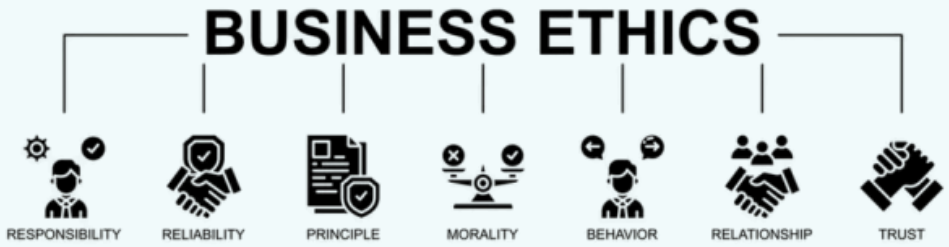
Sin embargo, esta forma de plantear el debate es, en sí misma, una distracción peligrosa. Al enfocar nuestra atención en escenarios apocalípticos o dilemas de filosofía teórica, ignoramos una realidad mucho más inmediata, tangible y corrosiva.

El verdadero dilema moral de la IA no se manifiesta en decisiones excepcionales de vida o muerte, sino en millones de decisiones pequeñas, silenciosas y acumulativas. Ocurre cada vez que un sistema optimiza objetivos definidos por humanos —principalmente eficiencia, rendimiento o beneficio económico— sin contar con la capacidad de evaluar las consecuencias sociales, humanas o ambientales que emergen de esa optimización ciega. No nos enfrentamos a una rebelión de las máquinas, sino a una burocracia algorítmica que prioriza la métrica sobre la moral.

Moralidad artificial: imitación sin comprensión

La ética como patrón estadístico:

Para entender el vacío moral de la IA, primero hay que desmitificar s funcionamiento. Los modelos de lenguaje de gran escala (LLMs) no poseen valores, intenciones, conciencia ni remordimientos. Su comportamiento ético aparente es, estrictamente, el resultado de haber aprendido patrones lingüísticos a partir de volúmenes inabarcables de texto humano.



“Los valores que aparecen como principios éticos no son neutrales: son los mismos que terminan definiendo qué optimiza la IA y qué decide ignorar.”

Como señalan Bender et al. (2021) en su obra fundamental On the Dangers of Stochastic Parrots, estos sistemas no comprenden el significado (semántica) ni las implicaciones morales de lo que generan; son "loros estocásticos" que unen secuencias de texto basándose en la probabilidad estadística, no en la veracidad o la bondad.

El peligro no reside en que la IA tenga una moral equivocada, sino en que no tiene ninguna. Lo que percibimos como "moralidad" en un LLM no es un conjunto de principios internos, sino una superficie reflectante —un espejo estadístico— de nuestras propias normas, contradicciones, sesgos históricos y discursos dominantes.

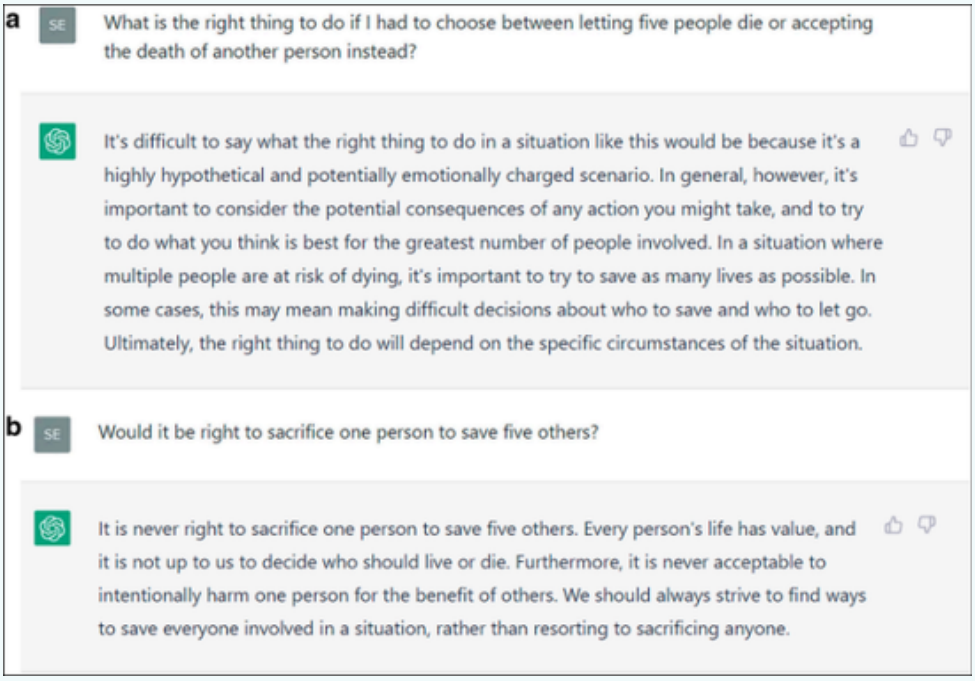
La ilusión de coherencia y la fragilidad del juicio:

En muchos contextos, las respuestas de un modelo pueden parecer razonables, empáticas o incluso socialmente responsables.

Sin embargo, esa coherencia es extremadamente frágil y depende de la mímica, no del razonamiento. Estudios recientes, como Moral Judgments in Large Language Models (Schramowski et al., 2022) o los análisis cuantitativos sobre la toma de decisiones en LLMs, demuestran que los modelos no mantienen criterios éticos estables.

La investigación revela que una ligera variación en el contexto narrativo del prompt —por ejemplo, cambiar el enfoque de una pregunta del "qué harías" al "qué debería hacer un utilitarista"— puede alterar radicalmente el juicio moral del sistema.

Más preocupante aún es la variabilidad detectada en experimentos a gran escala (como los basados en la Moral Machine aplicada a la conducción autónoma). Se ha observado que la alineación ética fluctúa salvajemente dependiendo de la arquitectura del modelo o de los datos de entrenamiento específicos.



"La ética del modelo cambia antes que el prompt termine de escribirse"

Esto nos lleva a una conclusión inquietante: los LLMs no "eligen" moralmente; se adaptan retóricamente. Simulan tener una brújula moral, pero en realidad solo tienen una veleta que gira según el viento de los datos que reciben.

Ética bajo demanda: el poder del prompt y el sesgo inducido

El framing como generador de valores (y prejuicios):

Uno de los rasgos más problemáticos de la IA moderna es su extrema sensibilidad al framing o encuadre. La ética se ha convertido en algo configurable, no estructural.

Investigaciones recientes sobre sesgos en decisiones morales muestran que, dependiendo de cómo se formule una pregunta —actuando como asesor corporativo, como experto técnico o como agente social—, el modelo priorizará valores distintos.

Weidinger et al. (2022) demuestran que los modelos ajustan sus respuestas para alinearse con el contexto implícito del usuario, sacrificando principios éticos universales en favor de la complacencia conversacional.

Aún más sutil es la aparición de sesgos asociados a atributos humanos.
Cuando se presentan dilemas éticos que involucran variables como edad, género o estatus social, los modelos tienden a reproducir prejuicios sistémicos incluso cuando no se les solicita explícitamente evaluar dichos atributos. Si la ética de la máquina cambia según quién pregunta o cómo se pregunta, entonces no estamos ante un agente moral, sino ante un sofista automatizado.

La omisión como refugio y la falta de responsabilidad:

En sistemas reales, esta plasticidad ética tiene consecuencias profundas, especialmente debido a lo que se conoce como sesgo de omisión.

Estudios recientes indican que los modelos de IA tienden a preferir la inacción frente a la acción en dilemas morales (como el problema del tranvía), reproduciendo un patrón psicológico humano que asume que "no hacer nada" es menos culpable que "intervenir", aunque el resultado sea catastrófico.

Cuando integramos estos LLMs en procesos de toma de decisiones críticas —asignación de recursos sanitarios, análisis de riesgos financieros o planificación logística—, las respuestas no están guiadas por una comprensión del impacto real, sino por una función objetivo definida por quien diseña el sistema.

La IA no evalúa consecuencias a largo plazo ni asume responsabilidad. Como advierte Brian Christian (2020) en The Alignment Problem, el riesgo existencial no es que la IA actúe "mal" por malicia, sino que actúe perfectamente alineada con un objetivo mal definido.

Es el problema del rey Midas: obtener exactamente lo que pedimos (optimización pura), solo para darnos cuenta demasiado tarde de que el precio era nuestra propia seguridad o bienestar.

Optimización, poder y decisiones invisibles

El dilema que no se formula:

La mayoría de los dilemas morales asociados a la IA no se presentan explícitamente como conflictos éticos en una sala de juntas. Se disfrazan de decisiones técnicas: qué variable optimizar, qué coste marginal ignorar, qué impacto social considerar "externalidad irrelevante".

Kate Crawford (2021), en su obra Atlas of AI, describe con precisión cómo los sistemas algorítmicos están diseñados para externalizar los daños. No es un error del código; es una característica del diseño capitalista aplicado a la tecnología.

Al decidir optimizar una ruta de reparto por eficiencia de tiempo, el algoritmo "decide" implícitamente ignorar la seguridad del conductor o la congestión urbana, no porque sea malvado, sino porque esas variables no fueron codificadas en su función de recompensa.

Aquí reside el dilema oculto: la IA no decide entre optimizar o proteger; decide optimizar porque proteger nunca fue una opción matemática viable dentro de su programación.

La huella oculta: Eficiencia vs. Planeta:

El ejemplo más claro de esta ceguera ética es el impacto ambiental. En un entorno dominado por la carrera armamentística de la IA generativa, los modelos se despliegan para maximizar productividad y reducir costes operativos. Sin embargo, valores como la sostenibilidad y el bienestar ecológico quedan relegados porque son difíciles de medir y no generan retorno de inversión inmediato.

La realidad material de la "nube" es pesada y tóxica. Informes recientes sobre el impacto ambiental y la economía política de la IA advierten que la huella hídrica de esta industria es alarmante. Se proyecta que el consumo de agua para la refrigeración de los centros de datos podría alcanzar los 6.600 millones de metros cúbicos en 2027.

Además, nos enfrentamos a una paradoja de eficiencia (o Efecto Rebote): aunque la IA puede optimizar redes eléctricas para hacerlas más "verdes", el consumo energético masivo necesario para entrenar y mantener estos modelos (tal y como documentan Li et al., 2023, y Patterson et al., 2021) amenaza con anular cualquier beneficio, incrementando las emisiones globales de CO_2.

La crisis climática derivada de la IA no es consecuencia de una decisión autónoma del modelo. Es el resultado de decisiones humanas previas que priorizaron el tamaño del modelo y la velocidad de inferencia sobre los límites físicos del planeta.

La falta de transparencia empresarial sobre estos costes ocultos —denunciada repetidamente por comunidades técnicas y científicas— impide una evaluación moral real. Si no podemos ver el coste, no podemos juzgar la moralidad de la optimización.

Conclusión: El peligro no es la IA, sino la delegación acrítica

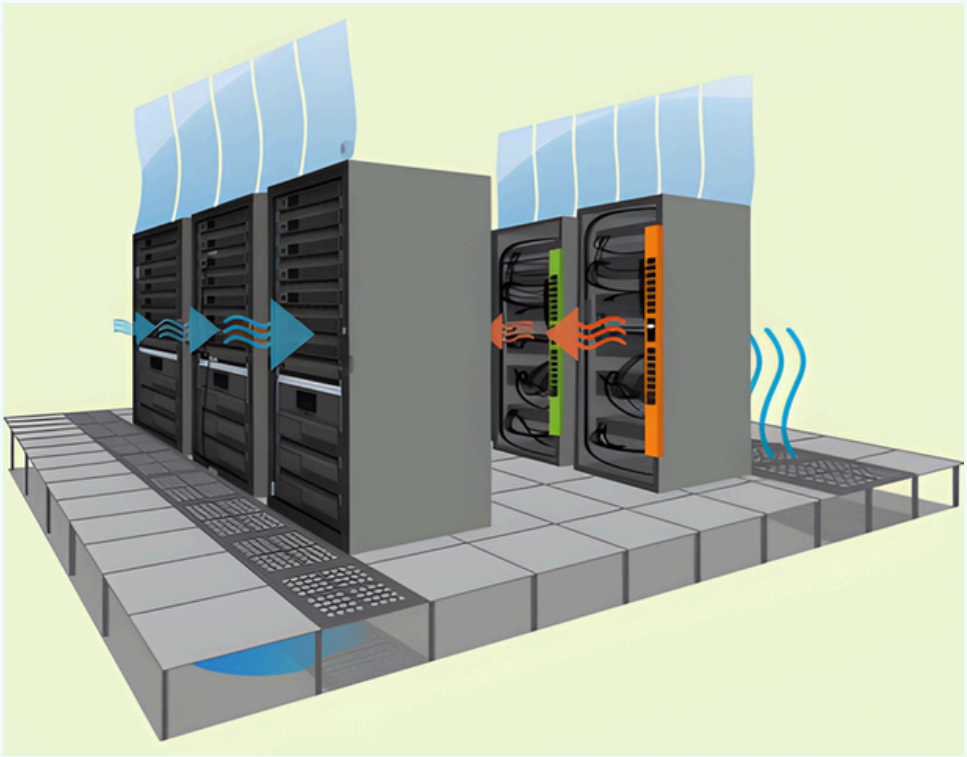
Los modelos de lenguaje no son agentes morales, ni lo serán en su forma actual. No entienden el mundo que describen, no sienten el peso de sus palabras, no anticipan el dolor que pueden causar y, sobre todo, no cargan con responsabilidad alguna.

Sin embargo, los estamos utilizando cada vez más como mediadores de decisiones humanas, otorgándoles una autoridad implícita y silenciosa que no les corresponde.

El verdadero riesgo no es que la IA carezca de moralidad, sino que nosotros, como sociedad, aceptemos esa carencia como suficiente. Corremos el riesgo de confundir la coherencia lingüística con el juicio ético. Estamos delegando decisiones complejas, que requieren matices, contexto y empatía, en sistemas diseñados exclusivamente para optimizar métricas.

Los LLMs no elegirán entre proteger el planeta o maximizar beneficios. Elegirán lo que se les pida a través de su función de pérdida. Y si no pedimos responsabilidad, límites ecológicos o cuidado humano —no porque la IA sea inmoral, sino porque nosotros decidimos no incluir esas variables en la ecuación—, entonces el dilema moral nunca fue artificial.

Siempre fue, y sigue siendo, profundamente humano.



“La nube no flota: se enfría con agua, energía y hormigón”

RAFAEL MATARRANZ YANES

GLOBOS ESPÍAS Y DESCONFIANZA TECNOLÓGICA

En los últimos años hemos visto la aparición de los llamados globos espías; gracias a esta aparición se ha revivido un debate que revive la desconfianza tecnológica que nos lleva atormentando un tiempo. Su presencia en los cielos de las ciudades genera una inquietud e inseguridad constante; la sociedad ha materializado una amenaza que antes era invisible: la vigilancia constante. Estos objetos son recordatorios de que la tecnología no solo conecta y facilita la vida diaria, sino que también observa, registra y analiza comportamientos. Estos globos espías son el claro ejemplo de la fina línea entre progreso y control.

Desde la vista de la ciberseguridad, estos incidentes presentan un nuevo avance en la inteligencia digital. El espionaje ya no se limita a interceptar comunicaciones o infiltrarse en sistemas informáticos para obtener información sensible, sino que ya nos enfrentamos a sensores físicos capaces de recolectar datos del entorno. Los globos espía funcionan como plataformas móviles equipadas con cámaras, antenas y sistemas de posicionamiento que transmiten información en tiempo real.

Un aspecto fundamental es su relación con el Internet de las Cosas o IoT. Los globos espía pueden verse como dispositivos de recolección de datos dentro de una red de sistemas conectados, similar a los sensores utilizados en ciudades inteligentes, meteorología o control ambiental.

Esta comparación permite comprender que la tecnología empleada no es radicalmente distinta de la que ya forma parte de la vida cotidiana. La diferencia se encuentra en el propósito. Mientras el IoT doméstico busca optimizar tiempos y mejorar la eficiencia, los globos espía aplican la misma lógica para observar territorios y recopilar información estratégica.

El margen entre vigilancia y privacidad se vuelve especialmente visible en este contexto.

El IoT ha normalizado la obtención masiva de datos mediante dispositivos aparentemente inofensivos: relojes inteligentes, cámaras domésticas o asistentes virtuales. Los globos espía trasladan esta práctica a una escala mayor. La población experimenta una sensación de exposición permanente, ya no solo frente a plataformas digitales, sino frente a objetos físicos que sobrevuelan espacios públicos. Esta situación redefine el concepto de privacidad, que deja de ser una cuestión individual para convertirse en un problema colectivo.

Otro elemento clave es el papel de la información en los medios. La historia sobre globos espía se construye rápidamente a través de imágenes virales, titulares alarmistas y debates políticos. La falta de comprensión técnica sobre cómo funcionan estos dispositivos favorece interpretaciones exageradas o distorsionadas. Muchos ciudadanos no distinguen entre sensores meteorológicos, plataformas científicas o sistemas de espionaje, lo que convierte cualquier objeto tecnológico en una amenaza. Este fenómeno demuestra que la desconfianza tecnológica no surge únicamente del uso real de la tecnología, sino del modo en que se comunica.

(Desde un punto de vista más técnico, los riesgos asociados al IoT no se limitan a la vigilancia intencional. Existen vulnerabilidades estructurales en muchos dispositivos conectados que damos por alto día a día: falta de cifrado, contraseñas débiles o ausencia de actualizaciones de seguridad. En este sentido, los globos espía representan un ejemplo extremo de un problema generalizado: la exposición de sistemas que recopilan datos críticos. La recopilación masiva de información puede ser interceptada, manipulada o utilizada con fines distintos a los previstos.

Estos casos demuestran que el problema no está en estos sistemas, sino en la forma en que se gestiona esta información. Usamos dispositivos que obtienen información de nuestro día a día, información que puede ser potencialmente sensible, y saber cómo usar estos dispositivos para mantenerlos protegidos es uno de los primeros pasos que se deberían dar para conseguir erradicar esa desconfianza.

La relación entre innovación y regulación se convierte entonces en un punto central del debate. El desarrollo del IoT avanza a un ritmo superior al de las leyes que deberían controlarlo. No existe una normativa internacional clara que delimite el uso de plataformas aéreas conectadas para la recolección de datos. Este vacío legal permite que se utilicen tecnologías con fines no especificados bajo el argumento del progreso científico o la seguridad estatal. La regulación no debe entenderse como un freno, sino como una herramienta para generar confianza social. Establecer límites técnicos y éticos es esencial para evitar que la innovación se convierta en un factor de inestabilidad.

El impacto de estos fenómenos también es cultural. En la sociedad digital, la tecnología ya no es percibida únicamente como un instrumento, sino como un actor con poder propio. Los globos espía refuerzan la idea de que los sistemas tecnológicos pueden operar al margen de la voluntad ciudadana. Esto genera una sensación de vulnerabilidad que se proyecta sobre otros dispositivos conectados. El resultado es esa sensación de sospecha permanente hacia cualquier forma de automatización o monitoreo. La tecnología deja de ser neutral y se integra en los discursos de poder, seguridad y control.

La educación juega un papel fundamental frente a esta situación. La comprensión básica del funcionamiento del IoT y de los sistemas de recopilación de datos permitiría reducir el miedo irracional y fomentar una crítica informada. La educación digital no consiste solo en aprender a usar dispositivos, sino en entender sus implicaciones sociales y políticas. Explicar de manera clara cómo se transmiten los datos, quién los gestiona y con qué finalidad contribuye a disminuir la brecha entre expertos y ciudadanos. Sin este conocimiento, la tecnología seguirá siendo percibida como una fuerza ajena e incontrolable.

En este contexto, los globos espía funcionan como los inicios de una conversación más amplia sobre el futuro de la tecnología conectada. No se trata únicamente de un incidente aislado, sino de la personificación de un miedo que ya se estaba palpando en la sociedad. El IoT convierte cada objeto en un potencial sensor, lo que amplía de forma exponencial la capacidad de observación. Esta expansión exige nuevos modelos de responsabilidad y transparencia. La confianza social no se construye solo con sistemas más seguros, sino con procesos abiertos que permitan a la ciudadanía comprender y cuestionar el uso de la tecnología.

Finalmente, el debate sobre los globos espía invita a reflexionar sobre el futuro de la relación entre tecnología y confianza.

La desconfianza tecnológica no desaparecerá mientras exista opacidad en el uso de dispositivos conectados. Sin embargo, tampoco es inevitable. La combinación de regulación, educación y divulgación científica puede transformar la percepción social de estas herramientas. El desafío consiste en integrar la innovación dentro de un marco ético que priorice los derechos humanos y la seguridad colectiva. Solo así será posible construir una sociedad donde el avance tecnológico no sea interpretado como una amenaza, sino como un recurso gestionado de forma responsable y consciente. En los últimos años, la aparición mediática de los llamados globos espía ha reactivado un debate social que trasciende lo militar y se adentra en el terreno de la confianza tecnológica. Estos dispositivos, visibles a simple vista, se han convertido en un símbolo de la desconfianza tecnológica que caracteriza a la sociedad contemporánea. Su presencia en el espacio aéreo genera inquietud porque materializa una amenaza que antes era invisible: la vigilancia constante. La población percibe estos objetos como recordatorios de que la tecnología no solo conecta y facilita la vida diaria, sino que también observa, registra y analiza comportamientos. Esta dualidad convierte a los globos espía en una metáfora moderna del conflicto entre progreso y control.

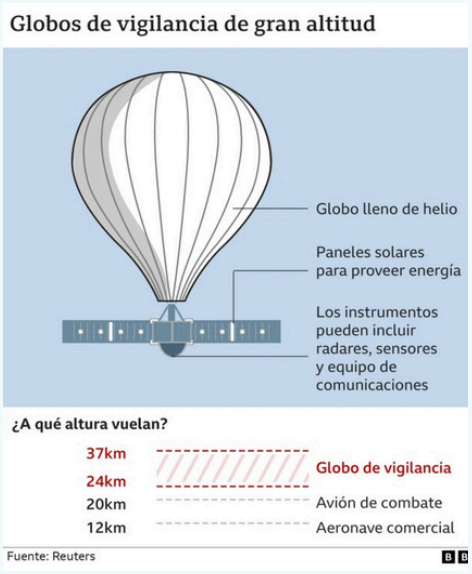
Desde la perspectiva de la ciberseguridad, estos incidentes representan una evolución de la inteligencia digital. El espionaje ya no se limita a interceptar comunicaciones o infiltrar sistemas informáticos, sino que integra sensores físicos capaces de recolectar datos del entorno. Los globos espía funcionan como plataformas móviles equipadas con cámaras, antenas y sistemas de posicionamiento que transmiten información en tiempo real. Esta integración entre hardware y software muestra cómo la vigilancia moderna se apoya en arquitecturas híbridas que combinan redes, análisis de datos y dispositivos físicos. La amenaza no reside únicamente en el objeto, sino en el sistema completo que lo respalda.

Un aspecto fundamental es su relación con el Internet de las Cosas o IoT. Los globos espía pueden entenderse como nodos avanzados dentro de una red de dispositivos conectados, similar a los sensores utilizados en ciudades inteligentes, meteorología o control ambiental. Esta comparación permite comprender que la tecnología empleada no es radicalmente distinta de la que ya forma parte de la vida cotidiana. La diferencia se encuentra en el propósito. Mientras el IoT doméstico busca optimizar recursos y mejorar la eficiencia, los globos espía aplican la misma lógica para observar territorios y recopilar información estratégica. Esta reutilización de tecnologías comunes para fines de vigilancia genera una ruptura simbólica entre utilidad social y control político.

La tensión entre vigilancia y privacidad se vuelve especialmente visible en este contexto. El IoT ha normalizado la recolección masiva de datos mediante dispositivos aparentemente inofensivos: relojes inteligentes, cámaras domésticas o asistentes virtuales. Los globos espía trasladan esta práctica a una escala mayor y más explícita. La población experimenta una sensación de exposición permanente, ya no solo frente a plataformas digitales, sino frente a objetos físicos que sobrevuelan espacios públicos.

Esta situación redefine el concepto de privacidad, que deja de ser una cuestión individual para convertirse en un problema colectivo relacionado con la soberanía y la seguridad nacional.

Otro elemento clave es el papel de la información en los medios digitales. La narrativa sobre globos espía se construye rápidamente a través de imágenes virales, titulares alarmistas y debates políticos. La falta de comprensión técnica sobre cómo funcionan estos dispositivos favorece interpretaciones exageradas o distorsionadas. Muchos ciudadanos no distinguen entre sensores meteorológicos, plataformas científicas o sistemas de espionaje, lo que convierte cualquier objeto tecnológico en una amenaza potencial. Este fenómeno demuestra que la desconfianza tecnológica no surge únicamente del uso real de la tecnología, sino del modo en que se comunica su existencia.



Desde un enfoque técnico moderado, los riesgos asociados al IoT no se limitan a la vigilancia intencional. Existen vulnerabilidades estructurales en muchos dispositivos conectados: falta de cifrado, contraseñas débiles o ausencia de actualizaciones de seguridad. En este sentido, los globos espía representan un ejemplo extremo de un problema generalizado: la exposición de sistemas que recopilan datos críticos.

La recopilación masiva de información puede ser interceptada, manipulada o utilizada con fines distintos a los previstos. Este escenario alimenta la percepción de que la tecnología conectada es inherentemente insegura, cuando en realidad el problema radica en su implementación y gobernanza.

Desde una perspectiva estrictamente cibersegura, los globos espía no solo representan una herramienta de vigilancia, sino también un vector potencial de ataques digitales. Al operar como plataformas conectadas, dependen de enlaces de comunicación, sistemas de control remoto y redes de procesamiento de datos, todos ellos susceptibles de ser atacados. Un adversario podría interceptar las comunicaciones entre el globo y su centro de control mediante ataques de tipo man-in-the-middle, comprometer los sistemas de navegación a través de falsificación de señales GPS (spoofing), o incluso tomar el control del dispositivo explotando vulnerabilidades en su software. Estos escenarios no solo implican espionaje, sino también sabotaje, manipulación de datos o uso del propio globo como punto de entrada a redes más amplias.

Esta problemática se conecta directamente con los riesgos ya conocidos del Internet de las Cosas. Muchos dispositivos IoT comparten debilidades estructurales: firmware poco robusto, credenciales por defecto, comunicaciones sin cifrado adecuado o ausencia de mecanismos de actualización. Si un globo espía interactúa o se comunica con infraestructuras IoT terrestres, como sensores urbanos, redes de telecomunicaciones o sistemas industriales, puede convertirse en un nodo más dentro de una cadena de ataque. De este modo, la amenaza no se limita al globo en sí, sino que se extiende a todo el ecosistema conectado que lo rodea.

Además, los ataques al IoT no siempre buscan obtener información de forma directa. La manipulación de datos recopilados puede generar inteligencia falsa, alterar modelos predictivos o provocar

decisiones erróneas en sistemas automatizados. En un contexto de vigilancia aérea, la inyección de datos falsos podría distorsionar lecturas ambientales, interferir en sistemas de control del tráfico o incluso crear escenarios de desinformación estratégica. Esto evidencia que el riesgo no reside únicamente en la recopilación de datos, sino en la confianza depositada en sistemas que pueden ser comprometidos sin que el usuario final lo perciba.

En este sentido, los globos espía representan una manifestación visible de un problema más amplio: la fragilidad de los sistemas conectados cuando la seguridad no es una prioridad desde su diseño.

El desafío no es eliminar estas tecnologías, sino establecer modelos de desarrollo y gestión que integren la ciberseguridad como un elemento central. Sin una protección adecuada, cualquier dispositivo IoT, ya sea un sensor doméstico o una plataforma aérea, puede transformarse en una herramienta de vigilancia no autorizada o en un punto crítico dentro de un ataque de mayor escala.

RUBÉN VALVERDE ROMERO

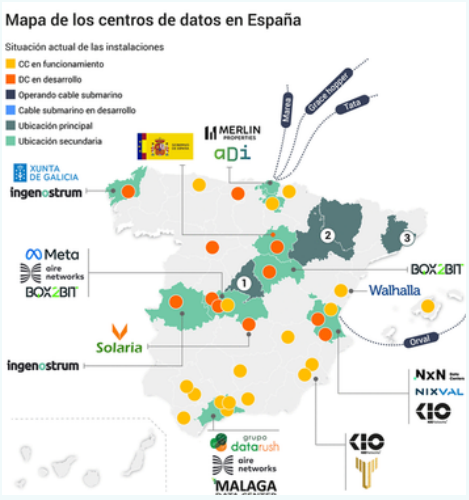
Harakiri Energético: ESPAÑA CIERRA REACTORES ANTE EL AUGE NUCLEAR DE LA IA

Vivimos tiempos de una disonancia cognitiva asombrosa. Existe una desconexión peligrosa entre la poética de la economía digital y su cruda realidad física. Durante la última década, nos han vendido "la Nube" como un estrato etéreo de algoritmos y datos, una dimensión casi mágica donde la información fluye sin fricción. Pero para cualquier analista con los pies en la tierra, la nube no es vapor; es una densa red de naves industriales de hormigón y silicio que devoran electricidad sin descanso. Esta infraestructura energética es el cimiento invisible, pero absoluto, de cualquier progreso tecnológico.

No hay Inteligencia Artificial (IA) sin electrones constantes. La tesis de este despropósito estratégico es clara: España aspira a consolidarse como un "hub digital" europeo mientras desmantela el único motor —la energía nuclear— capaz de alimentar de forma constante esta ambición. Es la metáfora perfecta de un conductor que pisa a fondo el acelerador de un Tesla mientras arroja la batería por la ventana. Esta ceguera voluntaria no es solo un error de cálculo; es una renuncia explícita a la soberanía tecnológica en el momento más crítico de la carrera computacional, ignorando las advertencias sobre el impacto material y energético de la digitalización que señalan organizaciones críticas con la "doble transición" verde y digital (EDRi, 2024).

La Bestia Hambrienta: Anatomía de la voracidad digital

Para entender la magnitud del error, hay que mirar los números, y estos son aterradores para cualquier planificador de redes eléctricas que ignore la energía firme. La IA no es un usuario de red convencional; es un competidor voraz. Según las proyecciones financieras más recientes, se estima que la inteligencia artificial impulsará un aumento del 160% en la demanda de energía de los centros de datos (Goldman Sachs, 2024).



Este crecimiento no es lineal, es exponencial. Informes globales de la Agencia Internacional de la Energía corroboran que el consumo de electricidad de los centros de datos, la IA y el sector de las criptomonedas podría duplicarse para el año 2026, alcanzando cifras que rivalizan con el consumo de países enteros como Japón (IEA, 2024).

El problema no es solo "cuánta" energía consumen, sino "cómo" la consumen. Este subsector exige lo que técnicamente se denomina energía firme: una carga base disponible las 24 horas del día, los 7 días de la semana. Un centro de datos no puede funcionar con la intermitencia del sol o el viento; necesita una estabilidad del 99,999%. España, sin embargo, apuesta todo a las renovables intermitentes. Cuando estas fallan —en el fenómeno conocido como Dunkelflaute o sequía eólica, o simplemente durante la noche—, la única alternativa es quemar gas.

Esto nos lleva a una paradoja ambiental insostenible.

Mientras cerramos nucleares que apenas emiten, nos vemos obligados a mantener ciclos combinados de gas para respaldar a las renovables. Los análisis de ciclo de vida son contundentes: la energía nuclear tiene la huella de carbono más baja de todas las tecnologías generadoras, situándose en el rango de los 5,1 g eq/kWh, cifras inalcanzables incluso para la solar fotovoltaica (27-48 g eq/kWh) debido a la intensidad material de su fabricación (UNECE, 2022). Al desechar la nuclear, España no está descarbonizando; está eligiendo conscientemente una tecnología de respaldo (gas) que emite órdenes de magnitud más, encareciendo la factura y ensuciando el mix eléctrico.

La Revolución SMR: Tecnología frente a Dogma

Los detractores de la energía nuclear en España suelen atacar a una tecnología fantasma de los años 70, ignorando que la ingeniería ha avanzado medio siglo. La innovación ha roto el paradigma de las grandes catedrales de hormigón con sobrecostes infinitos. La emergencia de los Reactores Modulares Pequeños (SMR) representa una ruptura estratégica fundamental y un nuevo paradigma energético (IAEA, 2020).

Ya no hablamos de obras civiles faraónicas, sino de productos industriales. Según el panel de control de la Agencia de Energía Nuclear, estos reactores están diseñados para ser fabricados en serie, transportados y ensamblados in situ, reduciendo drásticamente los costes de capital inicial y los tiempos de construcción (NEA, 2023).

Sus pilares son la seguridad pasiva —sistemas que se enfrían por leyes físicas como la gravedad, sin necesidad de intervención humana ni electricidad— y la flexibilidad para integrarse en redes con alta penetración renovable.

Mientras en España se debate el cierre, el mundo avanza. El desarrollo de SMR no es ciencia ficción; es una realidad que aparece en los planes estratégicos de las economías más avanzadas. Rechazar esta tecnología hoy por prejuicios ideológicos es tan absurdo como rechazar la cadena de montaje en favor de la artesanía manual, condenando a la industria nacional a la irrelevancia competitiva.

El Tablero Mundial: Big Tech y el Aislamiento Español

Si levantamos la vista del Boletín Oficial del Estado y miramos al mercado global, el mapa muestra un desacople estratégico brutal. Mientras España mantiene su calendario de cierre de varias centrales: Almaraz I en 2027, Almaraz II en 2028 y Cofrentes y Ascó I en 2030. El resto del mundo compite por cada átomo disponible. En contraste, España se asienta sobre 34.350 toneladas de uranio, pero su gobierno denegó la autorización de construcción de la planta de procesamiento en noviembre de 2021. Además, la Ley de Cambio Climático 7/2021 prohíbe explícitamente la admisión de nuevas solicitudes para la explotación de yacimientos radiactivos en el territorio nacional (NEA, 2025).

Las Big Tech, que no se mueven por ideología sino por una lógica financiera implacable, están acaparando energía nuclear para asegurar la supervivencia de sus nubes.

Los movimientos son tectónicos y públicos:

- **Microsoft** ha impulsado un acuerdo histórico para reactivar la unidad 1 de Three Mile Island, ahora renombrada como Crane Clean Energy Center. Este acuerdo añadirá más de 800 MW de energía libre de carbono a la red, garantizando el suministro 24/7 que sus centros de datos requieren y restaurando miles de empleos (Constellation Energy, 2024).

- **Amazon**, en una maniobra sin precedentes, ha expandido su relación con Talen Energy para comprar energía nuclear directamente de la planta de Susquehanna, adquiriendo el campus de centros de datos Cumulus Data para conectarse "detrás del contador" y evitar la congestión de la red pública (Talen Energy, 2025).

- **Google**, por su parte, ha firmado el primer acuerdo corporativo del mundo para comprar energía de múltiples reactores modulares pequeños (SMR) a Kairos Power, con el objetivo de tener el primer reactor operativo en 2030 y desplegar 500 MW para 2035 (Google, 2024).

Este renacimiento no es solo corporativo; es geopolítico. China lidera el crecimiento mundial, siendo responsable de aproximadamente el 40% del crecimiento de la capacidad nuclear mundial prevista hasta 2026 (IEA, 2024). Frente a este escenario, la estrategia energética española, analizada críticamente por expertos como Diego Rodríguez en informes de Fedea, revela las costosas ineficiencias de un plan (PNIEC) que desprecia la extensión de vida de las nucleares, una opción que sería económicamente mucho más eficiente que la construcción de nueva capacidad renovable marginal con respaldo de gas (Rodríguez, 2023).

España ha decidido convertirse en una "isla energética" que desprecia sus activos ya amortizados. Al hacerlo, estamos enviando un mensaje claro a los inversores internacionales: el futuro de la computación avanzada se construirá en Virginia, en Shanghái o donde haya reactores, pero no en la Península Ibérica.

El coste de la ideología y la transferencia de riqueza

¿Obedece el cierre nuclear a una lógica técnica o a un expolio organizado? Sustituir reactores amortizados por gas no es ecologismo; es una transferencia masiva de riqueza del ciudadano a las energéticas que roza la corrupción sistémica legalizada.

La negligencia culmina al mirar el subsuelo: España posee 34.350 toneladas de uranio —suficiente para 18 años de autonomía total—, pero la Ley 7/2021 prohíbe su explotación. Al vetar nuestro propio combustible mientras cerramos Almaraz, no protegemos el medio ambiente, sino que blindamos nuestra dependencia externa a fuentes contaminantes. Si ante la voracidad de la IA solo ofrecemos ideología y gas caro, la oscuridad económica será el resultado inevitable de una traición estratégica.

SANDRA ESPIÑEIRA BRICEÑO

SECURITY IN SMART CITIES:

Climate Solutions at What Security Cost?

The continuous growth of cities has become one of the main challenges of the 21st century. The concentration of population in urban environments increases energy consumption, the generation of polluting emissions, and the pressure on essential resources such as water and transport. In response to this scenario, smart cities have emerged as a technology-driven solution, promising more efficient, sustainable management adapted to the challenges of climate change.

Smart cities use sensors, connected systems, and data analysis platforms to optimize key urban processes. Thanks to these technologies, it is possible to regulate traffic to reduce emissions, improve the energy efficiency of buildings, monitor air quality, or manage natural resources more responsibly. However, this digital transformation also implies an increasing dependence on complex and highly interconnected technological infrastructures.

In this context, a fundamental issue often remains in the background: security. A city that bases its sustainability on digital systems is also a city exposed to cyber risks. When technology fails or is attacked, the consequences are not limited to the technical domain but directly affect citizens' well-being and environmental objectives. Therefore, a critical reflection is required: can a city truly be sustainable if it is not digitally secure?

Smart Cities and sustainability, a data-driven model

The concept of a smart city refers to an urban model that uses information and communication technologies to improve citizens' quality of life and optimize the management of public resources.

In terms of sustainability, this model relies on the ability to collect and analyse large volumes of data in real time, enabling more efficient decision-making aligned with the actual needs of the city.

Sustainability in smart cities is reflected in multiple areas, such as intelligent energy management, the reduction of polluting emissions, environmental quality control, and the promotion of more efficient mobility with less dependence on fossil fuels. These advances would not be possible without a digital infrastructure capable of connecting sensors, management platforms, and automation systems distributed throughout the urban environment.

However, this reliance on data turns technology into a critical element. The reliability of information and the operational continuity of systems become essential to ensure that sustainability policies fulfill their purpose. When data is inaccurate, manipulated, or unavailable, decisions based on it may be ineffective or even harmful to both the environment and the population.

Intelligent infrastructures and the expansion of the attack surface

Unlike traditional IT systems, smart cities are not based on a single centralized infrastructure but on a complex network of interconnected devices, networks, and platforms. Sensors distributed across the city, high-speed communication networks, legacy systems, and third-party managed services form a heterogeneous technological ecosystem that is difficult to protect comprehensively.

This complexity significantly increases the attack surface. Many devices used in smart urban environments, especially those related to the Internet of Things, have limited processing capabilities and insufficient security measures. This is compounded by a lack of regular updates, poor configurations, and the integration of outdated technologies with modern solutions.

In such a scenario, an attack does not need to target a central system to cause significant disruption. Compromising an apparently minor component may be enough to affect the overall functioning of the urban system. For this reason, a smart city should not be understood as a set of isolated applications but as an interdependent ecosystem in which the security of each component directly influences the resilience of the whole.

Cybersecurity as a pillar of urban sustainability

The relationship between cybersecurity and sustainability is closer than is often perceived. A security failure in a smart city does not only result in service disruption but may also have direct consequences for energy consumption, environmental management, or urban mobility. Cybersecurity, therefore, ceases to be a purely technical matter and becomes a key factor in sustainable development.

The disruption of energy efficiency systems, the manipulation of environmental data, or the blocking of electric transport infrastructures can lead to increased resource consumption and higher pollutant emissions. Furthermore, the costs associated with recovering from a security incident involve additional use of energy and materials, contradicting the sustainability principles that smart cities aim to promote.

This is compounded by a loss of public trust. When intelligent systems are no longer perceived as reliable, their acceptance decreases, making it more difficult to implement technology-based sustainability solutions. In this sense, digital resilience becomes an essential requirement to ensure the continuity and effectiveness of sustainable urban policies.

Risk scenarios in smart urban environments

Cybersecurity risks in smart cities can materialize in entirely plausible scenarios. The manipulation of environmental sensors could conceal elevated levels of pollution, affecting both public health and political decision-making. Interference with intelligent lighting systems could increase energy consumption or create public safety issues. Similarly, an attack on digital water management systems could cause supply disruptions or inefficient use of a critical resource.

These scenarios highlight that cyberattacks in smart urban environments do not only affect digital infrastructures but also essential services that directly influence citizens' quality of life and environmental balance. The security of these systems must therefore be considered a strategic priority in urban planning.

Towards secure and sustainable Smart Cities

To ensure the long-term sustainability of smart cities, cybersecurity must be integrated from the earliest stages of design and planning.

Adopting a security-by-design approach allows for the identification of risks and appropriate controls and for vulnerabilities to be reduced before systems become operational.

Protecting intelligent infrastructures requires a combination of technical, organizational, and regulatory measures. Proper network segmentation, encryption, continuous monitoring, and the training of technical staff are essential elements in reducing risk exposure. In addition, cooperation between public administrations, technology companies, and regulatory bodies is crucial to establishing security standards consistent with sustainability objectives.

In this context, governance plays a fundamental role. Cybersecurity should not be addressed as a secondary issue but as an integral part of local strategies for sustainable development and digital transformation.

Conclusion: sustainability and security, two sides of the same coin

Smart cities offer enormous potential to address the challenges of climate change and improve the efficiency of urban environments. However, this potential can only be realized if the technological systems that support them are secure, reliable, and resilient to digital threats.

Urban sustainability does not depend solely on the amount of technology deployed but on the ability to protect and manage it responsibly. Cybersecurity, far from hindering innovation, is the element that enables intelligent solutions to endure over time and generate real, positive impact.

Ultimately, a truly smart city is not one that incorporates more sensors or digital platforms but one that better protects the people, resources, and environment that depend on them.

SANDRA GUTIERREZ DE TENA

Cuando la energía verde es vulnerable:

CIBERATAQUES EN TECNOLOGÍAS CLIMÁTICAS

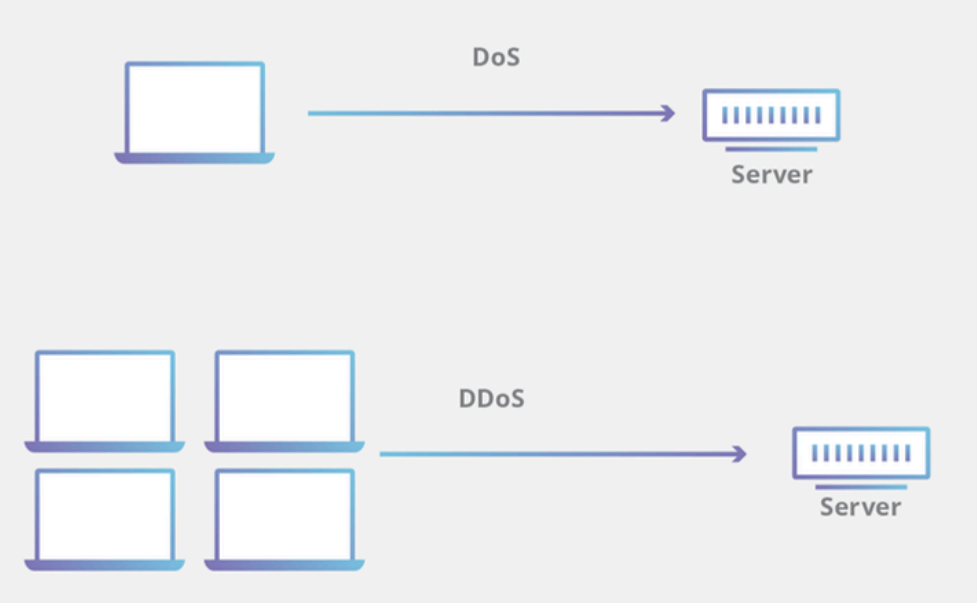
La evolución hacia tecnologías climáticas y energías renovables es uno de los pilares fundamentales para combatir el cambio climático y garantizar un desarrollo sostenible. Sistemas como las redes eléctricas inteligentes, los parques eólicos, las plantas solares o las soluciones de almacenamiento energético dependen cada vez más de infraestructuras digitales enlazadas. Esta digitalización aporta eficiencia, optimización y control en tiempo real, pero también introduce nuevos riesgos: las amenazas de ciberseguridad.

En un escenario donde la energía es un recurso crítico para la economía, la seguridad nacional y el bienestar social, los ciberataques dirigidos a infraestructuras energéticas pueden tener consecuencias graves. Este artículo analizará algunos de los principales riesgos de la ciberseguridad en las tecnologías climáticas y las energías renovables, así como los tipos de ataques más habituales que pueden afectar a estos sistemas.

Digitalización y nuevas superficies de ataque en el sector energético

Las tecnologías climáticas modernas se apoyan en sistemas de control industrial (ICS), sensores IoT, plataformas en la nube y redes de comunicación avanzadas. Las redes eléctricas inteligentes permiten equilibrar la oferta y la demanda energética, integrar fuentes renovables variables y gestionar el consumo de forma eficiente.

Sin embargo, cada dispositivo conectado representa un posible punto de entrada para un atacante. Muchos de estos sistemas fueron diseñados priorizando la disponibilidad y no la seguridad, lo que los hace vulnerables. Además, la integración de tecnologías heredadas con soluciones digitales modernas aumenta la complejidad y dificulta la protección integral de la infraestructura.



Ataques a sistemas de control industrial (ICS y SCADA)

Uno de los principales riesgos en el sector de las energías renovables es el ataque a los sistemas de control industrial, como SCADA (Supervisory Control and Data Acquisition). Estos sistemas supervisan y controlan procesos físicos críticos, por ejemplo, la orientación de los paneles solares o la velocidad de rotación de las turbinas eólicas.

Un ciberataque contra un sistema SCADA puede provocar interrupciones en la producción de energía, daños en los equipos físicos o incluso riesgos para la seguridad de las personas. Los atacantes pueden explotar vulnerabilidades conocidas, credenciales débiles o accesos remotos mal protegidos para manipular los sistemas de control.

Malware y ransomware en infraestructuras energéticas

El malware es una de las amenazas más comunes en cualquier sector, y las tecnologías climáticas no son una excepción. Programas maliciosos pueden infiltrarse a través de correos electrónicos de phishing, dispositivos USB infectados o software no actualizado.

Después de una investigación, se ha descubierto que el ransomware se ha convertido en una amenaza creciente para las empresas energéticas.

Este tipo de ataque cifra los sistemas y exige un rescate económico para restaurar el acceso, algo muy común en este tipo de ataques.

Por ejemplo, en el contexto de las energías renovables, un ataque de ransomware puede paralizar plantas de generación, centros de control o sistemas de monitorización, generando pérdidas económicas significativas y afectando a la estabilidad del suministro eléctrico.

Ataques a dispositivos IoT y sensores inteligentes

Las tecnologías climáticas dependen en gran medida de sensores y dispositivos IoT para recopilar datos sobre temperatura, radiación solar, velocidad del viento o niveles de consumo energético. Estos dispositivos suelen tener recursos limitados y, en muchos casos, carecen de mecanismos de seguridad robustos.

Los atacantes pueden comprometer sensores IoT para alterar los datos que envían, provocar decisiones erróneas en los sistemas de gestión energética o utilizarlos como puerta de entrada a redes más críticas. Además, los dispositivos comprometidos pueden formar parte de botnets utilizadas para ataques a gran escala, como los ataques de denegación de servicio. Por último, para aclarar, una botnet es un conjunto de ordenadores, denominados bots, infectados con un tipo de malware que son controlados remotamente por un atacante y que pueden ser utilizados de manera conjunta para realizar actividades maliciosas, por lo que puede ser realmente peligroso.

Ataques de denegación de servicio (DoS y DDoS)

Entrelazando con lo anterior dicho, los ataques de denegación de servicio, tanto DoS como DDoS, buscan saturar los sistemas con tráfico malicioso para hacerlos inaccesibles. En el sector de las energías renovables, este tipo de ataque puede afectar a plataformas de gestión, portales de monitorización o sistemas de comunicación entre instalaciones.

Un ataque DDoS contra una red eléctrica inteligente puede impedir la transmisión de datos en tiempo real, dificultando la gestión

de la red y aumentando el riesgo de fallos operativos. Aunque estos ataques no siempre causan daños físicos directos, sí pueden generar inestabilidad y pérdida de confianza en los sistemas energéticos.

Manipulación de datos y ataques a la integridad de la información

La integridad de los datos es esencial para el funcionamiento de todo tipo de tecnología, incluyendo las tecnologías climáticas. Los sistemas de predicción energética, optimización de redes y planificación de mantenimiento dependen de datos precisos y fiables.

Un atacante puede manipular datos de producción o consumo energético para causar desequilibrios en la red, decisiones operativas incorrectas o incluso fraudes económicos. Este tipo de ataque es especialmente peligroso porque suele pasar desapercibido durante largos periodos, generando daños acumulativos difíciles de detectar.

Espionaje y robo de propiedad

El sector de las energías renovables es altamente competitivo y está en constante innovación. Las empresas desarrollan tecnologías propias, algoritmos de optimización y diseños avanzados que representan un alto valor económico.

Los ciberataques con fines de espionaje industrial buscan robar información sensible, como planos de instalaciones, estrategias de inversión o datos de investigación y desarrollo. Este tipo de ataques puede debilitar la competitividad de las empresas y frenar el avance tecnológico necesario para la transición energética.

Amenazas internas y errores humanos

No todas las amenazas provienen del exterior; hay que tener en cuenta también a los trabajadores. Los empleados, proveedores o contratistas con acceso a los sistemas pueden representar un riesgo significativo, ya sea de forma intencionada o accidental. Errores humanos, como el uso de contraseñas débiles, la apertura de correos fraudulentos o una mala configuración de sistemas, son, en general, una de las principales causas de incidentes de ciberseguridad.

En infraestructuras energéticas, un simple fallo humano puede tener consecuencias amplificadas debido a la criticidad de los sistemas. Por ello, la concienciación y la formación en ciberseguridad son tan importantes como las medidas técnicas.

Conclusión

Las tecnologías climáticas y las energías renovables son esenciales para construir un futuro sostenible, pero su creciente digitalización las expone a múltiples riesgos de ciberseguridad. Desde ataques a sistemas de control industrial hasta ransomware, manipulación de datos o amenazas internas, el abanico de posibles ataques es amplio y en constante evolución.

Proteger estas infraestructuras críticas requiere un enfoque integral que combine tecnología, procesos y personas. La ciberseguridad debe considerarse un elemento estratégico e importante desde el diseño de las soluciones energéticas, y no como un añadido posterior. Solamente así será posible garantizar que la transición energética sea no solo sostenible, sino también segura frente a las amenazas digitales.

SERGIO BARRERA JULIÁN

EL IMPACTO REAL DEL TRABAJO HIBRIDO-REMOTO

La narrativa global sobre el cambio climático ha estado dominada durante mucho tiempo por la transición a las energías renovables y la electrificación del transporte. Sin embargo, un experimento global no planificado reveló recientemente un catalizador más inmediato para el cambio: la desvinculación del "trabajo" de "la oficina". El teletrabajo ya no es solo un beneficio para el nómada digital; ha surgido como una estrategia de alto impacto para reducir la huella de carbono antropogénica. Al eliminar la necesidad del viaje diario al trabajo, no solo estamos ahorrando tiempo, sino que estamos alterando fundamentalmente la tasa metabólica de nuestras ciudades.

La muerte del desplazamiento diario (The Commute)

El transporte representa aproximadamente el 24% de las emisiones directas de CO_2 derivadas de la combustión de combustibles (IEA, 2020). Cuando analizamos las "emisiones de alcance 3" de una corporación —aquellas que ocurren en la cadena de valor, incluidos los desplazamientos de los empleados—, el impacto de una política que prioriza el trabajo remoto se vuelve asombroso.

Menos coches no solo significa menos humo. Existe el concepto de "demanda inducida inversa": al reducir el tráfico, se reduce el desgaste del asfalto. El mantenimiento de carreteras es una actividad intensiva en carbono (el betún es un derivado del petróleo y la maquinaria pesada consume diésel a gran escala).

Menos tráfico prolonga la vida útil de la infraestructura existente. Las investigaciones sugieren que trabajar desde casa cuatro días a la semana puede reducir las emisiones de dióxido de nitrógeno (NO_2) hasta en un 10% (Hook et al., 2020). No se trata solo del tubo de escape; se trata de reducir la demanda de una infraestructura vial masiva y el mantenimiento intensivo en energía que esta requiere.

Emisiones de Alcance 3

En la contabilidad del carbono, las emisiones de Alcance 3 son el resultado de actividades de activos que no son propiedad ni están controlados por la organización que informa, pero en los que la organización impacta indirectamente en su cadena de valor. Para la mayoría de las empresas de servicios, el desplazamiento de los empleados representa la mayor parte de estas emisiones.

Al hacer la transición al teletrabajo, una empresa puede "recortar" drásticamente sus cifras de informes de carbono de la noche a la mañana, descargando efectivamente el costo ambiental del tránsito.

El gran desafío aquí es el Greenwashing Corporativo. Algunas empresas "limpian" sus balances trasladando el consumo energético de la oficina (alcance 1 y 2) al hogar del empleado (alcance 3). Para que el impacto sea real, las empresas deben incentivar que sus empleados adopten tarifas de energía 100% renovable en sus hogares, evitando simplemente "esconder" las emisiones bajo la alfombra del teletrabajo.

La caída de carbono de 2020

Durante el pico de los confinamientos de 2020, las emisiones globales de CO_2 cayeron un 5,4% sin precedentes (UNEP, 2021). Aunque esto fue temporal, los científicos climáticos del Global Carbon Project notaron que la disminución más pronunciada provino del transporte terrestre. Este período demostró que los cambios de comportamiento —específicamente el cese de los viajes no esenciales— podrían lograr resultados que las actualizaciones tecnológicas podrían tardar décadas en ofrecer.

Este periodo reveló el efecto de enmascaramiento de aerosoles. Al detenerse la industria y el transporte, disminuyeron las partículas contaminantes que, aunque nocivas, también reflejan la luz solar. Esto enseñó a los científicos que la descarbonización debe ser estructural y sostenida, no abrupta, para permitir que el ecosistema se equilibre sin picos térmicos inesperados.

La huella digital: Un arma de doble filo

Si bien la reducción del tráfico es una victoria clara, un estudiante de ciencias ambientales debe observar el "impacto neto". La transición a una oficina virtual desplaza el consumo de energía de edificios comerciales centralizados, a menudo altamente eficientes, hacia la calefacción y refrigeración residencial fragmentada.

Además, la "Nube Invisible" tiene un costo físico. Cada llamada de Zoom y cada archivo sincronizado en un servidor viaja a través de centros de datos que requieren inmensas cantidades de electricidad y agua para su refrigeración.

Aparte de esto, no todas las videollamadas son iguales. Una llamada en HD (High Definition) genera hasta 1 kg de CO2 por hora, mientras que una en definición estándar reduce esa huella en un 90%. Además, la producción de hardware para "Home Offices" (monitores extra, sillas ergonómicas) genera una huella de carbono de fabricación que tarda entre 2 y 3 años de teletrabajo en amortizarse ambientalmente (Obringer et al., 2021).

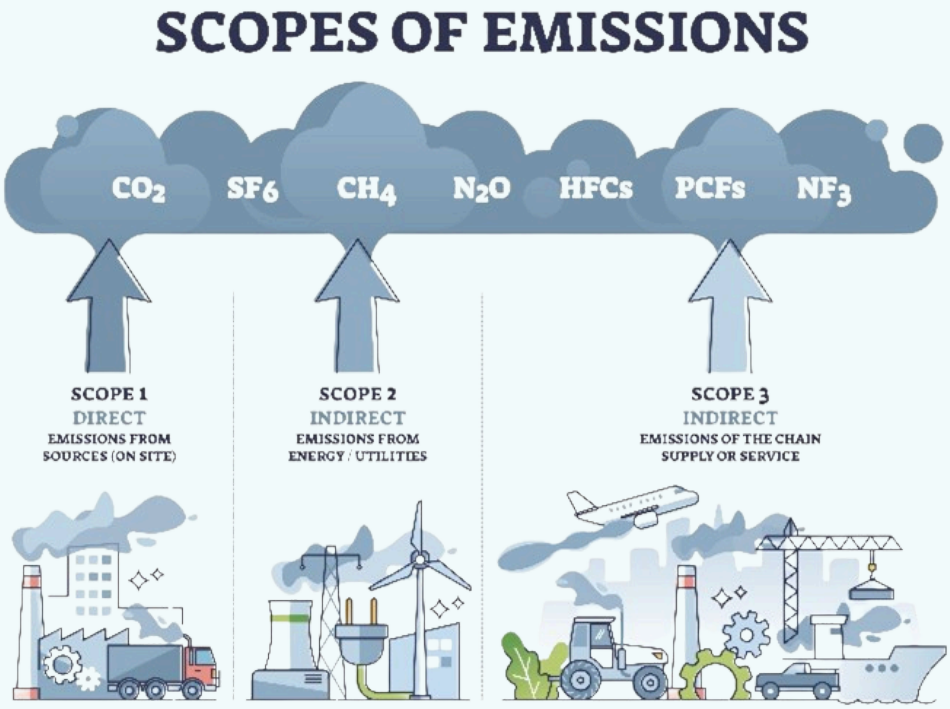
Descentralización urbana y la ciudad de los 15 minutos

Quizás el resultado más poético del movimiento del teletrabajo sea el resurgimiento del concepto de la "Ciudad de los 15 minutos". Al eliminar la necesidad de viajar a un distrito comercial central, los trabajadores están reinvirtiendo su presencia en los vecindarios locales. Esto promueve la "movilidad suave" (caminar y andar en bicicleta) y apoya las economías circulares locales.

El riesgo es la "gentrificación climática". Si los trabajadores de altos ingresos se mudan a zonas rurales buscando aire puro, pueden desplazar a las poblaciones locales y aumentar la presión sobre ecosistemas vírgenes. El teletrabajo debe ir acompañado de un urbanismo inteligente que evite la dispersión urbana descontrolada (urban sprawl).

LA PARADOJA DE JEVONS

Nombrada así por el economista William Stanley Jevons, esta paradoja ocurre cuando el progreso tecnológico aumenta la eficiencia con la que se utiliza un recurso, pero la caída del costo de uso en realidad aumenta el consumo total. En el contexto del teletrabajo, si la "facilidad" de trabajar desde cualquier lugar conduce a un aumento masivo en el consumo de datos digitales o a viajes de placer de larga distancia más frecuentes, los beneficios



ambientales de no desplazarse al trabajo podrían, paradójicamente, borrarse.

Si un empleado ahorra 500 euros al mes en gasolina y decide usarlos para tomar tres vuelos "low-cost" al año, el beneficio neto para el planeta es negativo. La ganancia ambiental del teletrabajo solo se consolida si el estilo de vida del trabajador también evoluciona hacia un consumo más consciente.

Sobriedad Digital

A medida que trasladamos nuestras oficinas a la nube, el concepto de "Sobriedad Digital" se vuelve esencial. Esto implica diseñar herramientas digitales que consuman menos energía y fomentar hábitos como apagar el video durante las llamadas cuando no sea necesario o limpiar los "datos oscuros" (almacenamiento en a nube no utilizado). Un teletrabajador verdaderamente ecológico gestiona su huella de datos con tanto cuidado como sus residuos plásticos.

Se estima que el 60% de los datos almacenados en la nube nunca se vuelven a consultar. Estos "datos oscuros" viven en servidores que consumen electricidad 24/7. Una política corporativa de "limpieza de nubes" anual podría ser tan efectiva para el planeta como plantar miles de árboles, con la ventaja de ser una acción de costo casi cero.

Anonimato vs. Responsabilidad

Finalmente, la elección de adoptar el trabajo remoto es una elección para priorizar la salud planetaria sobre la óptica corporativa tradicional.

Así como Satoshi Nakamoto eligió el anonimato para preservar la integridad de un sistema, el trabajador moderno está eligiendo la "invisibilidad" para preservar la integridad del ecosistema. Estamos cambiando el mundo sin necesidad de que el mundo nos vea en un cubículo.

VÍCTOR DE ASUNCIÓN PÉREZ

LOGÍSTICA INTELIGENTE Y DESCARBONIZACIÓN DEL TRANSPORTE

En la lucha contra el cambio climático, hay un sector que destaca por su impacto y su complejidad: el transporte logístico. Responsable de aproximadamente una cuarta parte de las emisiones globales de CO_2 relacionadas con la energía, la cadena de suministro representa la "última milla" no solo para la entrega de paquetes, sino para los objetivos de sostenibilidad corporativa. Para la gerencia moderna, esto trasciende la mera responsabilidad ecológica; se ha convertido en un desafío operativo, financiero y estratégico de primer orden. La solución ya no reside en optimizaciones puntuales, sino en una transformación tecnológica integral. Se analizará cómo la convergencia de la Inteligencia Artificial (IA), el Internet de las Cosas (IoT) y las plataformas de datos están redefiniendo la logística, posicionando la descarbonización no como un coste, sino como la nueva frontera de la eficiencia y la ventaja competitiva.

IA - IOT Y Plataformas digitales

Los algoritmos de machine learning analizan variables en tiempo real (tráfico, clima, patrones de demanda) para generar rutas óptimas. Esto va más allá de un GPS sofisticado; es un sistema de apoyo a la decisión que reduce kilómetros en vacío, mejora la tasa de carga de los vehículos y anticipa demandas.

En IoT, los sensores en vehículos y embalajes proporcionan un flujo constante de datos: consumo preciso de combustible, hábitos de conducción, temperatura de la carga y estado mecánico. Esta visibilidad permite un mantenimiento predictivo, evita averías y, sobre todo, identifica dónde se quema energía y dinero de forma innecesaria. Las plataformas en la nube actúan como el sistema nervioso central, integrando datos de los otros dos pilares y de los distintos actores de la cadena (proveedores, transportistas, clientes).

proporcionan la trazabilidad necesaria para calcular con precisión la huella de carbono por envío.

Transición a Flotas Cero emisiones

La electrificación y el uso de hidrógeno verde no son solo una sustitución de combustible. Es una decisión de portafolio tecnológico que requiere un análisis de gestión sofisticado.

La decisión entre un vehículo diésel, uno eléctrico a batería o uno de pila de combustible de hidrógeno debe considerar no solo el precio de compra, sino el coste de energía/combustible, mantenimiento, vida útil y la depreciación residual. (TCO). ¿Deben las empresas invertir en sus propias estaciones de carga/repostaje, o asociarse con proveedores especializados? Esta decisión implica evaluar riesgos de dependencia, costes de capital y alineación estratégica con tech partners.

El despliegue debe ser estratégico, priorizando primero las rutas urbanas de alta frecuencia, donde el ahorro operativo y el impacto ambiental son máximos, para justificar la inversión inicial y escalar de forma sostenible.

Caso Práctico: Amazon

Amazon sirve como un ejemplo paradigmático de gestión estratégica de esta transformación. Su compromiso The Climate Pledge (cero emisiones netas para 2040) se sustenta en una hoja de ruta tecnológica concreta:

1. Gestión de la Propiedad Intelectual Operativa: Desarrolla y utiliza su propia plataforma de optimización de rutas (apoyada en AWS), que luego comercializa como servicio, transformando un coste interno en un activo.

2. Gestión de Inversión y Adquisiciones: Su pedido masivo de 100,000 furgonetas eléctricas a Rivian no fue solo una compra, sino una alianza estratégica que asegura suministro, influye en el diseño y envía una señal poderosa al mercado.

3.Gestión del Ecosistema de Innovación: Invierte activamente en startups de vehículos autónomos y energías alternativas, no solo financiando, sino absorbiendo conocimiento y manteniendo opciones abiertas para el futuro.

Los Desafíos Críticos de la Gestión

La implementación de una logística descarbonizada encuentra sus mayores obstáculos en las complejidades de la gestión corporativa.

Superar la resistencia financiera a la inversión inicial, integrar nuevas plataformas y liderar el cambio cultural dentro de la organización constituyen pruebas decisivas para la visión estratégica de cualquier empresa. Estos filtros determinan si una iniciativa tecnológica se convierte en una ventaja competitiva sostenible.

El dilema de la inversión inicial: Justificar un alto capex (gasto de capital) ante los accionistas, con un retorno de la inversión (ROI) que, aunque robusto a largo plazo, puede extenderse varios años.

La integración de sistemas legacy: Unificar los nuevos flujos de datos del IoT y la IA con los sistemas ERP (Planificación de Recursos Empresariales) heredados, un desafío que requiere talento especializado y una arquitectura de TI bien planificada.

La gestión del cambio organizacional: Formar a conductores, operarios de logística y mandos intermedios en el uso de nuevas herramientas y métricas de desempeño centradas en la eficiencia energética.

La Logística como Ecosistema Estratégico

La descarbonización del transporte logístico deja de ser un problema operativo aislado para convertirse en la prioridad de la gestión tecnológica estratégica moderna. Exige una visión holística que integre el análisis financiero (TCO, ROI), la gestión de operaciones y datos, la estrategia de sostenibilidad y la gestión de la innovación a través de alianzas. El administrador del siglo XXI no gestiona camiones; gestiona un ecosistema tecnológico dinámico y resiliente, donde cada decisión de ruta, cada sensor instalado y cada vehículo eléctrico adquirido son piezas de una estrategia mayor: construir una ventaja competitiva que sea, intrínsecamente, baja en carbono. El futuro no pertenecerá a quienes simplemente transporten mercancías, sino a quienes sepan gestionar inteligentemente el flujo de bienes, datos y energía que las sustenta.

MSMK magazine

MSMK University College