MSMK Magazine

Tecnologías emergentes: El futuro digital

#7

Tech and Employment: Empowering Tomorrow's Talent

MSMK University College

7.ª Edición - Tecnologías emergentes: El futuro digital

En esta edición de MSMK Magazine, exploramos cómo las tecnologías emergentes se convierten en las protagonistas del empoderamiento del talento y la transformación empresarial. A lo largo de la revista, se analiza el impacto real del 6G y la hiperconectividad, la saturación del mercado frente a la "IA basura", las vulnerabilidades en los asistentes digitales y el papel de la computación cuántica como la próxima revoluciónaún por descubrir.

También examinamos la ciberseguridad en la robótica autónoma y los dilemas éticos que surgen de las interfaces cerebro-computadora y la privacidad neurológica. Una entrega que profundiza en la vanguardia digital para entender sus dinámicas, anticipar sus amenazas y liderar el cambio en un entorno en constante mutación.

CONTENIDO

CONTENIDO

AXEL BRAOJOS PEREZ

LA HIPER-CONECTIVIDAD DEL 6G

La sexta generación de redes móviles (6G) representa un paradigma revolucionario que trasciende las limitaciones actuales de conectividad, prometiendo una era de hiperconectividad sin precedentes. Esta tecnología emergente no solo amplifica las capacidades de velocidad y latencia, sino que redefine fundamentalmente la interacción entre humanos, máquinas y el entorno digital. La evolución de las redes de comunicación móvil ha seguido un patrón predecible de mejoras incrementales cada década. Sin embargo, el 6G marca una ruptura paradigmática que va más allá de las mejoras cuantitativas para introducir capacidades cualitativamente diferentes.

Mientras que el 5G se centró en tres pilares fundamentales: banda ancha móvil mejorada , comunicaciones muy confiables de baja latencia y comunicaciones masivas. El 6G expande este marco hacia un ecosistema de hiperconectividad que integra inteligencia artificial nativa, comunicaciones terahertz y experiencias inmersivas multisensoriales. La hiperconectividad del 6G no es simplemente una extensión del 5G, sino una reconceptualización fundamental de lo que significa estar conectado en el siglo XXI.

Esta transformación tecnológica promete velocidades de hasta terabits por segundo, latencias submilisegundo y la capacidad de conectar simultáneamente millones de dispositivos por kilómetro cuadrado. Más allá de las métricas técnicas, el 6G aspira a crear un "Internet de Todo" (IoE) donde la distinción entre el mundo físico y digital se desvanece, estableciendo las bases para una sociedad verdaderamente hiperconectada que redefine los límites de la experiencia humana y la interacción tecnológica.

Aplicaciones revolucionarias de la hiperconectividad

Las comunicaciones holográficas representan una de las aplicaciones más revolucionarias del 6G. Utilizando frecuencias terahertz y procesamiento de inteligencia artificial en tiempo real, será posible transmitir representaciones tridimensionales completas de personas y objetos. Esta capacidad transformará sectores fundamentales de la sociedad moderna.

En el ámbito educativo, se crearán aulas virtuales donde estudiantes de todo el mundo pueden interactuar con hologramas de profesores y compañeros, eliminando las barreras geográficas y democratizando el acceso a educación de calidad. La medicina experimentará una revolución similar, con consultas médicas holográficas que permiten exámenes físicos remotos detallados, mientras que el entretenimiento ofrecerá experiencias inmersivas donde los usuarios pueden "estar presentes" en eventos deportivos o conciertos desde la comodidad de sus hogares.

El 6G habilitará el "internet táctil", permitiendo la transmisión de sensaciones físicas a través de la red.

Esta capacidad revolucionaria incluye aplicaciones médicas avanzadas como cirugías robóticas remotas con retroalimentación háptica completa, rehabilitación física asistida por IA con sensores táctiles distribuidos y diagnósticos médicos que incorporan datos sensoriales múltiples. En el sector industrial, el “internet táctil” facilitará el control remoto de maquinaria industrial con precisión táctil, entrenamiento de operarios mediante simulaciones hápticas realistas y mantenimiento predictivo basado en sensores multisensoriales que pueden detectar anomalías antes de que se conviertan en fallas críticas.

La hiperconectividad del 6G permitirá la creación de ecosistemas urbanos verdaderamente inteligentes. Estos sistemas incluirán gestión de tráfico autónoma, donde los sistemas de transporte se autoorganizan en tiempo real, infraestructura adaptativa con edificios que ajustan automáticamente su consumo energético según las condiciones ambientales y la ocupación, y servicios públicos personalizados que anticipan y responden a las necesidades individuales de los ciudadanos. Esta integración creará ciudades que no solo son más eficientes, sino también más habitables y sostenibles.

Ventajas tecnológicas sin precedentes

El 6G introduce mejoras cuantitativas dramáticas respecto a generaciones anteriores. Mientras el 5G alcanza velocidades máximas de 20 Gbps, el 6G promete hasta 1 Tbps, representando una mejora de 50 veces. La latencia se reduce de 1 milisegundo en 5G a 0.1 milisegundos en 6G, una mejora de 10 veces que habilita aplicaciones en tiempo real verdaderamente críticas.

La densidad de conexión aumenta de 1 millón de dispositivos por kilómetro cuadrado en 5G a 10 millones en 6G, mientras que la eficiencia energética mejora 100 veces, abordando las preocupaciones ambientales asociadas con el crecimiento exponencial del tráfico de datos.

A diferencia de generaciones anteriores donde la inteligencia artificial era un complemento, el 6G integra IA como componente arquitectónico fundamental. Esto permite redes autooptimizantes que se reconfiguran automáticamente para maximizar el rendimiento, predicción de demanda que anticipa patrones de tráfico y asigna recursos proactivamente, y seguridad adaptativa que detecta y responde automáticamente a amenazas cibernéticas emergentes. Esta integración nativa de IA transforma el 6G de una simple red de comunicación en un ecosistema inteligente que aprende y evoluciona continuamente.

El 6G incorpora principios de sostenibilidad desde su diseño fundamental. La eficiencia energética ultraalta reduce dramáticamente el consumo energético por bit transmitido, mientras que las redes verdes integran fuentes de energía renovable directamente en la infraestructura de red. La optimización inteligente de recursos utiliza el espectro y los recursos computacionales de manera más eficiente que nunca, contribuyendo a los objetivos globales de sostenibilidad ambiental.

Desafíos críticos y riesgos emergentes

Las frecuencias terahertz, fundamentales para las capacidades del 6G, presentan desafíos técnicos únicos. Estas frecuencias sufren de propagación limitada y alta atenuación atmosférica, requieren línea de vista directa para comunicaciones efectivas y necesitan infraestructura densa y costosa para su implementación. Estos desafíos técnicos podrían limitar la cobertura inicial del 6G a áreas urbanas densas, potencialmente exacerbando la brecha digital entre regiones urbanas y rurales.

A pesar de las mejoras en eficiencia energética, la demanda exponencial de datos podría resultar en un aumento neto del consumo energético global. Esta paradoja energética representa uno de los desafíos más significativos para la implementación sostenible del 6G, requiriendo innovaciones adicionales en tecnologías de energía renovable y gestión inteligente de recursos.

El 6G debe prepararse para la era de la computación cuántica, que podría comprometer los sistemas criptográficos actuales. Esto requiere el desarrollo urgente de criptografía postcuántica, implementación de protocolos de seguridad cuántica y gestión sofisticada de identidades en entornos hiperconectados. La capacidad de recopilar datos granulares de millones de dispositivos plantea preocupaciones sin precedentes sobre la privacidad personal y la vigilancia masiva, requiriendo marcos regulatorios completamente nuevos para proteger los derechos individuales.

La implementación del 6G podría exacerbar la brecha digital existente. Los costos elevados de infraestructura favorecen áreas urbanas, los requerimientos técnicos excluyen dispositivos más antiguos y la necesidad de alfabetización digital avanzada podría marginar a poblaciones vulnerables. La hiperconectividad podría crear una dependencia societal peligrosa de la infraestructura de red, con consecuencias catastróficas en caso de fallos sistémicos o ataques cibernéticos coordinados.

Impacto transformador en la sociedad

El 6G promete generar un impacto económico global estimado en trillones de dólares. Esta transformación incluye nuevos modelos de negocio basados en experiencias inmersivas y datos en tiempo real, aumentos dramáticos en la productividad industrial a través de automatización avanzada y optimización de procesos, e innovación disruptiva que habilitará industrias completamente nuevas que aún no podemos imaginar completamente.

La hiperconectividad requiere marcos regulatorios completamente nuevos para la gestión de datos personales en entornos de Internet de Todo, responsabilidad algorítmica en sistemas autónomos y soberanía digital y seguridad nacional. La automatización habilitada por el 6G podría desplazar trabajos tradicionales mientras crea nuevas oportunidades en sectores emergentes, requiriendo programas masivos de reentrenamiento y adaptación laboral.

La implementación del 6G seguirá un cronograma gradual que incluye desarrollo de estándares y prototipos entre 2025-2027, despliegue inicial en mercados selectos entre 2028-2030, y adopción masiva con maduración tecnológica entre 2030-2035. Este cronograma permite una transición gradual que puede mitigar algunos de los riesgos asociados con cambios tecnológicos disruptivos.

Conclusiones y perspectivas futuras

La hiperconectividad del 6G representa tanto una oportunidad transformadora como un desafío civilizacional. Sus capacidades técnicas sin precedentes prometen revolucionar sectores desde la medicina hasta el entretenimiento, creando posibilidades que apenas comenzamos a imaginar. Sin embargo, la implementación exitosa del 6G requiere una aproximación holística que considere no solo los aspectos técnicos, sino también las implicaciones sociales, económicas y éticas.

El éxito del 6G no se medirá únicamente por sus capacidades técnicas, sino por su capacidad de crear un futuro más equitativo sostenible y humano. La comunidad académica, la industria y los gobiernos deben colaborar estrechamente para asegurar que la hiperconectividad del 6G sirva como catalizador para el progreso humano, no como fuente de nuevas divisiones sociales.

Los gobiernos deben invertir en infraestructura de investigación y desarrollo, desarrollar marcos regulatorios adaptativos, e implementar programas de alfabetización digital inclusiva. La industria debe priorizar la colaboración internacional en estándares técnicos, invertir en seguridad y privacidad desde el diseño y desarrollar modelos de negocio sostenibles. La academia debe enfocarse en investigación interdisciplinaria sobre impactos societales, formación de profesionales especializados y desarrollo de soluciones éticas y sostenibles.

La era de la hiperconectividad está al alcance de nuestras manos. La pregunta no es si llegará, sino cómo la moldearemos para beneficio de toda la humanidad. El futuro que construyamos con el 6G dependerá de las decisiones que tomemos hoy sobre su desarrollo, implementación y gobernanza. Solo a través de un enfoque colaborativo, ético y centrado en el ser humano podremos asegurar que la hiperconectividad del 6G cumpla su promesa de crear un mundo mejor conectado, más inteligente y más equitativo para las generaciones futuras.

DAVID LANCHEROS IPUS

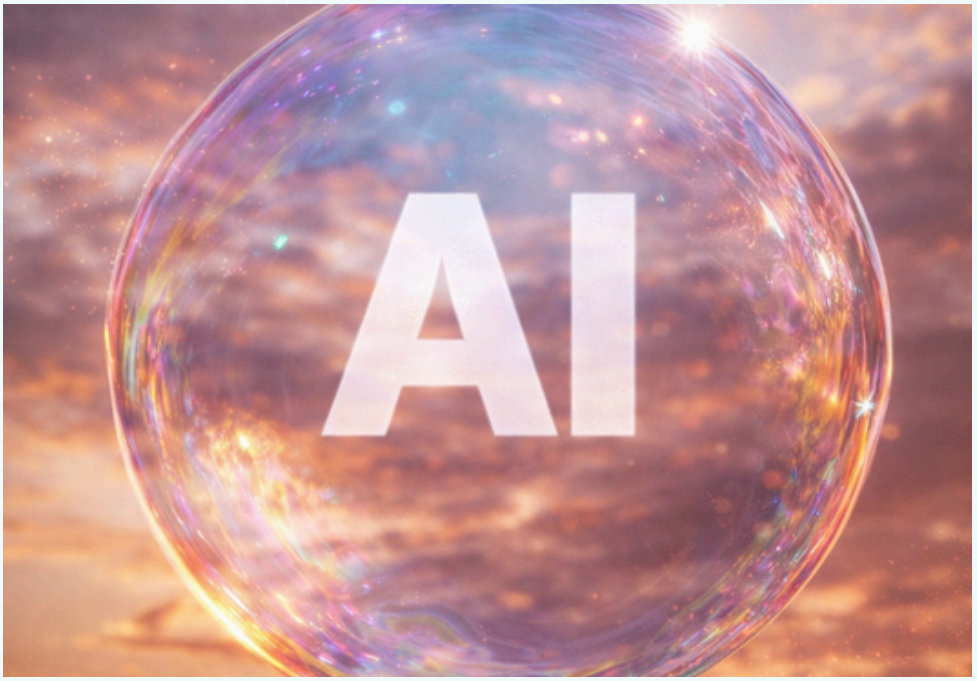
LA MODA DE LA IA: ¿FÁBRICA DE EMPRESAS BASURA?

¿Estamos revolucionando el mercado actual con la inteligencia artificial o lo estamos llenando de “basura”? No es una sorpresa la cantidad de herramientas capaces de redactar, programar o tomar decisiones por nosotros, que nos facilitan el día a día. Esto nos abre una ventana llena de oportunidades en cualquier ámbito y miles de startups han sabido aprovechar dicha oportunidad: envolver un modelo de IA ajeno con una interfaz bonita y llamarlo producto revolucionario. El resultado es un entorno saturado de herramientas casi idénticas, poco efectivas y fácilmente copiables. En pocas palabras, empresas con mucha visibilidad, pero con una durabilidad casi nula. ¿Hasta qué punto colocar “IA” al final de cualquier producto o marca dejará de estar de moda… y hasta qué punto está llenando el mercado de compañías y herramientas inservibles?

Cuando todas las herramientas parecen la misma

Un buen ejemplo lo encontramos en algo tan cotidiano como lo es un simple documento en PDF. Hoy existen decenas de herramientas “inteligentes” que prometen resumir, comprimir, editar, juntar o exportar PDFs: desde servicios clásicos como Adobe Acrobat hasta ChatPDF, AskYourPDF, PDF.ai, Humata, Paperpal y otros similares. Todas nos ofrecen más o menos lo mismo: subes tu archivo, sin saber muy bien qué hay detrás, haces preguntas y recibes resúmenes, siempre acompañados del típico anuncio publicitario que parece resolverlo todo.

Estas herramientas compiten entre sí con ligeras diferencias, pero rara vez con una propuesta realmente única o verdaderamente inteligente. Para el usuario medio, muchas de estas opciones son poco notables o poco revolucionarias; pero para el mercado, son la señal de que la IA ha facilitado tanto crear productos,, pasando de la escasez a la abundancia de herramientas casi clonadas y obsoletas.



Mucho ruido, poco valor real para el usuario.

El problema es que, en la práctica, muchas de estas herramientas aportan muy poco valor. Un informe de Menlo Ventures sobre el estado de la IA de consumo en 2025 muestra que el 91% de los usuarios recurre casi siempre a su asistente favorito (ChatGPT, Gemini, etc.) para casi cualquier tarea, a pesar de la existencia de cientos de apps especializadas. Es decir, la mayoría prueba primero “la IA de siempre” y solo cambia si otra herramienta es claramente superior; ¿el porqué? Porque cada registro nuevo, cada interfaz distinta o cada clic extra hace que el usuario abandone. Por eso terminamos con un catálogo infinito de aplicaciones “con IA” que casi nadie integra en su rutina diaria, alimentando la percepción de que se está inflando una burbuja de productos más pensados para subirse a la moda que para resolver problemas reales.

Cuando el “copiloto” es solo un disfraz

El punto preocupante es la cantidad de aplicaciones y empresas “fantasma” cuya supuesta inteligencia propia no es más que una capa encima de un modelo famoso como ChatGPT o Gemini. Muchos SaaS se presentan como soluciones de “IA avanzada” cuando, en realidad, lo único que hacen es enviar tu texto a la API de un modelo externo y devolver la respuesta en su interfaz, exactamente como describen los tutoriales de “ChatGPT wrapper” donde nos enseñan a montar un chatbot sin escribir código. Varios expertos alertan ya de que numerosos productos de este tipo están “disfrazando” un simple wrapper como si fuera un SaaS completo, ofreciendo muy poco más que lo que ya tendrías usando directamente el asistente original. Un análisis sobre el “cementerio de startups de IA” lo resume así: en la era del “prompt-as-a-startup” vimos cientos de

páginas que presumían de estar “powered by GPT-3” con diseños llamativos y promesas grandiosas, pero bajo el capó solo había una llamada a la API, sin tecnología propia ni valor añadido.

Privacidad, fatiga y desconfianza

Pero, realmente, el problema de estas empresas y aplicaciones fantasma tiene consecuencias muy concretas que muchas veces pasamos por alto, ya sea por la rapidez de la acción, la “innovación” o simplemente por ser la opción más accesible. Por un lado, varios expertos alertan de que muchos “wrappers” de IA introducen riesgos legales y de privacidad que los usuarios no tienen en cuenta.

En la práctica, la app recoge tus datos y luego los envía a un tercero, y a menudo no se explica con claridad dónde acaban, por dónde pasan ni durante cuánto tiempo se conservan, lo que puede generar incumplimientos de normativas como el GDPR. A esto se suma la sobrecarga de elección para el usuario: la abundancia de herramientas casi idénticas genera desconfianza y puede terminar dañando la percepción general de la IA o incluso de la aplicación original en la que se apoya.

La “IA” deja de ser innovación y se convierte en una simple etiqueta

Y es por eso que este tipo de escenarios ha cambiado la percepción que tenemos de la inteligencia artificial actualmente. Hace apenas unos años, ver “IA” en la descripción de un producto o aplicación sonaba a algo innovador y casi futurista; hoy, en cambio, parece que todo lleva IA: desde una simple tostadora hasta la app de notas más básica que puede haber, y ese sello se ha convertido más en reclamo de marketing que en garantía de valor. Cada semana aparecen nuevas empresas y “expertos” que prometen soluciones definitivas, mientras empieza a aparecer la fatiga ante tantos proyectos que sólo añaden una capa de IA por encima sin demostrar una verdadera efectividad. Diversos análisis muestran la aparición de una burbuja de hype: el problema es que estamos en una especie de montaña inflada, donde se ha metido IA en todas partes mucho más rápido de lo que la gente y las empresas han cambiado realmente su forma de trabajar, y cualquier ajuste económico, regulatorio o de confianza podría hacer que esa espuma se desinfle de golpe y cree un impacto verdaderamente significativo.

¿Qué copilot queremos y qué empresas deberían seguir?

Al final, la pregunta no es si toda nueva empresa debe tener IA, sino qué tipo de “copiloto” estamos construyendo y fomentando. Si seguimos dando importancia a productos que solo añaden una capa de IA como reclamo de marketing, seguiremos llenando el mercado de empresas basura: poco útiles, intercambiables y desconectadas de problemas reales. En cambio, los copilotos y empresas que merezcan la pena serán aquellos que se integren de verdad en el trabajo diario, entiendan la operativa, consigan un equilibrio entre sencillez y eficacia, usen los datos de la organización con cuidado, aporten eficiencia medible y sean honestos sobre qué pueden y qué no pueden hacer.

Cuando la moda pase y la burbuja se desinfle, probablemente esa será la diferencia entre las compañías que desaparezcan con su “IA” de escaparate y las que sigan ahí, usando la inteligencia artificial como lo que siempre debió ser: una herramienta al servicio del negocio, y no un disfraz brillante para ocultar la falta de valor.

GABRIEL FALCAO SANTOS

VULNERABILIDADES EN LOS ECOSISTEMAS DE ASISTENTES DIGITALES

La intersección entre la transformación digital y la transición ecológica representa uno de los desafíos más complejos de la gobernanza global contemporánea.

En el centro de toda esta "transición gemela" se encuentran los asistentes digitales y los ecosistemas de inteligencia artificial, herramientas que prometen optimizar la gestión de los recursos que, de forma simultánea, introducen vectores de vulnerabilidad que podrían sabotear los esfuerzos de mitigación del cambio climático. Los asistentes de voz, como interfaces del IoT, actúan como el nexo entre la voluntad humana y la infraestructura física, controlando todo, desde el consumo eléctrico doméstico, hasta la gestión de redes inteligentes de energía.

Sin embargo, su fragilidad frente a ataques cibernéticos, desde la inyección de comandos inaudibles hasta la suplantación de identidad en mercados de aplicaciones, no solo compromete la privacidad del usuario, sino que tiene el potencial para generar picos de demanda energética artificiales y desperdicio masivo de recursos.

El nexo entre la inteligencia artificial y la demanda energética global

El despliegue masivo de asistentes digitales y modelos de lenguaje de gran escala ha alterado de forma profunda la dinámica de consumo eléctrico en los centros de datos globales. Estos nodos de procesamiento están encargados de transformar señales acústicas en intenciones computacionales; para ello, requieren una infraestructura energética que crece a un ritmo sin precedentes. La demanda de electricidad por parte de los centros de datos es impulsada principalmente por la inferencia y el entrenamiento de IA; se proyecta que alcance los 945 TWh para el 2030, lo que representaría un incremento mayor de 130% respecto a los niveles registrados en el 2024.

Este crecimiento conlleva una presión proporcional sobre las emisiones de gases de efecto invernadero. Mientras que en 2024 la participación de la IA en la demanda total de los centros de datos oscilaba entre el 5% y el 15%, las proyecciones para el final de la década sitúan este valor entre el 35% y el 50%. En términos de huella de carbono, se traduciría a una emisión anual asociada que podría escalar de los 180 millones de toneladas de CO_2 hasta 360 y 500 millones para el 2030.

Arquitectura técnica y superficie de ataque de los asistentes de voz

La arquitectura de un asistente digital moderno se divide en varias capas de procesamiento, cada una con vectores de ataques específicos que podrían ser explotados para comprometer la eficiencia energética y seguridad física. El proceso comenzaría en la capa de captura de audio, donde los micrófonos de sistemas microelectromecánicos convierten las ondas sonoras en señales eléctricas. Después, el reconocimiento automático del habla transcribe el audio a texto, generalmente en la nube, utilizando redes neuronales profundas para filtrar el ruido. La fase de comprensión del lenguaje natural analiza el texto para identificar la intención del usuario y extraer entidades. Finalmente, el sistema gestiona el diálogo, interactúa con dispositivos externos y genera una respuesta mediante síntesis de voz (TTS).

Vulnerabilidades en el ecosistema de skills: squatting y masquerading

El crecimiento de los asistentes digitales ha sido impulsado por mercados de aplicaciones de terceros. Aunque la estructura de estos mercados facilita los ataques basados en la ambigüedad fonética y el engaño cognitivo.

El voice squatting ocurre cuando un desarrollador malicioso registra una aplicación con un nombre fonéticamente similar a una legítima. Por ejemplo, si un usuario intenta abrir una herramienta financiera como `Capital One´, podría activar involuntariamente una skill maliciosa llamada `Capital Won`. De todas formas, una solicitud para revisar el medidor de energía podría ser interceptada por una aplicación fraudulenta que manipule los datos de consumo.

Por otro lado, el Voice Masquerading permite que una app simule haber terminado su ejecución mientras que esta permanece activa y escuchando. El atacante podría reproducir un tono de despedida falso para luego incitar al usuario a revelar la información sensible o mantener el dispositivo consumiendo recursos en segundo plano para tareas como la minería de criptomonedas, afectando la factura eléctrica y la red local.

HUGO HERNÁNDEZ MORENO

Edge Computing: CUANDO LA NUBE NO ES SUFICIENTEMENTE RÁPIDA

Hay una ley de la física que ningún ingeniero de Google, Amazon o Microsoft puede reescribir: La velocidad de la luz es 300.000 kilómetros por segundo. Suena rápido. Y lo es, hasta que necesitas que una máquina tome una decisión de vida o muerte en menos de diez milisegundos.

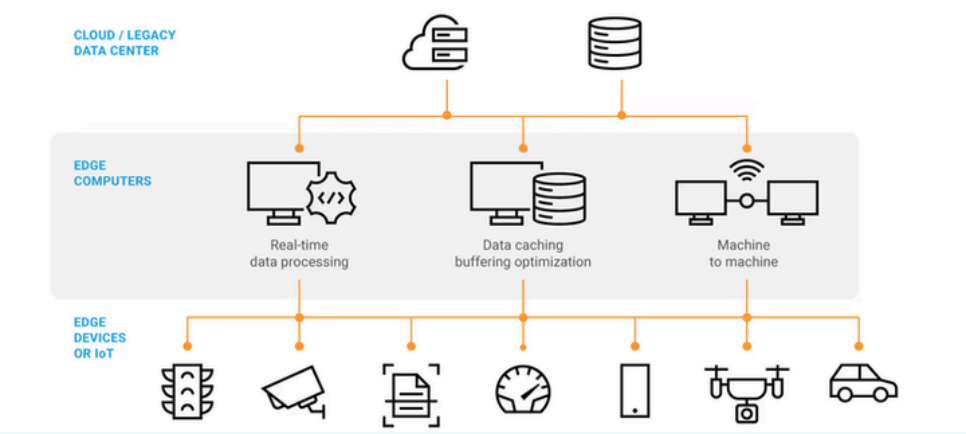
Un vehículo autónomo circulando a 120 km/h recorre 33 centímetros en ese intervalo. Si el algoritmo que detecta al peatón que acaba de cruzar vive en un datacenter en Dublín, la petición viaja de Madrid a Irlanda y vuelve antes de que el freno actúe. La latencia mínima real entre Madrid y Frankfurt en condiciones óptimas ronda los 20-30 ms. Para streaming de vídeo, es imperceptible. Para conducción autónoma o cirugía robótica remota, puede ser la diferencia entre un accidente y no tenerlo.

Este es el problema que nadie había articulado bien durante la primera era del cloud: la centralización tiene un techo físico. Y entender ese techo es entender por qué Edge Computing no es una moda tecnológica, sino una respuesta arquitectural inevitable a los límites de la naturaleza.

¿Qué significa procesar en el borde?

Para resolver ese problema, primero hay que nombrarlo con precisión. Edge Computing no es simplemente "procesar cerca del usuario", es una reconfiguración profunda de dónde vive la inteligencia computacional: desde centros de datos centralizados hasta el borde de la red, lo más próximo posible a donde se generan los datos.

La arquitectura se organiza en tres capas. En el nivel más cercano al mundo físico están los propios dispositivos (sensores, cámaras, actuadores), capaces de ejecutar modelos ligeros de inferencia localmente. Un nivel más arriba se sitúan los nodos edge: pequeños servidores desplegados en



torres de telecomunicaciones, fábricas, hospitales o vehículos, con capacidad de cómputo real pero sin la escala de un datacenter. Y en la cima sigue existiendo el cloud, encargado del entrenamiento de modelos, almacenamiento histórico y coordinación global.

La clave es que la decisión se toma donde tiene que tomarse, no donde hay más potencia disponible. Pero ¿qué ha llevado exactamente a que esta arquitectura pase de ser una idea interesante a convertirse en infraestructura crítica desplegada a escala global?

Los tres drivers que lo hicieron explotar

La respuesta no es una sola causa, son tres presiones simultáneas que convergieron y forzaron el cambio.

La primera es la latencia. El coche autónomo con el que abrimos este artículo no es un experimento de laboratorio: Tesla Full Self-Driving ejecuta sus redes neuronales en hardware propio dentro del vehículo, no en servidores remotos. La cirugía robótica asistida requiere latencias por debajo de 10 ms para que el cirujano no perciba retardo entre su movimiento y el del instrumental. Las redes eléctricas inteligentes necesitan detectar y responder a fallos en milisegundos para evitar apagones en cascada. En todos estos casos, esperar la respuesta de la nube no es una limitación técnica superable con mejor hardware; es un problema de física.

La segunda presión es regulatoria. El Reglamento General de Protección de Datos europeo y legislaciones equivalentes en todo el mundo imponen restricciones reales sobre dónde pueden residir ciertos datos. Los historiales médicos de un paciente en España no pueden transitar libremente por servidores en Virginia. Los datos biométricos capturados en fábricas europeas tienen restricciones de transferencia.

El edge resuelve este problema de raíz: si el dato nunca sale del dispositivo o del nodo local, el problema regulatorio desaparece. Los smartphones modernos ya ejecutan reconocimiento facial y modelos de lenguaje compactos completamente offline, sin enviar nada a ningún servidor externo.

La tercera es económica. La escala del Internet de las Cosas ha roto los modelos de negocio del cloud puro. Una planta industrial moderna puede generar varios terabytes de datos de sensores al día. Subir todo eso a la nube para procesarlo es energéticamente ineficiente, costoso y técnicamente innecesario, dado que el 90% de esos datos no necesita persistencia. El edge filtra, agrega y descarta en origen, enviando al cloud únicamente lo que merece almacenarse. Es la diferencia entre fotografiar todo lo que ves y solo hacer fotos cuando algo es relevante.

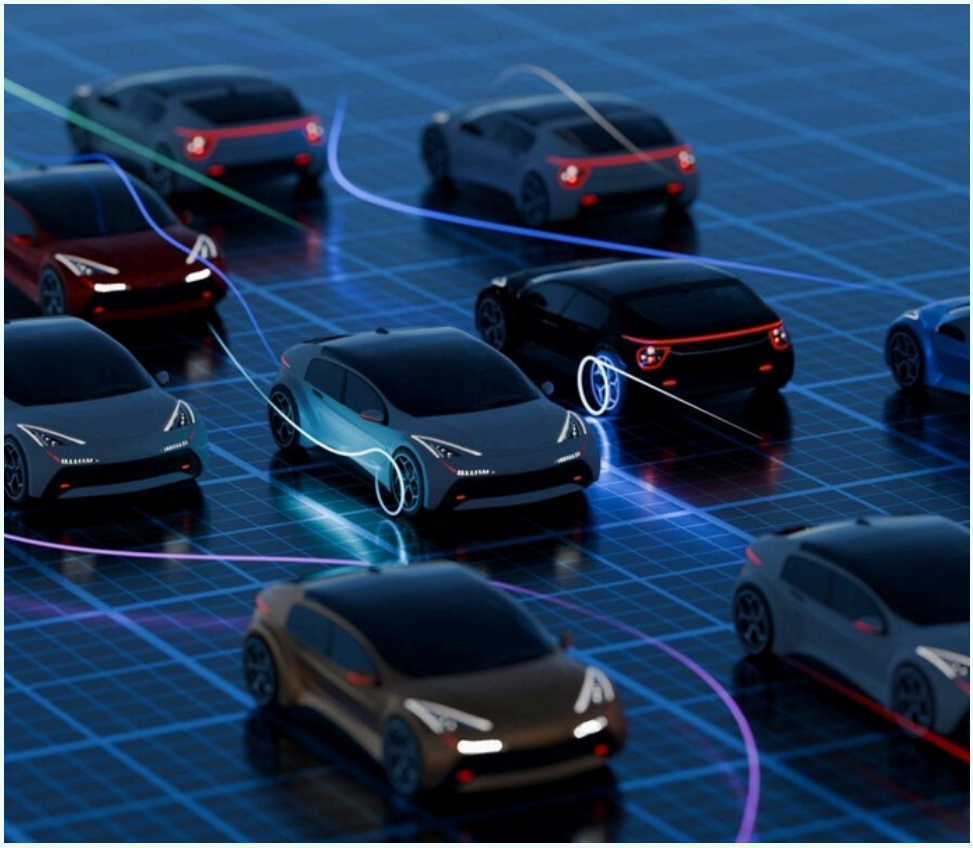
Tres presiones distintas, la misma conclusión: el centro no puede con todo.

¡Lo que ya existe hoy, no mañana!

Estas presiones no son teóricas; ya han producido infraestructura real y desplegada. El edge computing dejó de ser una promesa hace tiempo.

Cloudflare Workers es quizás el ejemplo más elocuente: una plataforma que permite ejecutar código en más de 300 ciudades simultáneamente, con latencias medias por debajo de 50 ms desde cualquier punto del planeta. No es marketing, es una red de nodos edge reales que ejecuta millones de funciones al día. En el espacio industrial, NVIDIA Jetson se ha convertido en el estándar de facto para inferencia en el borde: el hardware que impulsa drones de inspección, robots de almacén y sistemas de visión en líneas de producción, todo en un módulo del tamaño de una tarjeta de crédito consumiendo entre 5 y 60 vatios. AWS Greengrass y Azure IoT Edge permiten desplegar contenedores directamente en dispositivos edge y ejecutar lógica de negocio sin conexión, sincronizando con la nube solo cuando es necesario. Y en el ámbito médico, hospitales en Japón y Corea del Sur ya procesan resonancias magnéticas con IA localmente, sin que los datos de pacientes abandonen el edificio.

El patrón común en todos estos casos es el



mismo la inteligencia se acerca al problema, no al revés.

Los retos que quedan por resolver

Sin embargo, ninguna arquitectura emerge sin fricciones, y el edge tiene las suyas —y son serias.

La seguridad es la más urgente. Un datacenter centralizado tiene un perímetro bien definido y un equipo dedicado a protegerlo. Una red de miles de nodos distribuidos por fábricas, hospitales y carreteras presenta una superficie de ataque masiva y heterogénea. Cada nodo es un punto de entrada potencial, y orquestar actualizaciones de seguridad en entornos tan dispersos sigue siendo un problema abierto que herramientas como K3s y KubeEdge están empezando a resolver. A esto se suma la fragmentación del ecosistema: decenas de plataformas incompatibles, SDKs propietarios y estándares de interoperabilidad aún inmaduros que ralentizan la adopción.

Y hay una pregunta energética que merece atención: miles de nodos pequeños pueden consumir más energía en total que un datacenter centralizado y optimizado si no se diseña la carga de trabajo con cuidado.

Pero estos son retos de ingeniería, no objeciones fundamentales. Y la industria los está resolviendo.

La pregunta que define la próxima década no es si el edge reemplazará al cloud; no lo hará, son arquitecturas complementarias. La pregunta real es cuánta inteligencia necesita vivir en el borde para que los sistemas que construimos sean verdaderamente autónomos, seguros y responsivos. Y si la respuesta al comienzo de este artículo era un peatón cruzando delante de un coche que no puede esperar en Dublín, la respuesta al final es que ese coche ya no espera.

Ya decide solo.

IGNACIO QUIROZ COSCOLLANO

AI AS A DOUBLE-EDGED SWORD IN CYBERSECURITY

For decades, cybersecurity was built on a simple premise: humans defend, machines execute. Security systems followed predefined rules, analysts interpreted alerts, and threats were identified through patterns that experts could understand and anticipate. The digital world, while complex, remained largely governed by human decision-making.

Today, that balance is shifting. Artificial intelligence is no longer just a supporting tool but an active participant in the system. From detecting anomalies in network traffic to responding to threats in real time, AI is increasingly embedded in the core of cybersecurity operations. Systems no longer just follow instructions; they learn, adapt, and, in some cases, act autonomously.

This transformation introduces a fundamental change in how security is conceived. The scale and speed of modern digital environments exceed human capacity, making automation not just useful but necessary. AI enables organizations to process vast amounts of data, identify subtle patterns, and react to threats faster than any human team could. In this sense, it represents a significant leap forward in defensive capabilities.

However, this same technological shift is not exclusive to defenders. The tools that allow systems to learn and adapt can also be leveraged to exploit, deceive and scale attacks in ways that were previously unimaginable. The intelligence that strengthens security also expands the potential of those seeking to bypass it.

This duality defines the current moment. Artificial intelligence is not simply enhancing cybersecurity; it is reshaping the entire landscape, creating an environment where both defense and threat evolve simultaneously. In this context, the challenge is no longer just to protect systems but to understand and manage a digital ecosystem in which machines are increasingly making decisions on both sides of the equation.

AI as a dual force: Machines protecting and attacking

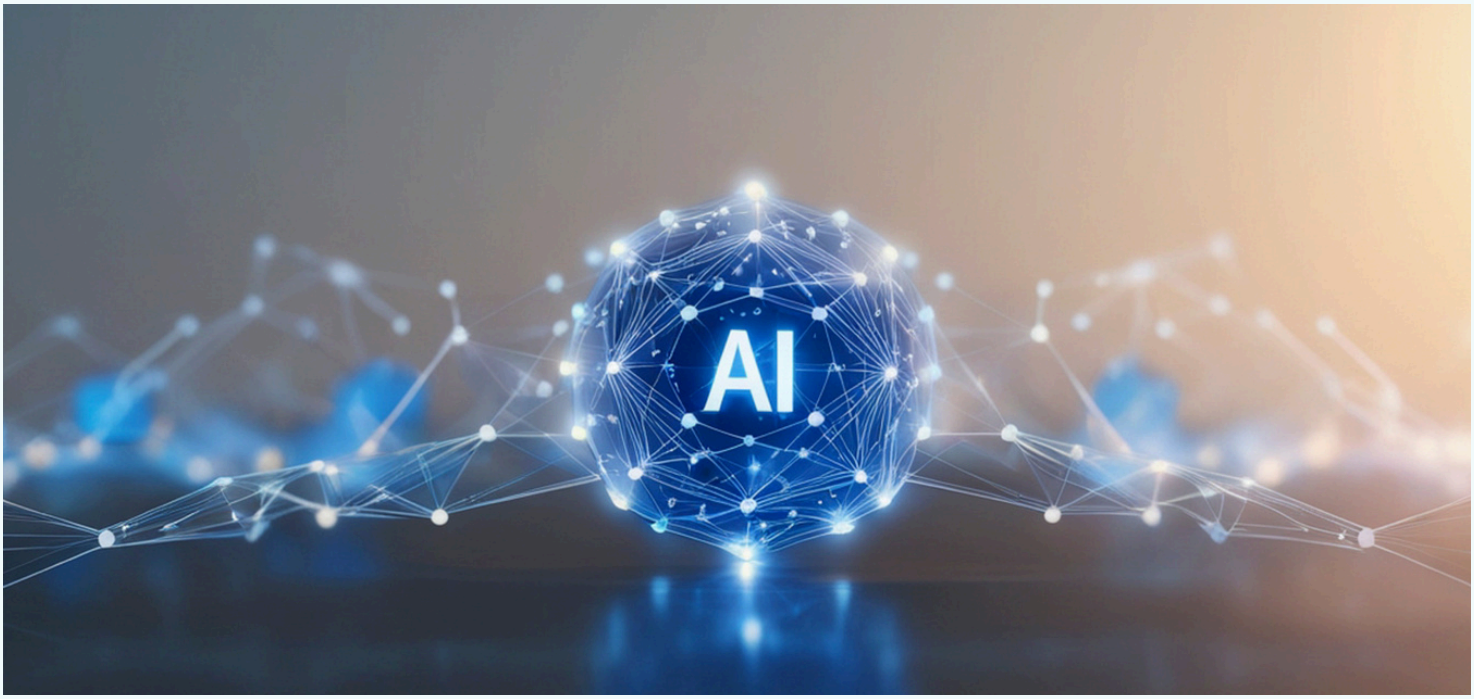
As digital infrastructures grow in complexity, the volume and speed of potential threats have surpassed what human operators alone can effectively manage. Modern networks generate vast streams of data, where malicious activity is often hidden within subtle deviations rather than obvious patterns. In this context, artificial intelligence has become a critical component of cybersecurity, not by replacing human expertise, but by extending it beyond its natural limits.

On the defensive side, AI-driven systems are particularly effective at identifying anomalies. Instead of relying solely on predefined rules or known threat signatures, they learn what “normal” behavior looks like within a system and detect deviations that may indicate a security incident. This shift from reactive to adaptive defense allows organizations to identify previously unknown threats, including those that do not match any existing database of attacks.

Beyond detection, AI also enables automated response. When a potential threat is identified, systems can isolate affected components, block suspicious activity or trigger containment protocols in real time. This capability is especially relevant in environments where seconds can determine the scale of an incident. The ability to respond at machine speed reduces reliance on manual intervention and significantly limits the window of opportunity for attackers.

Another key contribution lies in predictive security. By analyzing historical data and identifying emerging patterns, intelligent systems can anticipate potential vulnerabilities before they are exploited. This forward-looking approach transforms cybersecurity from a reactive discipline into a proactive one, where the objective is not only to respond to incidents but to prevent them from occurring.

However, these same capabilities are not exclusive to defenders. The tools that enable systems to learn, adapt, and predict can also be leveraged to enhance offensive strategies. As AI becomes more accessible, the barrier to executing sophisticated cyberattacks continues to decrease.



What once required advanced technical expertise can now be automated, optimized, and scaled through intelligent systems. AI can be used to scan systems for vulnerabilities at a speed and scale far beyond human capability, accelerating the discovery phase of an attack. In parallel, it enables the development of more adaptive and evasive forms of malware, capable of modifying their behavior in response to the environment they encounter. Unlike traditional threats, these systems do not rely on fixed patterns, making them significantly harder to detect.

At the same time, AI enhances social engineering techniques. AI-generated content — from highly convincing phishing messages to synthetic audio and video — increases both the realism and personalization of attacks. By analyzing publicly available data, attackers can craft highly targeted interactions, blurring the line between authentic and manipulated information.

What makes this transformation particularly significant is not any single capability but the combination of automation, adaptability, and scale. AI allows both defenders and attackers to operate with unprecedented efficiency, reshaping the nature of cybersecurity into a dynamic interaction between intelligent systems.

The new asymmetry: speed, scale and automation

Cybersecurity at machine speed

The integration of artificial intelligence into both defensive and offensive strategies has fundamentally altered the balance of cybersecurity. What was once a contest defined by human expertise and reaction time is now shaped by systems capable of operating at machine speed. This shift introduces a new kind of asymmetry, one not based solely on resources or knowledge but on the ability to process, adapt, and act faster than the opponent.

In traditional cybersecurity models, time played a critical role. Detecting a threat, analyzing it, and responding effectively required a sequence of human-driven actions. While this process was not instantaneous, it allowed for interpretation, validation, and strategic decision-making. With AI, this timeline is compressed. Detection, analysis, and response can occur almost simultaneously, often without direct human intervention. This acceleration affects both sides. Defensive systems can identify and contain threats in real time, minimizing damage and reducing response windows. At the same time, attackers can launch, modify, and replicate attacks at a similar pace. The result is an environment where actions and counteractions unfold continuously, creating a cycle of rapid escalation that challenges traditional control mechanisms.

Scale further amplifies this dynamic. AI enables operations to be conducted across thousands or even millions of targets simultaneously. For defenders, this means monitoring vast and complex infrastructures; for attackers, it means the ability to probe multiple systems at once, searching for the smallest vulnerability. The interaction between these two forces creates a highly dynamic and often unpredictable landscape.

Automation adds a final layer to this transformation. As systems become more autonomous, decision-making shifts from human operators to algorithms. While this increases efficiency, it also reduces transparency. Decisions are made faster, but not always with clear visibility into the reasoning behind them. This raises important questions about control, oversight

and accountability in environments where speed often takes precedence over understanding.

Trust, control and the limits of AI

Can we trust systems we don't fully understand?

As artificial intelligence becomes more deeply embedded in cybersecurity, it introduces a fundamental tension between performance and understanding. AI systems are capable of detecting patterns and making decisions at a level of complexity that often exceeds human comprehension. While this capability enhances efficiency, it also challenges one of the core principles of security: trust.

Many AI models, particularly those based on advanced machine learning techniques, operate as "black boxes." They produce results, identifying threats, flagging anomalies or triggering responses, without offering clear explanations of how those conclusions were reached. In cybersecurity, where decisions can have immediate and significant consequences, this lack of transparency creates a critical dilemma. Systems may be highly effective, but if their reasoning cannot be verified, their reliability becomes difficult to assess.

This issue is compounded by the risk of errors. False positives can lead to unnecessary disruptions, blocking legitimate activity or triggering costly responses. False negatives, on the other hand, may allow threats to go undetected. In both cases, the problem is not simply technical accuracy but the degree to which humans can understand, challenge, and correct the decisions made by AI systems.

Over-reliance on automation further amplifies these risks. As organizations increasingly depend on AI to manage security operations, there is a tendency to reduce human oversight, especially in high-speed environments where manual intervention is impractical. However, removing humans from the decision-making loop can create blind spots. Systems may function correctly under normal conditions but fail in unexpected scenarios that fall outside their training data.

There is also a broader question of control. If both defensive and offensive capabilities are increasingly driven by adaptive systems, the cybersecurity landscape becomes less predictable. Actions taken by one system can trigger automated responses in another, creating chains of interaction that are difficult to anticipate or fully manage. In such an environment, maintaining control is no longer just a matter of technical capability but of understanding how these systems behave collectively.

Ultimately, the challenge is not whether AI should be used in cybersecurity, but how it should be governed. Trust cannot be based solely on performance; it must also be grounded in transparency, accountability, and the ability to intervene when necessary. As systems become more intelligent, ensuring that they remain understandable and controllable becomes a central concern.

JOAO GABRIEL GUIMARAES

Los connectomics: DESREGULACIÓN DEL EJE HPA Y DOPAMINA EN LA ERA DIGITAL

Para un ingeniero de software, el cerebro es el sistema definitivo y la “conectómica” es el estudio del cerebro como una matriz: qué neuronas (nodos) están conectadas y con qué peso sináptico (aristas). Sin embargo, este grafo no es estático, sino justamente lo contrario, ya que está sujeto a cambios biológicos como la neuroplasticidad. El problema actual es que factores externos están "hackeando" estos algoritmos, específicamente a través del eje HPA (responsable por la conexión del cerebro y el intestino) y el sistema dopaminérgico.

Eje HPA: El Protocolo de Gestión de Crisis

El eje HPA es el termostato biológico de supervivencia. Ante una amenaza (física o psicológica), el hipotálamo inicia una cascada hormonal: libera CRH, que estimula la pituitaria para liberar ACTH, lo que finalmente lleva a las glándulas adrenales a disparar cortisol en el torrente sanguíneo.

En condiciones ideales, este es un sistema de retroalimentación negativa (feedback loop) extremadamente eficiente. El cortisol actúa como la señal de apagado: cuando llega al hipotálamo y al hipocampo, les indica que detengan la producción, restaurando la homeostasis una vez que el peligro ha pasado. Es un protocolo de "gestión de crisis": se desvía energía de procesos no esenciales (digestión, sistema inmune, pensamiento a largo plazo) hacia la supervivencia inmediata.

La Crisis Moderna: Estrés Crónico

El problema surge cuando la "amenaza" no es un depredador, sino un flujo constante y de baja intensidad: notificaciones de Slack a medianoche, plazos de entrega poco realistas, ruido urbano y ansiedad financiera. El eje HPA permanece activado continuamente, inundando el cerebro con cortisol. Esto ya no es un pico de crisis, es un ataque de denegación de servicio (DoS) a los receptores de cortisol en el hipocampo. Al estar constantemente saturados, estos receptores pierden sensibilidad (downregulation), y el bucle de retroalimentación negativa falla. El cerebro pierde su capacidad de apagarse.

Dopamina: El Algoritmo de Recompensa Hijackeado

La dopamina es frecuentemente malinterpretada como la "molécula del placer". Desde un enfoque técnico, es más preciso definirla como un algoritmo de predicción de error de recompensa (RPE). La dopamina no se dispara ante el placer per se, sino ante la señal de una recompensa inminente o cuando la recompensa supera las expectativas. Es el motor de la motivación, el que nos impulsa a buscar comida, conocimiento o interacción social.

El Protocolo de Recompensas Variables

La economía de la atención actual (redes sociales, videojuegos, aplicaciones de citas) ha perfeccionado el uso de "recompensas variables". Esta técnica, originada en las máquinas tragamonedas, es la forma más potente de secuestrar el sistema dopaminérgico. Al no saber cuándo llegará la próxima recompensa (un like, un mensaje, un objeto raro), el cerebro libera picos masivos y frecuentes de dopamina en previsión.

Consecuencia: Homeostasis y Falta de Sensibilidad

Ante esta hiperestimulación constante, el cerebro recurre a su mecanismo de defensa: la homeostasis. Para protegerse de la sobrecarga de señal, reduce drásticamente la densidad de receptores de dopamina (en especial los receptores D2).

Esto crea un círculo vicioso: el umbral para sentir motivación sube, mientras que los placeres simples de la vida (como estudiar ingeniería) pierden su atractivo, ya que su "pago" dopaminérgico es demasiado lento y bajo en comparación con los "picos" digitales.

Estado	Contexto	Densidad de Receptores (D2)	Consecuencia Funcional
Saludable	Estímulos naturales (comida, conversación, aprendizaje lento).	Alta	Alta sensibilidad a placeres cotidianos; motivación sostenible a largo plazo.
Desregulado	Hiperestimulación digital (redes sociales, pornografía, juegos variables).	Baja (***Downregulation***)	Tolerancia; se requiere un estímulo cada vez más intenso para sentir algo; **anhedonia basal**.

Tabla de comparación de la sensibilidad dopaminérgica

Conectómica y neuroplasticidad El "refactoring" Malicioso

Cuando el cortisol alto y la dopamina desregulada coexisten, el conectoma sufre una reconfiguración física:
1. Atrofia en el córtex prefrontal (PFC): Se pierden conexiones en el área encargada del "control top-down" (la lógica).
2. Hipertrofia en la amígdala: El nodo del miedo se vuelve más grande y conectado.
3. Resultado: El cerebro se vuelve un sistema puramente reactivo, perdiendo su capacidad de planificación a largo plazo.

Analogía de software: Es como si un script malicioso borrara las funciones de "Optimización" y "Planificación" de tu código para sustituirlas por bucles de if-then (sobreposición de condicionales) basados únicamente en pánico e impulsos.

Casos de Estudio: Evidencia en el Hardware Humano

Evidencia 1: Uso compulsivo de internet y redes sociales: Múltiples estudios de conectómica han comparado el cerebro de individuos con uso patológico de internet frente a controles sanos. Los resultados muestran una integridad estructural reducida en la materia blanca que conecta las regiones prefrontales con las subcorticales (el sistema de recompensa). Es decir, el cableado físico que permite al "adulto" en tu cerebro (PFC) decir "no" a otra hora de scrolling está físicamente dañado.

Evidencia 2: El Efecto del Estrés Crónico en la Conectividad Funcional: Investigaciones han demostrado que sujetos sometidos a estrés crónico presentan una conectividad funcional reducida dentro de la Red Neuronal por Defecto (DMN, por sus siglas en inglés), una red crucial para la introspección y la planificación a largo plazo. Al mismo tiempo, muestran una hiperconectividad dentro de la red de prominencia (salience network), lo que los mantiene en un estado de alerta constante y distractibilidad.

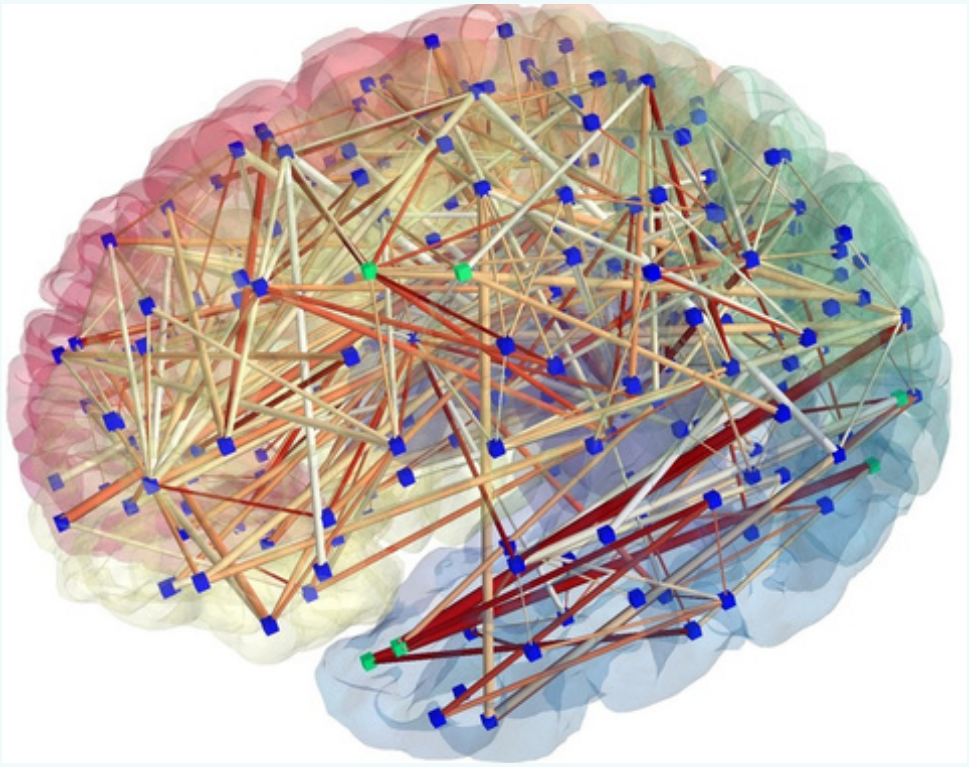
Consecuencias y Funciones Ejecutivas

Función Ejecutiva	Impacto de la Desregulación	Consecuencia en Ingeniería
Memoria de Trabajo	Saturada por señales de estrés (Cortisol)	Incapacidad para debuguear problemas complejos.
Inhibición de Impulsos	Fallo en la conexión PFC-Amígdala	Procrastinación compulsiva ("Doomscrolling").
Flexibilidad Cognitiva	Rigidez en el grafo conectómico	Dificultad para aprender nuevos stacks tecnológicos.

Conclusión

Como programador y/o desarrollador, es de gran importancia entender que no solo programamos máquinas, sino que nuestro propio "hardware" biológico está siendo constantemente programado y optimizado por el entorno y el software (ambiente/fenotipo) que consumimos. La conectómica nos ofrece una verdad innegable: las conexiones neuronales que no se usan se podan, y las que se hiperestimulan se refuerzan.

El estilo de vida actual, caracterizado por un eje HPA crónicamente activado y un sistema dopaminérgico saturado de recompensas variables, está "reescribiendo" el conectoma hacia un estado de impulsividad, anhedonia y disfunción ejecutiva. Recuperar la soberanía cognitiva requiere una "higiene dopaminérgica" y estrategias de gestión del estrés, entendiendo que el objetivo no es solo la salud mental, sino la preservación de la infraestructura neuronal que nos permite pensar, crear y resolver problemas complejos.



JORGE MADRID VALNICKAS

OSINT SATELITAL DE ALTA RESOLUCIÓN Y PRIVACIDAD ESPACIAL

Durante décadas, observar la Tierra desde el espacio fue un privilegio exclusivo de las superpotencias. En la Guerra Fría, los satélites eran mastodontes que requerían presupuestos incalculables, y sus precisas fotografías se consideraban alto secreto de Estado para ocultar su verdadero alcance.

Sin embargo, este histórico monopolio gubernamental se ha desmoronado por completo. La miniaturización electrónica y la fuerte entrada de capital privado han impulsado una nueva era. Hoy, la tecnología aeroespacial comercial lanza dispositivos pequeños y económicos masivamente. Esto genera un flujo de datos geoespaciales accesible para cualquiera con internet, democratizando una capacidad de vigilancia global sin precedentes.

El boom de los microsatélites comerciales

La estandarización de componentes ha permitido a empresas privadas desplegar enjambres enteros de pequeños satélites de bajo coste. Estas constelaciones orbitales operan de forma sincronizada, fotografiando la totalidad del globo casi a diario. Ya no dependemos del paso esporádico de un gran dispositivo estatal; ahora la observación terrestre es un flujo continuo que actualiza nuestra visión en tiempo récord.

Mucho más que fotos: el poder del radar SAR

La revolución no se limita a la luz visible. Los equipos modernos incorporan avanzados sensores multiespectrales y radares de apertura sintética (SAR) capaces de penetrar densas nubes y la más absoluta oscuridad. Esta tecnología militar democratizada garantiza una monitorización ininterrumpida del terreno, demostrando que factores tradicionales como el mal clima o la noche ya no sirven para ocultar infraestructuras.

El nuevo arsenal del analista OSINT

La democratización de estas imágenes ha revolucionado por completo la disciplina de la inteligencia de fuentes abiertas. Lo que antes requería costosos despliegues sobre el terreno, hoy se ejecuta desde cualquier oficina conectada a la red. Analistas de seguridad, periodistas e incluso ciudadanos curiosos utilizan este flujo de datos espaciales para auditar eventos globales y verificar información en tiempo real. Sin embargo, este enorme poder analítico es un arma de doble filo. Del mismo modo que facilita la investigación digital legítima para destapar delitos, también proporciona a actores maliciosos una valiosa inteligencia táctica para planificar operaciones hostiles desde la comodidad del anonimato.

Rastreando amenazas desde el navegador

Las modernas plataformas en la nube permiten a los investigadores acceder a catálogos masivos e históricos con apenas unos pocos clics. Utilizando software OSINT avanzado, los analistas pueden geolocalizar bases de cibercriminales, documentar incidentes o auditar infraestructuras críticas. Esta inmensa facilidad operativa convierte la verificación visual en una competencia técnica indispensable para cualquier profesional dedicado a la ciberdefensa.

Cuando el mundo físico facilita el ciberataque

Esta transparencia radical presenta un grave riesgo sistémico para las organizaciones empresariales. Un atacante motivado puede estudiar fotografías detalladas para descubrir la ubicación exacta de los centros de datos o analizar los turnos del personal de vigilancia.

Esta fase de reconocimiento previo resulta fundamental para ejecutar intrusiones físicas y elaborar campañas avanzadas de ingeniería social con un alto grado de éxito.

El fin de la privacidad espacial

El avance descontrolado de la tecnología satelital plantea serios dilemas éticos que afectan directamente a nuestra vida diaria. Hasta hace poco, los muros de una vivienda o el vallado de una empresa garantizaban un nivel básico de intimidad frente a observadores externos. Sin embargo, la persistente mirada desde la órbita terrestre anula por completo estas defensas tradicionales, dejando al descubierto nuestros hábitos, bienes e infraestructuras. Esta realidad nos obliga a replantear el concepto de la privacidad física en la era digital. No es solo una cuestión de ética, sino un problema operativo de seguridad, ya que el acceso público a este nivel de detalle visual facilita enormemente el reconocimiento previo para cualquier tipo de ataque.

La falsa sensación de alejamiento

Alejarse de las grandes ciudades ya no garantiza la invisibilidad. Un refugio aislado en la montaña o un centro de datos construido en mitad del desierto son fotografiados a diario por estas constelaciones orbitales con la misma nitidez que el centro de una capital. Esta realidad destruye por completo el anonimato geográfico, demostrando que la distancia kilométrica ya no sirve como escudo contra la vigilancia remota.

Riesgos cotidianos para el ciudadano

Para la persona de a pie, el peligro reside en la creación involuntaria de un registro histórico de sus movimientos físicos. Detalles rutinarios, como alteraciones en su propiedad, los vehículos estacionados o sus horarios de entrada, quedan documentados permanentemente. Esta inmensa huella geoespacial permite a terceros aplicar técnicas de minería de datos para deducir estilos de vida y vulnerabilidades personales sin necesidad de hackear un solo dispositivo.

Desafíos de seguridad

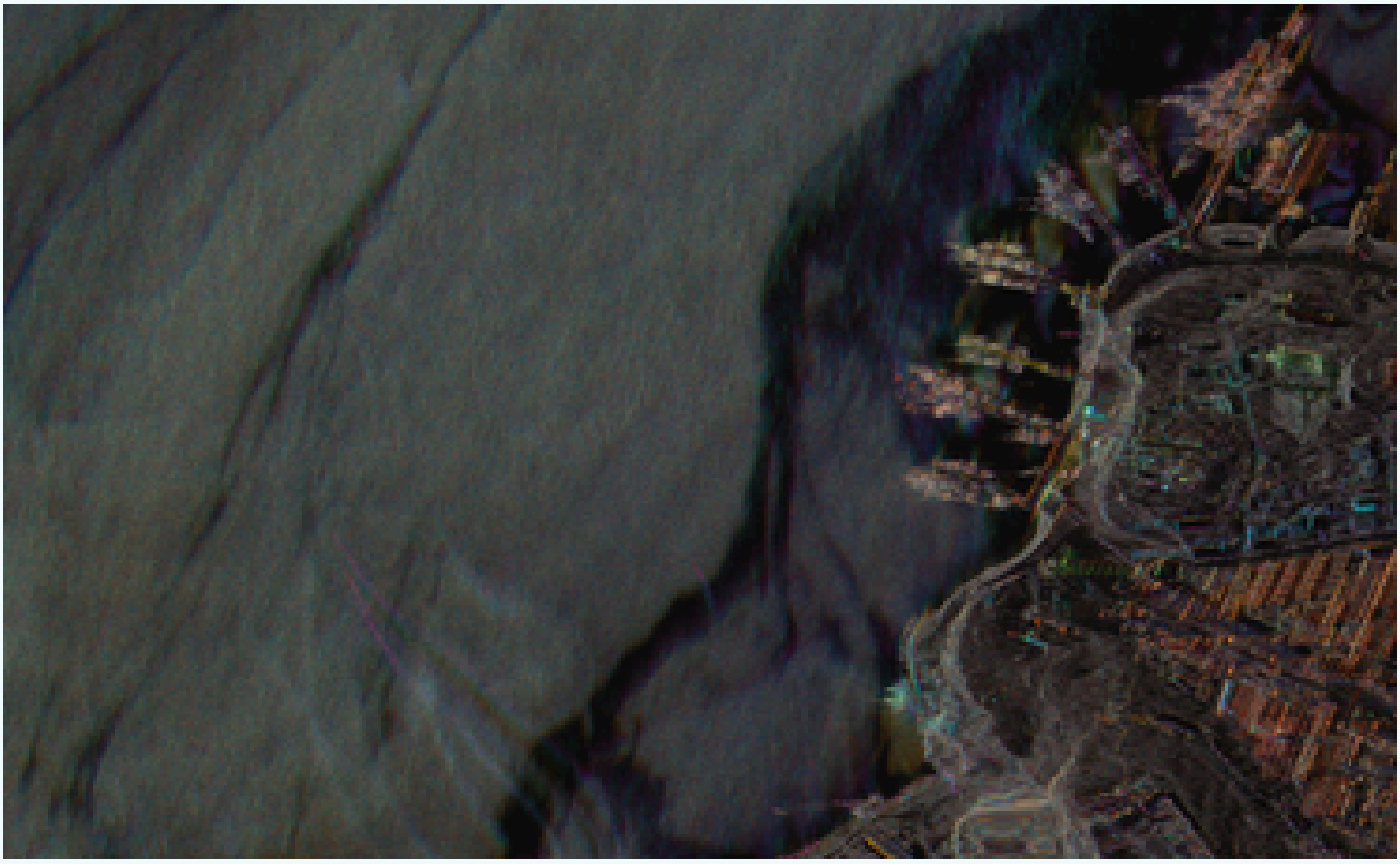
Desde la perspectiva de la seguridad corporativa e institucional, la disponibilidad pública de fotografías extremadamente detalladas exige adaptar las estrategias de defensa de forma inmediata. Los equipos de protección ya no solo deben blindar las redes informáticas terrestres, sino también intentar mitigar la exposición visual constante desde la estratosfera. El reconocimiento de un objetivo, paso inicial e indispensable en cualquier cadena de ataque, se ha vuelto un proceso trivial gracias a estas herramientas. Por ello, las organizaciones de todos los sectores deben incorporar obligatoriamente la evaluación de su huella visible en su gestión de riesgos para anticiparse a estas nuevas amenazas externas.

OPSEC orbital y tácticas de ofuscación

Para intentar contrarrestar esta brutal exposición, muchas instalaciones críticas están adoptando contramedidas avanzadas de ocultación que antes eran exclusivas del ámbito militar. Desde la instalación de redes de camuflaje térmico hasta el diseño de techos disruptivos que engañan al ojo del analista, la seguridad perimetral evoluciona rápidamente. Esta disciplina emergente busca enmascarar actividades sensibles y dificultar drásticamente el análisis visual directo del adversario.

La integración cibernética y física

El mayor desafío actual radica en asumir que la protección digital y la del mundo real son totalmente inseparables. Un atacante motivado puede analizar fotografías satelitales gratuitas para descubrir exactamente qué subestación eléctrica alimenta a un servidor crítico antes de lanzar un ataque informático combinado. Por tanto, lograr una verdadera resiliencia institucional exige una estrategia integral que defienda tanto las redes como la infraestructura física frente a estas amenazas.



Regulación y vacíos legales internacionales

La innovación tecnológica en la órbita terrestre ha superado con creces la capacidad de los legisladores para establecer normativas efectivas. El derecho internacional vigente fue redactado hace décadas, pensado estrictamente para los Estados soberanos en conflicto y no para las empresas privadas de la actualidad.

La absoluta falta de leyes claras sobre la recolección comercial de imágenes y su altísimo nivel de detalle genera un preocupante escenario de desamparo. Aunque ciertos países intentan censurar áreas críticas, la naturaleza global del espacio aéreo hace que estas prohibiciones locales resulten ineficaces.

Nos enfrentamos a la urgente necesidad de establecer un marco normativo moderno y verdaderamente adaptado a estas realidades.

Los límites de la resolución y la censura

Históricamente, algunos gobiernos limitaban por ley la resolución máxima a la que se podían comercializar fotografías de sus territorios sensibles. Sin embargo, la feroz competencia internacional ha obligado a relajar estas restricciones. Este fenómeno evidencia que aplicar políticas restrictivas de forma unilateral es inútil frente a un mercado de tecnología espacial donde siempre habrá un proveedor extranjero dispuesto a vender la captura sin censura.

El futuro de la legislación espacial

Los expertos jurídicos coinciden en que el camino a seguir no es la prohibición estricta, que resulta técnica y comercialmente inaplicable, sino exigir una trazabilidad absoluta en el uso de los datos. Las futuras leyes internacionales deberán equilibrar la libertad de información con la protección ciudadana. Promover activamente la ética digital será el pilar fundamental para lograr salvaguardar nuestros derechos civiles frente al persistente escrutinio satelital corporativo.

Repensando la seguridad en un mundo transparente

En definitiva, la accesibilidad masiva a estas imágenes nos obliga a entender la protección de una forma mucho más amplia. Ya no basta con blindar contraseñas o redes informáticas si la ubicación de nuestros servidores críticos o nuestras rutinas diarias quedan expuestas a vista de pájaro. Como futuros profesionales, el verdadero reto será diseñar estrategias que protejan esta huella física con el mismo rigor que aplicamos al entorno virtual. Aprender a convivir con la inteligencia geoespacial implicará encontrar un equilibrio realista: aprovechar su enorme potencial informativo sin renunciar a nuestro derecho básico a la privacidad.

PABLO DEL RÍO MARTÍNEZ

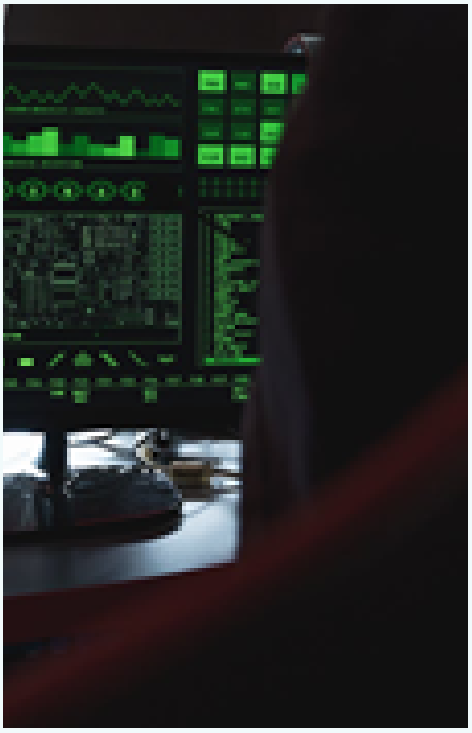
CIBERSEGURIDAD EN INTERNET OF THINGS

Vivimos rodeados de dispositivos inteligentes. Desde relojes que monitorizan nuestra salud hasta frigoríficos que nos sugieren la lista de la compra o asistentes de voz que nos responden a cualquier duda en segundos. El Internet de las Cosas (IoT) ha dejado de ser una promesa futurista para convertirse en una realidad integrada en nuestro día a día.

Pero en medio de esta comodidad, surge una pregunta: ¿Qué tan seguros son estos dispositivos?

Porque mientras nosotros ganamos comodidad y eficiencia, también estamos ampliando, sin darnos cuenta, la superficie de ataque frente a posibles ciberamenazas. Cada dispositivo conectado es, posiblemente, una puerta de entrada.

Y sí, puede sonar exagerado, pero no lo es tanto: tu cámara de seguridad, tus bombillas inteligentes o incluso tu cafetera conectada podrían ser el eslabón más débil de toda tu red. Puede que nadie quiera hackear tu tostadora, pero sí podrían utilizarla como punto de acceso para algo más interesante.



El problema: dispositivos inteligentes, seguridad limitada

El crecimiento del IoT ha sido tan rápido que, en muchos casos, la seguridad no ha evolucionado a la misma velocidad. Muchos dispositivos se diseñan priorizando la funcionalidad, la rapidez de salida al mercado o el coste, dejando la ciberseguridad en segundo plano.

Traduciéndose en prácticas como:
- Contraseñas por defecto que nunca se cambian
- Sistemas sin actualizaciones de seguridad
- Protocolos de comunicación poco seguros
- Falta de cifrado en los datos

El resultado es un ecosistema altamente conectado, pero también altamente vulnerable.
Un ejemplo claro fue la botnet Mirai, que en 2016 utilizó miles de dispositivos IoT (cámaras de vigilancia, grabadoras digitales, etc.) para lanzar uno de los mayores ataques de denegación de servicios. Lo preocupante no fue solo el ataque en sí, sino lo fácil que resultó comprometer dispositivos aparentemente inofensivos. Según el INCIBE, el principal método de infección de Mirai fue mediante el uso de credenciales por defecto en estos dispositivos.

Más allá del hogar, un riesgo para empresas y ciudades

Aunque solemos pensar en IoT exclusivamente para el uso doméstico, su impacto va mucho más allá. Empresas, industrias y ciudades están adoptando dispositivos conectados a gran escala:

sensores, maquinaria, sistemas de control o logística inteligente que permiten optimizar procesos y tomar decisiones.

En este contexto, el IoT se convierte en una pieza clave para la eficiencia y la transformación digital. Sin embargo, también amplía considerablemente la superficie de ataque. Una vulnerabilidad ya no solo compromete datos, sino que puede afectar a la continuidad del negocio y seguridad de las operaciones.

Imaginemos, por ejemplo, una fábrica paralizada por un ataque a sus sistemas automatizados o una ciudad inteligente con fallos en infraestructuras críticas como el transporte o la energía. En estos casos, el impacto va más allá de lo digital: afecta a procesos reales, a servicios esenciales e incluso a la seguridad de las personas.

Por todo ello, la ciberseguridad deja de ser únicamente un problema técnico para convertirse en un riesgo estratégico. Proteger los sistemas deja de ser únicamente un problema del área de IT, sino una prioridad a nivel organizativo que impacta directamente en la resiliencia, la reputación y la continuidad de cualquier entidad.

Demasiados dispositivos, poco control

Una de las mayores ventajas del IoT es precisamente su escala. Ya no hablamos de un par de dispositivos conectados, sino de ecosistemas formados por decenas, cientos o incluso miles de ellos, interactuando entre sí y generando datos de forma constante. Esta hiperconectividad permite automatizar procesos, optimizar recursos y mejorar la toma de decisiones en tiempo real, tanto en entornos domésticos como empresariales.

Este crecimiento exponencial complica enormemente la gestión de la seguridad. Mantener todos los dispositivos actualizados, monitorizar posibles vulnerabilidades o detectar comportamientos anómalos se convierte en una tarea compleja, especialmente en entornos empresariales donde conviven múltiples tecnologías, fabricantes y niveles de criticidad.

A esto se suma un factor clave: la falta de visibilidad. En muchos casos, ni siquiera se cuenta con un inventario completo de los dispositivos conectados a una red. Esto implica que pueden existir puntos vulnerables desconocidos, dispositivos obsoletos o configuraciones inseguras que pasan desapercibidos hasta que ya es demasiado tarde. En otras palabras, no se puede proteger aquello que no se conoce.

Además, existe un componente humano que no podemos ignorar. Tanto a nivel individual como corporativo, la concienciación en ciberseguridad, aunque cada vez mayor, sigue siendo limitada. Es habitual encontrar dispositivos con configuraciones por defecto, contraseñas débiles o malas prácticas derivadas del desconocimiento o la falta de tiempo.

En muchos casos, los riesgos no se perciben hasta que el problema ya ha ocurrido. Y cuando se trata de entornos conectados, ese problema rara vez afecta a un solo dispositivo; puede escalar rápidamente y comprometer todo el ecosistema.

Soluciones prácticas para un IoT más seguro

En Europa, ETSI EN 303 645 se ha consolidado como estándar de referencia para IoT de consumo: evita contraseñas universales por defecto, exige mantener el software actualizado y exige procesos para gestionar vulnerabilidades durante la vida del producto.

A nivel de arquitectura, Zero Trust, impulsado por NIST, plantea un cambio de enfoque: dejar de confiar automáticamente en todo lo que está dentro de la red y pasar a un sistema donde cada acceso se verifica de manera continua.

Aplicado al IoT, esto se traduce en identidad por dispositivo, mínimos privilegios, segmentación y registro/monitorización.

En el hogar, las medidas más rentables rara vez son sofisticadas: actualizar firmware, cambiar contraseñas, no abrir la administración del router o del dispositivo a Internet y aislar IoT en una red separada si es posible.

INCIBE lo resume en guías para ciudadanía y empresas centradas en configuración segura y mantenimiento.

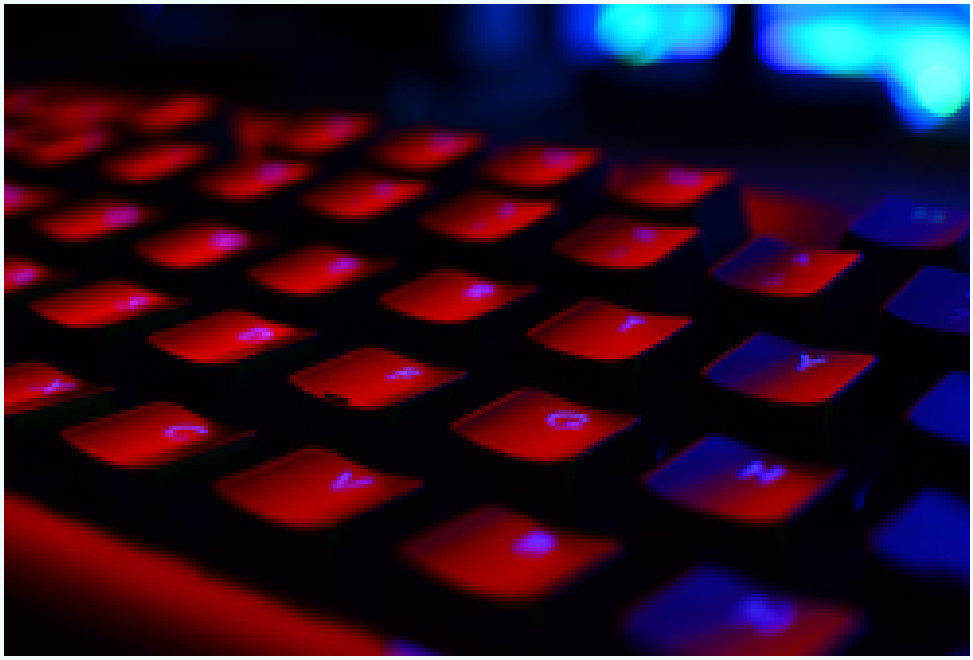
Sin embargo, más allá de la tecnología, hay un elemento fundamental: la responsabilidad compartida. La seguridad no depende únicamente de los fabricantes o de los sistemas, sino también del uso que hacemos de ellos.

Conclusión. Todo conectado, todo expuesto y todo por proteger

El Internet de las Cosas representa una de las mayores revoluciones tecnológicas de nuestro tiempo. Nos ofrece un mundo más eficiente, automatizado y conectado, donde la tecnología se integra de forma casi invisible en nuestra vida diaria. Pero esa misma conectividad implica exposición. Cada nuevo dispositivo es una oportunidad… pero también un riesgo.

La clave no está en frenar la innovación, sino en acompañarla con una cultura de seguridad sólida. Porque en un mundo donde todo está conectado, la pregunta ya no es si estamos expuestos, sino si estamos preparados.

Y quizá la próxima vez que un dispositivo inteligente nos haga la vida más fácil, también deberíamos preguntarnos si lo estamos haciendo lo suficientemente seguro.

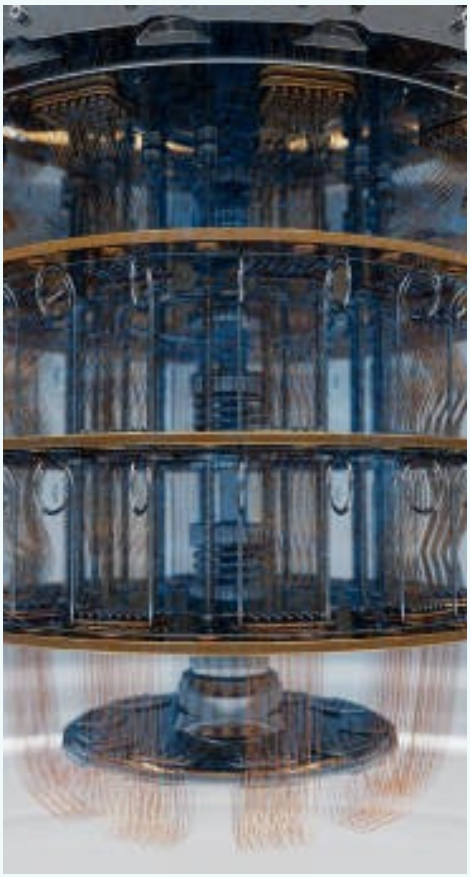


PABLO GARCÍA OLLERO

La computación cuántica: LA PRÓXIMA REVOLUCIÓN EMPRESARIAL QUE AÚN NO CONOCEMOS

La computación cuántica se ha convertido en una de esas ideas que todo el mundo reconoce, pero que pocos saben explicar con precisión. Se menciona como la próxima gran revolución tecnológica, como una herramienta capaz de resolver problemas imposibles para los ordenadores actuales, como el siguiente paso inevitable en la evolución de la informática. Y, sin embargo, cuanto más se habla de ella, más se diluye su significado.

El problema no es la falta de información, sino la forma en la que se interpreta. Se presenta como una mejora de lo existente —un ordenador más rápido, más potente— cuando en realidad no encaja dentro de esa lógica. No es una evolución lineal de la computación clásica, sino un cambio en la forma de abordar ciertos problemas. Y tratar de entenderla como una versión superior de lo que ya conocemos no solo es incorrecto, sino que impide ver dónde reside realmente su valor.



Según el National Institute of Standards and Technology (NIST, 2023), los sistemas cuánticos no están diseñados para tareas generales, sino para problemas donde la complejidad crece de forma exponencial. No sustituyen al ordenador clásico; operan en un espacio distinto. Y es precisamente ahí donde empieza a tomar forma su verdadero impacto.

Cuando el problema deja de ser calculable

Un ordenador clásico funciona sobre una estructura determinista: bits que representan valores concretos, operaciones secuenciales y resultados definidos. La computación cuántica introduce un cambio más profundo. El qubit no representa un estado fijo, sino una distribución de probabilidades que evoluciona hasta el momento de la medición. No es que el sistema "pruebe todas las soluciones a la vez", como suele simplificarse, sino que permite describir problemas donde el número de estados posibles hace inviable cualquier enfoque tradicional.

Esto no convierte a la computación cuántica en una herramienta universal. Al contrario, delimita con precisión su utilidad. No tiene sentido utilizarla para tareas cotidianas como procesar texto o ejecutar software convencional. En esos contextos, la computación clásica ya es extremadamente eficiente. La ventaja cuántica aparece únicamente cuando el problema deja de ser manejable mediante estructuras deterministas: simulaciones moleculares, optimización de sistemas complejos o modelado de interacciones con múltiples variables dependientes.

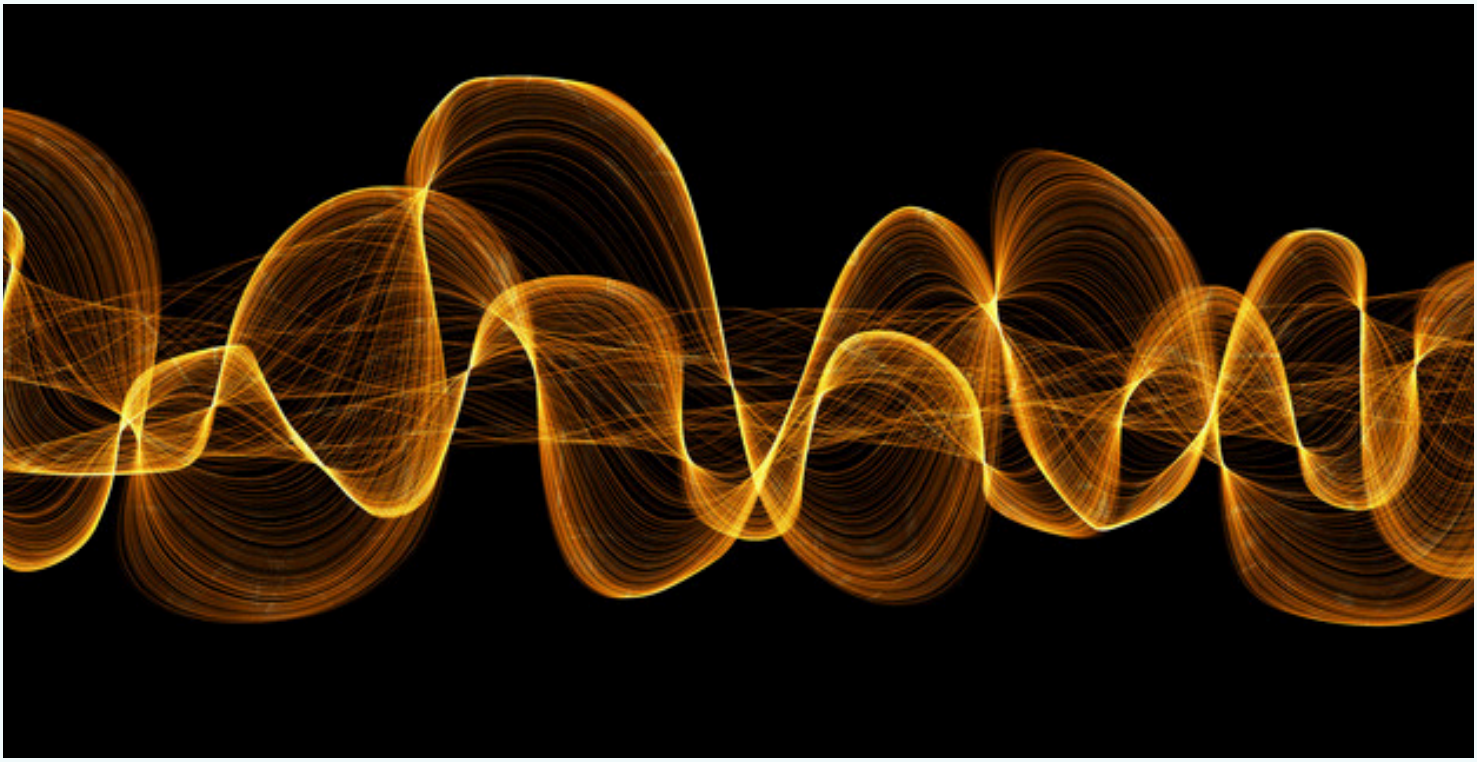
Como señala Preskill (2018) al definir la era NISQ (Noisy Intermediate-Scale Quantum), los dispositivos actuales son todavía limitados, ruidosos y altamente especializados. No estamos ante una tecnología madura ni generalista, sino ante una herramienta en desarrollo cuya potencia reside precisamente en su especificidad. No cambia todo; cambia aquello que ya era difícil de resolver.

Decidir mejor cuando todo se vuelve complejo

Esa especialización, lejos de ser una limitación, es lo que explica su interés empresarial. Las organizaciones no necesitan mejorar todos sus procesos, sino aquellos donde la complejidad condiciona el resultado. Y es en ese punto donde la computación cuántica empieza a adquirir sentido práctico.

El informe McKinsey Quantum Technology Monitor (2025) sitúa el mayor impacto potencial en sectores donde las decisiones dependen de sistemas altamente interdependientes: energía, farmacéutica, finanzas y logística. El valor estimado oscila entre 0,9 y 2 billones de dólares para 2035, no como consecuencia de una mejora general de la productividad, sino como resultado de decisiones más precisas en entornos complejos.

Un ejemplo concreto se encuentra en la optimización del tráfico urbano. Un estudio reciente basado en modelos híbridos de quantum annealing mostró reducciones de congestión de hasta un 25%, con resultados cercanos a los mejores algoritmos clásicos (Arranz et al., 2025, arXiv). No se trata de



una ventaja absoluta, sino contextual. Pero en escenarios donde cada variable afecta a cientos de otras, incluso pequeñas mejoras pueden tener consecuencias estructurales.

La computación cuántica no produce más; reduce la incertidumbre en decisiones que ya eran críticas. Y en ese margen es donde se construye su valor.

Toda revolución empieza siendo irrelevante

Las primeras computadoras eran máquinas enormes, costosas y de utilidad limitada. Durante años, su impacto fue marginal fuera de entornos muy concretos. Y, sin embargo, acabaron convirtiéndose en la base invisible de casi toda la infraestructura moderna.
La computación cuántica se encuentra en una fase comparable. Los sistemas actuales son inestables, difíciles de escalar y dependientes de entornos controlados. Pero eso no impide que su desarrollo avance. Empresas como IBM ya plantean arquitecturas híbridas que combinan computación clásica y cuántica, con hojas de ruta orientadas a sistemas tolerantes a fallos (IBM Quantum Roadmap, 2025). volverse vulnerables.

Mientras tanto, algunos sectores comienzan a adaptarse incluso antes de que la tecnología esté completamente madura. La criptografía es el ejemplo más claro. En 2024, el NIST publicó los primeros estándares de criptografía postcuántica, anticipando un escenario donde los sistemas actuales de cifrado podrían volverse vulnerables.

El cambio no es inmediato, pero ya está condicionando decisiones presentes. Y eso es, en sí mismo, una señal de transición.

Cuando la inteligencia artificial deja de ser determinista

Más capacidad no implica más comprensión

La intersección entre inteligencia artificial y computación cuántica amplifica esta idea, pero también introduce nuevos niveles de incertidumbre. En la práctica, el desarrollo actual se centra en áreas como la optimización del entrenamiento, la búsqueda en espacios complejos o los modelos híbridos. No existe, por ahora, evidencia sólida de que la computación supere de forma sistemática a los métodos clásicos en aprendizaje automático.

Una revisión publicada en npj Digital Medicine (Wilkinson et al., 2025) analizó miles de estudios sobre quantum machine learning y concluyó que la mayoría carecen de validación en entornos reales. Los resultados son prometedores, pero todavía inconsistentes. La tecnología no ha demostrado una ventaja generalizada, sino casos específicos donde podría aportar valor.

Sin embargo, centrarse únicamente en el rendimiento puede ser una forma de perder de vista lo esencial. El cambio no está solo en cuánto mejora un modelo, sino en cómo se construye y cómo representa el problema.

La probabilidad como estructura y la complejidad que no podemos simplificar

La computación clásica trabaja bajo una lógica determinista: incluso cuando introduce probabilidad, lo hace como una aproximación o como una forma de gestio-

nar incertidumbre externa. La computación cuántica, en cambio, opera en un marco donde la incertidumbre no es un defecto del sistema, sino una propiedad inherente.

Los estados no son únicos ni fijos, sino distribuciones que evolucionan hasta el momento de la medición. Esto no implica que el sistema sea caótico, sino que su comportamiento no puede describirse mediante una única trayectoria definida. La probabilidad deja de ser una herramienta para convertirse en la estructura misma del sistema, y ese cambio, aunque técnico en apariencia, tiene implicaciones más profundas de lo que parece.

Es en este punto donde aparece una analogía inevitable con el cerebro humano. No porque el cerebro funcione de manera cuántica —una idea que sigue siendo especulativa y sin evidencia concluyente—, sino porque ambos sistemas comparten una característica fundamental: su resistencia a ser simplificados. El cerebro no es una máquina lineal. Es un sistema dinámico, altamente interconectado, donde múltiples procesos ocurren de forma simultánea y donde el contexto altera constantemente el resultado. No responde a reglas simples ni a una lógica fácilmente reducible. La computación cuántica, en su propia naturaleza, también escapa a esa simplificación.

Y ahí es donde surge la intuición: no en la equivalencia, sino en la similitud estructural de la complejidad.

Simular, entender y el límite que no es técnico

Sin embargo, esa similitud abre una frontera que conviene tratar con cautela.

Una revisión en Neuroscience & Biobehavioral Reviews (Seth et al., 2025) muestra que no existe consenso científico sobre qué es la consciencia ni cómo emerge. Existen múltiples teorías —desde la Integrated Information Theory hasta el Global Workspace Model—, pero ninguna ha logrado establecer una explicación completa y verificable.

Esto introduce una distinción clave que suele pasarse por alto: podemos simular un sistema sin comprenderlo. Podemos reproducir patrones de comportamiento, generar respuestas coherentes o incluso imitar procesos complejos sin tener acceso a los mecanismos internos que los originan. La simulación es una aproximación funcional, no necesariamente una explicación, y esto resulta especialmente relevante cuando hablamos del cerebro.

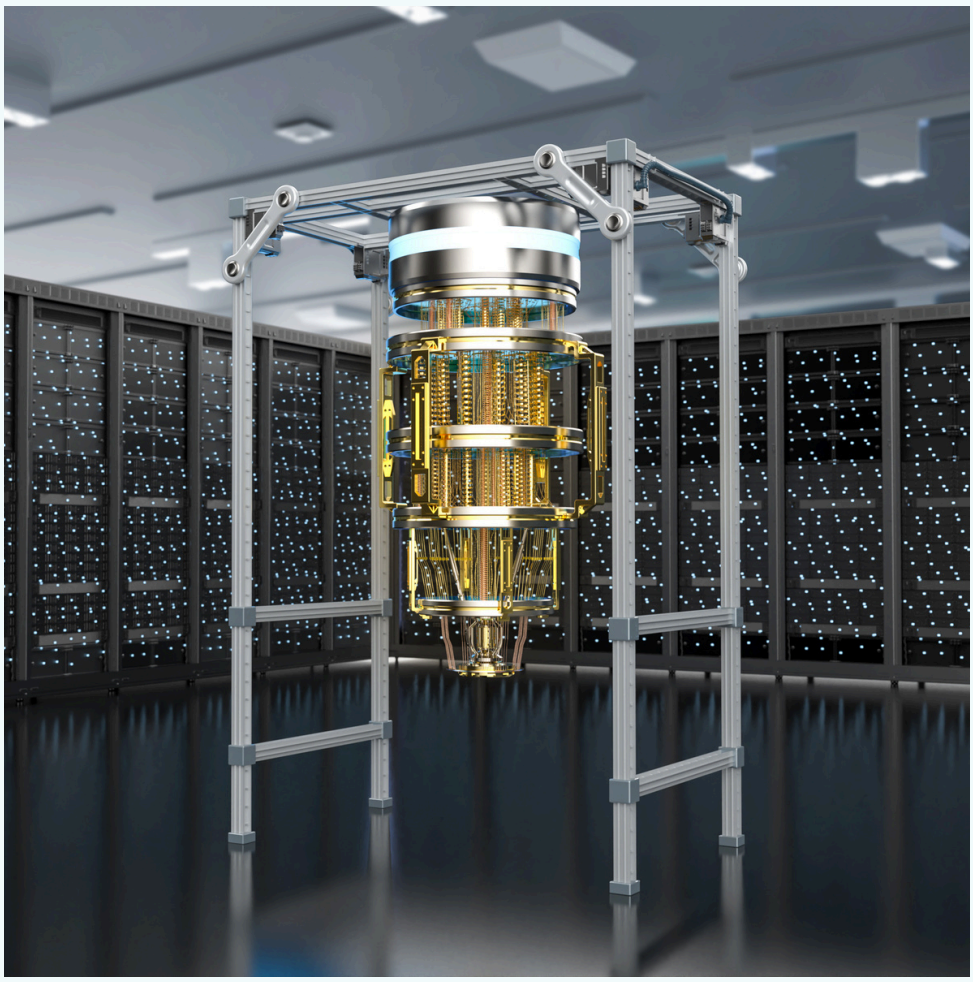
Si no entendemos el sistema original, ¿qué significa realmente replicarlo? ¿Es suficiente con reproducir su comportamiento externo para afirmar que lo hemos simulado, o la consciencia implica algo que no puede reducirse a una estructura computacional, por compleja que sea? ¿Podría un sistema avanzado —clásico o cuántico— generar una forma de experiencia interna, o simplemente estaríamos proyectando significado sobre una simulación cada vez más precisa?

Por ahora, no hay respuestas claras. Y quizá eso no sea una limitación tecnológica, sino una frontera conceptual.

La computación cuántica puede ofrecernos nuevas herramientas para modelar sistemas complejos. Puede ampliar nuestra capacidad de representar incertidumbre, explorar combinaciones y optimizar estructuras que hoy resultan inabarcables. Pero no elimina el problema fundamental.

El límite no está en lo que las máquinas pueden calcular, sino en lo que nosotros somos capaces de entender sobre lo que calculan. Y en ese sentido, la frontera que abre la computación cuántica no es solo tecnológica.

Es, inevitablemente, humana.



RAFAEL MATARRANZ YANES

EL CAMPO DE BATALLA DIGITAL: DRONES Y CIBERATAQUES

En las últimas décadas, la idea tradicional de guerra ha cambiado mucho y con ella la forma en que entendemos los conflictos. Ya no se trata solo de pelear en un lugar físico o enfrentarse cara a cara entre ejércitos. Hoy en día, el campo de batalla es una mezcla de lo digital y lo físico que están constantemente conectados. Por ejemplo, los drones vigilan áreas importantes mientras, al mismo tiempo, ciberataques silenciosos pueden afectar sistemas clave a miles de kilómetros. Este llamado “campo de batalla digital” trae nuevos retos para la seguridad global y cambia la importancia de áreas como la ciberseguridad y el análisis forense digital.

El avance tecnológico ha sido el principal factor de este cambio. Antes, la guerra giraba en torno a controlar territorio y tener más armas físicas. Pero con internet, las redes globales y la digitalización, el control en lo cibernético se volvió crucial. Estados y otros actores utilizan ahora herramientas digitales para cumplir objetivos militares, políticos o económicos sin tener que mandar tropas. Los ataques a infraestructuras vitales, las campañas de desinformación y el espionaje cibernético son parte común de los conflictos modernos.

En este contexto, los drones son uno de los elementos más visibles de la guerra actual. Son vehículos aéreos sin piloto que combinan eficiencia, precisión y menos riesgos para las personas, lo que los hace útiles en operaciones militares. Sirven para vigilar, hacer reconocimiento o atacar objetivos clave. Además, como son relativamente accesibles, no solo los usan ejércitos, sino también grupos no estatales, lo que complica aún más el panorama político y militar.

Pero el valor de los drones no está solo en su parte física, sino en cómo se conectan con otros sistemas tecnológicos. Necesitan software, comunicaciones inalámbricas, GPS y redes de datos para funcionar. Por eso, pueden ser vulnerables a ataques cibernéticos. Un dron puede ser interceptado o manipulado mediante técnicas como el spoofing de GPS o la interferencia en señales. Esto muestra que la ciberseguridad es una parte esencial en cualquier sistema militar moderno, no solo un apoyo extra.

Los ciberataques son una herramienta poderosa y flexible en este nuevo escenario. No necesitan presencia física y se pueden hacer de forma remota manteniendo el anonimato, lo que dificulta identificar al responsable. Ataques como la denegación de servicio, malware avanzado o espionaje continuo pueden paralizar infraestructuras, cortar comunicaciones y robar información sensible sin disparar un solo tiro.

La combinación de drones y ciberataques ha dado lugar a la guerra híbrida, una estrategia que mezcla diferentes aspectos del conflicto para ser más efectiva. Por ejemplo, un ciberataque puede desactivar sistemas de defensa antes de un ataque con drones, o los drones pueden enviar información en tiempo real que se procesa digitalmente. Esto permite actuar con más precisión y dificulta la reacción del adversario.

En este escenario, el análisis forense digital es fundamental. No solo investiga lo que pasó después de un ataque, sino que también ayuda a mejorar la defensa y entender las tácticas de los atacantes. Con los drones, esto implica recuperar registros de vuelo, estudiar comunicaciones interceptadas o identificar manipulaciones. Así, se pueden reconstruir eventos y, a veces, encontrar a los responsables.

Sin embargo, hacer análisis forense en guerra digital tiene sus retos. La información puede ser muy volátil, hay cifrados avanzados y falta de estándares en varios sistemas, lo que complica reunir y analizar pruebas.

Además, los atacantes usan métodos sofisticados para esconder su identidad, haciendo aún más difícil saber quién está detrás. A pesar de eso, seguir desarrollando herramientas y métodos en esta área es clave para mantener la seguridad en un entorno cada vez más complicado.

Más allá de la parte técnica, el uso de drones y ciberataques plantea dudas éticas y legales. Poder atacar sin que haya una persona controlando directamente, como ocurre con drones autónomos, abre debate sobre quién es responsable y cómo se debe usar la fuerza. Por otro lado, los ciberataques desafían las leyes tradicionales porque no siempre está claro cuándo un ataque digital se considera un acto de guerra. Esto muestra que hace falta crear reglas internacionales que se ajusten a esta nueva realidad.

Mirando al futuro, es probable que la importancia de estos elementos siga creciendo. La inteligencia artificial en drones dará más autonomía y capacidad de decisión, mientras que los ciberataques serán cada vez más avanzados y automáticos. Ejemplos como enjambres de drones que trabajan juntos o sistemas ciberfísicos completamente integrados podrían cambiar aún más cómo se desarrollan los conflictos.

En este contexto, los expertos en ciberseguridad y análisis forense digital tendrán un papel muy importante. Su capacidad para encontrar vulnerabilidades, responder a incidentes y analizar ataques será fundamental para proteger tanto el ámbito militar como el civil. Capacitarse en estas áreas no solo abre oportunidades laborales, sino que también ayuda a proteger infraestructuras y sistemas clave en un mundo cada vez más conectado.

En resumen, el campo de batalla digital no es algo que venga en el futuro, sino una realidad que evoluciona constantemente. La combinación de drones y ciberataques ha cambiado la manera en que se llevan los conflictos, creando nuevas dinámicas que requieren enfoques multidisciplinarios.

Conocer bien este entorno es vital para anticipar amenazas y desarrollar defensas efectivas. En un mundo donde unas líneas de código pueden causar tanto daño como armas tradicionales, el conocimiento se vuelve la herramienta más importante para enfrentar los retos del siglo XXI.

RUBÉN VALVERDE ROMERO

LA IA APLICADA A LA BIOINFORMÁTICA

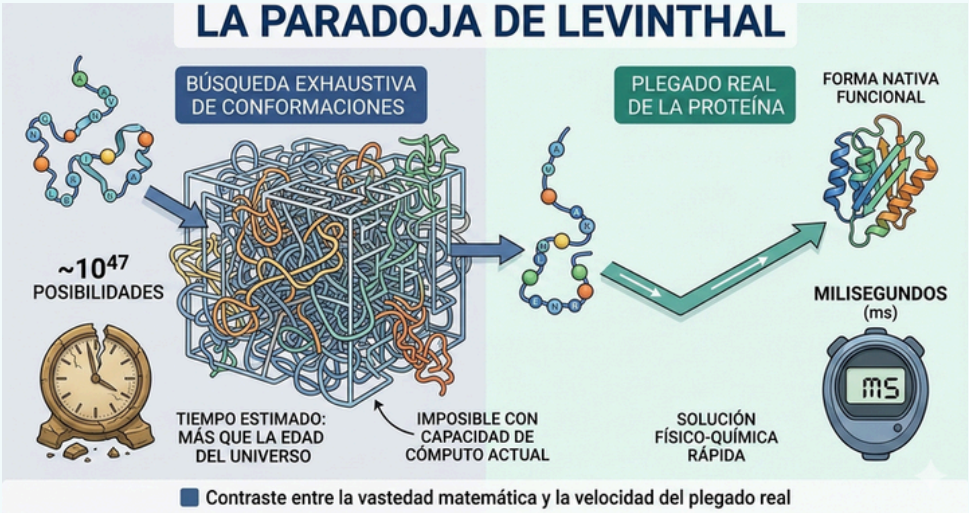
En 2022, el equipo de DeepMind publicó en la base de datos AlphaFold Protein Structure Database las estructuras predichas de más de 200 millones de proteínas, cubriendo prácticamente la totalidad de los organismos secuenciados conocidos (Varadi et al., 2022). Para poner esa cifra en perspectiva: la comunidad científica había tardado más de sesenta años en determinar experimentalmente las estructuras de 170.000 proteínas mediante cristalografía de rayos X y criomicroscopía electrónica. AlphaFold2 multiplicó ese acervo por más de mil en cuestión de meses.

El impacto fue inmediato y transversal. Investigadores en malaria utilizaron las estructuras predichas de proteínas del parásito Plasmodium falciparum para identificar dianas terapéuticas previamente inaccesibles (Gane et al., 2023). En oncología, la disponibilidad masiva de estructuras de proteínas mutadas ha acelerado el diseño de inhibidores a medida. En biotecnología, el diseño de enzimas industriales —que antes requería años de mutagénesis dirigida y cristalografía— ha pasado a apoyarse en estructuras computacionales como punto de partida validado. La herramienta está disponible gratuitamente, lo que ha democratizado el acceso a la biología estructural para laboratorios sin los recursos de las grandes farmacéuticas.

El Problema: Un Espacio de Búsqueda Intratable

Para comprender qué resolvió AlphaFold2, es necesario entender la naturaleza del problema al que se enfrentaba. Las proteínas son cadenas de aminoácidos que, una vez sintetizadas, se pliegan espontáneamente en una forma tridimensional específica. Esa forma determina su función: una enzima que cataliza una reacción, un receptor que transmite una señal, una proteína estructural que da rigidez a una célula. Conocer la estructura es, en muchos casos, conocer el mecanismo de acción.

El desafío computacional es de una magnitud difícil de intuir. Según la estimación clásica conocida como la paradoja de Levinthal, una proteína de tamaño moderado tendría del orden de 10^47 conformaciones posibles si cada enlace rotable tomase únicamente tres posiciones discretas (Levinthal, 1969). Una búsqueda exhaustiva de ese espacio sería físicamente imposible, incluso con toda la capacidad de cómputo actual.



Contraste entre la vastedad matemática y la velocidad del plegado real

Sin embargo, la proteína encuentra su forma correcta en milisegundos mediante un proceso físico-químico aún no completamente comprendido. Los métodos previos al aprendizaje automático —basados en minimización de energía potencial y búsqueda heurística, como Rosetta o I-TASSER— eran eficaces cuando existían proteínas homólogas con estructura conocida. El problema sin resolver era el de las proteínas huérfanas: aquellas sin parientes estructurales en las bases de datos. Precisamente las más interesantes desde el punto de vista terapéutico.

Mecanismo: Tres Representaciones y una Geometría Impuesta

La contribución central de AlphaFold2 no fue escalar los enfoques anteriores, sino rediseñar la representación del problema. Jumper et al. (2021) describieron una arquitectura que construye y refina simultáneamente tres niveles de información:

La representación MSA. Para cada proteína de consulta, el modelo genera un Multiple Sequence Alignment (MSA) con homólogos evolutivos extraídos de bases de datos como UniRef90 y MGnify. Esta matriz de secuencias alineadas no es un simple enriquecimiento de datos: codifica información de coevolución. Cuando dos posiciones i y j de una proteína varían de forma correlacionada a lo largo de millones de años de evolución, es porque probablemente se encuentran en contacto físico en la estructura tridimensional. El MSA convierte la historia evolutiva de una proteína en señal geométrica.

La representación de pares. Complementariamente, el modelo mantiene una matriz L × L —donde L es la longitud de la secuencia— en la que cada celda (i, j) acumula información sobre la relación entre el residuo i y el residuo j: distancia probable, orientación relativa, tipo de contacto. Esta representación es el vehículo principal de razonamiento geométrico de la red. El módulo de estructura. En las fases finales, el modelo trabaja directamente con marcos de referencia rígidos en SE(3) —el grupo matemático que describe rotaciones y traslaciones en el espacio tridimensional— para refinar las posiciones de cada átomo.

El bloque que integra estas representaciones es el Evoformer, un transformer modificado en el que la atención estándar se sustituye parcialmente por operaciones triangulares. La lógica es geométrica: si se conocen las relaciones entre los pares (i, k) y (k, j), es posible actualizar la relación (i, j) de forma consistente. Este mecanismo, denominado triangle multiplicative update, propaga información de contacto de forma globalmente coherente, algo que los transformers convencionales aplicados a secuencias no garantizan (Jumper et al., 2021). La fase de refinamiento estructural utiliza Invariant Point Attention (IPA), un mecanismo de atención diseñado para ser equivariante a rotaciones y traslaciones globales: Si la proteína completa se desplaza o rota en el espacio, las relaciones internas predichas permanecen inalteradas. Esta propiedad no es un detalle técnico menor; es una condición necesaria para que el modelo sea físicamente coherente, ya que la estructura nativa de una proteína está definida únicamente hasta isometría global.

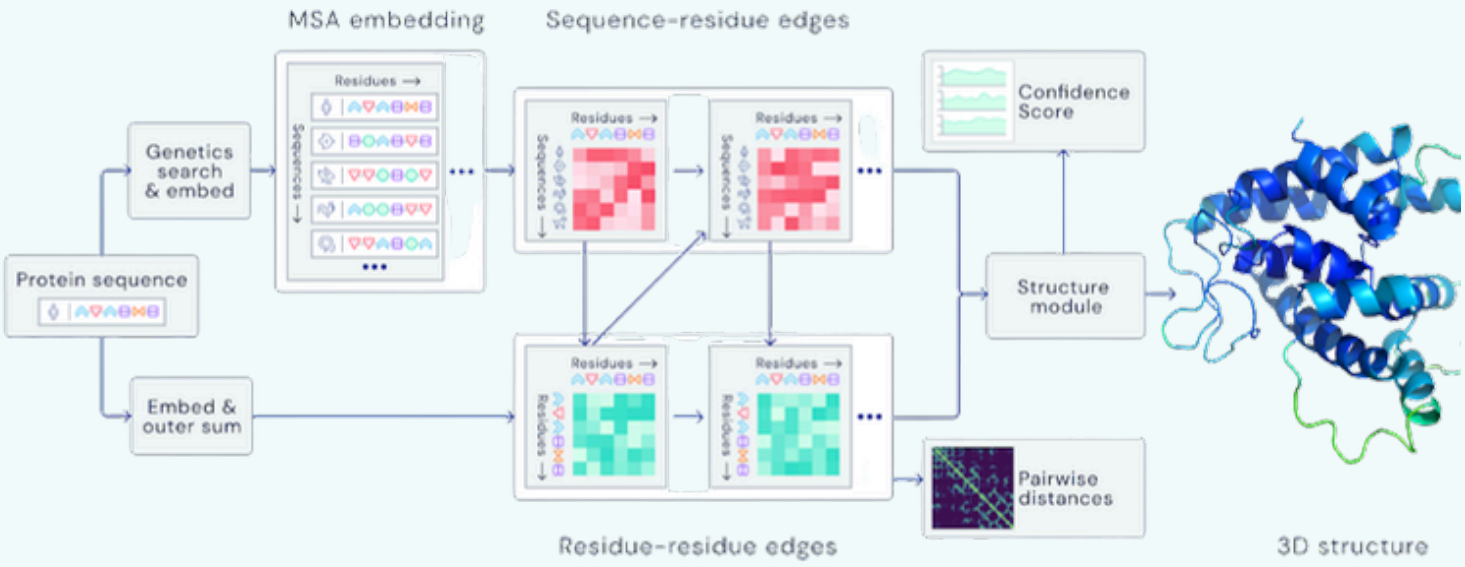
El entrenamiento incorpora además dos decisiones de diseño con impacto directo en el rendimiento. El primero es el reciclado iterativo: la red se aplica varias veces sobre la misma entrada, utilizando la predicción de cada iteración como punto de partida de la siguiente, de forma análoga a como un método de gradiente desciende hacia un mínimo. El segundo es la autodestilación: el modelo se preentrena con predicciones propias de alta confianza sobre proteínas sin estructura experimental conocida, ampliando el conjunto de entrenamiento efectivo muy por encima de las estructuras disponibles en el Protein Data Bank (Jumper et al., 2021).

Implicaciones: Un Cambio de Paradigma en Biología Estructural

Los resultados en CASP14 —el benchmark internacional bianual de predicción de estructura proteica— fueron concluyentes. AlphaFold2 obtuvo una mediana de GDT_TS de 92,4 sobre 100, superando al segundo clasificado por un margen mayor que el que separaba a este del resto del campo (Jumper et al., 2021). El comité evaluador del CASP señaló que el problema central del protein folding había sido resuelto a efectos prácticos para la mayoría de las proteínas globulares.

Las consecuencias prácticas se han ido materializando con rapidez. En el ámbito del descubrimiento de fármacos, la disponibilidad de estructuras de alta confianza permite realizar virtual screening basado en estructura —el proceso de evaluar computacionalmente millones de moléculas contra una diana proteica— sin necesidad de cristalografía experimental previa. Esto no elimina la experimentación, pero desplaza el cuello de botella hacia fases más avanzadas del proceso, reduciendo costes y tiempos en la fase de identificación de hits (Gane et al., 2023).

La arquitectura del Evoformer ha demostrado además una capacidad de generalización más allá de las proteínas. AlphaFold- Multimer extiende el enfoque a complejos proteína-proteína (Evans et al., 2021), mientras que RoseTTAFoldNA adapta representaciones similares para ácidos nucleicos (Baek et al., 2023). AlphaFold3, publicado en 2024, amplía el marco a proteínas con ligandos pequeños, ADN y ARN, consolidando la pair representation con operaciones triangulares como una primitiva arquitectónica de uso general para problemas de relaciones entre entidades biológicas (Abramson et al., 2024).



Para la comunidad de aprendizaje automático, la lección de AlphaFold2 trasciende la biología. El modelo no ganó CASP14 por ser el más grande ni por disponer de más datos. Lo hizo porque cada componente de su arquitectura codificaba una propiedad geométrica real del problema: la coevolución como señal de contacto, la consistencia triangular como regularizador implícito, la equivariancia como restricción física. El inductive bias estructural —cuando refleja fielmente la geometría del dominio— puede ser más determinante que la escala paramétrica.

Conclusión

AlphaFold2 representa uno de los casos más documentados en los que el aprendizaje automático ha resuelto un problema científico abierto de relevancia directa para la sociedad. Su impacto no se limita a un benchmark: ha transformado la forma en que los laboratorios de todo el mundo abordan la biología estructural, el diseño de proteínas y el desarrollo de fármacos.

La decisión de publicar sus predicciones de forma abierta y gratuita amplifica ese impacto al ponerlo al alcance de cualquier investigador con conexión a internet. Desde la perspectiva del diseño de sistemas de aprendizaje automático, el modelo establece un principio de vigencia general: la elección de representación y la codificación explícita de las simetrías del problema no son decisiones secundarias, sino el núcleo de la solución. En un campo donde la tendencia dominante es escalar arquitecturas existentes, AlphaFold2 recuerda que entender el problema sigue siendo el paso previo más rentable.

SANDRA ESPIÑEIRA BRICEÑO

CYBERSECURITY IN THE AGE OF AUTONOMOUS ROBOTICS

For many years, cybersecurity has mainly focused on protecting data, networks and information systems. However, the development of technologies such as artificial Intelligence and machine learning have led to the emergence of systems capable of interacting autonomously with the physical environment. In this context, autonomous robotics has become one of the most disruptive innovations of the twenty-first century.

Autonomous robots are no longer limited to executing pre-programmed tasks. Instead, they can perceive their surroundings, process information in real time, and make decisions without direct human intervention. This capability has significantly improved efficiency across multiple sectors, from industrial production to healthcare services. Nevertheless, this increasing level of autonomy also introduces new risks, as any vulnerability within these systems may result not only in digital consequences but also in physical harm.

This article aims to examine the main cybersecurity challenges in autonomous robotics and to highlight the importance of developing secure systems in an increasingly interconnected world.

The expansion of autonomous robotics

Autonomous robotics has experienced significant growth in recent years, driven by the convergence of various digital technologies. In industrial environments, collaborative robots work alongside human operators, improving productivity and reducing errors. In the logistics sector, automated systems optimize warehouse management and distribution processes, while in healthcare, robots are increasingly used for assistance and even for surgical procedures.

This progress has been made possible by advances in areas such as Computer Vision, which enables robots to interpret visual data and recognise patterns, as well as improvements in data processing capabilities. However, this evolution also increases technological dependency and expands the potential attack surface. As robots become increasingly connected to networks and external systems, they become more vulnerable to cyber threats.

Main threats in autonomous robotics

The complexity of autonomous robots, which integrate multiple technological components, makes them particularly vulnerable to several types of cyber threats. Firstly, systems based on artificial intelligence may be targeted through attacks aimed at altering their behavior.

Techniques such as data poisoning or model manipulation can lead to incorrect decision-making processes.

In addition, the sensors that allow robots to perceive their environment represent a critical point of vulnerability. Signal interference or the creation of misleading stimuli may cause the system to misinterpret reality, potentially resulting in operational failures or unsafe situations. Furthermore, the connectivity of these devices increases the risk of unauthorized access. If an attacker gains access to the network, they may be able to control the robot or alter its functionality.

Finally, vulnerabilities in software and firmware must not be overlooked. Coding errors or a lack of regular updates can be exploited by attackers, highlighting the importance of effective vulnerability management.

Impact of cyberattacks

Unlike other areas of cybersecurity, attacks on autonomous robotic systems can have consequences that go beyond the digital domain. A cyberattack may disrupt industrial processes, leading to significant financial losses for organizations. In certain contexts, such as manufacturing or healthcare, these failures may also pose direct risks to human safety.

The impact also extends to the reputational level. Organizations affected by security incidents may lose the trust of customers and stakeholders, making it more difficult to adopt modern technologies. Therefore, ensuring the security of these systems is not only a technical challenge but also a strategic priority.

Protection strategies

To address these challenges effectively, it is crucial to adopt a comprehensive approach to cybersecurity in autonomous robotics.

Firstly, security must be integrated from the preliminary stages of system design. This approach, commonly referred to as “security by design," helps to identify and mitigate vulnerabilities before deployment.

Moreover, protecting communications is a key factor. The use of secure protocols, data encryption, and network segmentation can significantly reduce the risk of unauthorized access and data manipulation. Continuous monitoring also plays a crucial role, as it allows organizations to detect abnormal behavior in real time and respond quickly to potential threats.

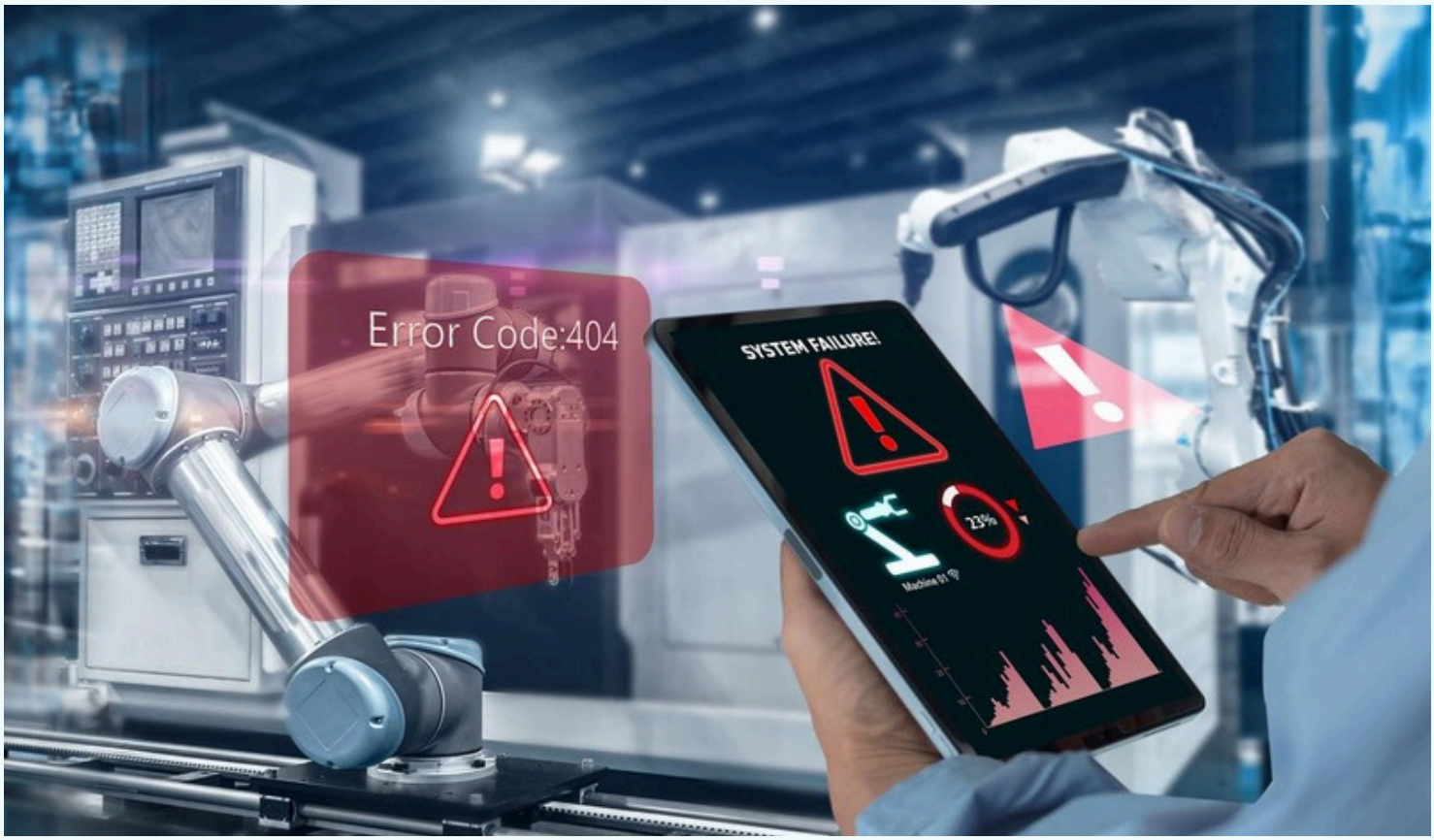
Finally, regular software updates and effective vulnerability management are essential to maintaining system security. Identifying and correcting weaknesses reduces exposure to cyberattacks and enhances the resilience of autonomous robotic systems.

Conclusion

Autonomous robotics represents one of the most significant developments in the digital future, with an increasing impact across a wide range of economic sectors. Its ability to improve efficiency and optimize processes makes it a key technology within digital transformation. However, this progress also introduces important cybersecurity challenges that must not be ignored.

As these systems become more autonomous and interconnected, it is essential to develop solutions that ensure their safety and reliability. Protecting autonomous robots is not only about safeguarding data but also about preventing physical risks and maintaining trust in technology.

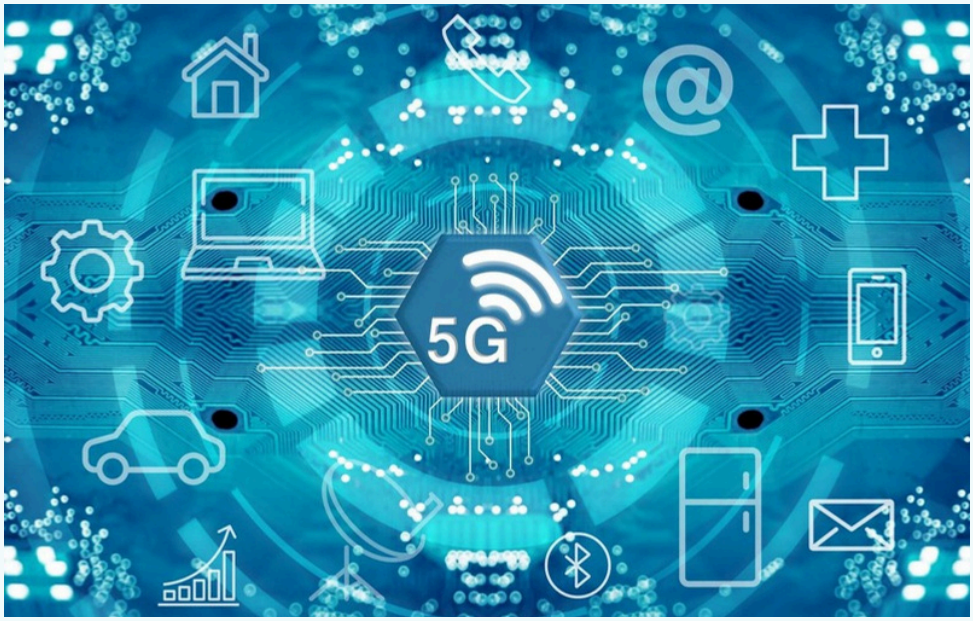
Ultimately, cybersecurity is a fundamental element for the sustainable development of autonomous robotics, as protecting machines ultimately means protecting people.



SANDRA GUTIERREZ DE TENA

EVOLUCIÓN DE LOS CIBERATAQUES

Para empezar, la historia de los ciberataques es, en muchos sentidos, la historia de la propia evolución tecnológica. Cada avance que facilita la vida digital también abre nuevas oportunidades para quienes buscan aprovecharse de las vulnerabilidades.



En las últimas décadas, la aparición de tecnologías emergentes como la inteligencia artificial, el IoT, la computación en la nube, el 5G o el blockchain ha transformado radicalmente el panorama de la ciberseguridad. Los ataques ya no son simples experimentos de aficionados, sino operaciones sofisticadas, automatizadas y, en muchos casos, altamente lucrativas. Entender cómo han evolucionado es clave para comprender los riesgos actuales y prepararse para el futuro.

De los primeros virus al cibercrimen organizado

En los primeros años, los ciberataques eran relativamente simples. Muchos virus se creaban por curiosidad o para demostrar habilidades técnicas. Se propagaban mediante disquetes, archivos adjuntos o descargas poco seguras, y su impacto solía ser visible: mensajes en pantalla, archivos dañados o sistemas lentos. Aunque molestos, estos ataques eran relativamente fáciles de detectar y, en muchos casos, de eliminar.

Con la expansión de internet y la digitalización de servicios, la situación cambió. El cibercrimen comenzó a avanzar cada vez más. Los atacantes descubrieron que podían obtener beneficios económicos robando datos, extorsionando a empresas o vendiendo accesos a sistemas comprometidos. Surgieron nuevas amenazas como el phishing, que engaña a los usuarios para que revelen contraseñas, o el ransomware, que bloquea archivos y exige un pago para liberarlos.

Lo que antes eran ataques genéricos se convirtió en campañas dirigidas. Los atacantes empezaron a estudiar a sus víctimas, a utilizar técnicas de ingeniería social y a permanecer dentro de los sistemas durante largos periodos sin ser detectados. Este cambio marcó el inicio de una nueva era en la que la sofisticación y la planificación se volvieron fundamentales.

La IA: una herramienta poderosa, tanto para bien como para mal

La inteligencia artificial ha transformado muchos sectores, y la ciberseguridad no es la excepción. Las empresas utilizan algoritmos para detectar comportamientos sospechosos, analizar grandes volúmenes de datos y responder rápidamente a incidentes. Sin embargo, los atacantes también han adoptado estas herramientas.

Hoy en día, la IA se emplea para crear ataques más convincentes. Por ejemplo, los correos de phishing ya no son mensajes mal redactados. Ahora pueden ser personalizados, con información específica de la víctima extraída de redes sociales o bases de datos filtradas. Esto aumenta enormemente la probabilidad de éxito.

Además, la inteligencia artificial permite generar voz y texto de forma automática. Esto ha dado lugar a estafas en las que se imita la voz de un directivo para solicitar transferencias urgentes, o se crean mensajes extremadamente creíbles. Incluso el malware puede adaptarse al entorno, modificando su comportamiento para evitar ser detectado. Es un juego constante del gato y el ratón, donde cada mejora defensiva genera nuevas tácticas ofensivas.

IoT y la explosión de dispositivos vulnerables

El internet de las cosas (IoT) ha introducido millones de dispositivos conectados: cámaras, relojes inteligentes, electrodomésticos, sensores industriales y muchos más. Cada uno de ellos representa una posible puerta de entrada. El problema es que muchos se diseñan con la funcionalidad como prioridad, dejando la seguridad en segundo plano.

Contraseñas por defecto, actualizaciones inexistentes o configuraciones inseguras son errores comunes. Los atacantes

aprovechan estas debilidades para tomar control de miles de dispositivos y crear redes masivas llamadas botnets. Estas redes pueden lanzar ataques coordinados, como saturar servicios web o distribuir malware.

El riesgo aumenta cuando estos dispositivos forman parte de infraestructuras críticas. Un sensor manipulado o un sistema industrial comprometido puede tener consecuencias físicas reales. Ya no se trata solo de datos robados, sino de interrupciones en servicios esenciales, fallos en procesos industriales o incluso riesgos para la seguridad de las personas.

La nube: comodidad con nuevos desafíos

La nube ha revolucionado la forma de trabajar. Las empresas pueden almacenar datos, ejecutar aplicaciones y escalar recursos sin necesidad de infraestructura propia. Sin embargo, esta flexibilidad también introduce nuevos riesgos.

Uno de los problemas más comunes es la mala configuración. Bases de datos expuestas, permisos excesivos o claves de acceso mal protegidas han provocado filtraciones masivas. A menudo, no se trata de fallos del proveedor, sino de errores humanos al configurar los servicios.

Además, los atacantes han aprendido a aprovechar estos entornos. Pueden secuestrar recursos para minar criptomonedas, utilizar cuentas comprometidas para desplegar malware o moverse lateralmente dentro de la infraestructura. La nube, que facilita tanto la innovación, también permite escalar ataques con gran rapidez.

El impacto del 5G

La llegada del 5G promete mayor velocidad y menor latencia, pero también implica que más dispositivos estarán conectados simultáneamente. Esto amplía la superficie de ataque. La virtualización de redes, característica del 5G introduce nuevas capas de software que pueden contener vulnerabilidades. Además, el 5G impulsa el crecimiento del IoT, creando entornos altamente interconectados. Un fallo en un dispositivo puede propagarse rápidamente. Los ataques coordinados desde miles de dispositivos conectados se vuelven más viables, y la protección requiere enfoques más dinámicos.

Esta conectividad también significa que los ciberataques pueden tener efectos más amplios. Un incidente en una red puede afectar múltiples servicios, desde transporte hasta comunicaciones, generando un impacto mayor que en generaciones anteriores de tecnología.

Blockchain y criptomonedas: nuevas oportunidades para el fraude

El blockchain se diseñó con la seguridad en mente, pero no está libre de riesgos. Las plataformas de intercambio de criptomonedas han sido objetivo frecuente de robos, y los contratos inteligentes mal diseñados han permitido explotaciones complejas.

Las criptomonedas también han facilitado la monetización del cibercrimen. El ransomware, por ejemplo, depende en gran medida de pagos en criptodivisas, que son más difíciles de rastrear. Además, han surgido campañas de phising dirigidas específicamente a usuarios de carteras digitales.

Aunque la tecnología ofrece ventajas en transparencia y descentralización, su uso indebido demuestra que la seguridad no depende solo del diseño técnico, sino también de la implementación y del comportamiento de los usuarios.

Automatización del cibercrimen

Otro cambio importante es la automatización. Hoy existen herramientas que permiten lanzar ataques con pocos conocimientos técnicos. Kits de explotación, malware como servicio y mercados clandestinos han democratizado el acceso al cibercrimen.

Esto significa que más actores pueden participar. Decir que no todos son expertos, algunos simplemente compran herramientas y las utilizan. Como resultado, el número de ataques ha aumentado significativamente. Los sistemas son escaneados constantemente en busca de vulnerabilidades, y cualquier fallo puede ser explotado en cuestión de minutos.

Esta industrialización del cibercrimen ha creado una economía. Se venden datos robados, accesos a redes corporativas y servicios completos de ataque. Es un ecosistema organizado, con roles y especialización.

Deepfakes y la nueva era de la manipulación

Las tecnologías de creación de contenido han dado lugar a los deepfakes, videos y audios falsos extremadamente convincentes. Estos se utilizan para suplantar identidades, difundir desinformación o cometer fraudes.

Un atacante puede crear un video falso de un ejecutivo solicitando una transferencia urgente o un audio que imite a un familiar. Este tipo de ataques explota la confianza humana y puede ser difícil de detectar. Además, la manipulación de contenido puede tener impactos sociales y políticos significativos.

La combinación de ingeniería social y deepfakes representa una evolución importante, ya que los ataques ya no se limitan a explotar vulnerabilidades técnicas, sino también psicológicas.

Infraestructuras críticas bajo amenaza

A medida que sectores como energía, salud y transporte se digitalizan, se convierten en objetivos atractivos. Los ataques a hospitales han demostrado cómo el ransomware puede paralizar servicios médicos. En el sector energético, la manipulación de sistemas puede provocar apagones.

Estos ataques suelen ser más complejos y, en algunos casos, están vinculados a intereses geopolíticos. La interdependencia entre sistemas aumenta el riesgo de efectos en cadena. Un incidente en un sector puede afectar a otros, amplificando el impacto.

La protección de estas infraestructuras requiere cooperación entre organizaciones y una estrategia coordinada. La ciberseguridad ya no es solo un problema técnico, sino también estratégico.

¿Cómo será el futuro?

Todo indica que los ciberataques seguirán evolucionando. La inteligencia artificial ofensiva será más común, los dispositivos conectados continuarán creciendo y surgirán nuevas tecnologías con sus propias vulnerabilidades. También se espera un aumento del ransomware dirigido y de las campañas combinadas con desinformación.

El tiempo de respuesta será cada vez más crítico. Las vulnerabilidades se explotarán rápidamente, y las organizaciones deberán adoptar un enfoque más proactivo.

La seguridad basada en confianza cero, la monitorización continua y la colaboración serán esenciales.

Conclusión

La evolución de los ciberataques refleja la velocidad del avance tecnológico. Cada innovación trae consigo nuevas oportunidades, pero también nuevos riesgos. La IA, el IoT, la nube, el 5G y el blockchain han transformado el panorama, haciendo que las amenazas sean más sofisticadas y difíciles de detectar.

Frente a estos tipos de escenarios, la ciberseguridad se convierte en una prioridad estratégica. No basta con reaccionar. Es necesario anticiparse, formar más a los usuarios y diseñar sistemas seguros desde el principio. La tecnología seguirá avanzando, y con ella también lo harán los ciberataques.

Mantenerse preparado será clave para proteger el entorno digital del que dependemos cada día, anticipando amenazas emergentes, fortaleciendo la colaboración, adoptando tecnologías seguras y fomentando el aprendizaje sobre temas de ciberseguridad en todos los ámbitos.

SERGIO BARRERA JULIÁN

BRAIN-COMPUTER INTERFACES Y PRIVACIDAD NEUROLÓGICA

La neurotecnología ha avanzado de forma exponencial en la última década, pasando de ser un campo exclusivo de la investigación médica a convertirse en una industria multimillonaria con aplicaciones comerciales. Las interfaces cerebro-computadora (BCI) permiten una comunicación directa entre el cerebro humano y dispositivos externos, abriendo posibilidades que pertenecían al ámbito de la ciencia ficción.

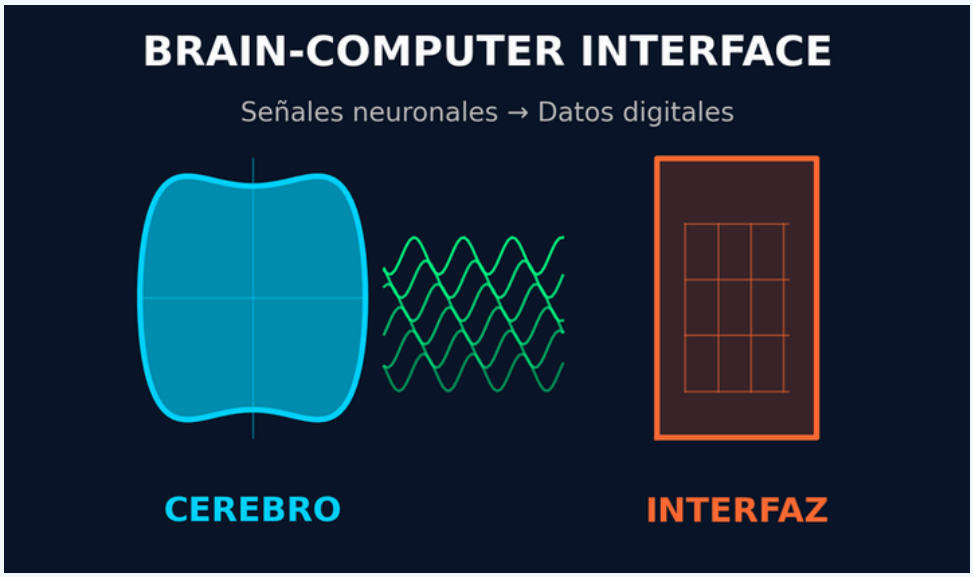
Sin embargo, esta revolución plantea una pregunta fundamental: ¿quién es el dueño de nuestros pensamientos? Cuando un dispositivo puede leer, interpretar y almacenar la actividad neuronal, la frontera más íntima del ser humano —la mente— queda expuesta a los mismos riesgos de vigilancia, explotación y manipulación que ya hemos experimentado con nuestros datos digitales.

La evolución de las Interfaces cerebro-computadora

El concepto de BCI tiene sus raíces en los experimentos de Hans Berger en 1924, cuando registró por primera vez la actividad eléctrica del cerebro humano mediante electroencefalografía (EEG). Durante décadas, estas tecnologías permanecieron confinadas a laboratorios de neurociencia, utilizadas principalmente para el diagnóstico de trastornos como la epilepsia.

El salto cualitativo llegó en 2006, cuando el sistema BrainGate permitió a un paciente tetrapléjico mover un cursor únicamente con su pensamiento. Desde entonces, empresas como Neuralink (fundada por Elon Musk en 2016), Synchron, Blackrock Neurotech y Kernel han acelerado el desarrollo de implantes neuronales cada vez más sofisticados.

En enero de 2024, Neuralink implantó su primer chip cerebral en un ser humano, marcando un hito histórico. El dispositivo, denominado "Telepathy", permitió al paciente controlar un cursor y jugar videojuegos usando solo su actividad cerebral. Este evento catalizó un debate global sobre las implicaciones éticas y de privacidad de la neurotecnología.



El problema de la privacidad neurológica

La privacidad neurológica —o neuroprivacidad— se refiere al derecho de un individuo a mantener la confidencialidad de su actividad cerebral y los datos derivados de ella. A diferencia de otros tipos de datos personales, los neurodatos son cualitativamente diferentes: no revelan lo que hacemos o decimos, sino lo que pensamos, sentimos y deseamos.

Neurodatos: la nueva frontera de la vigilancia. Los dispositivos BCI generan flujos continuos de datos neuronales que pueden revelar estados emocionales, niveles de atención, intenciones motoras e incluso predisposiciones a enfermedades neurológicas. Investigadores de la Universidad de Ginebra demostraron en 2023 que es posible decodificar imágenes visuales directamente desde la actividad cerebral con una precisión del 80% (Benchetrit et al., 2023). El peligro no es solo teórico. Empresas como Meta y Apple están invirtiendo miles de millones en neurotecnología de consumo. Auriculares con sensores EEG integrados ya se comercializan para "mejorar la productividad". Cada minuto de uso genera datos que pueden ser recopilados, almacenados y vendidos sin el consentimiento explícito del usuario.

¿Qué son los neurodatos?

Los neurodatos son información obtenida de la medición directa o indirecta de la actividad del sistema nervioso: señales eléctricas (EEG), cambios en el flujo sanguíneo cerebral (fMRI, fNIRS) y patrones de activación neuronal. A diferencia de los datos biométricos convencionales, son dinámicos y revelan estados mentales en tiempo real. En la UE, el RGPD los considera "datos relativos a la salud". Sin embargo, esta clasificación resulta insuficiente dado el nivel de intimidad que revelan, lo que ha llevado a expertos como Rafael Yuste a abogar por una categoría jurídica completamente nueva.

El caso de Chile: pioneros en neuroderechos

En octubre de 2021, Chile se convirtió en el primer país del mundo en aprobar una reforma constitucional que protege explícitamente los neuroderechos. El artículo 19 de la Constitución fue modificado para establecer que "el desarrollo científico y tecnológico estará al servicio de las personas con respeto a la integridad física y psíquica". Esta legislación fue impulsada por el neurocientífico Rafael Yuste, director del Centro de Neurotecnología de Columbia, quien publicó en 2017 la Declaración de Morningside, proponiendo cinco neuroderechos fundamentales.

Estos cinco neuroderechos son: (1) privacidad mental; (2) identidad personal, protegiendo el sentido de yo frente a la manipulación; (3) libre albedrío; (4) acceso equitativo a la mejora cognitiva; y (5) protección contra sesgos algorítmicos en la neurotecnología.

Sin embargo, la implementación práctica enfrenta obstáculos significativos. La velocidad del desarrollo tecnológico supera la capacidad de los marcos regulatorios para adaptarse. Mientras Chile debatía su ley, Neuralink ya realizaba ensayos clínicos en humanos.

La economía de los neurodatos

El mercado global de BCI alcanzó un valor estimado de 2.100 millones de dólares en 2022 y se proyecta que supere los 13.500 millones para 2030, con un CAGR del 17,1% (Grand View Research, 2023).

El modelo de negocio de la atención. Así como las redes sociales monetizan la atención, las empresas de neurotecnología podrían monetizar directamente los estados mentales. Emotiv y NeuroSky ya ofrecen auriculares EEG de consumo que miden estados emocionales y niveles de atención.

El riesgo de un "capitalismo de vigilancia neurológica" es real. Si los marcos regulatorios no evolucionan al mismo ritmo que la tecnología, las corporaciones podrían acceder a la última frontera de la privacidad humana: nuestros pensamientos.

La paradoja del consentimiento informado

¿Cómo puede un usuario dar consentimiento "informado" cuando ni siquiera los desarrolladores comprenden completamente qué información puede extraerse de los neurodatos?

Los algoritmos de aprendizaje automático descubren correlaciones inesperadas, revelando información que el usuario nunca consintió compartir. El consentimiento informado se convierte en una ficción jurídica aplicada a la neurotecnología.

El dilema ético: curar vs. controlar

Las BCI representan una esperanza real para millones de personas con discapacidades neurológicas.

Pacientes con ELA, lesiones medulares, parálisis cerebral y trastornos neurodegenerativos podrían recuperar capacidades motoras y sensoriales. En 2023, la EPFL logró que un paciente parapléjico volviera a caminar mediante un "puente digital" cerebro-médula espinal (Lorach et al., 2023).

Sin embargo, la misma tecnología que permite curar también permite controlar. Si un dispositivo puede estimular áreas del cerebro para restaurar el movimiento, también podría modular emociones, alterar recuerdos o influir en decisiones. Investigadores de Washington demostraron en 2019 que es posible implantar falsos recuerdos en ratones mediante optogenética.

La militarización de la neurotecnología es otro factor preocupante. DARPA lleva años financiando programas de BCI militares, incluyendo el programa N3. China ha declarado la neurotecnología como área estratégica en su plan quinquenal y financia activamente BCIs de doble uso.

Sobriedad neurotecnológica: un marco para el futuro

Así como la "sobriedad digital" promueve un uso más consciente de la tecnología, necesitamos un marco de "sobriedad neurotecnológica" que guíe el desarrollo de las BCI.

Minimización de datos neuronales: Los dispositivos BCI deben recopilar únicamente los datos estrictamente necesarios para su función declarada.

Procesamiento local obligatorio: los neurodatos brutos nunca deberían salir del dispositivo. Todo el procesamiento debe realizarse en el propio dispositivo (edge computing).

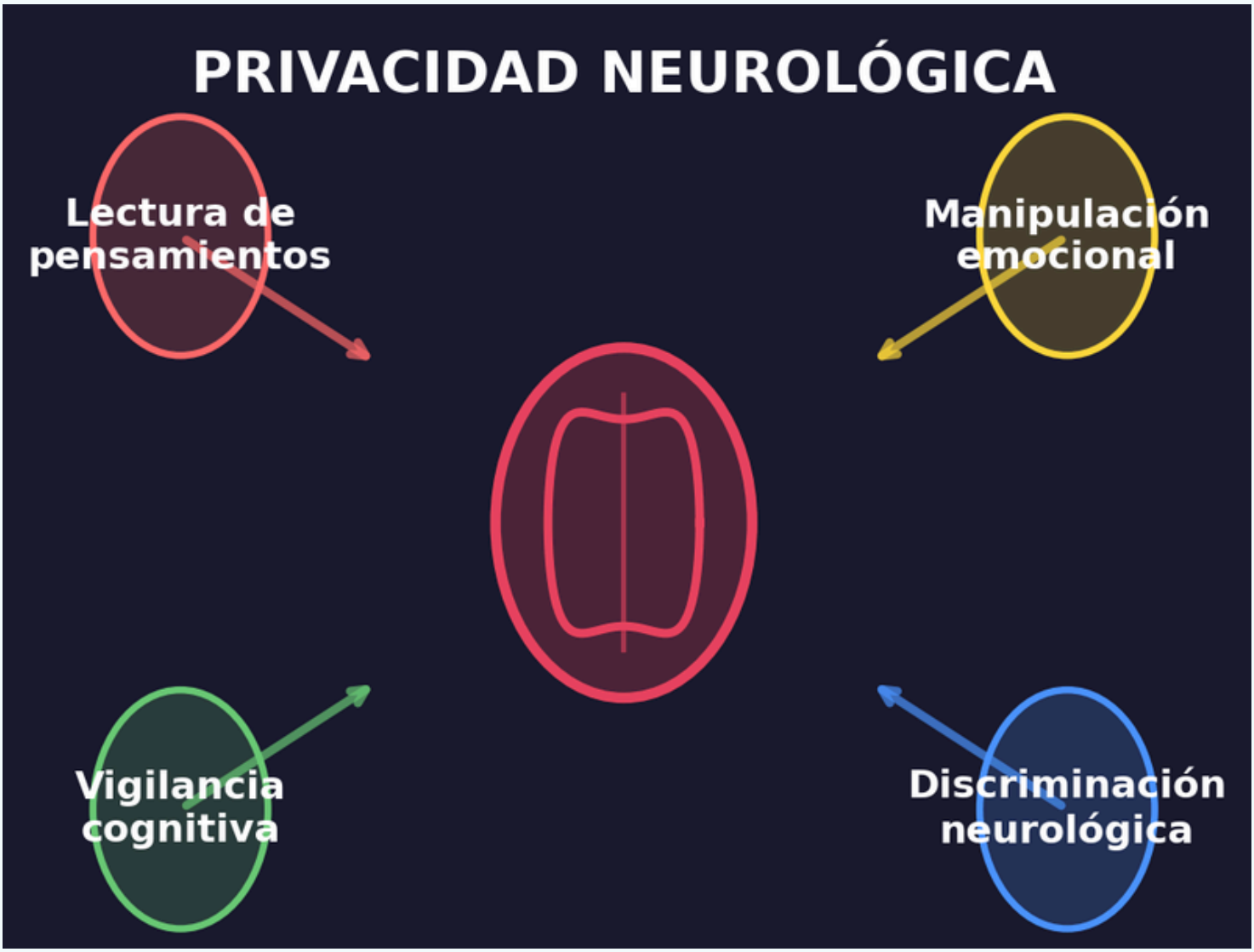
Derecho al silencio cognitivo: Toda persona debe tener el derecho absoluto a desconectar cualquier dispositivo BCI en cualquier momento, sin consecuencias laborales, sociales o legales.

El futuro: entre la utopía y la distopía

La neurotecnología tiene el potencial de ser la mayor revolución en la historia de la humanidad o su mayor amenaza. La diferencia depende de las decisiones que tomemos ahora. Si permitimos que las BCI sigan el mismo patrón que las redes sociales —donde la regulación llegó demasiado tarde—, las consecuencias serán exponencialmente peores. Los datos de navegación revelan nuestros intereses; los neurodatos revelan nuestra identidad.

Aún estamos a tiempo. Chile demuestra que la protección legislativa de los neuroderechos es posible. La creciente conciencia sobre la privacidad de datos ha creado un terreno fértil para la regulación preventiva.

Como sociedad, debemos exigir que la neurotecnología se desarrolle bajo un principio fundamental: la mente humana es un espacio inviolable. No es un recurso para extraer, ni un mercado para explotar, ni un campo de batalla para dominar. Es la esencia misma de lo que nos hace humanos.



MSMK Magazine

MSMK University College