

[ IA Y BIOMETRÍA ]

## El camino hacia un acceso más seguro y eficiente

El reconocimiento facial y otras tecnologías biométricas se están consolidando impulsadas por la inteligencia artificial. Estas soluciones además de mejorar la precisión y velocidad elevan los estándares de protección de datos en entornos cada vez más exigentes.

**Por: Rodrigo M. Ancamil**

**En aeropuertos, estadios o conciertos, cada vez es más común que los accesos no dependan de una tarjeta ni de una clave, sino del rostro de una persona.**

La autenticación biométrica ha ganado terreno como método de identificación, y la inteligencia artificial (IA) está acelerando esta transformación, otorgando a las organizaciones la posibilidad de utilizar

varios datos biométricos a la vez, para componer la identidad de un empleado.

Hernán Sánchez, arquitecto de Soluciones en AMD Latinoamérica, explica que los avances en IA, combinados con tecnologías como las NPU (Neural Processing Units), están revolucionando la forma en que se procesan y protegen los datos biométricos. "Hoy en día los datos biométricos usados como recurso de identificación presencial y unívoca de un individuo son fundamentales y su uso es cada vez más frecuente".

La seguridad de estos sistemas no depende solo del algoritmo que reconoce un rostro o una huella digital, sino también del procesamiento que ocurre tras bambalinas. AMD, por ejemplo, incorpora en sus procesadores capas de protección a nivel de silicio, capaces de analizar desde el BIOS del equipo hasta bloquear su ejecución si detectan una vulnerabilidad. "Estas tecnologías de seguridad de AMD han sido estudiadas y experimentadas por Microsoft, y en un desarrollo conjunto se han escrito las bases de Microsoft Pluton Security Processor", agrega Sánchez.

Las NPU, por su parte, permiten analizar comportamientos sospechosos,

detectar patrones anómalos en tiempo real y mejorar la velocidad y precisión del reconocimiento facial, sin sobrecargar el sistema ni comprometer su eficiencia energética. "El uso de NPU permite hacerlo velozmente sin ocupar otros recursos del sistema y adicionalmente lo hace con alto grado de eficiencia energética", afirma.

Si en el pasado los lectores de huella eran vulnerables por almacenar datos sin cifrado o los sistemas de reconocimiento facial podían engañarse con una foto, hoy la combinación de IA, hardware seguro y aprendizaje automático ha elevado el estándar. "El uso de algoritmos avanzados de redes neuronales profundas permitió un elevado grado de evitar engaños, tener mayor velocidad y precisión", recuerda Sánchez.

En un mundo donde la IA ya no es exclusiva de grandes corporaciones, la posibilidad de ejecutar procesos de verificación biométrica incluso desde pequeños dispositivos portátiles plantea un escenario prometedor: más seguridad, menos fricción y, sobre todo, más control. "Esto es un factor de vital importancia en la democratización del acceso a la AI", concluye.

