*Revista CIES – ISSN-e 2216-0167. Volumen 16. Número 1. Año 2025. Páginas 3-5. Dirección de Investigaciones – Institución Universitaria Escolme (Medellín, Colombia)*

Editorial:

# Ciberseguridad: Investigación académica que se anticipe a lo inimaginable

**Dr. Julio Leyrer H.**
Departamento de Ingeniería Mecánica, Facultad de Ingeniería y Ciencias, Universidad de La Frontera, Chile. julioleyrer@ufrontera.cl

En la actualidad, la irrupción violenta de la inteligencia artificial y su estrecha relación con el uso fraudulento de datos está modificando nuestros propios conceptos de seguridad y confianza, generando la necesidad de que la investigación académica no solo sea descriptiva o reactiva, sino que se anticipe a las amenazas informáticas. Ya no basta con cambiar la contraseña de nuestras cuentas o mantener actualizados los sistemas de antivirus. Hoy corremos el riesgo de convertirnos en autores de hechos fraudulentos que ni siquiera hemos imaginado. Como ejemplo, está lo ocurrido en Emiratos Árabes Unidos, donde, a principios de 2020, delincuentes utilizaron tecnología de IA para clonar la voz de un "director" y convencer a un gerente bancario de autorizar transferencias por 35 millones de dólares (Lemos, 2021). Entretanto, en Arizona (Estados Unidos), se reportó un supuesto secuestro en el que la voz clonada de una menor fue usada para exigir un rescate millonario a su madre (GMA Team, 2023), mientras que en ámbitos académicos han circulado denuncias sobre la suplantación de investigadores para acceder a fondos o información sensible. No obstante, estos hechos son del pasado y ahora cabe preguntar, qué ocurre con aquellas amenazas que todavía no han sido previstas, y si existe un modo de anticiparse a riesgos incluso no creados.

En esta línea, existen algunas alternativas como es la adopción de gemelos digitales (digital twins), cuyo propósito es modelar toda la infraestructura informática y simular escenarios potenciales de ataque antes de que ocurran en el mundo real (Tao et al., 2019). Un gemelo digital consiste en una representación virtual dinámica y fidedigna de sistemas, dispositivos y procesos (Tao et al., 2019). En el ámbito de la ciberseguridad, esta tecnología facilita la identificación de vulnerabilidades y la optimización de protocolos de defensa (Barricelli et al., 2019). Otro recurso preventivo es el uso de ciberlaboratorios o "cyber ranges", plataformas que permiten recrear entornos virtuales donde administradores de sistemas e investigadores pueden entrenar, experimentar y desarrollar respuestas ante múltiples clases de incidentes (Mir et al., 2021). Sin desmedro de lo anterior, la importancia de que la investigación profundice sobre ciberseguridad no debe limitarse a contrarrestar de manera reactiva los métodos maliciosos ya existentes, sino que también a promover el desarrollo de tecnologías esenciales capaces de ofrecer una infraestructura basal que no sea permeable a riesgos de seguridad futuros.

Se trata de una visión proactiva y robusta, que busca desafiar los límites actuales del conocimiento, similar a la de Haber y Stornetta (1991), quienes a principios de la década de 1990 propusieron la idea de un registro inmutable con sellado temporal —base de lo que hoy conocemos como blockchain—, posteriormente popularizada con la publicación del paper de Bitcoin de Nakamoto en 2008 (Nakamoto, 2008). Más allá de las criptomonedas, dicha innovación ha posibilitado la creación de contratos inteligentes, identidad digital descentralizada y trazabilidad en cadenas de suministro, reduciendo los riesgos de manipulación de datos. De igual modo, la validación de identidades a través de blockchain sin intermediarios centralizados disminuye la probabilidad de un robo masivo de información y abre la puerta a nuevas maneras de proteger la integridad de los usuarios y de sus activos digitales.

Con todo esto en mente, resulta imposible no preguntarse cómo evolucionarán las amenazas a medida que la inteligencia artificial alcance niveles de autonomía todavía impensados. De ahí surge la urgente necesidad de impulsar una investigación profunda, en la cual el sector académico, junto con el empresarial y gubernamental, unan esfuerzos para ir más allá de las respuestas inmediatas y plantear soluciones esenciales en el ámbito de la seguridad informática. Solo así lograremos que las tecnologías emergentes se conviertan en verdaderas aliadas, en lugar de percibirlas como fuentes constantes de riesgo que amenazan nuestro bienestar social y personal.

## REFERENCIAS


Barricelli, B. R., Casiraghi, E. y Fogli, D. (2019). A Survey on Digital Twin: Definitions, Characteristics, System Architecture, and Tenants. *IEEE Access*, *7*, 167653–167671. https://doi.org/10.1109/ACCESS.2019.2953499

GMA Team. (13 de abril de 2023). Mom warns of hoax using AI to clone daughter's voice. ABC News. https://abcnews.go.com/GMA/Family/mom-warns-hoax-ai-clone-daughters-voice/story?id=98551351

Haber, S. y Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology, 3*(2), 99–111. https://doi.org/10.1007/BF00196791

Lemos, R. (20 de octubre de 2021). *Deepfake Audio Nabs $35M in Corporate Heist*. Darkreading. https://www.darkreading.com/cyberattacks-data-breaches/deepfake-audio-scores-35-million-in-corporate-heist

Mir, Z. H., Dharmapurikar, S. y Luo, B. (2021). A Survey on Cyber Range Technologies for Security Training and Innovation. En 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC) (pp. 1–7). IEEE.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

Tao, F., Zhang, H., Liu, A. y Nee, A. Y. C. (2019). Digital Twin in Industry 4.0: A State-of-the-Art. *IEEE Transactions on Industrial Informatics, 15*(4), 2405–2415. https://doi.org/10.1109/TII.2018.2873186