Confianza digital: activo a desarrollar

DOI: 10.29236/sistemas.n179a2

La confianza digital es un activo estratégico fundamental para sociedades crecientemente dependientes de ecosistemas digitales hiperconectados que redefinen el riesgo.

Diego Andrés Zuluaga Urrea

La transformación digital ha dejado de ser únicamente un proceso de modernización tecnológica. Cada vez más desarrolla la economía, la industria, la operación de infraestructuras críticas y otros sistemas que controlan el mundo físico desde el mundo virtual (ciberfísicos), así como la interacción entre gobiernos, empresas y sociedad civil en entornos digitalizados.

Por ello, la confianza digital se ha convertido en un activo estratégico fundamental para nuestra sociedad, ya que vivimos no solo en el mundo físico sino en el virtual y permitimos cada vez más que nuestra vida se desarrolle en este mundo virtual y que la tecnología digital tome cada vez más decisiones y acciones que afectan el mundo físico que nos rodea y que presta los servicios esenciales que requerimos en la sociedad actual, a la vez que facilita el desarrollo de los productos y servicios que consumimos en nuestra vida diaria.

Sin embargo, a diferencia de otros activos tecnológicos o financieros, el desarrollo de esta confianza digi-

tal aún es limitado, difuso y, en muchos casos, subestimado o dejado de lado por las diferentes instituciones, gobiernos y empresas. En un contexto caracterizado por redes altamente interconectadas, automatización avanzada, virtualización de servicios e inteligencia creciente de los sistemas, la confianza ya no puede asumirse como una consecuencia natural de la tecnología, sino como una capacidad que debe diseñarse, construirse y mantenerse de forma explícita. Su ausencia no solo incrementa el riesgo, sino que compromete la estabilidad operativa, la resiliencia organizacional, la credibilidad organizacional e institucional y el uso futuro de los ecosistemas digitales en su conjunto.

En los últimos años ha comenzado a consolidarse una nueva visión sobre la evolución del riesgo digital y operacional. Por ejemplo, el estudio: *How can reimagining risk prepare you for an unpredictable world?* de EY introduce el concepto de entorno NAVI para describir un mundo crecientemente No lineal, Acelerado, Volátil e Interconectado [1]. Según este enfoque, los riesgos modernos ya no evolucionan de manera aislada ni predecible. Por el contrario, interactúan entre sí, se aceleran mutuamente y generan efectos en cascada capaces de impactar simultáneamente operaciones, cadenas de suministro, reputación, estabilidad financiera e infraestructura crítica, creando policrisis que deben ser gestionadas a tiempo para evitar impactos significativos en los servicios prestados por las instituciones y empresas o en ellas mismas.

En este contexto NAVI, la confianza digital deja de ser únicamente un atributo tecnológico o reputacional para convertirse en una capacidad estratégica de resiliencia organizacional. La capacidad de anticipar, adaptarse, responder y mantener continuidad operacional frente a escenarios impredecibles debe ser uno de los principales diferenciadores de las organizaciones modernas.

Ya que La sociedad está comenzando a delegar crecientemente decisiones críticas a sistemas digitales autónomos. Algoritmos y plataformas participan en procesos financieros, médicos, logísticos, industriales y de infraestructura crítica. Esto convierte la confianza digital no solo en un requisito tecnológico, sino en un elemento esencial de gobernanza y estabilidad social.

Emergen preguntas fundamentales como: ¿qué tan confiables son los ecosistemas digitales sobre los cuales estamos construyendo nuestra dependencia económica y social para estos entornos NAVI? Y ¿Cómo debemos desarrollar la confianza digital en nuestras organizaciones en esta nueva era donde la IA acelera los riesgos?

Ya no basta con digitalizar procesos, migrar servicios a la nube o

incorporar inteligencia artificial. El verdadero reto consiste en garantizar que los ecosistemas digitales sean seguros, resilientes, verificables y sostenibles frente a amenazas crecientemente sofisticadas y dinámicas, especialmente aceleradas por el uso creciente de la Inteligencia artificial agentica.

La confianza digital dejó de ser únicamente un atributo reputacional para convertirse en una propiedad esencial de la infraestructura tecnológica moderna que rige nuestra sociedad.

Actualmente ciudadanos, gobiernos, industrias y empresas dependen de plataformas digitales para operar procesos críticos: energía, salud, servicios financieros, telecomunicaciones, logística, producción industrial y servicios públicos. En consecuencia, cualquier afectación sobre la confianza del ecosistema digital puede traducirse en impactos económicos, sociales e incluso institucionales.

Este cambio de paradigma resulta particularmente relevante para países Latinoamericanos como Colombia, donde la acelerada digitalización convive con desafíos relacionados con ciberseguridad, madurez institucional, baja protección de la infraestructura crítica y débil fortalecimiento de capacidades especializadas.

Después de más de tres décadas observando la evolución de Internet, las telecomunicaciones, la infraestructura tecnológica y la ciberseguridad en Colombia y América Latina, resulta evidente que estamos entrando en una etapa distinta del riesgo digital.

Durante muchos años la ciberseguridad se enfocó principalmente en proteger información. Hoy el problema es considerablemente más complejo. La seguridad digital protege continuidad operacional, estabilidad económica, confianza institucional, la seguridad física y defensa nacional a la vez que protege de afectaciones a sistemas ciberfísicos que soportan la infraestructura crítica nacional, la industria, sistemas médicos avanzados, entre otros, es decir los servicios esenciales que la sociedad requiere para su funcionamiento, evitando no sólo que estos fallen sino que se descontrolen y puedan causar impactos sobre las vidas humanas y el medio ambiente [2].

La convergencia entre tecnologías de información IT y las de operación OT, la hiperconectividad, la virtualización de servicios, la dependencia de terceros y la creciente incorporación de inteligencia artificial han transformado radicalmente la superficie de exposición de las organizaciones.

“La ciberseguridad es la base de nuestro mundo digital. Está en el centro de la confianza y permitirá que la sociedad aproveche plenamente las transformaciones impul-

sadas por nuevas tecnologías como la inteligencia artificial y la computación cuántica…" -Michael Miebach, CEO de Mastercard [3]

El modelo NAVI acelera esa complejidad. Los ecosistemas digitales modernos funcionan como redes profundamente interdependientes donde convergen infraestructuras distribuidas, automatización avanzada, plataformas cloud, inteligencia artificial, dispositivos IoT, entornos industriales conectados, servicios virtualizados y cadenas de suministro digitales globales.

En este contexto, la confianza digital no puede entenderse únicamente como un asunto tecnológico. Se trata de una capacidad multidimensional que involucra seguridad, resiliencia, gobernanza, privacidad, integridad, trazabilidad y capacidad de recuperación.

Diversos organismos internacionales han desarrollado aproximaciones complementarias sobre este concepto. El World Economic Forum define relaciona la confianza digital como *" la expectativa de las personas de que las tecnologías y los servicios digitales, y las organizaciones que los proporcionan, protegerán los intereses de todas las partes interesadas y respetarán las expectativas y los valores de la sociedad.*" y las relaciona en su modelo con la capacidad de las organizaciones para garantizar seguridad de las personas y la operación(Safety), la ciberseguridad, transparencia, reparabilidad, auditabilidad, privacidad, interoperabilidad y equidad de la tecnología, agrupando estos conceptos en las dimensiones de Seguridad y confiabilidad, supervisión y rendición de cuentas, ética, inclusividad y uso responsable, [4].

La OECD ha insistido en que la confianza constituye un habilitador esencial para el crecimiento sostenible de la economía digital. Por su parte, marcos desarrollados por NIST como el CSF 2.0 han contribuido a operacionalizar conceptos asociados a gestión de riesgo, resiliencia y arquitecturas de confianza y pueden usarse como marco de referencia para la construcción de entornos seguros y resilientes [5].

La confianza digital adquiere entonces una dimensión estratégica nacional, Cuando una sociedad pierde confianza en sus sistemas digitales, el impacto trasciende lo tecnológico: disminuye la adopción de servicios, aumenta la incertidumbre, se debilita la legitimidad institucional y se afecta la estabilidad económica.

Sin embargo, la aparición de nuevas generaciones de inteligencia artificial está introduciendo un punto de inflexión aún más complejo en la evolución del riesgo digital. La IA ya no representa únicamente una herramienta de automatización o productividad. Está comenzando a convertirse en un multiplicador operacional capaz de alterar signi-

ficativamente la dinámica entre defensores y atacantes.

Las discusiones recientes alrededor de capacidades emergentes de modelos avanzados reflejan una preocupación creciente: la posibilidad de que agentes inteligentes reduzcan las barreras técnicas necesarias para ejecutar ataques complejos y amplifiquen la capacidad ofensiva de actores maliciosos o incluso actúen completamente de manera autónoma descubriendo y explotando los entornos de interés de los atacantes.

Más allá del debate mediático, el problema de fondo es estratégico. Las nuevas inteligencias artificiales incrementarán la capacidad operacional tanto de los defensores como de los atacantes.[6]

Solo entre abril y mayo de 2026 tres agentes de OpenAI, Anthropic y Microsoft sobrepasaron la barrera del 80% de efectividad en la generación de Pruebas de concepto funcionales de vulnerabilidades dentro del CyberGym de UC Berkeley [7] lo que muestra que las capacidades actuales superan equipos humanos especializados en velocidad y escala, ampliando significativamente el panorama de amenazas.

Actividades como reconocimiento de infraestructura, identificación y explotación de vulnerabilidades, phishing avanzado, evasión de controles o desarrollo de malware pueden ejecutarse con mayor automatización y escala. La velocidad de evolución de las amenazas también aumentará, dificultando los mecanismos tradicionales de detección.

Incluso esta evolución ya no pertenece únicamente al terreno teórico. Investigaciones recientes de Trend Micro documentaron campañas dirigidas contra sectores gubernamentales y financieros en América Latina donde actores maliciosos utilizaron capacidades de IA agentica para automatizar diferentes etapas del ciclo de ataque, desde reconocimiento inicial hasta despliegue de herramientas ofensivas y exfiltración de información [8].

Con lo cual se evidencia cómo la inteligencia artificial comienza a reducir las barreras técnicas necesarias para ejecutar operaciones avanzadas, aumentando la velocidad, escala y adaptabilidad de los ataques. Este tipo de escenarios marca un punto de inflexión particularmente relevante para la confianza digital en entornos NAVI, donde la hiperconectividad y la dependencia de cadenas de suministro digitales amplifican el impacto potencial de incidentes cibernéticos sobre múltiples organizaciones y sectores simultáneamente.

Además, la combinación de inteligencia artificial generativa, deepfakes y manipulación sintética afectará directamente la capacidad de verificar la legitimidad de personas,

transacciones y comunicaciones generando erosión de la autenticidad digital con lo cual, “ver” o “escuchar” dejará de ser suficiente como mecanismo de validación.

Por otro lado, desde la perspectiva de cadenas de suministro digitales, las organizaciones operan dentro de ecosistemas interconectados que incluyen proveedores cloud, integradores, plataformas SaaS, open source, OT, IoT y terceros. La confianza ya no depende únicamente de la seguridad interna, sino de toda la cadena de suministro.

La automatización ofensiva impulsada por IA permitirá explotar eslabones débiles y comprometer ecosistemas completos con velocidades sin precedentes. La experiencia internacional ya ha demostrado el impacto global de incidentes en cadena de suministro [9].

La industrialización progresiva del cibercrimen impulsada por IA, estamos entrando en una etapa donde campañas ofensivas completas podrán ejecutarse de manera crecientemente automatizada, incluyendo reconocimiento, explotación, evasión y monetización [10].

En este escenario, la confianza digital dependerá cada vez más de la capacidad de las organizaciones para gestionar riesgos sistémicos e interdependencias complejas dentro de ecosistemas digitales altamente distribuidos.

En infraestructuras críticas, donde convergen tecnologías IT y OT, el riesgo adquiere implicaciones operacionales y físicas. Por ello, marcos especializados como ISA/IEC 62443 resultan fundamentales para la seguridad industrial [11].

Como plantea EY, las organizaciones más resilientes evolucionan desde enfoques tradicionales de gestión de riesgo hacia modelos de *Risk Strategists*, donde el riesgo deja de gestionarse únicamente desde cumplimiento y pasa a integrarse directamente con estrategia, resiliencia, gobernanza y toma de decisiones [1].

Esta transición resulta especialmente relevante en ciberseguridad, donde los modelos tradicionales basados únicamente en prevención perimetral ya no son suficientes frente a amenazas hiperconectadas, automatizadas y potenciadas por inteligencia artificial.

Todo esto obliga a replantear profundamente las estrategias tradicionales de ciberseguridad frente a amenazas adaptativas. Las organizaciones deben fortalecer capacidades de ciberresiliencia, inteligencia de amenazas, monitoreo continuo, gestión de terceros, seguridad de cadena de suministro y gobernanza de inteligencia artificial.

La conversación ya no es sobre proteger sistemas, sino sobre preservar la confianza operacional de

ecosistemas digitales en entornos NAVI.

En un mundo donde los sistemas digitales controlan progresiva y determinadamente procesos físicos esenciales, desarrollar confianza digital en la sociedad dejará de ser opcional para convertirse en una condición de estabilidad económica y organizacional, resiliencia institucional y seguridad nacional.

Latinoamérica y en especial Colombia enfrentan aquí una oportunidad estratégica. La transformación digital del país debe evolucionar hacia un modelo de confianza digital y ciberresiliencia que permita afrontar las multicrisis a las que ya están acostumbradas en el mundo físico ahora en el mundo digital.

La confianza digital no es cumplimiento, es estrategia

Los países y organizaciones que logren integrar y consolidar ecosistemas digitales resilientes y confiables tendrán ventajas significativas en innovación, estabilidad y confianza pública que redundará en desarrollo económico para el largo plazo.

En un mundo hiperconectado, la confianza será uno de los principales diferenciadores estratégicos. Y la ciberresiliencia dejará de ser un tema técnico para convertirse en un pilar de la competitividad empresarial y nacional.

Referencias

[1] McCowan, S., Krumbmüller, F. & Jaggi, G. (2025). *How can reimagining risk prepare you for an unpredictable world?* EY Insights. https://www.ey.com/en_us/insights/consulting/how-can-reimagining-risk-prepare-you-for-an-unpredictable-world

[2] ZULUAGA, Diego, et al. *Escenarios de alto impacto por ciberseguridad en sistemas industriales del sector eléctrico*. Madrid: CCI-CIGRE, 2023. ISBN 978-84-126727-6-3. Disponible en: https://www.cci-es.org/activities/escenarios-de-alto-impacto-por-ciberseguridad-en-sistemas-industriales-sector-electrico/

[3] World Economic Forum. (2026). *Global Cybersecurity Outlook 2026*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

[4] World Economic Forum. (2022). *Earning digital trust: Decision-making for trustworthy technologies*. World Economic Forum. https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf

[5] National Institute of Standards and Technology. (2024). *Cybersecurity framework (CSF) 2.0*. https://www.nist.gov/cyberframework

[6] World Economic Forum. (2025). *Artificial intelligence and cybersecurity: Balancing risks and rewards*. World Economic Forum. https://reports.weforum.org/docs/WEF_Artificial_Intelligence_and_Cybersecurity_Balancing_Risks_and_Rewards_2025.pdf

[7] International Conference on Learning Representations. Wang, Z., Shi, T., He,

J., Cai, M., Zhang, J., & Song, D. (2026). *CyberGym: Evaluating AI agents' real-world cybersecurity capabilities at scale*. *In Proceedings of the Fourteenth International Confe-rence on Learning Representations (ICLR 2026)*. https://openreview.net/forum?id=2YvbLQEdYt

[8] Trend Micro. (2026). *Vibe hacking: Two AI-augmented campaigns target government and financial sectors in Latin America*. https://www.trendmicro.com/en_us/research/26/e/vibe-hacking-two-ai-augmented-campaigns-target-government-and-financial-sectors-in-latin-america.html

[9] IBM Security. (2025). *Cost of a data breach report 2024*. https://www.ibm.com/security/data-breach

[10] Trend Micro. (2025). *The AI-fication of cyberthreats: Security predictions for 2026*. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/the-ai-fication-of-cyberthreats-trend-micro-security-predictions-for-2026

[11] International Society of Automation. (2026). *ISA/IEC 62443 series of standards*. International Society of Automation. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Diego Andrés Zuluaga Urrea. *Ingeniero de Sistemas, Especialista en Gerencia y Executive MBA con más de 25 años de experiencia y certificaciones en ciberseguridad, gestión de riesgos, privacidad, seguridad de la información y protección de sistemas de control industrial. Actualmente es CSO para Latinoamérica y responsable del gobierno de seguridad para mercados internacionales del grupo AXA, desde Madrid, España. Lideró la construcción de la regulación y guías de ciberseguridad en el sector eléctrico colombiano, ha aportado en diferentes escenarios para la seguridad de las infraestructuras críticas nacionales. Es coordinador nacional del Centro de Ciberseguridad Industrial y líder del capítulo SC D2 de CIGRE. Ha sido, consultor internacional, conferencista y docente universitario en América Latina y Europa, además de autor y revisor de múltiples publicaciones especializadas. Ha recibido reconocimientos nacionales e internacionales, entre ellos en dos oportunidades el premio continental "Americas Information Security Leadership Awards" de ISC².*