La confianza digital: el activo invisible que sostiene el futuro

DOI: 10.29236/sistemas.n179a1

Jeimy J. Cano M.

Andres R. Almanza J.

Durante años, la conversación sobre el mundo digital estuvo dominada por la tecnología. Hablamos de transformación digital, automatización, computación en la nube, inteligencia artificial, plataformas, datos y ciberseguridad. Sin embargo, a medida que las organizaciones avanzan en su proceso de transformación, emerge una pregunta más retadora: ¿qué es realmente lo que permite que las personas, las empresas, las instituciones y entidades gubernamentales adopten, apropien, utilicen y asuman estos entornos digitales?

La respuesta parece sencilla, pero encierra un desafío particular: la confianza.

La confianza ha sido históricamente el fundamento de las relaciones humanas, comerciales e institucionales. Hoy, en un contexto donde gran parte de las relaciones ocurren a través de sistemas, algoritmos, plataformas y ecosistemas digitales, la confianza se ha convertido en un activo estratégico que determina la viabilidad misma de los modelos de negocio y de las sociedades digitales.

Ya no es suficiente con que un servicio y/o producto funcione de acuerdo con su especificación. Debe ser confiable y mostrar confiabilidad. Ya no es suficiente asegurar la confidencialidad, la integridad y la disponibilidad. Es necesario entender con claridad sobre cómo se comporta, quién lo administra y cuáles son sus principios de gobernanza. Tampoco es suficiente incorporar nuevas tecnologías; es preciso asegurar que estas sean distinguidas como transparentes, responsables y alineadas con las expectativas de las personas y los objetivos de negocio, más aún en contextos donde la inteligencia artificial ha transformado la realidad empresarial.

La confianza digital, de acuerdo con Saveljeva & Volkova (2025) se fundamenta en cuatro pilares esenciales: la capacidad, la confiabilidad, la integridad y la dimensión de la apertura.

La capacidad abarca la competencia técnica y la seguridad del sistema para operar con estabilidad y desempeño. La confiabilidad se centra en la intención positiva hacia el usuario y la calidad del soporte recibido durante su experiencia. Por su parte, la integridad asegura que la organización actúe bajo principios éticos y cumpla con las normativas de protección de datos vigentes. Finalmente, la apertura asegura la transparencia, auditabilidad y trazabilidad de los procesos, permitiendo la verificación externa de las operaciones.

La integración de estas dimensiones permite reducir los riesgos y fomentar interacciones bien fundadas en entornos tecnológicos complejos.

Este desafío adquiere una relevancia particular en América Latina y el Caribe. La región enfrenta simultáneamente importantes oportunidades de desarrollo digital y brechas estructurales. Organismos internacionales han señalado que millones de personas aún carecen de acceso significativo a Internet, mientras persisten desigualdades en conectividad, capacidades digitales y acceso a servicios tecnológicos (OECD, 2023; OECD 2025). A ello se suma una realidad histórica caracterizada por bajos niveles de confianza interpersonal e institucional, un factor que inevitablemente se proyecta sobre los entornos digitales.

En este contexto, la confianza digital deja de ser un asunto exclusiva-

mente tecnológico para convertirse en un desafío sistémico. Involucra liderazgo, gobernanza, regulación, cultura organizacional, diseño de servicios, ética, transparencia, resiliencia y responsabilidad.

Las organizaciones más interconectadas están comprendiendo que la confianza no es el resultado accidental de hacer bien las cosas. Es un concepto multidimensional que debe diseñarse, desarrollarse, medirse, gestionarse y gobernarse. Se diseña desde la estrategia, se asegura en los procesos, se despliega en los productos y servicios, y se valida permanentemente en cada interacción con clientes, ciudadanos, colaboradores y socios de negocio.

La innovación tecnológica acelera aún más esta necesidad. La inteligencia artificial, la automatización de decisiones, los ecosistemas interconectados y las nuevas formas de intercambio digital están redefiniendo la manera como se generan valor y se construyen relaciones. En este escenario, la pregunta ya no es únicamente cómo innovar más rápido, sino cómo hacerlo motivando, preservando y fortaleciendo la confianza.

De igual forma, la resiliencia también adquiere una nueva lectura. Durante mucho tiempo se pensó en llegar a organizaciones capaces de evitar cualquier falla (OECD, 2023; NIST, 2024). Hoy comprendemos que la complejidad creciente de los entornos digitales hace prácticamente imposible eliminar la incertidumbre. Por tanto, lo relevante es desarrollar capacidades para responder, adaptarse, aprender, reinventarse y permanecer aun frente a la inevitabilidad de la falla. La confianza se consolida no porque los incidentes nunca ocurran, sino porque las organizaciones demuestran que pueden gestionarlos con transparencia, responsabilidad, preparación y eficacia, porque pueden tomar decisiones responsables, y adicionalmente porque toda la organización desde su nivel directivo hasta su nivel operacional está involucrada en ello.

Esta edición de la Revista Sistemas invita precisamente a reflexionar sobre esta transición. Una transición que desplaza el foco desde la protección aislada hacia la construcción integral de confianza. Desde la tecnología como herramienta hacia la confianza como propósito, como una perspectiva multidimensional. Desde la gestión de riesgos como obligación hacia la generación de valor como resultado.

Quizás uno de los mayores aprendizajes de esta era digital sea reconocer que la tecnología puede conectar sistemas, automatizar procesos y acelerar decisiones, pero solamente la confianza (que no es ausencia de eventos adversos o errores) es capaz de sostener relaciones duraderas entre personas, organizaciones y sociedades cuando las cosas no ocurren como esta-

ban planeadas. En última instancia, el futuro digital no será definido por quienes desarrollen más tecnología, sino por quienes logren inspirar, demostrar y mantener mayores niveles de confianza en ella.

Referencias

Saveljeva, J., & Volkova, T. (2025). A Survey on Digital Trust: Towards a Validated Definition. *Digital, 5*(2), 14. https://doi.org/10.3390/digital5020014

OECD/CAF (2023), *Digital Government Review of Latin America and the Caribbean: Building Inclusive and Responsive Public Services*, OECD Digital Government Studies, OECD Publishing, Paris. https://doi.org/10.1787/29f32e64-en.

OECD (2025), *OECD Survey on Drivers of Trust in Public Institutions in Latin America and the Caribbean 2025 Results*, OECD Publishing, Paris. https://doi.org/10.1787/ea3385cf-en.

NIST (2024) National Institute of Standards and Technology. *Cybersecurity framework (CSF) 2.0*. U.S. Department of Commerce. https://www.nist.gov/cyberframework

Jeimy J. Cano M., Ph.D, CFE, CICA. Ingeniero y Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Especialista en Derecho Disciplinario, Universidad Externado de Colombia; Ph.D en Business Administration, Newport University, CA. USA. y Ph.D en Educación, Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.

Andreés R. Almanza J., CISM, Ingeniero Ingeniería de Sistemas de la Universidad Católica de Colombia y Master en seguridad de la información de la, Universidad Oberta de Catalunia. Especialista en Seguridad de Redes de la Universidad Católica de Colombia, . Profesional certificado como Certified Information Security Manager (CISM), por la Information Systems Audit and Control Association (ISACA) .Catedrático de la Facultad de Administración de la Universidad Exetrnado de Colombia. Miembro del comité editorial de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.director general CISOS.CLUB y la Asociación de Profesionales de Seguridad y Ciberseguridad (APSIC)