El CISO como arquitecto de la confianza

Liderazgo, gobernanza y resiliencia digital en entornos NAVI latinoamericanos

DOI: 10.29236/sistemas.n179a8

Resumen

La evolución del riesgo digital ha transformado profundamente el rol del Chief Information Security Officer (CISO). En contextos caracterizados por aceleración tecnológica, interdependencia sistémica, volatilidad regulatoria y expansión de amenazas híbridas, la seguridad dejó de ser una función estrictamente técnica para convertirse en un componente estructural de la gobernanza organizacional. Este artículo examina el papel del CISO como articulador de confianza digital en organizaciones que operan en entornos NAVI—No lineales, Acelerados, Volátiles e Interconectados— con especial énfasis en América Latina. A partir de literatura académica, marcos de gobernanza y reportes especializados, se analiza cómo la confianza digital emerge de la interacción entre capacidades técnicas, liderazgo estratégico, comunicación organizacional y legitimidad institucional. El artículo propone el concepto de "arquitectura de confianza" como marco integrador para comprender la función contemporánea del CISO, entendida como la articulación de capacidades técnicas, organizacionales, comunicacionales y éticas que permiten sostener confianza digital en escenarios complejos. Asimismo, se reconocen los límites, tensiones y riesgos de sobredimensionar dicho rol. Se concluye que la confianza no puede entenderse únicamente como consecuencia de controles tecnológicos eficaces, sino como resultado de dinámicas organizacionales sostenidas que integran transparencia, resiliencia y capacidad adaptativa.

Palabras clave
CISO, confianza digital, gobernanza, liderazgo adaptativo, resiliencia organizacional, riesgo sistémico, ciberseguridad estratégica, América Latina.

Andrés R. Almanza Junco.

1. Introducción

Durante la última década, la ciberseguridad dejó de ocupar un lugar periférico en las organizaciones para convertirse en una preocupación de nivel estratégico. Los incidentes recientes demuestran que las brechas digitales ya no representan únicamente interrupciones técnicas: afectan reputación, continuidad operacional, legitimidad institucional y estabilidad económica.

El ataque contra instituciones del Estado costarricense en 2022 evidenció cómo un incidente cibernético puede escalar hacia una crisis nacional, afectando servicios públicos esenciales y obligando a declarar estado de emergencia (Mandiant, 2023; Porrúa et al., 2025). Casos similares en entidades financieras, compañías tecnológicas y organizaciones de salud en América Latina han demostrado que la fragilidad digital tiene consecuencias sistémicas.

En este contexto, el rol del Chief Information Security Officer (CISO) ha experimentado una transformación significativa. Tradicionalmente asociado con controles técnicos, gestión de vulnerabilidades y supervisión operativa, el CISO contemporáneo enfrenta expectativas crecientemente vinculadas con liderazgo, gobernanza y comunicación estratégica.

Sin embargo, esta evolución plantea una pregunta crítica: ¿hasta qué punto la seguridad puede entenderse únicamente como una capacidad tecnológica? La evidencia sugiere que los incidentes más disruptivos rara vez se explican exclusivamente por fallas técnicas. Frecuentemente involucran decisiones organizacionales, debilidades culturales, fragmentación de responsabilidades y deterioro de la confianza institucional.

A partir de esta premisa, este artículo sostiene que el valor estratégico del CISO no reside únicamente en proteger infraestructuras digitales, sino en contribuir a la construcción y sostenimiento de confianza digital dentro y fuera de la organización. No obstante, esta afirmación requiere matices importantes. La confianza no depende exclusivamente del CISO ni puede ser producida unilateralmente desde la función de seguridad. Más bien, emerge de la interacción entre estructuras de gobernanza,

capacidades organizacionales, comunicación transparente y comportamiento institucional consistente.

Para analizar esta problemática, el artículo adopta el concepto de entornos NAVI (EY, 2025) —No lineales, Acelerados, Volátiles e Interconectados— desarrollado por la firma de consultoría EY, como evolución conceptual de marcos previos como VUCA y aproximaciones posteriores como BANI.

El concepto NAVI busca enfatizar la intensidad de las interdependencias digitales y la velocidad con que las crisis pueden propagarse entre organizaciones, industrias y sociedades. Aunque NAVI representa una aproximación emergente proveniente del ámbito de consultoría estratégica, resulta útil como lente interpretativo para comprender dinámicas contemporáneas de interdependencia digital. Desde esta perspectiva, el artículo explora tres preguntas principales:

1. ¿Por qué la confianza digital se ha convertido en un componente central de la gobernanza contemporánea?
2. ¿Qué papel puede desempeñar el CISO en la construcción de dicha confianza?
3. ¿Cuáles son los límites y tensiones de atribuirle al CISO un rol de “arquitecto de confianza”?

La intención no es idealizar la función del CISO ni convertirla en solución universal frente al riesgo digital. Por el contrario, el objetivo es comprender cómo la seguridad, el liderazgo y la confianza convergen en organizaciones cada vez más dependientes de sistemas digitales complejos.

2. Entornos NAVI y transformación del riesgo organizacional

Las organizaciones contemporáneas operan en escenarios crecientemente complejos. La digitalización acelerada, la hiperconectividad y la dependencia de ecosistemas tecnológicos externos han modificado profundamente la naturaleza del riesgo corporativo.

El modelo VUCA —Volatility, Uncertainty, Complexity and Ambiguity— surgió inicialmente en contextos militares y posteriormente fue adoptado por la literatura de management para describir entornos caracterizados por incertidumbre y cambio acelerado (Bennett & Lemoine, 2014). Posteriormente, surgieron aproximaciones como BANI, que intentaron describir la fragilidad emocional y sistémica de los entornos contemporáneos. Más recientemente, EY propuso el modelo NAVI como evolución conceptual orientada a enfatizar dinámicas de no linealidad, aceleración, volatilidad e interconexión digital (Bax & Jaggi, 2025).

El concepto NAVI utilizado en este artículo busca enfatizar cuatro características estructurales:

- **No linealidad:** pequeñas vulnerabilidades pueden desencadenar impactos desproporcionados.
- **Aceleración:** las amenazas evolucionan más rápido que muchos procesos organizacionales.
- **Volatilidad:** las condiciones regulatorias, tecnológicas y reputacionales cambian constantemente.
- **Interconexión:** las organizaciones dependen de redes complejas de proveedores, plataformas y terceros.

El caso SolarWinds ilustra claramente esta lógica sistémica. La manipulación de actualizaciones de software permitió comprometer miles de organizaciones mediante una relación de confianza preexistente con un proveedor tecnológico (CISA, 2021; Mandiant, 2021). El incidente mostró que la superficie de riesgo ya no puede entenderse únicamente desde límites organizacionales internos.

Esta transformación tiene implicaciones profundas para la gobernanza corporativa. Los riesgos digitales dejaron de ser problemas aislados de departamentos tecnológicos para convertirse en riesgos estratégicos capaces de afectar continuidad operativa, reputación, cumplimiento regulatorio y estabilidad financiera.

3. Liderazgo adaptativo, transformacional y estratégico

Heifetz y Linsky (2002) acuñaron el concepto de liderazgo adaptativo para describir la capacidad de movilizar a las personas hacia la resolución de problemas que no tienen soluciones técnicas predefinidas. En este sentido, el CISO enfrenta un desafío típicamente adaptativo: la ciberseguridad no es un problema que se resuelve instalando una herramienta; es un proceso continuo de aprendizaje, adaptación y negociación cultural dentro de la organización.

Burns (1978) y Bass (1985) desarrollaron el concepto de liderazgo transformacional, que distingue entre líderes que transaccionan —dan y reciben dentro de reglas establecidas— y líderes que transforman —cambian las reglas, los valores y las motivaciones de sus seguidores. El CISO arquitecto de confianza opera en el espacio transformacional: no solo administra riesgos, sino que cambia la cultura de seguridad de la organización, eleva la madurez digital y redefine cómo la junta directiva y los equipos operativos perciben su función.

El liderazgo estratégico, por su parte, se define como la capacidad de anticipar, visionar, mantener flexibilidad y delegar autoridad para crear cambio estratégico cuando sea necesario (Ireland & Hitt, 1999). Para el CISO, esto significa operar simultáneamente en el presente operacional —respondiendo a incidentes— y en el futuro estratégico

—diseñando arquitecturas de seguridad alineadas con los objetivos del negocio.

4. Confianza digital y gobernanza organizacional

La confianza ha sido ampliamente estudiada en sociología, psicología organizacional y teoría institucional. Rousseau et al. (1998) la definen como la disposición a aceptar vulnerabilidad basada en expectativas positivas sobre la conducta de otro. Mayer, Davis y Schoorman (1995) complementan esta visión identificando tres factores fundamentales: competencia, integridad y benevolencia.

En contextos digitales, la confianza adquiere características particulares. Los individuos dependen cotidianamente de sistemas que no comprenden completamente, pero cuya confiabilidad deben asumir para operar social y económicamente. Luhmann (1979) y Giddens (1990) ya habían advertido que la modernidad depende crecientemente de la confianza en sistemas abstractos e infraestructuras complejas.

La confianza digital puede entenderse entonces como la expectativa razonable de que una organización gestionará de forma segura, ética y consistente los sistemas y datos que administra (WEF, 2022; WEFb, 2022). Según el WEF (2024), el 80% del valor de mercado de las empresas del S&P 500 corresponde a activos intangibles. La protección de estos activos no es responsabilidad exclusiva del CISO, pero su compromiso catastrófico —a través de una brecha de datos, un ataque de ransomware o una exposición regulatoria— puede destruir en horas lo que tomó años construir, esa confianza que requiere para desarrollarse en un ecosistema digital de gran tamaño.

Esta definición tiene implicaciones relevantes. La confianza digital no depende exclusivamente de la ausencia de incidentes. Ninguna organización puede garantizar inmunidad absoluta frente a amenazas sofisticadas. La confianza depende más bien de cómo la organización: gestiona sus riesgos, responde ante crisis, comunica incidentes, protege a sus partes interesadas, y demuestra coherencia institucional.

Finalmente, hay una razón de competitividad. En mercados donde la diferenciación es difícil y los consumidores son cada vez más conscientes del valor de su privacidad, la confianza digital se convierte en ventaja competitiva. Según Edelman (2023), el 71% de los consumidores globales considera que la confianza en una empresa es un factor determinante en sus decisiones de compra.

En América Latina, donde la desconfianza institucional es históricamente alta, las organizaciones que logran construir reputaciones sóli-

das de seguridad y transparencia digital obtienen una ventaja relacional significativa.

Desde esta perspectiva, la ciberseguridad deja de ser únicamente una disciplina de control para convertirse en un componente de legitimidad organizacional.

5. El CISO y la evolución hacia un rol estratégico

La literatura temprana sobre seguridad de la información estuvo dominada por enfoques económicos y técnicos centrados en optimización de inversiones y controles (Gordon & Loeb, 2002; Bodin et al., 2008).

En estos modelos, el rol del CISO aparecía principalmente como gestor operativo.

Posteriormente, investigaciones sobre comportamiento organizacional comenzaron a demostrar que muchos incidentes relevantes no derivaban exclusivamente de fallas tecnológicas, sino de problemas culturales, humanos y organizacionales (Crossler et al., 2013; Bada, M., & Sasse, A., 2014).

Este cambio amplió progresivamente las expectativas sobre el CISO. Organismos como ISACA (2023), NACD (2023) y Ribot (2025) han enfatizado la necesidad de que los líderes de seguridad desarrollen competencias vinculadas con: comunicación ejecutiva, influencia organizacional, pensamiento sistémico, liderazgo adaptativo, y gestión estratégica del riesgo.

La gobernanza corporativa contemporánea también ha contribuido a esta transformación. La ISO 37000:2021 y los principios de gobierno corporativo de la OCDE reconocen que los riesgos digitales deben formar parte de la supervisión estratégica de las organizaciones (OCDE, 2023).

En consecuencia, el CISO ya no opera exclusivamente como especialista técnico. En muchas organizaciones, se ha convertido en traductor entre complejidad tecnológica y toma de decisiones estratégicas. Así mismo, el Banco Interamericano de Desarrollo (BID & OEA, 2020) en su estudio sobre el impacto económico de los ciberataques en América Latina estimó pérdidas anuales superiores a 90.000 millones de dólares en la región, con efectos desproporcionadamente severos en economías con menor capacidad de respuesta institucional. En este escenario, el CISO que no opera como arquitecto de confianza no solo falla en su función técnica; falla en su responsabilidad estratégica con la organización y con el ecosistema al que pertenece.

Sin embargo, esta transición también introduce riesgos. Existe una tendencia creciente a sobredimensionar el rol del CISO, atribuyéndole responsabilidades que exceden sus capacidades reales o su autori-

dad institucional. La confianza organizacional no puede recaer únicamente en un individuo o función específica. Depende de estructuras más amplias de liderazgo y cultura corporativa.

6. Hacia una arquitectura de confianza

El concepto de arquitectura de confianza utilizado en este artículo se apoya en aproximaciones contemporáneas sobre *digital trust, governance by design* y resiliencia institucional promovidas por organismos como el WEF (2022), que plantean que la confianza digital debe incorporarse desde el diseño organizacional y no únicamente como capacidad reactiva de seguridad.

En este contexto, la arquitectura de confianza puede entenderse como la articulación estructurada de capacidades técnicas, organizacionales, comunicacionales y éticas que permiten generar, sostener y recuperar confianza digital en entornos complejos.

Esta aproximación no debe entenderse como un modelo cerrado ni como una metodología formalmente validada. Más bien, funciona como un marco integrador para comprender cómo distintas capacidades organizacionales contribuyen al sostenimiento de confianza digital.

Esta arquitectura involucra al menos cuatro dimensiones interdependientes.

6.1. Dimensión técnica

Incluye controles de seguridad, resiliencia tecnológica, monitoreo, respuesta a incidentes y protección de infraestructuras críticas. La competencia técnica sigue siendo condición necesaria para la confianza. Un liderazgo carismático sin capacidad operacional difícilmente puede sostener legitimidad frente a incidentes reales.

6.2. Dimensión organizacional

La confianza también depende de estructuras de gobernanza claras, roles definidos y alineación entre seguridad y estrategia corporativa. La posición del CISO dentro de la estructura organizacional resulta particularmente relevante. Estudios de ISACA (2023) sugieren que organizaciones donde el CISO posee acceso directo a niveles ejecutivos muestran mayores niveles de madurez y capacidad de respuesta. No obstante, la relación no es automática. Reportar al CEO o al directorio no garantiza influencia real ni transformación cultural.

6.3. Dimensión conversacional

La confianza posee un componente profundamente interpretativo. Las partes interesadas evalúan no solo lo que una organización hace, sino cómo comunica sus acciones. En escenarios de crisis, la transparencia se convierte en variable crítica. La comunicación en ciberseguridad requiere equilibrio entre honestidad, prudencia estratégica y manejo reputacional. Así las cosas, la confianza no depende

exclusivamente de mensajes correctos, sino de trayectorias organizacionales consistentes.

6.4. Dimensión ética y relacional

La confianza también involucra percepciones de integridad y coherencia institucional. El caso de Rappi en Colombia resulta ilustrativo porque muestra que la erosión de confianza puede originarse no solo en ciberataques, sino también en problemas de gobernanza del dato y cumplimiento regulatorio (Quinchía, 2021; Bloomberg Línea, 2021). Esto amplía el alcance de la discusión. La confianza digital no depende únicamente de proteger sistemas, sino de gestionar responsablemente la información y las relaciones con las partes interesadas.

Para pasar a través de todas estás dimensiones y poder operacionalizar estos elementos, una arquitectura de confianza podría observarse en organizaciones que integran al menos cinco capacidades: (1) supervisión ejecutiva del riesgo digital, (2) resiliencia operacional medible, (3) comunicación transparente de incidentes, (4) gobernanza de terceros y cadena de suministro, y (5) existencia de comités de revisión y rendición de cuentas, sobre decisiones tecnológicas (*accountability*).

Aunque estas capacidades no constituyen un modelo universal ni una metodología cerrada, pueden servir como indicadores observables de madurez organizacional en la construcción de confianza digital. Su relevancia no radica únicamente en la existencia formal de controles, sino en la capacidad de la organización para integrarlos dentro de procesos sostenibles de gobernanza, resiliencia y toma de decisiones. Para ello se ilustran estos elementos en la tabla 1.

7. Tensiones y límites del modelo

La idea del CISO como arquitecto de confianza posee utilidad estratégica, pero también enfrenta limitaciones importantes.

7.1. La paradoja de la transparencia

Una comunicación excesivamente abierta sobre vulnerabilidades puede producir efectos contraproducentes: deterioro reputacional, pérdida de confianza de inversionistas, incremento de presión regulatoria, o exposición frente a actores maliciosos.

La transparencia en ciberseguridad no puede entenderse como valor absoluto. Requiere criterio estratégico y comprensión contextual.

7.2. El riesgo de hipercentralización del CISO

Existe una tendencia creciente a convertir al CISO en símbolo organizacional de confianza digital. Sin embargo, esto puede generar expectativas imposibles de sostener. La seguridad depende de: cultura organizacional, recursos, decisiones ejecutivas, arquitectura tec-

Tabla 1. *Capacidades de una arquitectura de confianza*

Capacidad	Propósito organizacional	Indicadores o métricas observables
Supervisión ejecutiva del riesgo digital	Integrar el riesgo digital dentro de la gobernanza corporativa	Frecuencia de revisión del riesgo en junta directiva, participación del CISO en comités ejecutivos, existencia de indicadores de riesgo digital (KRIs)
Resiliencia operacional medible	Evaluar capacidad de continuidad recuperación y aprendizaje en las crisis cibernéticas	MTTR (*Mean Time to Recovery*), RTO/RPO, tiempo promedio de contención de incidentes, pruebas de continuidad ejecutadas
Comunicación transparente de incidentes	Preservar legitimidad y coordinación durante crisis	Tiempo de notificación, consistencia comunicacional, existencia de protocolos de crisis, cumplimiento regulatorio de divulgación
Gobernanza de terceros y cadena de suministro	Reducir exposición sistémica derivada de interdependencias	Evaluaciones de terceros, cobertura contractual de seguridad, monitoreo continuo de proveedores críticos. Mapeo y monitoreo de terceros críticos que soportan procesos esenciales del negocio que soportan las unidades claves de negocio.
Accountability sobre decisiones tecnológicas	Asegurar trazabilidad y responsabilidad organizacional	Registro de decisiones críticas, auditorías, mecanismos de supervisión ética y validación de riesgos tecnológicos

Nota: *Elaboración propia basada en principios de gobernanza digital, resiliencia organizacional y gestión de riesgo cibernético inspirados en marcos de NIST CSF 2.0 (2024), ISO 22301(2019) y World Economic Forum WEF (2021).*

nológica, cumplimiento regulatorio, y comportamiento humano colectivo.

Un CISO competente en una organización estructuralmente disfuncional difícilmente podrá construir confianza sostenible.

7.3. Fatiga y sostenibilidad del rol

La investigación reciente muestra altos niveles de agotamiento entre CISOs. Heidrick & Struggles (2023) reporta una permanencia promedio cercana a dos años en muchas organizaciones.

Esto introduce una contradicción estructural: la confianza requiere continuidad, mientras que el rol frecuentemente opera bajo presión extrema, alta exposición y expectativas ambiguas.

La sostenibilidad del liderazgo en ciberseguridad emerge, así como un problema organizacional y no exclusivamente individual.

7.4. Limitaciones regionales latinoamericanas

En América Latina, las dinámicas de confianza digital se desarrollan en un entorno marcado por profundas asimetrías institucionales, económicas y tecnológicas. Estas diferencias impactan directamente la capacidad de gobiernos y organizaciones para construir modelos sostenibles de resiliencia y gobernanza digital. El *2025 Cybersecurity Report* del Banco Interamericano de Desarrollo (BID) advierte que la región mantiene niveles heterogéneos de madurez en capacidades nacionales de ciberseguridad, preparación institucional, resiliencia operacional y coordinación estratégica frente a incidentes cibernéticos (Porrúa et al., 2025). Esta disparidad no solo ocurre entre países, sino también entre sectores económicos y organizaciones dentro de un mismo ecosistema nacional.

Adicionalmente, el informe conjunto de la Organización de los Estados Americanos (OEA) y el BID sobre ciberseguridad en América Latina y el Caribe señala que persisten desafíos estructurales relacionados con restricciones presupuestarias, fragmentación regulatoria, baja integración estratégica de la ciberseguridad y dependencia tecnológica externa (BID & OEA, 2020). Estas condiciones generan contextos donde la confianza digital no puede depender únicamente de capacidades tecnológicas, sino también de factores organizacionales, regulatorios e institucionales más amplios.

La región también enfrenta brechas significativas de digitalización e inclusión tecnológica. El Programa de las Naciones Unidas para el Desarrollo (PNUD) ha señalado que la digitalización en América Latina avanza de manera desigual y que las limitaciones de acceso, capacidades digitales y apropiación tecnológica continúan profundizando brechas económicas y sociales (Programa de las Naciones Unidas para el Desarrollo [PNUD], 2023). En una línea similar, el Banco Mundial advierte que el acceso desigual a infraestructura digital y conectividad limita la competitividad regional y ralentiza la capacidad de transformación digital sostenible (Banco Mundial, 2022).

Desde una perspectiva institucional, la Comisión Económica para América Latina y el Caribe (CEPAL) ha destacado que los procesos de transformación digital en la región siguen condicionados por niveles

heterogéneos de desarrollo estatal, gobernanza digital y articulación de políticas públicas, generando capacidades desiguales para responder a riesgos emergentes asociados a entornos digitales (CEPAL, 2024). Complementariamente, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) identifica que muchos países latinoamericanos aún enfrentan desafíos relevantes en integración de gobierno digital, interoperabilidad institucional y fortalecimiento de capacidades públicas para la gestión de ecosistemas digitales complejos (OCDE, 2023).

En este contexto, modelos de gobernanza y confianza digital desarrollados en entornos norteamericanos o europeos no siempre resultan directamente transferibles a realidades latinoamericanas caracterizadas por volatilidad institucional, restricciones operativas y madurez desigual entre sectores económicos. A ello se suma un elemento particularmente crítico: la confianza, entendida como componente esencial de cohesión social y crecimiento económico, continúa siendo un desafío estructural para la región. El BID ha señalado que los bajos niveles de confianza interpersonal e institucional afectan la cooperación, la legitimidad organizacional y la capacidad de articular respuestas sostenibles frente a desafíos colectivos (BID, 2022).

Finalmente, la creciente presión reputacional alrededor de conceptos como resiliencia, transformación digital y confianza también introduce el riesgo de que algunas organizaciones privilegien narrativas de legitimidad sobre transformaciones estructurales reales de seguridad y gobernanza. En consecuencia, la confianza digital no puede reducirse a cumplimiento normativo o comunicación corporativa, sino que requiere capacidades sostenibles, verificables y articuladas dentro de modelos consistentes de resiliencia organizacional.

8. Discusión: confianza, resiliencia y legitimidad institucional

La discusión contemporánea sobre ciberseguridad frecuentemente oscila entre dos extremos problemáticos.

El primero es el reduccionismo técnico: asumir que la seguridad depende fundamentalmente de herramientas, controles y automatización. El segundo es el reduccionismo narrativo: asumir que liderazgo, comunicación o cultura pueden compensar debilidades estructurales de seguridad. Ambas posiciones son insuficientes.

La evidencia sugiere que la resiliencia organizacional emerge precisamente de la interacción entre capacidades técnicas y legitimidad institucional. Las organizaciones más resilientes no son necesariamente aquellas que evitan todos los incidentes, sino aquellas capaces de: absorber impactos, adap-

tarse rápidamente, preservar coordinación interna, y sostener confianza externa durante crisis.

En este contexto, el CISO puede desempeñar un papel relevante como articulador entre dominios tradicionalmente separados: tecnología, negocio, riesgo, cumplimiento, comunicaciones, y gobernanza.

Sin embargo, su efectividad dependerá menos de atributos heroicos individuales y más de la capacidad organizacional para integrar la seguridad dentro de su modelo de decisión estratégica.

Conclusiones

La transformación digital ha convertido la confianza en un componente central de la competitividad y legitimidad organizacional. En entornos caracterizados por interdependencia tecnológica y riesgo sistémico, la seguridad ya no puede entenderse exclusivamente como problema operativo.

El rol del CISO ha evolucionado en respuesta a esta realidad. Cada vez más organizaciones esperan que sus líderes de seguridad participen en conversaciones estratégicas, traduzcan complejidad técnica y contribuyan a la resiliencia institucional. No obstante, esta evolución requiere evitar simplificaciones.

El CISO no puede ser concebido como único responsable de la confianza digital. La confianza emerge de sistemas organizacionales más amplios donde intervienen gobernanza, cultura, liderazgo ejecutivo, ética institucional y capacidad adaptativa.

El concepto de arquitectura de confianza propuesto en este artículo busca precisamente enfatizar esa naturaleza sistémica. Su valor no reside en convertir al CISO en figura centralizadora, sino en reconocer que la seguridad contemporánea depende de relaciones organizacionales complejas que exceden la dimensión tecnológica.

En América Latina, este desafío adquiere particular relevancia debido a contextos marcados por volatilidad institucional, madurez desigual y aceleración digital asimétrica.

Las organizaciones que comprendan esta complejidad probablemente estarán mejor preparadas no solo para enfrentar incidentes, sino para sostener legitimidad y resiliencia en escenarios crecientemente inciertos.

En última instancia, la confianza digital no representa un estado permanente ni una garantía absoluta. Es una construcción dinámica, vulnerable y continuamente negociada entre organizaciones, tecnologías y sociedades. El valor estratégico del CISO contemporáneo reside, quizás, no en prometer control total sobre dicha incertidumbre, sino en ayudar a las organizacio-

nes a gestionarla con mayor transparencia, coherencia y capacidad adaptativa.

Referencias

Bada, M., & Sasse, A. (2014). Cyber security awareness campaigns: Why do they fail to change behaviour? *Proceedings of the International Conference on Cyber Security for Sustainable Society*. https://discovery.ucl.ac.uk/id/eprint/1468954/

Bass, B. M. (1985). *Leadership and performance beyond expectations*. Free Press.

Bax, H. J., & Jaggi, G. (2025). *What if disruption isn't the challenge, but the chance?* EY. https://www.ey.com/en_gl/megatrends/what-if-disruption-is-not-the-challenge-but-the-chance

Bennett, N., & Lemoine, G. J. (2014). What a difference a word makes: Understanding threats to performance in a VUCA world. *Business Horizons, 57*(3), 311–317. https://www.sciencedirect.com/science/article/abs/pii/S0007681314000020

Banco Interamericano de Desarrollo (BID), & Organización de los Estados Americanos (OEA). (2020). *Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe*. https://publications.iadb.org/es/publications/spanish/viewer/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Banco Interamericano de Desarrollo (BID). (2022). *Confianza: la clave de la cohesión social y el crecimiento en América Latina y el Caribe* (Resumen ejecutivo). https://publications.iadb.org/es/publications/spanish/viewer/Confianza-la-clave-de-la-cohesion-social-y-el-crecimiento-en-America-Latina-y-el-Caribe-Resumen-ejecutivo.pdf

Banco Mundial. (2022). *El escaso acceso digital frena a América Latina y el Caribe: cómo solucionarlo*. https://blogs.worldbank.org/es/latinamerica/el-escaso-acceso-digital-frena-america-latina-y-el-caribe-como-solucionar-este

Bloomberg Línea. (2021). Multan a Rappi en Colombia por violaciones al régimen de protección de datos. https://www.bloomberglinea.com/2021/10/29/multan-a-rappi-en-colombia-por-violaciones-al-regimen-de-proteccion-de-datos/

Bodin, L., Gordon, L., & Loeb, M. (2008). Information security and risk management. *Communications of the ACM, 51*(4), 64–68. https://doi.org/10.1145/1330311.1330325

Burns, J. M. (1978). *Leadership*. Harper & Row.

Comisión Económica para América Latina y el Caribe (CEPAL). (2024). *América Latina y el Caribe en la segunda mitad de la década digital*. https://repositorio.cepal.org/server/api/core/bitstreams/e4ca636c-2b8a-4138-8c62-b685540d9b99/content

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Cybersecurity and Infrastructure Security Agency. (2021). *Advanced persistent*

threat compromise of government agencies, critical infrastructure, and private sector organizations. CISA Advisory AR21-112A

Edelman. (2023). *Edelman trust barometer 2023: Global report*. Edelman Trust Barometer 2023

Giddens, A. (1990). *The consequences of modernity*. Stanford University Press.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4), 438–457. https://doi.org/10.1145/581271.581274

Heidrick & Struggles. (2023). *Global CISO survey 2023: The evolving role of the chief information security officer*. https://www.heidrick.com/en/insights/cybersecurity/2023-global-chief-information-security-officer-survey

Heifetz, R., & Linsky, M. (2002). *Leadership on the line: Staying alive through the dangers of leading*. Harvard Business Review Press.

Ireland, R. D., & Hitt, M. A. (1999). Achieving and maintaining strategic competitiveness in the 21st century: The role of strategic leadership. *Academy of Management Perspectives, 13*(1), 43–57. https://doi.org/10.5465/ame.1999.1567311

ISACA. (2023). *State of cybersecurity 2023: Global update on workforce efforts, resources and cyberoperations*. https://www.isaca.org/resources/reports/state-of-cybersecurity-2023

International Organization for Standardization. (2021). *ISO 37000:2021 — Governance of organizations: Guidance*. ISO.

ISO. (2019). *Security and resilience — Business continuity management systems — Requirements*. ISO. https://www.iso.org/standard/75106.html

Luhmann, N. (1979). *Trust and power*. John Wiley & Sons.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709–734. https://doi.org/10.5465/amr.1995.9508080335

Mandiant. (2021). *M-Trends 2021 Special Report*. https://services.google.com/fh/files/misc/rpt-mtrends-2021-en.pdf

Mandiant. (2023). *M-Trends 2023 Special Report*. https://www.mandiant.com/resources/reports/m-trends-2023-special-report?auHash=iTAkoIVQOJBJJ8XvjFW34_KB6WJNeNAZ1HV2I3AEXdE&ref=guptadeepak.com

National Association of Corporate Directors. (2023). *Director's handbook on cyber-risk oversight* (4th ed.). https://isalliance.org/wp-content/uploads/2023/03/Cyber-Risk-Oversight-Handbook_WEB.pdf

NIST. (2024). The NIST cybersecurity framework (CSF) 2.0. *The NIST Cybersecurity Framework (CSF) 2.0*, *2.0*(29). https://doi.org/10.6028/nist.cswp.29

Organisation for Economic Co-operation and Development (OECD). (2023). *Digital government review of Latin America and the Caribbean*. https://www.oecd.org/content/dam/oecd/es/publications/reports/2023/09/digit

al-government-review-of-latin-america-and-the-caribbean_75a4be05/7a127615-es.pdf

Programa de las Naciones Unidas para el Desarrollo (PNUD). (2023). *La digitalización: motor de inclusión y crecimiento en América Latina*. https://www.undp.org/es/peru/noticias/la-digitalizacion-motor-de-inclusion-y-crecimiento-en-america-latina

Porrúa, M., Moncayo, G., Paz, S., Nowersztern, A., Bejarano, J. F., Baudino, M. F., Bordese, M. P., Barret, K., Baena, C. E., Jaramillo, M., Garces, O., & Isidro, A. (2025). *2025 Cybersecurity Report: Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean*. https://doi.org/10.18235/0013872

Quinchía, A. Z. (2021). Superindustria multa a Rappi por violación a protección de datos. *El Colombiano*. https://www.elcolombiano.com/negocios/multan-a-rappi-por-violacion-al-regimen-de-proteccion-de-datos-personales-JI15954739

Ribot, S. (2025). *The CISO Dilemma*. Kornferry.com. https://www.kornferry.com/institute/the-ciso-dilemma

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review, 23*(3), 393–404. https://doi.org/10.5465/amr.1998.926617

WEF. (2021). *Principles for Board Governance of Cyber Risk*. World Economic Forum. https://www.weforum.org/publications/principles-for-board-governance-of-cyber-risk/

WEF. (2022). *Earning Digital Trust: Decision-Making for Trustworthy Technologies*. World Economic Forum. https://www.weforum.org/publications/earning-digital-trust-decision-making-for-trustworthy-technologies/

WEF. (2022b). *Principles for board governance of cyber risk*. https://www.weforum.org/publications/principles-for-board-governance-of-cyber-risk/

World Economic Forum. (2024). *Global risks report 2024*. https://www.weforum.org/publications/global-risks-report-2024/

Andrés Ricardo Almanza Junco CISM, Ingeniero de Sistemas y Especialista de Seguridad de la Univesidad Católica de Colombia, Master en Seguridad de la Información de la Universidad Oberta de Catalunia, certificado como CISM por ISACA Internacional, Certificado como ISO 27001 Senior Lead Implementer and 27005 Lead Manager from PECB, Formación Ejecutiva Líderes Globales, Business Administration and Management por la Universidad de los Andes, Executive Certificate in Cybersecurity Leadership & Strategy por Florida Internation University, Certificado como Coach Profesional Internacional by INILID | Master in Leadership and Organizational Development with Coaching & Executive Master's in Leadership Skills Developed in Harvard & Coach Profesional avalado por International Coach Federation by EIDHI International University – USA. Profesor de la Universidad Externado de Colombia, director general de la Asociación de Profesionales de Seguridad y Ciberseguridad APSIC y CISOS.CLUB.