Revista de Pensamiento Estratégico y Seguridad CISDE

CISDE Journal, 11(1), 2026

Recibido: 13-05-2025 / Revisado: 07-08-2025
Aceptado: 11-08-2025 / Publicado: 30-05-2026

De la autenticación a la resiliencia en la estrategia institucional: evolución de IAM en la era Zero Trust

From authentication to resilience in institutional strategy: the evolution of IAM in the Zero Trust era

Juan Carlos Castro-Ortiz[1,2], Francisco José Martínez-López[1]

[1] Universidad de Huelva, España
[2] CISO, España

juankarloz@gmail.com , francis@uhu.es

RESUMEN. La gestión de identidades y accesos (IAM, por sus siglas en inglés) se ha convertido en el eje central de la ciberseguridad moderna. En un contexto marcado por la expansión del trabajo remoto, la adopción de la nube y la proliferación de dispositivos conectados, la identidad digital ha reemplazado al perímetro tradicional como principal línea de defensa. Este artículo analiza la evolución de IAM desde su concepción como herramienta de control hasta su papel como pilar estratégico dentro del modelo Zero Trust. Se abordan los errores más comunes en su implementación, la importancia de una gobernanza transversal, y la necesidad de integrar IAM con arquitecturas Zero Trust y tecnologías emergentes como la inteligencia artificial, el aprendizaje automático o la criptografía poscuántica. Asimismo, se examinan los beneficios tangibles de su adopción, tanto en términos de resiliencia cibernética como de eficiencia operativa y cumplimiento normativo. El estudio concluye que la combinación de IAM y Zero Trust no solo fortalece la seguridad organizacional, sino que también impulsa la transformación digital y la confianza en ecosistemas empresariales e institucionales cada vez más distribuidos y complejos.

ABSTRACT. Identity and Access Management (IAM) has become the cornerstone of modern cybersecurity. In a context shaped by remote work, cloud adoption, and the proliferation of connected devices, digital identity has replaced the traditional network perimeter as the main line of defense. This article analyzes the evolution of IAM from its origins as a control mechanism to its current role as a strategic pillar within the Zero Trust model. It explores the most common implementation errors, the importance of cross-functional governance, and the need to integrate IAM with Zero Trust architectures and emerging technologies such as artificial intelligence, machine learning, and post-quantum cryptography. The paper also examines the tangible benefits of this integration in terms of cyber resilience, operational efficiency, and regulatory compliance. The study concludes that combining IAM with Zero Trust not only strengthens organizational security but also drives digital transformation and trust across increasingly distributed and complex corporate and institutional ecosystems.

PALABRAS CLAVE: Gestión de identidades y accesos, IAM, Zero Trust, Autenticación multifactor, Resiliencia digital, Ciberseguridad.

KEYWORDS: Identity and Access Management, IAM, Zero Trust, Multifactor authentication, Digital resilience.

Castro-Ortiz, J. C., y Martínez-López, F. J. (2026). De la autenticación a la resiliencia en la estrategia institucional: evolución de IAM en la era Zero Trust. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 11(1), 47-57. https://doi.org/10.54988/cisde.2026.1.1804

1. Introducción

La transformación digital ha redefinido por completo los fundamentos de la ciberseguridad corporativa, situando la gestión de identidades y accesos (Identity and Access Management, IAM) en el epicentro de las estrategias de protección digital. En un entorno donde las fronteras entre lo interno y lo externo se difuminan a causa del auge del trabajo remoto, la computación en la nube y la interconexión global de sistemas, confiar únicamente en modelos perimetrales ha dejado de ser suficiente. En este nuevo paradigma, la identidad digital se erige como el perímetro de seguridad moderno, determinando la capacidad de una organización para resistir ataques y garantizar su continuidad operativa.

IAM trasciende la mera dimensión tecnológica: constituye un factor estratégico que involucra procesos, personas y políticas corporativas. Su propósito esencial —asegurar que la persona adecuada accede al recurso adecuado, en el momento adecuado y por el motivo correcto— puede parecer simple, pero su ejecución práctica es compleja. Requiere la integración de sistemas heterogéneos, la aplicación de controles adaptativos y el equilibrio constante entre seguridad y experiencia de usuario.

Las estadísticas recientes evidencian la magnitud del desafío. Más del 50 % de los incidentes de hacking registrados por Verizon (2022) se originan en credenciales comprometidas, ya sea por contraseñas compartidas, por defecto o robadas. Casos como los de Anthem (2015), Cisco Webex (2018) o el Hospital Universitario de Vermont (2020) demuestran que los fallos en la gestión de identidades pueden tener consecuencias devastadoras, tanto económicas como reputacionales.

A pesar del desarrollo de soluciones avanzadas, muchas organizaciones siguen cayendo en los mismos errores: adquieren herramientas de IAM que apenas utilizan, carecen de métricas claras y gestionan identidades de forma fragmentada (García-Río, Baena-Luna, Palos-Sánchez y Aguayo-Camacho, 2022). En consecuencia, los proyectos terminan percibiéndose como obstáculos burocráticos en lugar de como habilitadores del negocio.

En este contexto, el paradigma de Zero Trust Architecture (ZTA) surge como una evolución natural del modelo IAM. Bajo el principio de "nunca confiar, siempre verificar", Zero Trust asume que ninguna red —ni interna ni externa— es segura por defecto. Cada solicitud de acceso debe autenticarse y autorizarse de forma continua, considerando factores contextuales como el comportamiento del usuario, el dispositivo empleado o la sensibilidad de los datos solicitados. De esta manera, IAM se convierte en el núcleo operativo de Zero Trust, proporcionando la base para aplicar controles dinámicos, segmentar redes y reducir el movimiento lateral de los atacantes.

Más allá de la seguridad, IAM impacta directamente en la eficiencia operativa, el cumplimiento normativo y la experiencia digital de usuarios y clientes (Infante-Moro, Infante-Moro y Gallardo-Pérez, 2022). Un acceso denegado por error o un proceso de alta excesivamente lento puede derivar en pérdidas de productividad, desmotivación o abandono de clientes. Su correcta implementación, por el contrario, refuerza la confianza digital y acelera la transformación tecnológica.

En suma, IAM se ha consolidado como el nuevo perímetro de seguridad y elemento clave de la resiliencia digital. Este artículo explora su evolución en la era Zero Trust, analizando el estado actual de su implantación, los desafíos de gobernanza, la integración con tecnologías emergentes y las tendencias que definirán el futuro de la identidad digital en las organizaciones.

2. Revisión de la literatura

La gestión de identidades y accesos (Identity and Access Management, IAM) ocupa hoy un lugar central en el debate sobre la ciberseguridad moderna (Rose et al., 2019; Hasan, 2024). Lejos de ser una disciplina puramente técnica, IAM representa el punto de convergencia entre la seguridad de la información, la gobernanza corporativa y la eficiencia operativa. Sin embargo, a pesar de su relevancia estratégica, la distancia

entre el discurso y la práctica sigue siendo considerable (Luján-Salamanca, Infante-Moro, Infante-Moro, Gallardo-Pérez, 2024). Numerosas organizaciones invierten en herramientas avanzadas, pero no logran consolidar un modelo de identidad eficaz, coherente y sostenible.

El espejismo de la herramienta

Uno de los errores más recurrentes consiste en la adquisición de soluciones de IAM sin una estrategia clara de adopción (Bashir, 2024). En muchos casos, estas plataformas terminan infrautilizadas —convertidas en shelfware— porque fueron implementadas como respuesta reactiva a una auditoría, a un incidente o a una exigencia regulatoria (Hasan, 2024). Sin una gobernanza sólida ni una cultura de seguridad madura, los proyectos se limitan a habilitar funciones básicas (Crowther et al., 2024), como la autenticación multifactor, dejando sin uso módulos críticos de automatización, federación o gestión de privilegios. El resultado es una inversión costosa con escaso retorno y un impacto operativo mínimo.

Gobernanza y responsabilidades difusas

La falta de definición sobre quién debe liderar IAM constituye otro obstáculo estructural (Bashir, 2024; Hasan, 2024). Dependiendo del enfoque de cada organización, el control recae sobre seguridad, infraestructura o negocio, lo que genera sesgos y conflictos. Cuando IAM se centraliza exclusivamente en el área de seguridad, tiende a volverse rígido y burocrático; bajo infraestructura, puede priorizar la eficiencia sobre la protección; y bajo negocio, corre el riesgo de reducirse a un trámite operativo.

Para evitarlo, cada vez más organizaciones apuestan por un Centro de Excelencia en IAM (IAM CoE) (Crowther et al., 2024), un órgano transversal que integra visiones de ciberseguridad, tecnología y negocio. Este enfoque promueve el equilibrio entre seguridad, usabilidad y agilidad operativa, asegurando que la identidad digital sea tratada como un activo estratégico y no como un simple requisito técnico.

Equipos reactivos y cultura del "bombero"

En la práctica cotidiana, muchos equipos de IAM trabajan en modo reactivo, centrados en resolver incidencias diarias —bloqueos de cuentas, altas y bajas de usuarios, restablecimiento de contraseñas— sin tiempo para planificar o mejorar procesos (Ganesh, Rajaram y Sobia, 2024). La ausencia de métricas y acuerdos de nivel de servicio (SLAs) perpetúa la sensación de caos: todo parece urgente, nada se prioriza y el área se percibe como un cuello de botella.

La adopción de SLAs claros y medibles (por ejemplo, tiempo máximo de alta de usuarios o de revocación de accesos tras una baja) permite profesionalizar la función, reducir la carga operativa y mejorar la percepción interna del servicio.

Consecuencias reales: brechas de seguridad

Los errores en la gestión de identidades no son fallos administrativos, sino potenciales detonantes de incidentes críticos (Domínguez, 2016). La historia reciente demuestra que la mayoría de las brechas de seguridad graves tienen su origen en credenciales comprometidas o en una gestión deficiente de accesos privilegiados (Verizon, 2023).

Ejemplos notables incluyen el caso de Anthem (2015), con 78,8 millones de registros robados tras el uso de credenciales sin autenticación multifactor; Cisco Webex (2018), donde un extrabajador mantuvo acceso a servicios críticos durante meses; o el Hospital Universitario de Vermont (2020) (Motiwala, Wolcott y Anderson, 2022), paralizado por un ransomware originado en credenciales expuestas. Estos casos evidencian que la ausencia de controles básicos puede desembocar en pérdidas millonarias y graves daños reputacionales (Verizon, 2023).

Madurez organizativa

El nivel de madurez de IAM varía ampliamente entre organizaciones, pudiendo clasificarse en tres estadios:

a) Nivel básico: procesos manuales y alta exposición al riesgo; la identidad se gestiona mediante hojas de cálculo o tickets manuales.
b) Nivel intermedio: inversión tecnológica significativa, pero uso parcial de funcionalidades; las políticas existen, pero la operativa sigue siendo manual.
c) Nivel avanzado: integración plena con Zero Trust, automatización del ciclo de vida y gobernanza madura. IAM actúa como habilitador de negocio y como base de la resiliencia digital.

La mayoría de las organizaciones se sitúan en el segundo nivel, atrapadas entre la inversión tecnológica y la falta de alineación estratégica. Alcanzar el nivel avanzado exige una visión global que combine procesos, tecnología y cultura (Hasan, 2024).

Desde una perspectiva académica, la literatura sobre IAM ha evolucionado de forma paralela al cambio de paradigma en la seguridad de la información. Los primeros enfoques se centraban principalmente en el control de accesos y la autenticación básica, entendiendo la identidad como un componente técnico subordinado a la infraestructura de red. Sin embargo, los trabajos más recientes coinciden en que esta visión resulta insuficiente en entornos caracterizados por la movilidad, la externalización de servicios y la adopción de arquitecturas cloud y multicloud (Rose et al., 2019).

Diversos autores destacan que la principal debilidad de los modelos tradicionales no reside únicamente en la tecnología, sino en la ausencia de una visión integrada de la identidad como activo organizativo. En este sentido, Hasan (2024) subraya que muchas iniciativas de IAM fracasan porque se abordan como proyectos aislados, sin una alineación clara con los objetivos de negocio ni con la estrategia global de ciberseguridad. Esta desconexión genera soluciones fragmentadas que, lejos de reducir el riesgo, incrementan la complejidad operativa y la superficie de ataque.

La literatura también pone de manifiesto una tensión recurrente entre seguridad y usabilidad. Mientras que los equipos de seguridad tienden a priorizar controles restrictivos, las áreas de negocio demandan agilidad y experiencias de acceso fluidas. Bashir (2024) señala que esta dicotomía ha sido históricamente uno de los principales frenos a la adopción efectiva de IAM, dando lugar a resistencias internas y a la proliferación de prácticas inseguras, como el uso de credenciales compartidas o la reutilización de contraseñas.

En respuesta a estas limitaciones, los modelos más avanzados proponen una gobernanza transversal de la identidad, en la que IAM deja de ser responsabilidad exclusiva del área técnica para convertirse en un elemento compartido entre seguridad, tecnología y negocio. Estudios recientes destacan que la creación de estructuras formales de gobierno, como los Centros de Excelencia en IAM, contribuye a mejorar la coherencia de las políticas de acceso, la trazabilidad y la capacidad de adaptación ante cambios organizativos o regulatorios (Crowther et al., 2024).

Asimismo, la revisión de la literatura evidencia que la madurez de IAM no puede evaluarse únicamente en función del número de herramientas desplegadas, sino de su grado de integración y automatización. Ganesh, Rajaram y Sobia (2024) coinciden en que muchas organizaciones se sitúan en un nivel intermedio de madurez, caracterizado por una inversión tecnológica significativa pero un aprovechamiento limitado de sus capacidades. Esta brecha entre potencial y uso real constituye uno de los principales retos actuales en la gestión de identidades.

En conjunto, los estudios revisados permiten concluir que la evolución de IAM responde a una transición desde enfoques reactivos y fragmentados hacia modelos estratégicos, gobernados y orientados a la resiliencia. Esta evolución sienta las bases conceptuales para su integración con el paradigma Zero Trust, que amplía y

redefine el papel de la identidad en la arquitectura de seguridad contemporánea.

3. Metodología

El presente trabajo adopta una metodología cualitativa de carácter descriptivo y analítico, orientada a examinar la evolución conceptual y estratégica de la gestión de identidades y accesos (IAM) en el marco del paradigma Zero Trust. El objetivo metodológico no es la validación empírica mediante experimentación o análisis estadístico, sino la identificación, interpretación y síntesis de patrones, enfoques y buenas prácticas que emergen de la literatura especializada y de los principales marcos de referencia en ciberseguridad.

El estudio se apoya en una revisión analítica de fuentes primarias y secundarias procedentes de revistas científicas, estándares técnicos, informes institucionales y publicaciones de referencia en el ámbito de la seguridad de la información. La selección de las fuentes se realizó atendiendo a criterios de relevancia, actualidad y reconocimiento académico o institucional, priorizando trabajos recientes sin excluir aportaciones fundamentales necesarias para la contextualización teórica. Este enfoque permite capturar tanto la evolución histórica de IAM como su estado actual y sus tendencias emergentes.

Desde el punto de vista del diseño metodológico, se opta por un enfoque integrador que permite contrastar distintos modelos y perspectivas sin limitar el análisis a un contexto organizativo específico. Esta decisión resulta especialmente adecuada en un ámbito caracterizado por una rápida evolución tecnológica y una fuerte dependencia del contexto, donde los estudios de caso aislados o las generalizaciones cuantitativas pueden ofrecer una visión parcial del fenómeno. A través de un proceso iterativo de comparación conceptual, se identificaron convergencias y divergencias entre los enfoques revisados, lo que facilitó la estructuración del análisis en torno a ejes comunes como la gobernanza de la identidad, la automatización del ciclo de vida, la autenticación adaptativa y la resiliencia organizativa.

Dado el carácter conceptual del estudio, no se emplean muestras estadísticas ni técnicas cuantitativas. No obstante, el análisis incorpora evidencias documentadas de incidentes de seguridad, modelos de madurez y casos de aplicación sectoriales recogidos en la literatura, utilizados con fines ilustrativos y comparativos. Este planteamiento permite contextualizar los resultados y reforzar su validez interpretativa sin pretender establecer generalizaciones universales.

Entre las limitaciones del estudio se encuentra la ausencia de validación empírica directa mediante estudios de caso longitudinales o análisis experimentales, lo que abre la puerta a futuras investigaciones orientadas a contrastar los marcos conceptuales analizados en contextos organizativos específicos. A pesar de esta limitación, la metodología adoptada resulta adecuada para cumplir el objetivo del trabajo: ofrecer una visión estructurada, crítica y actualizada sobre la evolución de IAM en la era Zero Trust y su contribución a la resiliencia digital desde una perspectiva estratégica y organizativa.

4. Resultados

Los resultados obtenidos a partir del análisis de la literatura y de los marcos conceptuales revisados permiten identificar una serie de patrones recurrentes en la evolución de la gestión de identidades y accesos (IAM) y su integración con el modelo Zero Trust. Dado el carácter cualitativo del estudio, estos resultados se presentan como observaciones analíticas sistematizadas y no como mediciones cuantitativas, permitiendo extraer conclusiones sobre tendencias, niveles de madurez y efectos organizativos asociados a la adopción de arquitecturas de seguridad basadas en la identidad.

El análisis confirma una transformación progresiva del rol de IAM dentro de las organizaciones. La evidencia revisada muestra que IAM ha dejado de concebirse como un mecanismo puramente técnico de control de accesos para consolidarse como un elemento estructural de la estrategia de ciberseguridad. Esta evolución del papel de la identidad puede sintetizarse en la Figura 1, que representa a IAM como núcleo integrador de los principales dominios de seguridad en arquitecturas contemporáneas.

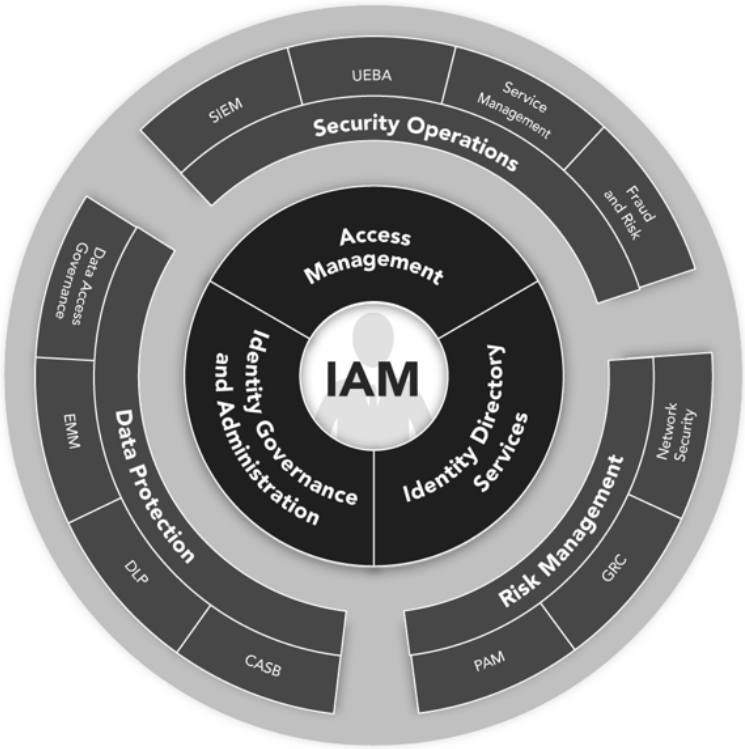

Figura 1. IAM como núcleo integrador de la arquitectura de seguridad en entornos Zero Trust. Fuente: Elaboración propia a partir de la literatura revisada.

En los modelos más avanzados, la identidad se configura como el nuevo perímetro de seguridad, posibilitando la aplicación efectiva de principios como la autenticación continua, el privilegio mínimo y la verificación contextual. Este cambio de enfoque resulta especialmente relevante en entornos distribuidos y dinámicos, donde los modelos perimetrales tradicionales han demostrado ser insuficientes (Rose et al., 2019; Hasan, 2024).

De forma estrechamente vinculada a esta evolución, los resultados ponen de manifiesto el papel crítico de la gobernanza de la identidad como factor de éxito o fracaso en los programas de IAM. La literatura analizada coincide en señalar que los enfoques fragmentados, en los que la gestión de identidades se distribuye de manera difusa entre distintas áreas organizativas, generan ineficiencias operativas, inconsistencias en las políticas de acceso y un incremento del riesgo de exposición (Bashir, 2024). En contraste, las organizaciones que adoptan una gobernanza transversal y estructuras específicas, como los Centros de Excelencia en IAM, logran una mayor coherencia en la definición y aplicación de políticas, una reducción de incidencias y una alineación más efectiva entre los objetivos de seguridad y las necesidades del negocio (Crowther et al., 2024).

Los resultados evidencian asimismo una relación directa entre el nivel de madurez de IAM y la capacidad de las organizaciones para reducir el impacto de los incidentes de seguridad. Los casos documentados en la literatura muestran que una gestión deficiente de credenciales y accesos privilegiados continúa siendo uno de los principales vectores de ataque, con consecuencias significativas tanto en términos operativos como reputacionales (Verizon, 2023; Motiwala, Wolcott y Anderson, 2022). En cambio, la aplicación de controles alineados con el modelo Zero Trust, apoyados en una gestión robusta de identidades, contribuye a limitar el movimiento lateral de los atacantes y a mejorar la capacidad de contención ante escenarios de compromiso inicial.

Castro-Ortiz, J. C., y Martínez-López, F. J. (2026). De la autenticación a la resiliencia en la estrategia institucional: evolución de IAM en la era Zero Trust. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 11(1), 47-57. https://doi.org/10.54988/cisde.2026.1.1804

Otro resultado relevante es el impacto positivo de la automatización del ciclo de vida de identidades en la eficiencia operativa y la seguridad. La provisión y revocación automática de accesos reduce los tiempos de alta y baja de usuarios, minimiza la existencia de cuentas huérfanas y disminuye la dependencia de procesos manuales propensos a errores. La literatura revisada destaca que la automatización no solo mejora la experiencia digital de empleados y colaboradores, sino que constituye un requisito fundamental para la escalabilidad de las arquitecturas Zero Trust en entornos complejos y distribuidos (Ganesh, Rajaram, y Sobia, 2024).

El análisis también revela diferencias significativas en la adopción y efectividad de IAM y Zero Trust en función del nivel de madurez organizativa. En organizaciones con estructuras de gobierno consolidadas y una estrategia clara de seguridad, IAM se implementa como un sistema integrado que abarca tanto identidades humanas como no humanas, con políticas coherentes y automatizadas. En estos contextos, los principios de Zero Trust se aplican de forma progresiva y alineada con los procesos de negocio, lo que facilita su adopción y reduce la fricción operativa (Rose et al., 2019). Por el contrario, en organizaciones con menor madurez, la adopción de IAM suele estar orientada a la resolución de problemas puntuales, con implementaciones reactivas de controles como la autenticación multifactor o el acceso condicional. Esta aproximación limita los beneficios del modelo Zero Trust y puede generar una falsa sensación de seguridad al no abordar aspectos estructurales como la gobernanza, la automatización del ciclo de vida o la gestión de accesos privilegiados (Hasan, 2024).

Finalmente, los resultados ponen de relieve la importancia de la integración de IAM con otros componentes del ecosistema de seguridad. Cuando los eventos de identidad se correlacionan con señales procedentes de sistemas de monitorización, detección y respuesta, las decisiones de acceso pueden ajustarse en tiempo real, reforzando la protección sin sacrificar la experiencia del usuario. Este enfoque integrado consolida a IAM como un elemento central de la arquitectura de seguridad y refuerza el carácter dinámico y contextual del modelo Zero Trust, contribuyendo de forma directa a la resiliencia organizativa (Verizon, 2023).

5. Conclusiones

Los resultados obtenidos permiten situar la gestión de identidades y accesos (IAM) como un elemento central en la redefinición de las estrategias de ciberseguridad contemporáneas. Más allá de confirmar tendencias ya apuntadas en la literatura, el análisis pone de relieve que la adopción efectiva de IAM y del modelo Zero Trust no depende únicamente de la disponibilidad tecnológica, sino de la capacidad de las organizaciones para integrar la identidad como un activo estratégico dentro de sus modelos de gobierno y de toma de decisiones. Esta integración exige superar enfoques instrumentales y comprender la identidad como un componente estructural que conecta seguridad, operación y negocio en entornos cada vez más distribuidos y dinámicos.

Desde una perspectiva aplicada, uno de los principales desafíos identificados reside en la brecha existente entre la conceptualización de IAM como pilar de seguridad y su implementación real en organizaciones complejas. Aunque los principios de Zero Trust gozan de un amplio consenso teórico, su materialización requiere un grado de madurez organizativa que muchas entidades aún no han alcanzado. El análisis sugiere que los programas de IAM resultan más eficaces cuando se abordan como iniciativas de transformación organizativa, incorporando de forma explícita aspectos de gobernanza, gestión del cambio y alineación con los procesos de negocio, y no como proyectos técnicos aislados o respuestas reactivas a exigencias regulatorias.

Esta lógica se extiende al diseño de las arquitecturas de seguridad. Las organizaciones que continúan basando sus controles en supuestos de confianza implícita encuentran crecientes dificultades para adaptarse a entornos multicloud, altamente interconectados y sujetos a cambios constantes. En contraste, aquellas que sitúan la identidad en el centro de la arquitectura logran una aplicación más coherente de las políticas de acceso, una reducción de la superficie de ataque y una mejora en la capacidad de respuesta ante incidentes. Esta transición no implica únicamente la adopción de nuevas tecnologías, sino una revisión profunda de procesos, responsabilidades y mecanismos de control asociados a la gestión de accesos.

El análisis también permite observar cómo la relación entre seguridad y experiencia de usuario se ve directamente afectada por la forma en que se implementan los controles de identidad. Tradicionalmente percibida como un freno a la productividad, la ciberseguridad puede convertirse en un facilitador cuando los accesos se diseñan de forma contextual y adaptativa. La combinación de autenticación continua, automatización del ciclo de vida y análisis de comportamiento reduce la fricción sin comprometer la seguridad, favoreciendo una adopción más natural de los principios Zero Trust por parte de usuarios y áreas de negocio.

En términos de implantación, los hallazgos sugieren que la transición hacia una seguridad basada en identidad requiere un enfoque incremental y orientado a capacidades. Intentar desplegar Zero Trust como un proyecto monolítico suele derivar en fricción operativa, resistencia cultural y resultados inconsistentes. Los marcos de referencia analizados coinciden en que los avances más sostenidos se producen cuando se priorizan casos de uso concretos, alineados con activos críticos y con procesos reales de la organización, y se construyen de forma iterativa sobre una base de identidad robusta (Rose et al., 2019; NIST, 2020). En este contexto, IAM actúa como capa habilitadora que permite definir políticas de acceso coherentes, introducir verificación contextual y limitar el movimiento lateral sin depender de la ubicación de los usuarios o de la topología de red.

Desde esta perspectiva, un roadmap pragmático puede estructurarse en fases sucesivas que respondan a objetivos verificables. Una fase inicial suele centrarse en la higiene de identidad y el control básico, incluyendo el inventario de identidades, la revisión de roles y privilegios, la estandarización de mecanismos de autenticación y el fortalecimiento de los procesos de alta y baja. Fases posteriores permiten avanzar hacia políticas más dinámicas mediante acceso condicional, segmentación lógica, controles específicos para cuentas privilegiadas y mecanismos de verificación continua, hasta consolidar capacidades de automatización y respuesta que integren eventos de identidad con la monitorización y la detección. Este enfoque por etapas es coherente con la premisa de que la confianza debe ganarse de forma continua y adaptarse al riesgo real y al contexto de uso (Rose et al., 2019; NIST, 2020).

El análisis extrae asimismo implicaciones relevantes en materia de métricas y gobierno. En muchos proyectos de IAM, el éxito se mide todavía en términos de entregables tecnológicos, cuando la madurez real se refleja mejor en indicadores operativos y de riesgo. Métricas como el tiempo medio de provisión y desprovisión de accesos, la reducción de cuentas huérfanas, la disminución de incidencias asociadas a credenciales o la evolución del volumen de privilegios permanentes frente a permisos temporales permiten evaluar si IAM está reduciendo exposición y mejorando eficiencia, o si permanece como una capa burocrática con impacto limitado. La incorporación sistemática de este tipo de indicadores contribuye a un gobierno de la identidad sostenible y orientado a la mejora continua (Hasan, 2024).

Desde la óptica de la resiliencia, la discusión refuerza que la identidad se ha convertido en un vector crítico de ataque y, por tanto, en un punto prioritario de control. Los informes agregados sobre brechas continúan mostrando un peso significativo del compromiso de credenciales y de los fallos en la gestión de accesos como detonantes o aceleradores de incidentes (Verizon, 2023). En este marco, la aportación del modelo Zero Trust no se limita a endurecer el acceso, sino a reducir el impacto de un compromiso inicial mediante la restricción de privilegios, la limitación de superficies expuestas y la verificación continua, lo que se traduce en una mayor capacidad de contención y una reducción del radio de daño incluso cuando el incidente no puede evitarse por completo (Verizon, 2023; NIST, 2020).

La automatización emerge igualmente como un elemento clave para sostener este enfoque en el tiempo. A medida que las organizaciones crecen y operan en entornos distribuidos, la gestión manual del ciclo de vida de identidades se convierte en un factor de riesgo en sí mismo, generando retrasos, inconsistencias y acumulación de excepciones. La automatización permite reducir errores, mejorar la trazabilidad y escalar políticas de acceso contextualizadas, especialmente cuando se combina con mecanismos de detección avanzada y correlación de eventos (Ganesh, Rajaram y Sobia, 2024). Esta lógica resulta igualmente aplicable a identidades no humanas y accesos de servicios, cuyo crecimiento acelerado exige controles coherentes para evitar configuraciones frágiles y privilegios excesivos.

Castro-Ortiz, J. C., y Martínez-López, F. J. (2026). De la autenticación a la resiliencia en la estrategia institucional: evolución de IAM en la era Zero Trust. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 11(1), 47-57. https://doi.org/10.54988/cisde.2026.1.1804

Finalmente, el análisis sugiere una implicación organizativa de fondo: IAM y Zero Trust obligan a redefinir la responsabilidad sobre la identidad. Los enfoques fragmentados tienden a generar soluciones parciales y controles inconsistentes, mientras que los modelos de gobierno transversales favorecen la coherencia y la mejora continua (Bashir, 2024; Crowther et al., 2024). Este gobierno no debe entenderse como una estructura formalista, sino como un mecanismo de decisión que prioriza riesgos, simplifica políticas y alinea seguridad con operación. En este sentido, la adopción de Zero Trust apoyada en IAM no elimina la complejidad, sino que la redistribuye, exigiendo capacidades técnicas, disciplina de gobierno y una gestión del cambio que institucionalice la revisión continua, el control de privilegios y la mejora operativa de la identidad como proceso permanente.

6. Discusión y futuras líneas de investigación

El análisis desarrollado a lo largo del presente trabajo permite abrir un espacio de discusión que trasciende la descripción de tendencias y resultados observados, y que invita a reflexionar sobre los límites actuales del conocimiento en torno a la gestión de identidades y accesos (IAM) y su integración con el paradigma Zero Trust. Si bien la literatura revisada coincide en señalar el papel central de la identidad como nuevo perímetro de seguridad, persisten áreas de incertidumbre relacionadas con la efectividad real de estos modelos en contextos organizativos diversos y en escenarios de alta complejidad operativa.

Desde una perspectiva teórica, una de las principales cuestiones abiertas reside en la necesidad de avanzar hacia modelos de madurez más homogéneos y comparables que permitan evaluar de forma consistente el grado de adopción de IAM y Zero Trust entre organizaciones y sectores. La heterogeneidad de enfoques, herramientas y marcos conceptuales dificulta la comparación de resultados y la identificación de buenas prácticas transferibles. Futuras investigaciones podrían profundizar en la definición de indicadores estandarizados que permitan medir no solo la implantación tecnológica, sino también el impacto organizativo, cultural y operativo de la gestión de identidades como eje de la resiliencia digital.

Asimismo, el crecimiento exponencial de identidades no humanas —asociadas a servicios, aplicaciones, contenedores y dispositivos— plantea nuevos desafíos que aún no han sido suficientemente abordados de forma sistemática en la literatura. En este contexto, la gestión del ciclo de vida completo de la identidad digital constituye un elemento clave tanto para abordar los retos actuales como para orientar futuras líneas de investigación en sistemas IAM (Figura 2).

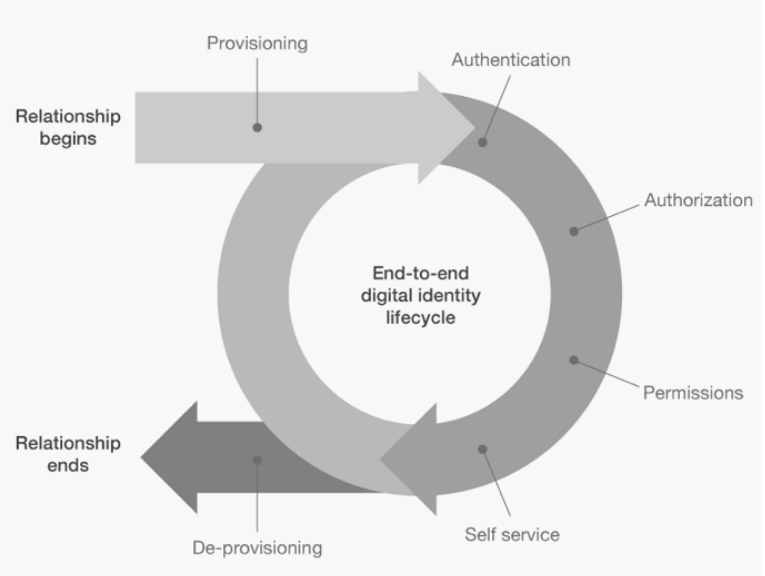

Figura 2. Ciclo de vida end-to-end de la identidad digital en sistemas de gestión de identidades y accesos (IAM). Fuente: Elaboración propia.

Castro-Ortiz, J. C., y Martínez-López, F. J. (2026). De la autenticación a la resiliencia en la estrategia institucional: evolución de IAM en la era Zero Trust. *Revista de Pensamiento Estratégico y Seguridad CISDE,* 11(1), 47-57. https://doi.org/10.54988/cisde.2026.1.1804

Aunque los principios de Zero Trust son conceptualmente aplicables a este tipo de identidades, su gestión a gran escala introduce complejidades adicionales en términos de gobernanza, automatización y control de privilegios. En este sentido, se identifican oportunidades de investigación orientadas a analizar cómo los modelos de IAM pueden adaptarse de forma efectiva a entornos altamente automatizados y distribuidos, sin comprometer la trazabilidad ni la seguridad.

Otra línea relevante de investigación futura se relaciona con el impacto organizativo y humano de los modelos de seguridad basados en identidad. Si bien los enfoques actuales enfatizan los beneficios en términos de reducción de riesgo y eficiencia operativa, existe un margen significativo para estudiar cómo la adopción de IAM y Zero Trust influye en la cultura de seguridad, en la percepción de los usuarios y en la relación entre las áreas técnicas y de negocio. Estudios empíricos que analicen estos factores podrían aportar evidencias valiosas para diseñar estrategias de implantación más sostenibles y alineadas con la realidad organizativa.

Finalmente, la rápida evolución del contexto tecnológico y regulatorio sugiere la necesidad de investigaciones longitudinales que evalúen la resiliencia de los modelos de identidad a lo largo del tiempo. La aparición de nuevas amenazas, tecnologías emergentes y exigencias normativas obliga a revisar de forma continua los supuestos sobre los que se construyen las arquitecturas de seguridad. En este marco, futuras investigaciones podrían explorar cómo la gestión de identidades y accesos puede evolucionar desde un enfoque reactivo hacia modelos predictivos y adaptativos, consolidándose no solo como un mecanismo de control, sino como un componente estratégico para la sostenibilidad y la confianza digital en ecosistemas complejos.

Financiación

Esta investigación no recibió financiación externa.

Cómo citar este artículo / How to cite this paper

Castro-Ortiz, J. C., y Martínez-López, F. J. (2026). De la autenticación a la resiliencia en la estrategia institucional: evolución de IAM en la era Zero Trust. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 11(1), 47-57. https://doi.org/10.54988/cisde.2026.1.1804

Referencias

Bashir, T. (2024). Zero Trust Architecture: Enhancing Cybersecurity in Enterprise Networks. Journal of Computer Science and Technology Studies. https://doi.org/10.32996/jcsts.2024.6.4.8.

Crowther, K., Alcaraz, C., & Pillitteri, V. (2024). Blending Shared Responsibility and Zero Trust to Secure the Industrial Internet of Things. IEEE Security & Privacy, 22, 96–102. https://doi.org/10.1109/MSEC.2024.3432208.

Domínguez, J. (2016). La ciberguerra como realidad posible contemplada desde la prospectiva. Revista de Pensamiento Estratégico y Seguridad CISDE, 1(1), 18-32.

European Banking Authority (EBA). (2023). Guidelines on ICT and security risk management under the EBA framework on internal governance (EBA/GL/2023/03). European Banking Authority. https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-ict-and-security-risk-management.

Ganesh, S., Rajaram, G., & Sobia, M. (2024). Next-Generation Threat Detection and Mitigation in 6G Wireless Networks Using IAM, ZTNA and Advanced Security Mechanisms. Journal of Electrical Systems. https://doi.org/10.52783/jes.2545.

García-Río, E., Baena-Luna, P., Palos-Sánchez, P. R., & Aguayo-Camacho, M. (2022). Amenazas de los gobiernos electrónicos: el desafío de la e-seguridad. Revista de Pensamiento Estratégico y Seguridad CISDE, 7(2), 87-107.

Hasan, M. (2024). Enhancing Enterprise Security with Zero Trust Architecture. arXiv preprint arXiv:2410.18291.

Hong, S., Xu, L., Huang, J., Li, H., Hu, H., & Gu, G. (2023). SysFlow: Toward a Programmable Zero Trust Framework for System Security. IEEE Transactions on Information Forensics and Security, 18, 2794–2809. https://doi.org/10.1109/TIFS.2023.3264152.

Infante-Moro, A., Infante-Moro, J. C., & Gallardo-Pérez, J. (2022). Factores claves para concienciar la ciberseguridad en los empleados. Revista de Pensamiento Estratégico y Seguridad CISDE, 7(1), 69-79.

Lin, J., Jiang, Q., Zhang, W., Lin, Z., & Du, X. (2024). Quantum-Enhanced Zero Trust Security: Evolution, Implementation, and Application. 2024 International Conference on Quantum Communications, Networking, and Computing (QCNC), 211–215. https://doi.org/10.1109/QCNC62729.2024.00040.

Luján-Salamanca, A., Infante-Moro, A., Infante-Moro, J. C., & Gallardo-Pérez, G. (2024). La ciberseguridad en las empresas: estudio bibliométrico. Revista de Pensamiento Estratégico y Seguridad CISDE, 9(2), 61-73. https://doi.org/10.54988/cisde.2024.2.1551.
Motiwala, A., Wolcott, C., & Anderson, D. (2022). Identity and Access Management in Healthcare: Risk Mitigation and Best Practices. Healthcare Information Management Journal, 51(3), 145–158. https://doi.org/10.1177/18333583221102134.
National Institute of Standards and Technology (NIST). (2020). Zero Trust Architecture (SP 800-207). https://doi.org/10.6028/NIST.SP.800-207.
Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2019). Zero Trust Architecture. NIST Special Publication 800-207. https://doi.org/10.6028/NIST.SP.800-207.
Verizon. (2023). Data Breach Investigations Report (DBIR). Verizon Communications. https://www.verizon.com/business/resources/reports/dbir/.
World Wide Web Consortium (W3C). (2023). Verifiable Credentials Data Model 2.0. W3C Recommendation. https://www.w3.org/TR/vc-data-model-2.0/.