



White Paper:

La Identidad Digital
en la Agenda del CIO/CTO

TEC360 CLOUD
EN COLABORACIÓN CON
JUAN IGNACIO TORRES



Índice

1. Introducción: La verdadera agenda de la transformación digital
2. El desafío tecnológico actual
3. Reencuadrando la identidad digital
4. Viabilidad tecnológica y evolución natural
5. El Marco de Desempeño en Identidad Digital de TEC360
6. De la teoría a la acción
7. El *Blueprint* Tecnológico de la Identidad Digital

Conclusiones y llamado a la acción



1. INTRODUCCIÓN: LA VERDADERA AGENDA DE LA TRANSFORMACIÓN DIGITAL

Uno de los temas más relevantes en la agenda de transformación digital de cualquier organización es lograr que su ecosistema digital funcione como un todo integrado: clientes, empleados, proveedores, socios y hasta aplicaciones deben interactuar de manera fluida, confiable y segura. No se trata solo de sumar más tecnología, sino de hacer que las piezas trabajen juntas sin fricciones.

Ese propósito, sin embargo, tropieza en la práctica. La deuda técnica en mecanismos de acceso heredados complica la integración; la escasez de talento especializado limita la capacidad de operar lo complejo; y el ritmo de la innovación supera la velocidad con la que las áreas de TI pueden entregar resultados visibles. No sorprende que, según Gartner, menos de la mitad de las iniciativas digitales logran cumplir sus objetivos, salvo cuando el CIO asume un involucramiento pleno, caso en el que la tasa de éxito sube al 71%.

En este contexto, la responsabilidad del CIO/CTO es clara: asegurar que esa interacción ocurra de manera segura, ágil y efectiva en costos. Y hacerlo con herramientas que eliminen deuda técnica, simplifiquen integraciones y entreguen resultados medibles para el negocio.

Si bien los CIO y CTO reconocen que la identidad digital puede aportar agilidad operativa y seguridad reforzada, con frecuencia esta iniciativa queda en segundo plano frente a otras prioridades de inversión. Proyectos como inteligencia artificial, analítica avanzada u omnicanalidad suelen recibir mayor atención inicial, pero a menudo encuentran límites en su ejecución por la ausencia de una columna vertebral sólida de identidad y acceso.

Un estudio de Forrester Consulting mostró que las organizaciones que implementaron gobernanza de identidad y acceso lograron un ROI del 211% en tres años, con recuperación en menos de seis meses, además de ahorros multimillonarios en auditorías y licenciamien-



to. Estos resultados demuestran cómo una arquitectura de identidad puede transformar la forma en que las organizaciones interactúan con su propio ecosistema.

En definitiva, la identidad digital ya no es solo un control técnico: es la infraestructura estratégica que permite a las organizaciones unirse, interactuar y crecer en un entorno donde la agilidad y la confianza definen quién gana y quién se queda atrás.

2. EL DESAFÍO TECNOLÓGICO ACTUAL

Aunque el valor de la identidad digital es ampliamente reconocido, en la práctica muchas organizaciones siguen enfrentando obstáculos que frenan su adopción como pilar estratégico. Estos desafíos no solo afectan la eficiencia operativa, sino que se convierten en barreras directas para la innovación y la resiliencia del negocio.



Deuda técnica heredada.

Gran parte de los entornos corporativos aún depende de aplicaciones legacy con cuentas locales, contraseñas heredadas y roles rígidos que no escalan. Los modelos de integración punto a punto, acumulados durante años, incrementan la complejidad y exponen vulnerabilidades difíciles de gestionar. Según Gartner, más del 60% de los CIO reconoce que la deuda técnica consume una parte significativa de sus presupuestos de TI, reduciendo su capacidad para invertir en proyectos de transformación.



Fragmentación del ecosistema digital.

La mayoría de las organizaciones opera en entornos híbridos: infraestructura on-premises combinada con múltiples nubes, SaaS y movilidad. Esta fragmentación multiplica las identidades y genera silos, duplicidades y puntos ciegos en la gestión de acceso. IDC estima que,



para 2025, el 80 % de las empresas trabajará en al menos tres entornos cloud, lo que amplía los retos de control y gobernanza en identidad y acceso.



Costos operativos ocultos.

Los costos derivados de la gestión manual de accesos siguen siendo altos: auditorías reactivas, certificaciones manuales y grandes volúmenes de tickets de soporte relacionados con contraseñas. Forrester calcula que los incidentes asociados a contraseñas pueden representar hasta el 40 % del presupuesto de help desk en organizaciones grandes, drenando recursos que podrían destinarse a innovación.



Fricción para el usuario y el negocio.

La lentitud en los procesos de alta y baja de usuarios afecta la productividad interna, mientras que experiencias digitales inconsistentes entre canales físicos e híbridos generan frustración y abandono de clientes. PwC reporta que un 32 % de los consumidores abandona una marca tras una sola mala experiencia de acceso o seguridad, lo que demuestra el impacto directo en crecimiento y fidelización.



Brechas de cumplimiento y seguridad.

Los modelos tradicionales de cumplimiento priorizan el “checklist” más que la efectividad real. La ausencia de trazabilidad en tiempo real dificulta detectar anomalías y responder ante incidentes, mientras que los privilegios mal gestionados amplifican riesgos de fraude interno y externo. El Foro Económico Mundial ha señalado la falta de controles de identidad confiables como uno de los factores críticos de riesgo para la economía digital global.



El costo de no actuar.

Cada año que se posterga la modernización de identidad se acumula más deuda técnica, aumentan los costos de operación y soporte, y disminuye la velocidad de innovación. Más aún, proyectos estratégicos como inteligencia artificial, omnicanalidad o Zero Trust seguirán quedándose a medias si no se apoyan en una base sólida de identidad digital confiable y gobernada.

3. REENCUADRANDO LA IDENTIDAD DIGITAL

La identidad digital ha dejado de ser un mecanismo de control aislado. En el nuevo contexto de negocios y tecnología, se convierte en la infraestructura estratégica que sostiene la innovación, la seguridad y la agilidad organizacional. No se trata únicamente de cumplir requisitos de auditoría o de habilitar inicios de sesión, sino de construir una base confiable sobre la cual la organización puede crecer e interactuar sin fricciones con todo su ecosistema digital.

Los enfoques tradicionales, centrados en cuentas locales, contraseñas heredadas y roles rígidos, han llegado a su límite. La alternativa es un modelo de identidad digital reencuadrado en tres principios transformadores:



Accountless.

En lugar de depender de cuentas dispersas en múltiples sistemas, la identidad se basa en identidades verificadas y trazables, asociadas a personas, dispositivos o servicios reales. Esto permite consolidar la gestión, eliminar silos y reforzar la trazabilidad. Desde la perspectiva de negocio, significa confianza ampliada y menos complejidad operativa.



Passwordless.

Las contraseñas estáticas han demostrado ser costosas, inseguras y generadoras de fricción. Sustituirlas por autenticación moderna —FIDO2, WebAuthn, MFA adaptativo, passkeys— elimina uno de los vectores de ataque más comunes y reduce drásticamente los costos de soporte. Para el negocio, representa experiencias más fluidas y seguras, incrementando productividad y fidelización.



Frictionless.

Las fronteras rígidas y los roles técnicos estáticos ya no responden a la realidad digital. El acceso debe ser dinámico y contextual, gobernado por políticas y señales de riesgo en tiempo real. Esto habilita la omnicanalidad, la movilidad y la colaboración con terceros sin añadir fricción innecesaria.

Plataforma de Gobierno Resiliente

Consolidar Identidades Eliminando Cuentas
Inventario de aplicaciones y cuentas, elimina repositorios locales de cuentas, integración mediante IA con Identidades Humanas, Físicas y Digitales (NHI)

Mejorar el Cumplimiento Automatizando la Certificación
Uso de IA para reducir la carga de certificación y se certifica basado en riesgos y cumplimiento



Eliminar la fricción y el riesgo erradicando las contraseñas

Sustituir la autenticación basada en contraseñas por passkeys y criptografía de clave pública

Dar accesos precisos y a la medida eliminando roles estáticos

Acceso basado en políticas y contexto asignado sobre demanda y por tiempo limitado



En conjunto, estos principios implican pasar de un modelo centrado en el “control defensivo” a una estrategia de confianza digital. El objetivo ya no es únicamente cumplir con checklists regulatorios, sino proporcionar visibilidad continua, habilitar automatización y asegurar cumplimiento verificable en tiempo real. En términos prácticos, la identidad digital deja de ser un freno para convertirse en un acelerador de innovación y nuevos modelos de negocio.

Este enfoque se apoya en tecnologías maduras y disponibles hoy: SSO, FIDO2, Zero Trust, Attack Surface Management (ASM), cloud y movilidad, todas probadas y ampliamente adoptadas en múltiples industrias. La diferencia está en cómo se articulan de manera coherente dentro de una arquitectura de identidad digital.

Además, los resultados pueden ser visibles de inmediato a través de quick wins: onboarding digital en horas en lugar de días, automatización de revisiones de acceso, reducción de cuentas huérfanas y mejoras sustanciales en la experiencia de usuario. Estos avances refuerzan el valor estratégico de la identidad digital y permiten sostener la transformación con métricas tangibles.

Así, la identidad digital reencuadrada no es un “proyecto más de TI”, sino el fundamento tecnológico y organizacional que conecta seguridad, agilidad y crecimiento empresarial.

4. VIABILIDAD TECNOLÓGICA Y EVOLUCIÓN NATURAL

La modernización de la identidad digital no es un salto al vacío, sino un compromiso directo con la eliminación de la deuda técnica acumulada en los mecanismos de acceso. Esta modernización se apoya en tecnologías maduras y probadas que ya forman parte del arsenal corporativo, pero que hoy operan de manera aislada o subutilizada.



Compromiso con la eliminación de deuda técnica.

La dependencia de cuentas locales, contraseñas heredadas y roles rígidos ha demostrado ser un obstáculo para la agilidad y la seguridad. Una estrategia de identidad digital moderna enfrenta estos retos de raíz, consolidando accesos y simplificando integraciones que históricamente han sido fuente de vulnerabilidades y costos ocultos.



Apalancamiento en tecnologías maduras.

Herramientas como SSO, FIDO2/WebAuthn, Zero Trust, Attack Surface Management (ASM), movilidad y cloud híbrida ya se utilizan ampliamente en el mercado. La clave está en articularlas dentro de un blueprint coherente de identidad digital, que permita gobernarlas como un sistema unificado en lugar de como piezas desconectadas.



Evolución progresiva.

Modernizar la identidad no significa reemplazarlo todo de inmediato. El camino es evolutivo: integrar lo existente, habilitar la convivencia con sistemas legacy y reducir deuda técnica de forma progresiva. Esta aproximación asegura continuidad operativa y genera confianza en la organización, al mismo tiempo que se avanza hacia un modelo más ágil y seguro.



Resultados rápidos y medibles.

Una de las principales ventajas de este enfoque es que los resultados pueden observarse en el corto plazo:

- Reducción inmediata de tickets de contraseñas, liberando recursos de soporte.
- Onboarding digital acelerado, que permite a nuevos empleados, clientes o socios operar en horas en lugar de días.
- Automatización de certificaciones de acceso, reduciendo esfuerzo manual y riesgo de error.



- Auditorías más rápidas y trazables, con datos centralizados y verificables.



Confianza tecnológica y estratégica.

Modernizar la identidad digital significa alinear lo probado con lo necesario. No se trata de adoptar tecnologías emergentes en fase experimental, sino de aplicar de manera integrada lo que ya ha demostrado su valor. Para los CIO y CTO, la verdadera decisión no es si avanzar hacia este modelo, sino cómo empezar de manera inteligente y escalable.

5. EL MARCO DE DESEMPEÑO EN IDENTIDAD DIGITAL DE TEC360

Adoptar un nuevo enfoque de identidad no solo requiere visión estratégica, también exige una forma clara de medir el progreso y demostrar resultados tangibles. El Marco de Desempeño en Identidad Digital de TEC360 cumple precisamente con ese propósito: ofrece una herramienta práctica para alinear la evolución tecnológica con los objetivos del negocio y, al mismo tiempo, monitorear la reducción de la deuda técnica que hoy afecta a los mecanismos de acceso.

Este marco se inspira en metodologías reconocidas —como el Business Agility Institute, Outcome-Oriented Enterprise Architecture y el Forrester Value Framework— y se estructura en seis dimensiones clave de desempeño:



1. Arquitectura y Evolución.

Evalúa la capacidad de la organización para avanzar desde entornos rígidos y legacy hacia arquitecturas modernas, abiertas y escalables. Permite medir la reducción progresiva de deuda técnica en aplicaciones y accesos.



2. Seguridad y Gestión de Riesgos.

Mide cómo las capacidades de identidad contribuyen a reducir riesgos de fraude, accesos indebidos y vulnerabilidades, ofreciendo al negocio un entorno más confiable y resiliente.



3. Cumplimiento y Confianza.

Pasa del cumplimiento reactivo a la confianza continua, con controles automatizados y trazabilidad total, que reducen costos y eliminan incertidumbre en auditorías.



4. Eficiencia Operativa.

Analiza la capacidad de la organización para automatizar procesos de acceso, reducir tiempos de integración y simplificar la administración, lo que libera recursos y elimina redundancias.



5. Experiencia del Usuario.

Evalúa la facilidad, coherencia y fluidez de las interacciones de empleados, clientes y socios. Menos fricción en el acceso significa más productividad, satisfacción y fidelidad.



6. Resultados de Negocio.

Conecta directamente la evolución de la identidad digital con indicadores estratégicos: velocidad de lanzamiento de nuevos servicios, reducción de costos, mejora en la confianza del cliente y capacidad de crecimiento.

En conjunto, estas dimensiones permiten a las organizaciones medir de manera integral cómo la modernización de la identidad no solo elimina deuda técnica, sino que además genera confianza, agilidad y valor de negocio sostenido.



Valor de Negocio

- Creación de valor
- Logro de objetivos
- Escalabilidad



Eficiencia operativa

- Reducción de carga operativa
- Disminución de fricción operativa
- Mejora de procesos



Experiencia del usuario

- Reducción de fricción de acceso
- Percepción y confianza del usuario
- Normalización de tecnologías

TEC360 IAM Value & Evolution Framework



Cobertura y Alineación

- Reducción de riesgos
- Agilidad y adaptabilidad



Confiabilidad y cumplimiento

- Cumplimiento
- Seguridad y control
- Trazabilidad y auditoría



Adaptabilidad y evolución

- Transformación estratégica
- Agilidad y adaptabilidad

6. DE LA TEORÍA A LA ACCIÓN

El marco de desempeño de TEC360 ofrece un lenguaje estratégico, pero su verdadero valor se materializa cuando se traduce en resultados concretos para la organización. El paso de la teoría a la práctica implica alinear las dimensiones de desempeño con outcomes de negocio claros, las capacidades necesarias para lograrlos y los OKR que permitirán medir el avance.



De dimensiones a business outcomes.

Cada dimensión del marco —arquitectura, seguridad, cumplimiento, eficiencia, experiencia y negocio— debe conectarse directamente con resultados tangibles: reducción de riesgo operacional, aceleración del lanzamiento de nuevos servicios, mejora en la experiencia digital del cliente o ahorro de costos en procesos de auditoría.



De outcomes a capacidades.

Una vez definidos los outcomes, la pregunta es: ¿qué capacidades de identidad necesitamos desarrollar o fortalecer para alcanzarlos? Esto abarca desde capacidades técnicas (passwordless, políticas contextuales, automatización de revisiones) hasta capacidades organizativas (definición de responsables de identidad, gobierno ágil, gestión del cambio).



De capacidades a OKR.

Los OKR se convierten en la herramienta práctica para gestionar el progreso. Permiten traducir aspiraciones estratégicas en objetivos claros, medibles y alineados con las prioridades del negocio, como “Reducir en 50 % los tiempos de onboarding digital” o “Eliminar el 80 % de cuentas huérfanas en seis meses”.



Considerar el ecosistema digital.

El punto de partida no es abstracto: cada organización tiene un ecosistema digital propio —aplicaciones legacy, entornos híbridos, nube pública, integraciones con socios— que define las condiciones de la transformación. Entender ese ecosistema es clave para establecer una hoja de ruta viable y realista.



Evaluar la madurez tecnológica y de conocimiento.

No todas las organizaciones cuentan con la misma base tecnológica ni con el mismo nivel de experiencia en el equipo. Evaluar la madurez en ambos frentes es esencial para diseñar un plan de transición que sea ambicioso pero alcanzable, que combine quick wins con proyectos de transformación estructural.

En conjunto, este enfoque permite a la organización aterrizar el marco conceptual en un plan de acción claro, que no solo mide la eliminación de deuda técnica, sino también el progreso hacia resultados de negocio visibles y sostenibles.



7. EL *BLUEPRINT* TECNOLÓGICO DE LA IDENTIDAD DIGITAL

Pasar de la visión a la ejecución requiere más que principios: exige un blueprint de identidad digital que guíe la evolución de la organización. Este blueprint no significa necesariamente adoptar nuevas tecnologías desde cero, sino aprovechar lo que ya existe, integrarlo de forma inteligente y complementarlo con capacidades modernas que aumentan el valor.



Un marco de integración, no de sustitución.

La **identidad digital** no se construye sobre la base de reemplazos radicales, sino sobre la capacidad de integrar directorios, aplicaciones legacy, servicios en la nube y plataformas modernas de autenticación en una experiencia única y coherente.



Elementos clave del blueprint:

- **Zero Trust.** La identidad como núcleo de un modelo donde cada acceso se verifica continuamente en función del contexto y del riesgo.
- **ASM (Attack Surface Management).** Visibilidad del perímetro real de identidades y accesos, para entender dónde existen vulnerabilidades y cómo reducir la superficie de ataque.
- **Cloud y movilidad.** Soporte para entornos híbridos y usuarios que acceden desde cualquier lugar, en cualquier dispositivo.
- **Autenticación moderna.** FIDO2, WebAuthn y MFA contextual, que habilitan el paso hacia passwordless y reducen tanto fricción como riesgo.
- **Automatización inteligente e IA.** Complemento para hacer revisiones de acceso más rápidas, detectar anomalías en tiempo real y responder con acciones automáticas.



No siempre es cuestión de tecnología nueva.

En muchos casos, el reto no es adquirir más herramientas, sino simplificar, integrar y sacar mayor provecho de lo que ya se tiene. La verdadera diferencia está en contar con un *blueprint* claro que guíe las inversiones, que elimine deuda técnica y que alinee cada decisión con los outcomes estratégicos del negocio.

En conclusión, el *blueprint* tecnológico de identidad digital actúa como la carta de navegación: asegura que los principios *accountless*, *passwordless* y *frictionless* no se queden en aspiraciones, sino que se conviertan en realidades medibles, apoyadas en Zero Trust, cloud, movilidad, autenticación moderna y automatización.

Conclusiones y llamado a la acción

La modernización de la identidad digital no es solo un proyecto tecnológico: es la oportunidad para que el área de Tecnología se consolide como un socio estratégico del negocio.

Adoptar este enfoque permite al área de TI:

- Liberarse de la deuda técnica que limita su capacidad de innovación.
- Demostrar métricas de valor claras, alineadas con los objetivos estratégicos de la organización.
- Reducir costos operativos y de auditoría, redirigiendo recursos hacia la transformación digital.
- Asegurar resiliencia y cumplimiento continuo, fortaleciendo la confianza del negocio en la gestión tecnológica.
- Ganar protagonismo en la agenda de crecimiento, al convertirse en el área que habilita nuevos modelos digitales y experiencias sin fricción.



El llamado a la acción es claro: no se trata de si la identidad digital debe modernizarse, sino de cómo hacerlo de forma planificada, medible y alineada al negocio. Con un marco de desempeño, un blueprint tecnológico y una visión clara, el área de Tecnología puede liderar la evolución de la organización desde una posición de solidez y credibilidad.

En definitiva, la identidad digital es la palanca que permite al área de TI pasar de ser percibida como un centro de costos a consolidarse como un motor de confianza, agilidad y valor para el negocio.



 @tec360cloud

 @tec360cloud

 info@tec360cloud.com

tec360cloud.com