https://doi.org/10.22201/dgtic.30618096e.2026.4.ESPECIAL.165

Núm. especial, abril 2026, págs. 10 - 27

# Implementación de un ecosistema de identidad digital autosoberana para credenciales académicas verificables en la Universidad Autónoma de Guerrero

*Implementation of a self-sovereign digital identity ecosystem for verifiable academic credentials at the Universidad Autónoma de Guerrero*

**Información del reporte:**



Para citar este reporte técnico:

Guzmán Nogueda, R., Hernández-Hernández, M., Huerta Patraca, G.A. y Álvarez Hilario, V. (2026). Implementación de un ecosistema de identidad digital autosoberana para credenciales académicas verificables en la Universidad Autónoma de Guerrero [número especial]. *Cuadernos Técnicos Universitarios de la DGTIC, 4,* páginas (10 - 27). https://doi.org/10.22201/dgtic.30618096e.2026.4.ESPECIAL.165

**Rosendo Guzmán Nogueda**
Universidad Autónoma de Guerrero
rgnogueda@uagro.mx
ORCID: 0009-0006-8216-3795

**Mario Hernández Hernández**
Universidad Autónoma de Guerrero
mhernandezh@uagro.mx
ORCID: 0000-0001-8330-4779

**Gustavo Antonio Huerta Patraca**
Universidad Veracruzana
gushuerta@uv.mx
ORCID: 0000-0001-5168-974X

**Valentín Álvarez Hilario**
Universidad Autónoma de Guerrero
13701@uagro.mx
ORCID: 0000-0002-5853-4246

## Resumen

La identidad autosoberana es un modelo de identidad digital en crecimiento cuyo objetivo es otorgar al usuario el control total y exclusivo sobre sus datos. Esto se logra a través del uso de credenciales verificables, las cuales actúan como la representación digital de documentos físicos y garantizan su autenticidad e integridad mediante algoritmos criptográficos. En el presente reporte técnico, se documentó el diseño e implementación de un ecosistema de identidad digital autosoberana

https://doi.org/10.22201/dgtic.30618096e.2026.4.ESPECIAL.165 **Núm. especial**, abril 2026, págs. 11 - 27

en la Universidad Autónoma de Guerrero para modernizar la emisión de documentos oficiales. La metodología se estructuró en cinco fases secuenciales: análisis de requerimientos institucionales, diseño arquitectónico fundamentado en estándares del World Wide Web Consortium, desarrollo de la capa de integración *middleware*, despliegue de la infraestructura de emisión y registro, así como validación mediante una prueba piloto controlada con egresados del programa Ponte Águila. El sistema integró el protocolo de identidad digital autosoberana QuarkID con el Sistema de Administración y Seguimiento Escolar existente, habilitando la emisión de títulos profesionales, certificados y credenciales estudiantiles como documentos verificables, almacenados en billeteras digitales bajo custodia exclusiva de cada estudiante. Los resultados obtenidos en la prueba piloto evidenciaron una reducción significativa de un 50% en tiempos de emisión, eliminación del riesgo de falsificación mediante firmas criptográficas y empoderamiento estudiantil al otorgarles control total sobre estos documentos. Entre las principales limitaciones identificadas, se encuentran la complejidad de integración con sistemas legados institucionales, la brecha de alfabetización digital en segmentos de la comunidad universitaria y la ausencia de un marco normativo nacional que otorgue reconocimiento legal explícito a las credenciales verificables. Los resultados obtenidos en el presente proyecto, implementado en la Universidad Autónoma de Guerrero, constituyen un modelo tecnológico robusto y replicable para instituciones de educación superior que buscan fortalecer la confianza documental mediante la transformación digital.

**Palabras clave:** *Blockchain*, credenciales verificables, cartera digital, identidad autosoberana, transformación digital.

## *Abstract*

*Self-sovereign identity is a growing digital identity model whose objective is to grant users full and exclusive control over their data. This is achieved through the use of verifiable credentials, which serve as the digital representation of physical documents and guarantee their authenticity and integrity through cryptographic algorithms. This technical report documents the design and implementation of a self-sovereign digital identity ecosystem at the Universidad Autónoma de Guerrero to modernize the issuance of official documents. The methodology was structured in five sequential phases: analysis of institutional requirements, architectural design based on World Wide Web Consortium standards, development of the middleware integration layer, deployment of the issuance and registry infrastructure, and validation through a controlled pilot test with graduates of the Ponte Águila program. The system integrated the QuarkID self-sovereign digital identity protocol with the existing Student Administration and Tracking System, enabling the issuance of professional degrees, certificates, and student credentials as verifiable documents stored in digital wallets under the exclusive custody of each student. The pilot test results demonstrated a significant reduction of 50% in issuance times, elimination of forgery risk through cryptographic signatures, and student empowerment by granting them full control over verifiable documents. Among the main limitations identified are the complexity of integration with legacy institutional systems, the digital literacy gap among segments of the university community, and the absence of a national regulatory framework that grants explicit legal recognition to verifiable credentials. The results obtained from the project implemented at the Universidad Autónoma de Guerrero, constitute a robust and replicable technological model for higher education institutions seeking to strengthen document trustworthiness through digital transformation.*

***Keywords:*** *Blockchain, digital transformation, digital wallet, self-sovereign identity, verifiable credentials.*

https://doi.org/10.22201/dgtic.30618096e.2026.4.ESPECIAL.165 **Núm. especial**, abril 2026, págs. 12 - 27

# 1. INTRODUCCIÓN

Obtener un título universitario ha sido históricamente un momento decisivo, el cual representa años de esfuerzo estudiantil y abre puertas a oportunidades profesionales y académicas. Sin embargo, a pesar de vivir en plena era digital, muchos de los procedimientos que sustentan tanto la emisión como la verificación de estos documentos vitales continúan operando con procesos por demás frustrantes del siglo pasado. En México, por ejemplo, emitir un título físico implica atravesar un proceso burocrático que puede extenderse por días o hasta meses completos, múltiples validaciones manuales, así como sellos y firmas que deben coordinarse entre diversas instancias; esto genera costos elevados y demoras molestas para los egresados.

Sin embargo, los problemas van más allá de la ineficiencia. El uso del papel crea vulnerabilidades serias. La falsificación de documentos académicos se ha convertido en una industria ilícita global que mueve más de 21 mil millones de dólares anuales (Eaton *et al.*, 2023). Dicha práctica no sólo socava la meritocracia, sino que erosiona la confianza pública en las instituciones educativas. Desde la perspectiva del egresado, el documento físico resulta frágil: puede perderse, sufrir daños o ser robado. Cuando un empleador extranjero necesita verificar un título mexicano, el proceso se vuelve tedioso, requiriendo comunicaciones transfronterizas y validaciones consulares que pueden tardar semanas. En este contexto, la transformación digital universitaria no puede limitarse a ofrecer clases en línea, aumentar el equipamiento de aulas o implementar inteligencia artificial de manera superficial. Debe abordar también la infraestructura administrativa con soluciones tecnológicas que fortalezcan la confianza desde sus cimientos.

Ante este panorama, emerge un nuevo paradigma en la gestión de identidad digital: la Identidad Digital Autosoberana, conocida como *Self-Sovereign Identity* (SSI). Este enfoque propone un cambio radical frente a modelos centralizados, donde una empresa o gobierno controla la identidad y modelos federados que dependen de proveedores como Google o Facebook. Con el modelo SSI, el individuo ocupa el centro del sistema, ejerciendo control total sobre su información personal y credenciales (Allen, 2016), como se muestra en la Figura 1. El paradigma se materializa mediante estándares abiertos del World Wide Web Consortium (W3C), específicamente a través de componentes como *Descentralized Ids* (DIDs) y Credenciales Verificables (VCs). Una VC funciona como el equivalente digital de una credencial física; por ejemplo, un título o licencia de conducir, pero con capacidades criptográficas avanzadas. Son documentos digitales resistentes a manipulaciones, verificables instantáneamente a escala global y permiten al portador compartir únicamente la información necesaria, respetando así el principio de privacidad por diseño.

https://doi.org/10.22201/dgtic.30618096e.2026.4.ESPECIAL.165 Núm. especial, abril 2026, págs. 13 - 27

**Figura 1**

*Comparativa entre paradigma tradicional y modelo de SSI de gestión de identidad digital*


La educación superior mexicana atraviesa actualmente un momento crítico en su proceso de transformación digital. La Universidad Autónoma de Guerrero (UAGro), institución pública estatal ubicada en el Estado de Guerrero, enfrenta desafíos particulares derivados tanto de procesos administrativos obsoletos como de crecientes demandas ciudadanas de transparencia. En respuesta, como parte de su estrategia institucional de modernización y combate a la corrupción, la UAGro emprendió la implementación de un sistema innovador para emitir documentos oficiales basado en tecnología de identidad autosoberana y credenciales verificables. Este proyecto trasciende la búsqueda de eficiencia operativa, pues representa un compromiso fundamental con la integridad académica y la confianza pública en la institución.

Migrar del modelo centralizado tradicional al modelo SSI ha implicado mucho más que un cambio tecnológico. Se realizó una reconceptualización de las relaciones de poder en la gestión de información académica. Tradicionalmente, la institución mantuvo poder absoluto sobre las credenciales, pudiendo modificarlas, revocarlas o negar acceso a ellas. SSI establece un equilibrio diferente: la institución conserva su autoridad como emisor legítimo, pero los individuos ganan soberanía sobre cómo usan y comparten sus credenciales (Tobin & Reed, 2017). Los componentes técnicos esenciales incluyen tres elementos: primero, los DIDs proporcionan identificadores únicos y persistentes sin depender de autoridades centrales; segundo, las VCs, las cuales son declaraciones criptográficamente seguras sobre un sujeto, emitidas por una autoridad confiable; tercero, las billeteras digitales permiten a los usuarios almacenar, gestionar y compartir selectivamente sus credenciales (W3C, 2022).

Los avances recientes en implementación de sistemas SSI en educación superior muestran resultados prometedores en contextos internacionales diversos. Investigaciones documentan que instituciones adoptantes de credenciales digitales verificables experimentaron mejoras sustanciales tanto en eficiencia administrativa como en reducción de fraude académico (Grech & Camilleri, 2017). El consorcio *Blockchain* para la Educación reportó casos exitosos en universidades europeas, donde los tiempos de verificación se redujeron extraordinariamente, pasando de semanas a apenas segundos (Jirgensons & Kapenieks, 2018). Estudios sobre interoperabilidad de credenciales digitales en ecosistemas educativos transnacionales evidenciaron además que los estándares W3C facilitan la movilidad estudiantil y profesional al eliminar barreras tradicionales de validación documental, aunque persisten desafíos importantes de gobernanza y adopción institucional (Grech *et al.*, 2021).

https://doi.org/10.22201/dgtic.30618096e.2026.4.ESPECIAL.165 Núm. especial, abril 2026, págs. 14 - 27

El objetivo central fue diseñar e implementar un ecosistema funcional de identidad digital autosoberana en la Universidad Autónoma de Guerrero, mediante la integración del protocolo QuarkID y una alianza estratégica con Extrimian, que habilita la emisión y verificación de credenciales académicas bajo estándares W3C Verifiable Credentials, con el propósito de fortalecer la seguridad documental, reducir los tiempos operativos de certificación y otorgar a los estudiantes control soberano sobre sus documentos académicos oficiales.

# 2. DESARROLLO TÉCNICO

## 2.1 METODOLOGÍA

El proyecto se desarrolló mediante una metodología estructurada en cinco fases que combinó análisis de requerimientos institucionales, diseño arquitectónico fundamentado en estándares W3C, integración con sistemas legados y validación operativa exhaustiva, como se muestra en la Figura 2. La primera fase consistió en analizar a profundidad el Sistema Administración y Seguimiento Escolar (SASE) que opera en la UAGro. Durante esta etapa, se identificaron flujos de datos, puntos críticos de integración y requisitos específicos de seguridad. Se llevaron a cabo sesiones de trabajo colaborativo con personal de la Dirección de Administración Escolar (DAE), Dirección General de Tecnologías de Información (DGTIC) y autoridades universitarias para mapear el proceso completo de emisión de documentos oficiales, desde que el estudiante realiza su solicitud hasta la entrega final del documento.

**Figura 2**

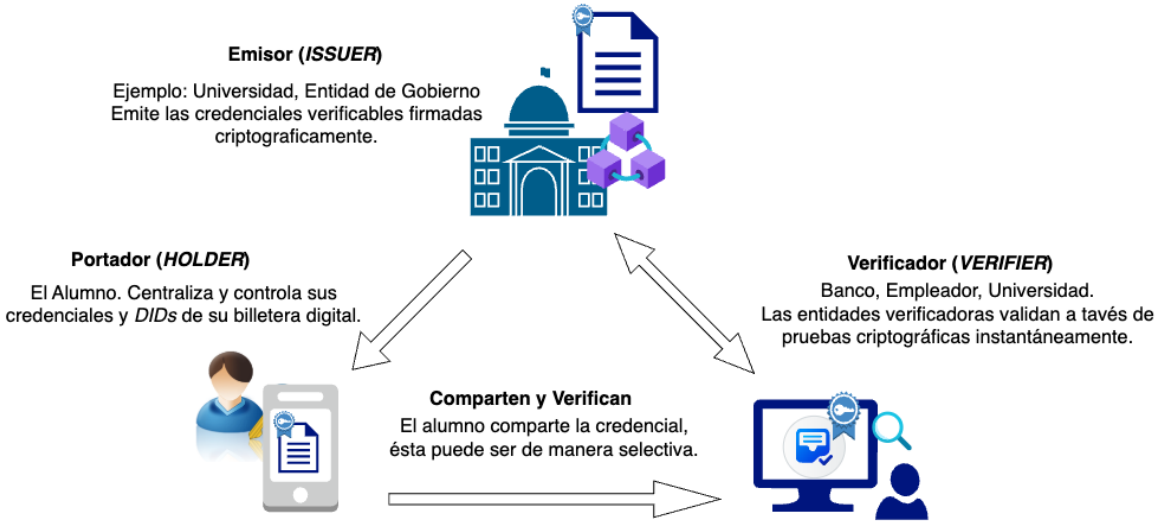
*Metodología de implementación del ecosistema SSI en cinco fases*


Durante la segunda fase, se diseñó la arquitectura del ecosistema SSI. Aquí, se adoptó el modelo del triángulo de confianza propuesto por el W3C (Sporny *et al.*, 2019), que establece tres roles fundamentales: el Emisor (UAGro), el Portador (estudiante o egresado) y el Verificador; la Figura 3 muestra un esquema del modelo mencionado.

https://doi.org/10.22201/dgtic.30618096e.2026.4.ESPECIAL.165 Núm. especial, abril 2026, págs. 15 - 27

**Figura 3**

*Triángulo de confianza del modelo SSI*




Para la implementación técnica, se seleccionó el protocolo QuarkID de identidad digital autosoberana, desarrollado por el gobierno de la ciudad de Buenos Aires, Argentina, una solución de código abierto que cumple con estándares W3C y ofrece componentes modulares para emisión, almacenamiento y verificación de credenciales. La decisión se basó en criterios múltiples: interoperabilidad, madurez tecnológica, disponibilidad de soporte técnico y alineación con objetivos institucionales de soberanía digital.

La tercera fase se enfocó en desarrollar la capa de integración *middleware*, que conectaría el SASE con la API de emisión utilizando el protocolo QuarkID. Se implementaron servicios REST, que transforman datos académicos desde el formato interno de la UAGro hacia el formato JSON-LD, los cuales requieren las credenciales verificables. Se establecieron esquemas específicos para tres tipos de documentos: título profesional, certificado de estudios de nivel medio superior y credencial de identidad estudiantil. Cada esquema incluyó atributos verificables como nombre del estudiante, programa académico, fecha de egreso, promedio obtenido y, cuando aplicó, número de cédula profesional.

En la cuarta fase, se implementó la infraestructura de emisión y verificación. Se configuraron nodos de la red universitaria para conectar y usar el protocolo QuarkID, que permitieron a la UAGro actuar como emisor autorizado mediante la creación de un DID institucional registrado en *blockchain*. Se desarrolló un portal web administrativo que facilita al personal de la DAE iniciar el proceso de emisión de credenciales una vez que validan los requisitos académicos del estudiante. Paralelamente, se seleccionó y personalizó la aplicación UAGro wallet, desarrollada con código abierto, para dispositivos iOS y Android. Esta billetera incorpora la identidad visual de la institución y se configuró específicamente para recibir credenciales del emisor UAGro.

https://doi.org/10.22201/dgtic.30618096e.2026.4.ESPECIAL.165 Núm. especial, abril 2026, págs. 16 - 27

La quinta fase validó el sistema mediante una prueba piloto controlada. Se seleccionó un grupo inicial de egresados del programa Ponte Águila, junto con estudiantes de nivel medio superior, para recibir sus credenciales en formato digital. Se diseñaron materiales de capacitación diversos: tutoriales en video, guías rápidas de instalación de la billetera y sesiones presenciales de apoyo. Se establecieron métricas de evaluación específicas para medir tiempo de emisión, tasa de adopción de la billetera, facilidad de uso reportada por usuarios y cantidad de verificaciones exitosas realizadas por terceros.

Durante todo el proyecto, se mantuvieron reuniones periódicas con el equipo técnico de Extrimian para resolver desafíos de implementación y ajustar configuraciones conforme surgían necesidades. Se documentaron exhaustivamente todos los procesos técnicos, esquemas de credenciales y protocolos de seguridad para garantizar tanto la replicabilidad como el mantenimiento futuro del sistema. La metodología empleada se fundamentó en principios consolidados de gestión de proyectos tecnológicos, mejores prácticas de integración de sistemas y estándares internacionales de identidad digital, asegurando que cada decisión técnica estuviera respaldada por análisis riguroso de requerimientos y evaluación sistemática de alternativas.

## 2.2 ARQUITECTURA DEL ECOSISTEMA IMPLEMENTADO

El ecosistema implementado se estructuró en cuatro capas tecnológicas principales que operan de manera coordinada. La primera es la capa de datos institucionales y está constituida por el SASE existente, que almacena la información académica verificada de estudiantes y egresados. Esta capa mantuvo su funcionamiento original sin requerir modificaciones estructurales, lo cual preservó la inversión tecnológica previa y minimizó riesgos operativos. El SASE continuó siendo la fuente de verdad para datos académicos, garantizando que únicamente información previamente validada mediante procesos institucionales formales pudiera incluirse en las credenciales.

La capa de integración *middleware* se desarrolló específicamente para este proyecto. Constituyó el puente técnico entre el SASE y la infraestructura de credenciales verificables. Esta capa implementa servicios web RESTful que extraen datos del SASE mediante consultas SQL autorizadas, transforman la información al formato JSON-LD, que requiere el estándar W3C de credenciales verificables, y la envían a la API de emisión de QuarkID. Se implementaron mecanismos robustos de autenticación mutua mediante certificados digitales y cifrado TLS para garantizar tanto la confidencialidad como la integridad de los datos en tránsito. Adicionalmente, se incorporaron validaciones de negocio que verifican que el estudiante cumpla todos los requisitos académicos y administrativos antes de autorizar la emisión de la credencial.

La capa de emisión y registro está conformada por la infraestructura de QuarkID operada por Extrimian. Aquí, se ejecuta el proceso criptográfico de generación de credenciales verificables. La UAGro, actuando como emisor autorizado, cuenta con un DID institucional registrado en una red *blockchain* pública que funciona como ancla de confianza. Cuando el *middleware* envía una solicitud de emisión, el servicio de QuarkID genera la credencial en formato JSON-LD, la firma digitalmente utilizando la clave privada asociada al DID de la UAGro, y registra un *hash* criptográfico de la credencial en *blockchain*. Este registro inmutable permite que, posteriormente, cualquier verificador compruebe la autenticidad de la credencial sin necesidad alguna de contactar a la universidad.

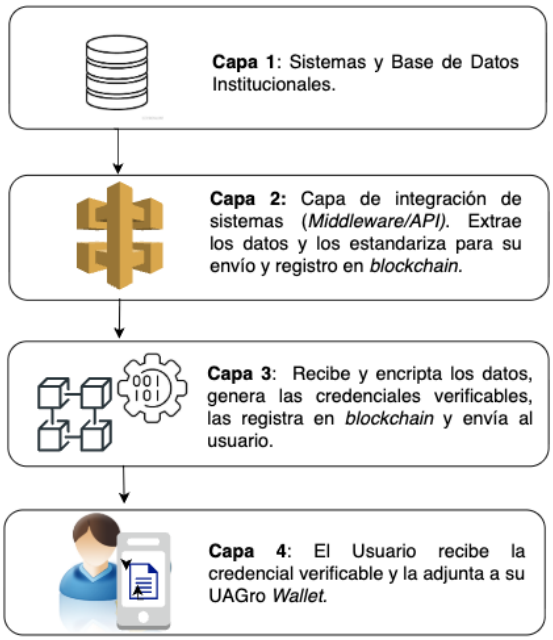
La capa de usuario final está representada por la aplicación UAGro wallet, una billetera digital móvil disponible tanto para dispositivos iOS como Android. Esta aplicación, desarrollada sobre código abierto

https://doi.org/10.22201/dgtic.30618096e.2026.4.ESPECIAL.165 Núm. especial, abril 2026, págs. 17 - 27

y personalizada con la identidad institucional, permite a los estudiantes recibir, almacenar y compartir sus credenciales de forma segura. Las credenciales se almacenan localmente en el dispositivo del usuario, cifradas con claves controladas exclusivamente por el propietario de la billetera. Cuando algún verificador solicita comprobar una credencial, el estudiante puede generar una presentación verificable que incluye únicamente los atributos necesarios, preservando así su privacidad. El verificador escanea un código QR generado por la billetera, obtiene la presentación firmada, verifica la firma criptográfica contra el DID de la UAGro registrado en *blockchain,* y confirma que la credencial no haya sido revocada. La Figura 4 muestra cómo se relacionan e interactúan estas capas para que el ecosistema SSI de la UAGro funcione de manera adecuada.

**Figura 4**

*Arquitectura tecnológica de cuatro capas del ecosistema SSI implementado en UAGro*

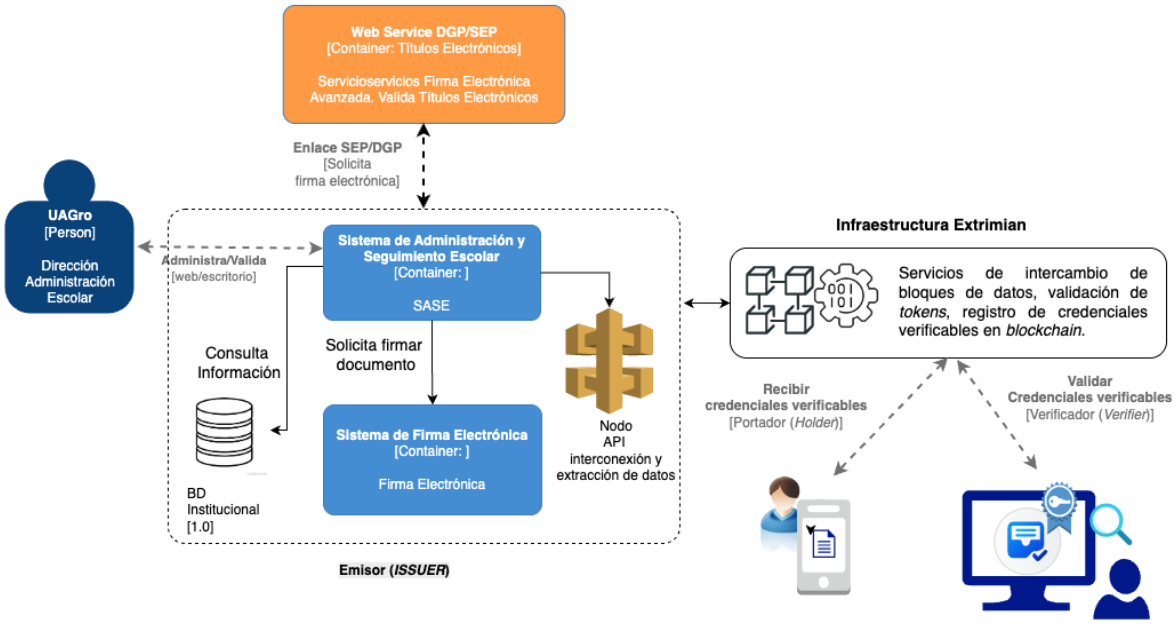



El flujo operativo completo para la emisión de las VCs funciona de la siguiente manera. Primero, el estudiante solicita su título o certificado a través de los canales tradicionales de la DAE; segundo, el personal administrativo valida el cumplimiento de requisitos académicos en el SASE y autoriza la emisión; tercero, el *middleware* extrae los datos validados y los envía a QuarkID; cuarto, QuarkID genera la credencial firmada y notifica al estudiante mediante correo electrónico o SMS que su credencial está disponible; quinto, el estudiante descarga UAGro wallet, completa un proceso de verificación de identidad, y recibe su credencial en la aplicación; sexto, cuando un empleador o institución educativa requiere verificar el título, el estudiante genera una presentación verificable desde su billetera; séptimo, el verificador escanea el código QR, obtiene la presentación y la valida automáticamente en la red *blockchain* sin requerir intervención de la UAGro. La Figura 5 muestra una representación esquemática de la relación entre los componentes tecnológicos que intervienen en el proceso de emisión de credenciales verificables, desde su generación hasta su recepción por parte del portador y su validación ante el verificador.

https://doi.org/10.22201/dgtic.30618096e.2026.4.ESPECIAL.165 Núm. especial, abril 2026, págs. 18 - 27

**Figura 5**

*Esquema de interacción entre componentes*




El ecosistema implementado también dota al estudiante de capacidad para portar y compartir sus documentos académicos de forma autónoma desde la UAGro wallet. Las figuras 6, 7, 8 y 9 presentan capturas de pantalla de la interfaz de la aplicación, a través de la cual, el estudiante gestiona y comparte sus credenciales. En la Figura 6, se visualizan las VCs que el estudiante ha recibido y adjuntado en su billetera digital. Cada una de estas VCs recibidas se van distribuyendo de manera ordenada por tiempo de recepción y tienen un nombre descriptivo que permite identificarlas de manera inmediata.

https://doi.org/10.22201/dgtic.30618096e.2026.4.ESPECIAL.165 Núm. especial, abril 2026, págs. 19 - 27

**Figura 6**

*Interfaz de UAGro wallet mostrando el listado de credenciales que el alumno ha recibido*


Al seleccionar la credencial de interés, el sistema despliega información con el detalle de su contenido junto con la opción de visualización del documento, como se muestra en la Figura 7.

**Figura 7**

*Interfaz de UAGro wallet mostrando los datos de una credencial verificable*

https://doi.org/10.22201/dgtic.30618096e.2026.4.ESPECIAL.165 Núm. especial, abril 2026, págs. 20 - 27

La Figura 8 muestra el documento en formato PDF con firmas digitales impresas y validadas por la Dirección General de Profesiones de la Secretaría de Educación Pública Federal.

**Figura 8**

*Interfaz de UAGro wallet mostrando el documento en formato PDF, validado y firmado*


La Figura 9 ilustra los mecanismos que tiene habilitados la UAGro wallet para permitir al alumno compartir sus credenciales verificables e imprimirlas en caso que se lo requieran.

**Figura 9**

*Interfaz de UAGro wallet con opciones para compartir sus credenciales verificables*

https://doi.org/10.22201/dgtic.30618096e.2026.4.ESPECIAL.165 Núm. especial, abril 2026, págs. 21 - 27

Los componentes de seguridad implementados incluyen múltiples capas de protección. A nivel criptográfico, se utilizan firmas digitales basadas en criptografía de curva elíptica que hacen computacionalmente inviable falsificar credenciales. A nivel de red, se implementó segmentación mediante VLANs y *firewalls* que aíslan los componentes críticos del resto de la infraestructura universitaria. A nivel de aplicación, se establecieron controles de acceso basados en roles que limitan las operaciones de emisión exclusivamente a personal autorizado de la DAE. A nivel de datos, se implementó el principio de minimización, donde las credenciales sólo incluyen información estrictamente necesaria, y se habilitó la divulgación selectiva que permite a los estudiantes compartir únicamente los atributos que cada verificador requiere.

Vale la pena destacar que la arquitectura implementada demuestra alta modularidad y extensibilidad. Cada capa opera de manera independiente con interfaces bien definidas, lo que facilitará futuras actualizaciones sin afectar otros componentes. Si, en el futuro, la UAGro decidiera migrar a un proveedor diferente de infraestructura SSI, sólo sería necesario modificar la capa de integración *middleware* sin tocar el SASE ni requerir cambios en las billeteras que ya usan los estudiantes. Esta característica arquitectónica resulta fundamental para proteger la inversión tecnológica y garantizar la sostenibilidad del sistema a largo plazo.

## 2.3 RESULTADOS DE LA IMPLEMENTACIÓN PILOTO

Los resultados obtenidos durante la fase piloto demostraron mejoras significativas en múltiples dimensiones operativas y de seguridad. En términos de eficiencia temporal, el cambio fue dramático. El tiempo promedio de emisión de un título profesional se redujo de 20 días en el proceso tradicional a menos de 24 horas con el nuevo sistema. Esta reducción significativa se logró al eliminar pasos manuales de impresión, firma física en cascada por múltiples autoridades, y trámites de registro ante dependencias gubernamentales que caracterizaban el proceso anterior. La credencial digital se genera automáticamente una vez que el personal de la DAE autoriza la emisión en el sistema, quedando disponible para el estudiante de forma prácticamente inmediata.

Respecto a seguridad y combate a la corrupción, la naturaleza criptográfica de las credenciales verificables hace que falsificarlas sea computacionalmente inviable. Cualquier alteración en los datos de la credencial invalida la firma digital, siendo detectada instantáneamente durante el proceso de verificación. Para validar esto, se realizaron pruebas de penetración simulando intentos de modificación de credenciales. En todos los casos, el proceso de verificación rechazó las credenciales alteradas. Esto ataca directamente el problema histórico de falsificación de documentos oficiales que ha afectado la credibilidad de las instituciones educativas mexicanas.

Desde la perspectiva del empoderamiento estudiantil, los egresados que participaron en el piloto expresaron alta satisfacción con el control y portabilidad de sus credenciales. Mediante la billetera digital, pueden compartir sus títulos un número ilimitado de veces sin costo adicional y de forma instantánea, simplemente generando códigos QR o enlaces de verificación. Esto contrasta marcadamente con el modelo tradicional, donde cada solicitud de copia certificada del título implicaba costos administrativos y tiempos de espera. El nuevo modelo eliminó completamente esta situación y otorgó autonomía total al egresado sobre sus documentos.

En términos de adopción tecnológica, durante la primera fase, se emitieron exitosamente credenciales de certificado de estudios de nivel medio superior para 150 estudiantes y títulos profesionales para

https://doi.org/10.22201/dgtic.30618096e.2026.4.ESPECIAL.165 Núm. especial, abril 2026, págs. 22 - 27

85 egresados del programa Ponte Águila. La tasa de descarga e instalación de UAGro wallet alcanzó el 78% entre los estudiantes notificados, cifra que se considera positiva tratándose de una tecnología completamente nueva. Las sesiones de capacitación presencial y los materiales de apoyo resultaron fundamentales para superar la brecha digital inicial, particularmente entre estudiantes de comunidades rurales con menor exposición a tecnologías móviles avanzadas. Esta última consideración reviste especial importancia, dado que la incorporación de nuevas tecnologías sin una estrategia de adopción debidamente planificada puede convertirse en un factor que profundice la brecha digital, particularmente en detrimento de los sectores con menor acceso y alfabetización tecnológica.

Se documentaron 42 verificaciones exitosas de credenciales realizadas por terceros durante el periodo piloto. Estas verificaciones fueron ejecutadas por empleadores locales, instituciones educativas en procesos de evaluación de solicitudes de posgrado y autoridades encargadas de comprobar la autenticidad de títulos. En todos los casos, el proceso de verificación tomó menos de 30 segundos desde el escaneo del código QR hasta la confirmación de autenticidad. Esto contrasta fuertemente con procesos tradicionales que pueden tardar días o incluso semanas cuando involucran validaciones transfronterizas.

Los desafíos técnicos identificados durante la implementación incluyeron principalmente la integración con el SASE. Fue necesario desarrollar adaptadores específicos para extraer información de bases de datos con esquemas completamente documentados y gestionar inconsistencias en formatos de información almacenada históricamente. Desde la perspectiva de gestión del cambio, el personal administrativo requirió un programa de capacitación intensivo. Fue crucial comunicar no sólo el uso operativo del sistema, sino el valor estratégico del cambio tecnológico en términos de seguridad y combate a la corrupción.

La experiencia de usuario con UAGro wallet, recabada a través de una encuesta breve en la fase piloto, reveló que los estudiantes valoraron particularmente la posibilidad de compartir sus credenciales mediante enlaces digitales al aplicar a empleos o programas académicos. Sin embargo, se identificó la necesidad de mejorar la experiencia para usuarios con menor alfabetización digital, específicamente en el proceso inicial de configuración de la billetera y verificación de identidad. Se planificaron mejoras iterativas en la interfaz de usuario basadas en retroalimentación directa de los estudiantes participantes.

## 3. DISCUSIÓN

La implementación del ecosistema SSI en la UAGro trasciende la simple modernización tecnológica. Constituye un acto de fortalecimiento de la confianza institucional. Al adoptar estándares globales transparentes y verificables del W3C, la UAGro envía un mensaje contundente sobre su compromiso con la integridad académica y la lucha contra la corrupción. Cada credencial verificable emitida representa una declaración de que la institución respalda sus procesos con la máxima seguridad criptográfica disponible, aumentando así tanto el prestigio institucional como el valor percibido de sus credenciales en mercados laborales y académicos.

Resulta importante comparar este modelo con otras formas de digitalización. Un documento PDF con firma electrónica avanzada representa ciertamente un avance respecto al papel, pero carece de granularidad para la privacidad, operando bajo un modelo de todo o nada donde el portador debe compartir el documento completo. Además, verificar PDFs firmados frecuentemente requiere *software* específico y conocimiento técnico por parte del verificador. Una base de datos centralizada con un portal

https://doi.org/10.22201/dgtic.30618096e.2026.4.ESPECIAL.165 **Núm. especial**, abril 2026, págs. 23 - 27

de consulta resuelve parcialmente el problema de verificación, pero mantiene a la Universidad como cuello de botella operativo y punto único de falla técnica, sin otorgar control real al egresado sobre sus propios documentos.

El modelo SSI implementado supera estas limitaciones al combinar tres características fundamentales de manera única. Primero, la autoridad del emisor se mantiene intacta mediante firmas digitales verificables criptográficamente. Segundo, tanto la portabilidad como el control se transfieren completamente al usuario mediante billeteras digitales bajo su custodia exclusiva. Tercero, la verificación se descentraliza, permitiendo que cualquier tercero confirme autenticidad sin depender de la disponibilidad de sistemas universitarios. Esta combinación de atributos resulta imposible de replicar con tecnologías tradicionales de digitalización.

Las implicaciones para la movilidad académica y laboral son prometedoras, aunque condicionadas al grado de adopción del estándar. Un egresado de la UAGro que aplique a un programa de posgrado en Europa o un empleo en Canadá podría reducir significativamente las demoras en la validación documental, siempre que el verificador extranjero cuente con infraestructura compatible con los estándares W3C, VC y DID. Experiencias comparables, como el proyecto EBSI (*European Blockchain Services Infrastructure*), sugieren que la verificación transfronteriza es técnicamente viable cuando las instituciones emisoras utilizan métodos DID interoperables (European Commission, 2023). Sin embargo, su adopción masiva requiere acuerdos de confianza institucional y marcos regulatorios que aún están en desarrollo a nivel global (Grech *et al*., 2021). En ese sentido, el caso UAGro representa un avance arquitectónico relevante que contribuye a nivelar el acceso a credenciales portables para egresados de instituciones latinoamericanas, aunque la promesa de verificación universal depende de la consolidación de ecosistemas de confianza más amplios que trascienden el ámbito técnico.

La experiencia de la UAGro se alinea con tendencias globales en transformación digital de educación superior. Investigaciones recientes sobre implementación de *blockchain* en credenciales académicas demuestran que las instituciones pioneras obtienen ventajas competitivas significativas al atraer estudiantes que valoran la portabilidad y verificabilidad de sus títulos (Ocheja *et al*., 2019). Sin embargo, el caso UAGro también evidencia que el éxito técnico debe complementarse necesariamente con estrategias robustas de gestión del cambio organizacional y capacitación exhaustiva de usuarios finales.

Los desafíos de interoperabilidad identificados señalan la necesidad de avanzar hacia ecosistemas más amplios de credenciales digitales. Aunque las credenciales emitidas en la UAGro son verificables globalmente gracias al uso de estándares W3C, la creación de un marco de confianza nacional que conecte sistemas de múltiples universidades mexicanas potenciaría significativamente el valor de la solución. Esto requeriría coordinación entre instituciones, acuerdos sobre esquemas de credenciales comunes y, potencialmente, intervención de autoridades educativas gubernamentales para establecer registros de DIDs institucionales reconocidos oficialmente.

El análisis de sostenibilidad financiera del proyecto reveló que los costos operativos del sistema SSI resultan significativamente menores que el modelo tradicional basado en papel. Se eliminaron gastos recurrentes de impresión, materiales físicos, logística de distribución y personal dedicado a validaciones manuales. La inversión inicial en el desarrollo del *middleware* e integración se amortizará en el mediano plazo mediante ahorros operativos. Adicionalmente, la reducción de tiempos de emisión liberó capacidad del personal administrativo para enfocarse en actividades de mayor valor agregado.

https://doi.org/10.22201/dgtic.30618096e.2026.4.ESPECIAL.165 Núm. especial, abril 2026, págs. 24 - 27

Las consideraciones sobre privacidad y protección de datos personales fueron centrales en el diseño del sistema. A diferencia de modelos centralizados, donde la institución retiene control perpetuo sobre información sensible, el modelo SSI implementado transfiere la custodia de datos al individuo inmediatamente después de la emisión. La universidad no mantiene registros de cuándo, dónde o con quién los estudiantes comparten sus credenciales, eliminando riesgos de vigilancia institucional y cumpliendo con principios fundamentales de privacidad por diseño establecidos en regulaciones como el GDPR europeo.

La gobernanza del ecosistema emergió como un aspecto crítico para la sostenibilidad a largo plazo. Se establecieron protocolos claros sobre quién puede autorizar emisiones, bajo qué condiciones pueden revocarse credenciales, cómo se gestionan actualizaciones de esquemas, y qué mecanismos de auditoría garantizan el uso apropiado del sistema. Estos aspectos de gobernanza, aunque menos visibles que la tecnología, resultaron igualmente fundamentales para mantener la confianza en el ecosistema y prevenir abusos.

## 4. CONCLUSIONES

La UAGro implementó exitosamente un ecosistema funcional de Identidad Autosoberana para emitir credenciales académicas, logrando transitar de un concepto teórico a una aplicación práctica de alto impacto. El sistema basado en el protocolo QuarkID y estándares del W3C demostró ser una solución viable y poderosa para enfrentar los desafíos de credencialización en educación superior. Los resultados de la fase piloto confirmaron que la tecnología SSI no sólo moderniza procesos administrativos, sino que fortalece fundamentalmente la integridad institucional y empodera a los estudiantes mediante control soberano sobre sus documentos oficiales, logrando, en ese sentido, el objetivo planteado.

La arquitectura implementada se caracteriza por su modularidad, permitiendo integración con sistemas legados sin requerir reemplazos costosos de infraestructura existente. La capa de *middleware* desarrollada sirvió como puente efectivo entre el SASE tradicional y la moderna infraestructura de credenciales verificables, demostrando que la transformación digital puede ser incremental y construir sobre inversiones tecnológicas previas. Esta característica resultará fundamental para facilitar la replicación del modelo en otras instituciones educativas mexicanas con restricciones presupuestarias similares.

Los beneficios cuantificados incluyen reducción de tiempos de emisión de 120 días a menos de 24 horas, eliminación computacional de posibilidades de falsificación mediante criptografía robusta, y empoderamiento estudiantil con capacidad de compartir credenciales ilimitadamente sin costos ni intermediarios. Estos resultados superan ampliamente las expectativas iniciales y validan la inversión en tecnología SSI como estrategia de transformación digital con retorno de inversión demostrable.

Los desafíos identificados, particularmente en integración de sistemas legados y gestión del cambio organizacional, proporcionan lecciones valiosas que guiarán futuras actualizaciones del sistema. La capacitación del personal administrativo y el diseño de experiencias de usuario accesibles para poblaciones con diversos niveles de alfabetización digital emergieron como factores críticos de éxito que deben priorizarse desde fases tempranas de implementación.

El trabajo futuro se enfocará en expandir la cobertura del sistema a toda la población de egresados de la UAGro y ampliar los tipos de credenciales emitidas para incluir constancias de calificaciones,

https://doi.org/10.22201/dgtic.30618096e.2026.4.ESPECIAL.165 Núm. especial, abril 2026, págs. 25 - 27

certificados de servicio social y diplomas de competencias específicas. Se explorará la consolidación de una credencial de identidad digital universitaria universal para estudiantes activos que permita acceso a servicios institucionales como biblioteca, transporte y sistemas académicos mediante autenticación basada en credenciales verificables.

A nivel de investigación futura, será crucial estudiar el impacto a largo plazo del sistema en la empleabilidad y movilidad académica de los egresados UAGro. Se requerirán estudios longitudinales que midan si poseer credenciales digitales verificables efectivamente facilita acceso a oportunidades profesionales internacionales y programas de posgrado en instituciones extranjeras. Adicionalmente, se deberá investigar la creación de un marco de confianza nacional que permita interoperabilidad entre sistemas de credenciales verificables de diferentes universidades mexicanas, creando un ecosistema educativo verdaderamente conectado.

El reconocimiento legal de las credenciales verificables por parte de autoridades gubernamentales mexicanas y colegios de profesionistas constituirá un paso fundamental para la adopción masiva de esta tecnología. Actualmente, aunque las credenciales son técnicamente verificables y criptográficamente seguras, su aceptación formal en trámites oficiales requiere marcos regulatorios actualizados que reconozcan explícitamente la validez jurídica de documentos digitales basados en estándares SSI.

El caso de la UAGro establece un precedente valioso que demuestra que instituciones públicas en países en desarrollo pueden implementar exitosamente tecnologías de vanguardia en identidad digital. El proyecto prueba que los desafíos técnicos, organizacionales y financieros son superables cuando existe compromiso institucional claro, alianzas estratégicas con proveedores tecnológicos especializados, y diseño centrado en las necesidades reales de los usuarios finales. Este modelo arquitectónico y operativo es replicable por otras universidades que busquen modernizar sus procesos de credencialización y fortalecer la confianza en el ecosistema educativo mediante transformación digital basada en estándares abiertos e interoperables.

**Declaración de contribución de autoría**

**Rosendo Guzmán Nogueda:** Analista, desarrollador e implementador de sistemas de información y ciberseguridad. Fungió como investigador responsable y ejecutor del proyecto. Su contribución abarcó el ciclo de vida del sistema: desde el levantamiento de requerimientos con las áreas de la Dirección de Administración Escolar y la DGTIC de la UAGro, el diseño arquitectónico del ecosistema SSI, la integración con el SASE y la configuración de la infraestructura de emisión mediante el protocolo QuarkID. Coordinó la fase piloto, diseñó los esquemas de credenciales verificables conforme a los estándares W3C VC y DID. En el plano académico, es el autor correspondiente del presente reporte técnico y responsable de la redacción, análisis de resultados y gestión del proceso de publicación.

**Dr. Mario Hernández Hernández:** Especialista en educación, diseño y desarrollo de sistemas de información. Participó como director de investigación del proyecto, aportando orientación metodológica y supervisión académica en todas las etapas del proceso. Su experiencia en diseño y desarrollo de sistemas de información fue determinante para establecer el marco conceptual que sustenta la arquitectura del ecosistema SSI implementado, así como para garantizar la coherencia entre los objetivos institucionales de la UAGro y las decisiones técnicas adoptadas durante el proyecto. Revisó y validó los criterios de evaluación de la fase piloto y la estructura del reporte técnico. Asimismo supervisó que los resultados obtenidos se articularan adecuadamente con la agenda de transformación digital de la institución.

https://doi.org/10.22201/dgtic.30618096e.2026.4.ESPECIAL.165 **Núm. especial**, abril 2026, págs. 26 - 27

**Dr. Gustavo Antonio Huerta Patraca:** Especialista en educación, pedagogía, identidad digital. Colaboró como co-director de investigación, aportando una perspectiva pedagógica y educativa enriqueciendo el análisis del impacto del sistema en la comunidad universitaria. Su experiencia en el ámbito de la educación superior y la innovación pedagógica fue clave para orientar el diseño de los materiales de capacitación. Contribuyó desde una óptica centrada en el usuario final, incorporando consideraciones sobre alfabetización digital, accesibilidad tecnológica y equidad en la adopción del sistema de identidad digital autosoberana, aspectos que resultaron determinantes para interpretar los resultados de adopción de la UAGro Wallet entre estudiantes de comunidades rurales. También participó en la revisión crítica del reporte técnico, así como de la información teórica y estructura general del reporte.

**Dr. Valentín Álvarez Hilario:** Especialista en educación, diseño y desarrollo de sistemas de información. Participó como tutor de investigación, brindando asesoría técnica y académica de manera continua durante el desarrollo del proyecto. Su experiencia en educación y desarrollo de sistemas de información contribuyó a reforzar la solidez metodológica del trabajo, particularmente en lo referente a la definición de métricas de evaluación de la implementación piloto y al análisis de los resultados cuantitativos obtenidos. Su retroalimentación fue valiosa en la etapa de revisión del reporte técnico, asegurando que los hallazgos se presentarán con el rigor académico requerido para su difusión en el contexto de la comunidad científica de tecnología educativa.

## REFERENCIAS

Allen, C. (2016). *The path to self-sovereign identity*. Life With Alacrity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

Asociación Nacional de Universidades e Instituciones de Educación Superior. (2018). *La educación superior en el siglo XXI: Líneas estratégicas de desarrollo*. ANUIES.

Eaton, S. E., Carmichael, J. J., & Pethrick, H. (Eds.). (2023). *Fake degrees and fraudulent credentials in higher education*. Springer. https://doi.org/10.1007/978-3-031-21796-8

European Commission. (2023). *European Blockchain Services Infrastructure* (EBSI): Overview and use cases. Publications Office of the European Union. https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI

Extrimian. (2024). *Self-sovereign identity solutions*. https://extrimian.io/es/

Grech, A., & Camilleri, A. F. (2017). *Blockchain in education*. European Commission, Joint Research Centre Science for Policy Report. https://doi.org/10.2760/60649

Grech, A., Sood, I., & Ariño-Blasco, S. (2021). Blockchain, self-sovereign identity and digital credentials: Promise versus praxis in education. *Frontiers in Blockchain*, 4. https://doi.org/10.3389/fbloc.2021.616779

Jirgensons, M., & Kapenieks, J. (2018). Blockchain and the future of digital learning credential assessment and management. *Journal of Teaching and Learning for Graduate Employability*, 9(1), 21-42. https://reference-global.com/issue/JTES/20/1

https://doi.org/10.22201/dgtic.30618096e.2026.4.ESPECIAL.165 **Núm. especial**, abril 2026, págs. 27 - 27

Naik, N., & Jenkins, P. (2020). Governing principles of self-sovereign identity applied to blockchain enabled privacy preserving identity management systems. *Proceedings of the 4th International Conference on Distributed Computing and Internet Technology*, 1-12. https://doi.org/10.1109/ICDCIT49267.2020.00014

Ocheja, P., Flanagan, B., & Ogata, H. (2019). Connecting decentralized learning records: A *blockchain based learning analytics platform. Proceedings of the 8th International Conference on Learning Analytics and Knowledge*, 265-269. https://doi.org/10.1145/3303772.3303832

Preukschat, A., & Reed, D. (2021). *Self-sovereign identity: Decentralized digital identity and verifiable credentials*. Manning Publications. https://www.manning.com/books/self-sovereign-identity

QuarkID. (2024). QuarkID protocol: *Open source self-sovereign identity protocol*. https://quarkid.org/

Sporny, M., Longley, D., & Chadwick, D. (2019). *Verifiable credentials data model 1.0*. W3C Recommendation. https://www.w3.org/TR/vc-data-model/

Sporny, M., Longley, D., & Sabadello, M. (2022). *Decentralized identifiers (DIDs) v1*.0. W3C Recommendation. https://www.w3.org/TR/did-core/

Tobin, A., & Reed, D. (2017). *The inevitable rise of self-sovereign identity*. The Sovrin Foundation. https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

W3C. (2022). *Verifiable credentials data model v1.1*. W3C Recommendation. https://www.w3.org/TR/vc-data-model/