TFC - Informe

UNRN Universidad Nacional de Río Negro

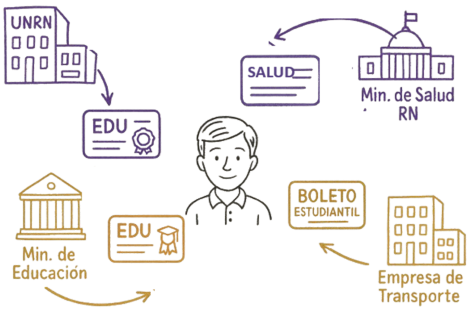
Credenciales Verificables de W3C: El estándar de W3C para la confianza y la seguridad en las credenciales digitales

Licenciatura en Sistemas

Autora: Rached Galera, María Sofía

Director: Cambarieri, Mauro Germán

Codirector: Garcia Martinez, Nicolas



Viedma, Río Negro, Argentina.

2025

1. Descripción del problema

La era digital ha transformado la forma en que interactuamos y acreditamos conocimientos, pero también ha generado un desafío crítico en la verificación de la autenticidad de las credenciales. Ante el aumento significativo de credenciales falsas e identidades digitales falsificadas, los métodos tradicionales de verificación se han vuelto largos, ineficientes y propensos a cometer errores. El presente trabajo final se enfoca en cómo un estándar abierto y descentralizado, como el de las Credenciales Verificables (VC) del World Wide Web Consortium (W3C), puede ofrecer una solución robusta y centrada en el usuario para esa problemática. Específicamente, se analiza su aplicación en el reconocimiento ágil y verificable de aprendizaje mediante microcredenciales en el ámbito educativo. Las Credenciales Verificables son fundamentales para la creación de un modelo confiable, seguro e interoperable de acreditación de saberes, buscando evitar intermediarios

En este trabajo final se muestra el análisis realizado sobre el estándar de las Credenciales Verificables (VC) desarrollado por el W3C. Dicho análisis nos permitió identificar su papel fundamental en la creación de un modelo confiable, seguro, interoperable y centrado en el usuario para la acreditación de saberes.

2. Objetivos

El propósito central de este trabajo fue examinar de manera detallada el papel del estándar W3C de Credenciales Verificables como fundamento para un modelo de credenciales digitales que sea confiable, seguro y, sobre todo, centrado en el usuario. Para alcanzar este objetivo, se buscó, en primer lugar, profundizar en los conceptos fundamentales, las características y el ecosistema que define el estándar W3C, comprendiendo cómo se estructuran las credenciales verificables y cómo se establece la confianza entre emisores, titulares y verificadores dentro de este modelo. Paralelamente, se analizó de manera específica la aplicación práctica de esta tecnología en la Licenciatura en Sistemas de la Universidad Nacional de Río Negro, evaluando cómo las credenciales verificables sustentan la iniciativa de microcredenciales, garantizando la seguridad, interoperabilidad, portabilidad y verificación instantánea de la información, así como la reducción de posibles fraudes. A partir de este análisis, también se identificaron los beneficios concretos

que aporta la adopción del estándar W3C al sistema de microcredenciales, resaltando cómo estas ventajas impactan en la calidad, eficiencia y confiabilidad de los procesos académicos y profesionales de los estudiantes.

3. Metodología de trabajo

La metodología empleada para este trabajo siguió un enfoque de análisis apoyado en el caso de estudio, combinando la revisión teórica con la observación práctica. La primera etapa consistió en un examen exhaustivo de la documentación y especificaciones del estándar W3C de Credenciales Verificables, con el fin de comprender en profundidad sus principios, su arquitectura, sus componentes esenciales y el modelo de confianza que sostiene toda la estructura de credenciales digitales. Posteriormente, se llevó a cabo un análisis del caso particular de la UNRN, evaluando cómo la Licenciatura en Sistemas podría implementar las microcredenciales y cómo la tecnología de credenciales verificables se adapta para cubrir las necesidades de validación y certificación académica en un contexto real. Finalmente, los hallazgos teóricos y prácticos se integraron para generar conclusiones claras sobre la pertinencia y efectividad del estándar W3C en el proyecto de la UNRN, al mismo tiempo que se esbozaron posibles líneas de trabajo futuras que podrían ampliar la aplicación de estas tecnologías en la educación superior y en el desarrollo de competencias profesionales.

4. Marco Teórico: Conceptos Fundamentales

4.1. ¿Qué es una credencial?

Una credencial puede entenderse como un conjunto de declaraciones emitidas por una autoridad reconocida, que reflejan información relevante sobre un individuo, organización o entidad. Estas declaraciones pueden abordar distintos aspectos, desde la identidad del titular hasta evidencias de competencias o logros alcanzados. En el mundo físico, un ejemplo clásico de credencial podría ser un pasaporte, una licencia de conducir o una tarjeta de seguro médico. Estas credenciales incluyen

información sobre el titular, como su nombre, fotografía o número de identificación; detalles sobre la autoridad emisora, como un gobierno municipal o un organismo de certificación; y especificaciones sobre la credencial en sí, por ejemplo, su tipo, período de validez o condiciones de uso. Además, contienen evidencia que demuestra que el titular cumple con los requisitos para recibirla, como un examen aprobado, un resultado de medición o un proceso de validación oficial.

4.2. ¿Que es una Credencial Verificable?

Cuando trasladamos el concepto de credencial al mundo digital, surge la credencial verificable (Verifiable Credential, VC). Una VC digitaliza toda la información que tradicionalmente se encuentra en una credencial física, pero incorporando tecnologías criptográficas como firmas digitales, lo que la hace más segura, confiable y resistente a falsificaciones. Estas credenciales permiten que los titulares puedan generar presentaciones verificables, que son compilaciones de una o varias VCs que pueden compartirse con terceros para demostrar determinadas competencias, logros o atributos, sin necesidad de revelar información adicional no relevante. A diferencia de las credenciales físicas, las VCs y sus presentaciones pueden transmitirse rápidamente y de manera segura, facilitando la confianza a distancia, agilizando procesos de verificación y reduciendo la dependencia de intermediarios. Así, las credenciales verificables combinan la solidez de la certificación tradicional con la flexibilidad, seguridad y eficiencia que ofrece la tecnología digital, convirtiéndose en una herramienta clave para la educación, la empleabilidad y la validación de competencias en entornos contemporáneos.

4.3. Microcredenciales

Tabla de conceptos principales

Concepto	**Qué es**	**Ejemplo o Aplicación**
Credencial Verificable (VC)	Es un conjunto de afirmaciones digitales	Un certificado de egreso emitido por la UNRN que

	firmadas criptográficamente que validan información sobre un sujeto o entidad. Garantiza seguridad, autenticidad y portabilidad.	acredita que un estudiante completó un curso.
Identificadores Descentralizados (DID)	Identificadores únicos que no dependen de una autoridad central, utilizados para reconocer a personas, organizaciones o dispositivos en el ecosistema digital.	***did:unrn:alumno123*** como identificador único de un estudiante en la UNRN.
Validación	Proceso mediante el cual un verificador comprueba la autenticidad, integridad y vigencia de una credencial sin necesidad de intermediarios.	Un sistema de RRHH verifica digitalmente el título académico de un postulante.
Pruebas de Conocimiento Cero (ZKP)	Técnica criptográfica que permite demostrar que se cumple una condición sin revelar los datos completos subyacentes.	Comprobar que alguien es mayor de edad sin mostrar su fecha de nacimiento exacta.

Identidad Auto-Soberana (SSI)	Modelo de identidad en el que el titular controla sus credenciales y decide qué información compartir y con quién.	Un estudiante elige mostrar solo el curso aprobado al inscribirse en un posgrado, sin revelar otros datos.
W3C	Organización que define estándares internacionales para credenciales digitales verificables y asegura interoperabilidad global.	La especificación oficial de las Credenciales Verificables.
Interoperabilidad	Capacidad de distintos sistemas para interpretar y validar credenciales de manera mutua, facilitando movilidad académica y laboral.	Una empresa en Europa valida una credencial emitida por la UNRN en Argentina.
Modelo de Confianza Descentralizado	Ecosistema donde la confianza no depende de una autoridad central, sino de criptografía y relaciones P2P.	UNRN emite la credencial, el estudiante la presenta, y una empresa la válida sin depender de servidores centrales.
Consorcios y Alianzas Estratégicas	Redes de instituciones académicas y de investigación que promueven estándares	Consorcio de Credenciales Digitales del MIT o iniciativa OpenEU.

	de credenciales digitales y microcredenciales.	
Protección de la privacidad	Principio según el cual el titular decide qué información compartir y con quién, garantizando confidencialidad.	Mostrar solo el nombre y el curso aprobado, sin datos personales adicionales.
Registro de Datos Verificables	Sistemas que almacenan información esencial para la emisión y verificación de credenciales: esquemas, estados de revocación, claves públicas, etc.	Base de datos blockchain que mantiene el estado de vigencia de una credencial emitida por la universidad.

5. Ecosistema de las Credenciales Verificables

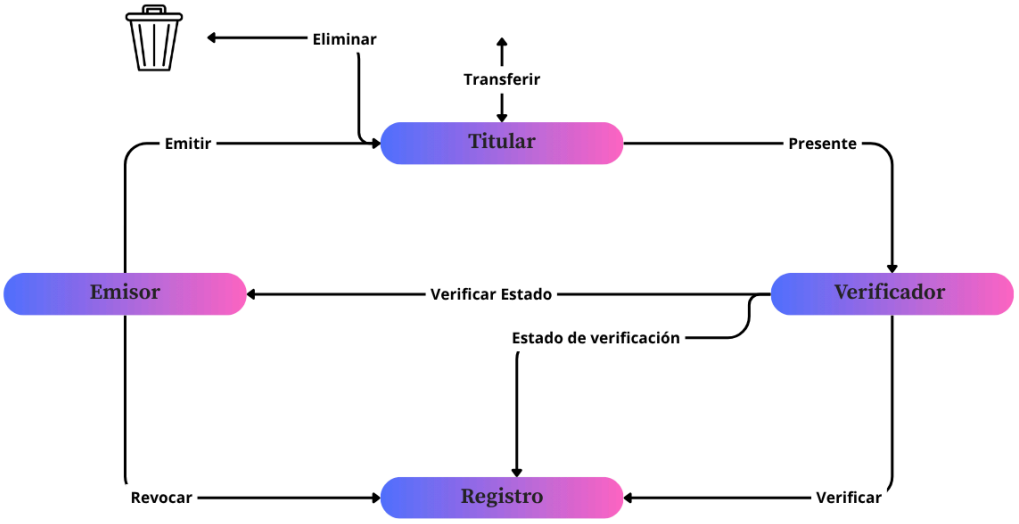
5.1. Credenciales – Ciclo de vida

Los roles y flujos de información en el ciclo de vida de las credenciales verificables son los siguientes:

- Un emisor emite una credencial verificable a un titular. La emisión siempre se produce antes de cualquier otra acción relacionada con una credencial.
- Un titular puede transferir una o más de sus credenciales verificables a otro titular.
- Un titular presenta una o más de sus credenciales verificables a un verificador, opcionalmente dentro de una presentación verificable.
- Un verificador verifica la autenticidad de la presentación verificable presentada y de las credenciales verificables. Esto debe incluir la

comprobación del estado de la credencial para la revocación de las credenciales verificables.

- Un emisor puede revocar una credencial verificable.
- Un titular puede eliminar una credencial verificable

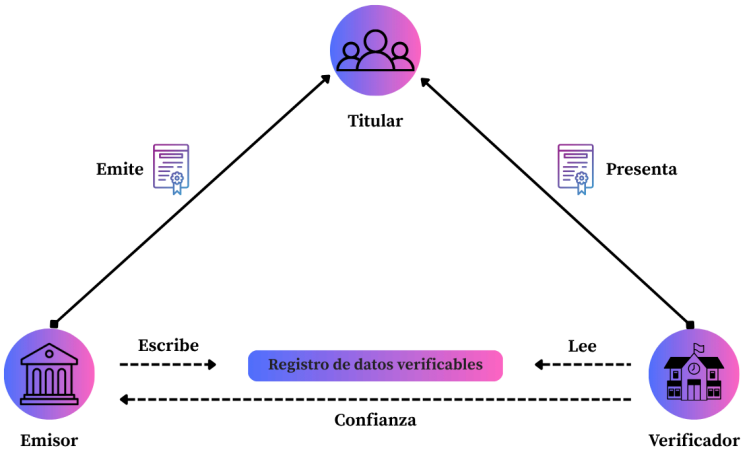


Ecosistema de credenciales verificables: ciclo de vida de una credencial

Elaboración propia hecho en Canva

5.2. Características

El funcionamiento del ecosistema VC se apoya en la estandarización de roles y procesos que facilitan la interoperabilidad entre diferentes plataformas tecnológicas y contextos institucionales. Esta estandarización permite que los distintos actores involucrados puedan interactuar bajo reglas comunes, promoviendo así la escalabilidad, la portabilidad y la reutilización de credenciales en diferentes dominios (educativo, profesional, gubernamental, etc.). A continuación, se describen con mayor profundidad los roles principales definidos por la especificación del W3C, que sirven como referencia para la implementación de soluciones basadas en credenciales verificables.



Ecosistema de credenciales verificables: triángulo de la confianza

Elaboración propia hecho en Canva

5.2.1. Emisor

El emisor, también conocido como issuer, es la entidad encargada de crear y emitir la credencial verificable. En otras palabras, es quien formula una serie de afirmaciones sobre un sujeto determinado (por ejemplo, un estudiante), y las encapsula en una credencial digital firmada criptográficamente, que luego puede ser validada por terceros.

Esta firma garantiza tanto la autenticidad de la fuente emisora como la integridad del contenido. Un caso típico de emisor es una universidad que genera un certificado de finalización de carrera o una microcredencial asociada a competencias específicas adquiridas en un curso, seminario o proyecto.

5.2.2. Titular

El titular, también llamado *holder*, es el usuario que recibe y almacena la credencial emitida, y que tiene la capacidad de presentarla ante terceros según lo considere conveniente.

En la mayoría de los casos, el titular es también el sujeto de las declaraciones contenidas en la credencial (por ejemplo, un estudiante que recibe una microcredencial por haber participado en un proyecto de investigación). El holder tiene el control sobre sus credenciales y es responsable de resguardarlas,

habitualmente en una *billetera digital*[1] o repositorio seguro.
Este enfoque promueve el principio de soberanía del usuario, ya que le otorga la facultad de decidir qué información compartir, con quién y bajo qué condiciones, fortaleciendo la privacidad y la autonomía individual en el manejo de datos personales.

5.2.3. Verificador

El verificador, también llamado verifier, es la entidad que recibe una presentación de credenciales por parte del titular y que se encarga de comprobar su validez, integridad y autenticidad.
La verificación se realiza mediante mecanismos criptográficos que permiten validar la firma digital del emisor y confirmar que la credencial no ha sido alterada. Esta operación puede hacerse de manera automatizada y sin necesidad de contactar directamente al emisor, gracias al uso de claves públicas y registros confiables.
Un ejemplo claro de verificador puede ser una empresa tecnológica que, al evaluar una postulación laboral, revisa una presentación verificable que demuestra la participación del candidato en un curso avanzado de inteligencia artificial avalado por una universidad pública. El verificador puede incluso definir criterios personalizados para aceptar credenciales (como restringirlas a instituciones nacionales, públicas, o acreditadas).

5.2.4. Registro de datos Verificables

Además de los roles principales mencionados, el ecosistema puede incluir infraestructuras que actúan como registros de datos verificables. Estos registros no son actores activos, sino componentes técnicos del sistema que almacenan y publican información crítica para la verificación, como identificadores descentralizados (DIDs), material criptográfico (claves públicas, esquemas de credenciales, reglas de revocación), y estados de las credenciales (vigente, revocada, vencida, etc.).

[1] Billetera Digital: aplicación segura (generalmente móvil o web) donde el titular almacena y gestiona sus VCs y DIDs, controlando la presentación y divulgación selectiva de información.

Este tipo de registro puede estar implementado como una base de datos tradicional, una red blockchain, un sistema gubernamental de identificación, o una combinación de ellos. Su función principal, dentro del ecosistema, es brindar a emisores y verificadores acceso confiable a información de soporte necesaria para validar una credencial sin comprometer la privacidad del titular.

Una característica destacada del ecosistema es la posibilidad de utilizar técnicas como las pruebas de conocimiento cero (Zero-Knowledge Proofs). Estas permiten al titular demostrar que cumple con un cierto criterio (por ejemplo, tener un título de grado) sin necesidad de mostrar la credencial completa ni revelar otros datos sensibles (como la fecha de nacimiento, el número de documento o el promedio final). Esta funcionalidad es parte del concepto de presentación verificable, que se explica a continuación.

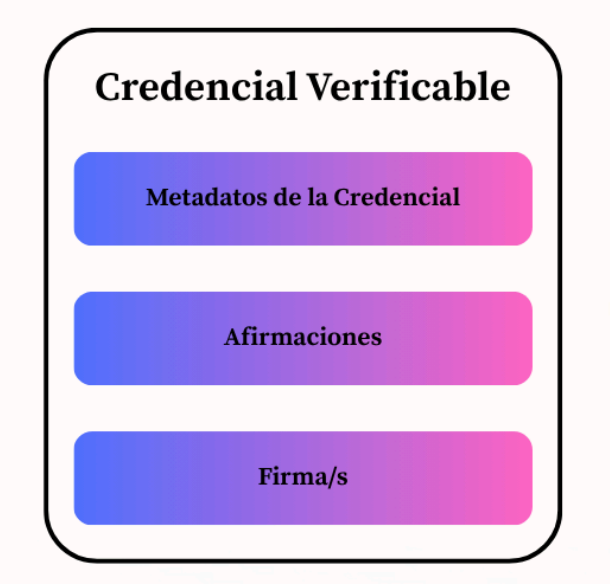
Este ecosistema, basado en estándares abiertos y tecnologías descentralizadas, permite construir una red de confianza que puede ser escalada a nivel institucional, nacional e internacional.
En el contexto de la UNRN, esta arquitectura se adapta perfectamente al modelo de microcredenciales en desarrollo, facilitando la emisión, gestión y verificación de certificaciones académicas que acompañen a los estudiantes y egresados en todo su recorrido profesional y educativo, dentro y fuera del país.

5.3. Credenciales

Dentro del contexto de la identidad digital y la certificación electrónica, una credencial se define como un conjunto estructurado de afirmaciones realizadas por una entidad emisora sobre una persona, organización u objeto.
Estas afirmaciones (también llamadas "claims") pueden abarcar una amplia variedad de datos: desde el nombre del titular, su pertenencia a una institución, su nivel de estudios alcanzado, o la participación en un proyecto determinado. A estas declaraciones se les suman metadatos esenciales como la fecha de emisión, la validez temporal, el identificador único, e incluso una imagen visual que represente la credencial.

Cuando estas credenciales están respaldadas mediante firmas criptográficas y mecanismos de verificación automática que aseguran su integridad y autenticidad, hablamos de credenciales verificables (Verifiable Credentials o VCs). Estas credenciales no solo permiten comprobar que la información no ha sido alterada, sino también quién la emitió y si sigue siendo válida.
La seguridad que ofrecen las VCs se basa en tecnologías criptográficas que impiden la manipulación o falsificación de datos, eliminando la necesidad de que un verificador tenga que consultar directamente con la entidad emisora.

Gracias a este modelo, las VCs pueden adoptar múltiples formatos y usos: desde un diploma universitario digital, una constancia de alumno regular, una licencia profesional, hasta una certificación de habilidades técnicas adquiridas a través de un curso específico. Lo más innovador de este enfoque es que estas credenciales no dependen de una infraestructura centralizada, por lo que pueden ser almacenadas en billeteras digitales personales (wallets) y presentadas de manera flexible, segura y autónoma por parte del titular.



Componentes de una Credencial Verificable
Elaboración realizada en napkin

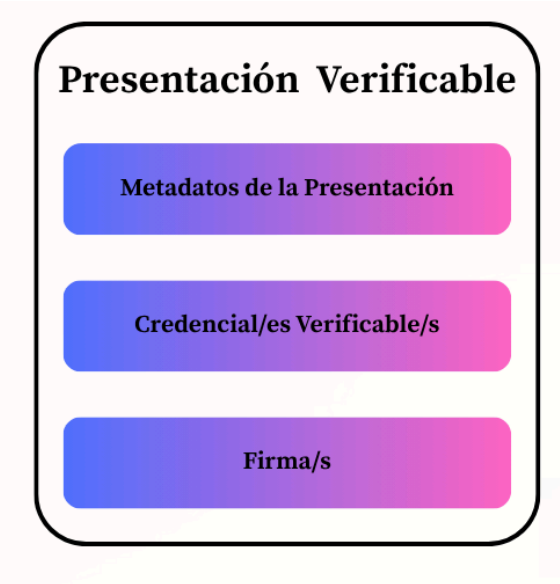
5.4. Presentaciones

Ahora bien, las credenciales no se utilizan por sí solas. Para demostrar que se posee una o varias credenciales ante un tercero (como un empleador, una universidad o una entidad gubernamental), el titular genera lo que se denomina una presentación verificable (Verifiable Presentation o VP). Esta presentación es un conjunto de datos que puede incluir una o más credenciales completas, partes específicas de ellas o incluso información adicional proporcionada directamente por el titular.

Una de las características más potentes de este mecanismo es que el titular conserva pleno control sobre lo que decide compartir. Gracias a lo que se conoce como divulgación selectiva, puede elegir mostrar únicamente ciertos datos dentro de una credencial, sin necesidad de revelar información personal o sensible que no sea relevante para el verificador. Por ejemplo, si una empresa solo necesita confirmar que un candidato tiene una certificación en "Desarrollo Backend", el titular puede generar una presentación que muestre solo esa información, ocultando detalles como la fecha de nacimiento o el número de documento.

Otra ventaja clave es que las presentaciones pueden agrupar información proveniente de diferentes emisores. Esto permite construir una narrativa coherente del perfil del titular, combinando, por ejemplo, una credencial de formación universitaria, una constancia de participación en un proyecto de investigación, y un certificado de competencias laborales emitido por una organización privada. Toda esta información, una vez reunida en una presentación verificable, puede ser validada por un tercero utilizando las claves públicas de cada emisor, sin necesidad de intermediarios.

Este modelo de presentación garantiza no solo la autenticidad y la integridad de la información compartida, sino también un grado elevado de privacidad, eficiencia y confianza, ideal para entornos académicos y profesionales que requieren verificaciones rápidas y seguras. En definitiva, las presentaciones verificables son la herramienta que articula el uso real de las credenciales, conectando al titular con los verificadores de forma ágil, segura y transparente.



Componentes de una Presentación Verificable
Elaboración realizada en napkin

6. Microcredenciales en la UNRN: Sustentabilidad y Aplicación de las VC

6.1. Las microcredenciales en la UNRN

La carrera de la Licenciatura en Sistemas de la Universidad Nacional de Río Negro (UNRN) se encuentra desarrollando una iniciativa pionera basada en la implementación de microcredenciales digitales, con el propósito de reconocer formalmente competencias específicas adquiridas por estudiantes y egresados durante su trayectoria universitaria.

Esta propuesta surge como una respuesta directa a los desafíos que enfrentan hoy las instituciones de educación superior, particularmente en un contexto donde el aprendizaje es cada vez más dinámico, fragmentado y orientado a la resolución de problemas concretos. Las microcredenciales buscan llenar un vacío en los sistemas tradicionales de certificación académica, aportando un mecanismo más ágil, modular y adaptativo para validar el conocimiento, las habilidades y las experiencias adquiridas por los estudiantes en diversos entornos formativos.

En carreras reguladas por el Estado, como la Licenciatura en Sistemas, el cumplimiento de normativas es fundamental. La UNRN debe respetar los lineamientos establecidos por la Ley de Educación Superior N.º 24.521, así como

las resoluciones ministeriales vigentes, como la Resolución 786/09 y su modificación posterior, la Resolución Ministerial 1558/2021, que definen contenidos curriculares básicos, cargas horarias mínimas, intensidad práctica y estándares de acreditación.
En este marco, el desarrollo de microcredenciales no busca reemplazar la estructura tradicional de títulos universitarios, sino complementarla. Lejos de contradecir las exigencias normativas, esta estrategia se presenta como una innovación que permite hacer visibles competencias específicas que muchas veces quedan implícitas o invisibilizadas dentro del título general de grado. Así, las microcredenciales abren nuevas posibilidades para certificar saberes en paralelo al cumplimiento de los estándares de calidad establecidos por los organismos regulatorios.

Uno de los mayores aportes de las microcredenciales es su capacidad para capturar y validar aprendizajes que trascienden los límites del aula tradicional. No se restringen únicamente a los contenidos previstos en los planes de estudio, sino que permiten reconocer habilidades desarrolladas en prácticas profesionales, investigaciones, proyectos interdisciplinarios, participación en hackatones, cursos extracurriculares, pasantías, capacitaciones en tecnologías específicas, entre otras experiencias formativas significativas. En este sentido, el sistema de microcredenciales se convierte en una herramienta fundamental para promover el aprendizaje permanente y visibilizar el esfuerzo académico en toda su complejidad y diversidad.

Además, esta propuesta responde a un cambio estructural en la relación entre el sistema educativo y el mundo del trabajo. El modelo clásico de titulación, basado en trayectos largos, estructurados y poco flexibles, comienza a mostrar limitaciones frente a las nuevas demandas del siglo XXI.
En muchos casos, un título de grado no alcanza por sí solo para evidenciar las capacidades concretas de un egresado, especialmente cuando se trata de tecnologías emergentes o habilidades específicas que cambian a gran velocidad. Este sistema permite desagregar el conocimiento, ofreciendo certificaciones más puntuales y adaptadas a contextos laborales cambiantes. Esto resulta particularmente útil para los empleadores, dado que les permite identificar de forma

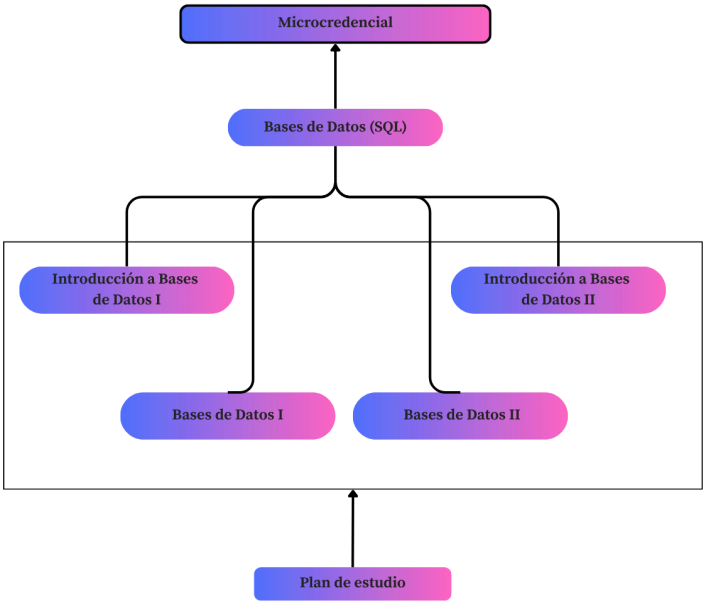
precisa qué competencias tiene una persona, sin necesidad de deducirlo a partir de su título general.

Por otro lado, el formato modular, acumulativo y portable de las microcredenciales habilita trayectos formativos más personalizados. Los estudiantes pueden elegir qué competencias quieren certificar, cómo integrarlas a su perfil y de qué manera construir una trayectoria profesional alineada con sus intereses. Pueden optar por cursar diferentes secuencias de microcredenciales en áreas específicas, como por ejemplo, programación web, inteligencia artificial, análisis de datos, y posteriormente combinarlas, integrandola a una diplomatura o incluso articularlas con su plan de estudios formal.
Esta lógica de apilamiento, cada vez más presente en el ámbito internacional, rompe con la linealidad del recorrido educativo y empodera al estudiante como protagonista de su propio proceso formativo.

En este contexto, la sustentabilidad del sistema de microcredenciales está estrechamente vinculada a su integración con tecnologías emergentes, especialmente las Credenciales Verificables (VCs) propuestas por el W3C. Estas tecnologías permiten garantizar la autenticidad, seguridad y verificabilidad de las certificaciones emitidas, sin depender de intermediarios o procesos manuales.
La posibilidad de emitir microcredenciales en formato VC no solo fortalece la confianza en su validez, sino que también facilita su interoperabilidad con plataformas externas, billeteras digitales y redes internacionales de validación. La adopción de esta tecnología, como se desarrolla en detalle en el apartado correspondiente, refuerza la proyección del proyecto y lo posiciona como una referencia en el ecosistema digital educativo de la región.

En suma, la iniciativa de microcredenciales impulsada por la UNRN se presenta como un instrumento clave para transformar la forma en que se reconoce el conocimiento en la educación superior. Permite acercar la formación universitaria a las necesidades reales del entorno, aumentar la empleabilidad de los egresados, empoderar a los estudiantes en la construcción de sus trayectorias, y dotar a la universidad de una herramienta ágil para responder a los cambios constantes del mundo académico y laboral. Es, al mismo tiempo, un acto de innovación, una

estrategia de mejora institucional y una apuesta por una educación más inclusiva, flexible y orientada al futuro.



Elaboración propia hecho en Canva

6.2. Objetivos de la Iniciativa de Microcredenciales en la UNRN

La implementación del sistema de microcredenciales en la Licenciatura en Sistemas de la Universidad Nacional de Río Negro surge como una respuesta innovadora y estratégica a las transformaciones que atraviesa el mundo académico, laboral y tecnológico. Esta iniciativa busca principalmente reconocer, validar y dar visibilidad a competencias específicas adquiridas por los estudiantes a lo largo de su trayecto formativo, que muchas veces no se reflejan de manera explícita en los títulos tradicionales. En un contexto donde la formación continua, la actualización permanente y la certificación ágil de saberes son cada vez más valoradas, las microcredenciales se convierten en una herramienta clave para responder a estas nuevas demandas.

Uno de los ejes fundamentales de este enfoque es diversificar la oferta de aprendizaje dentro de la carrera, habilitando trayectos formativos más flexibles, dinámicos y personalizados. Las microcredenciales permiten que cada estudiante pueda construir su perfil profesional de manera única, seleccionando aquellas competencias que se alinean con sus intereses, objetivos o necesidades del

entorno. De esta forma, es posible optar por una orientación más técnica o práctica con foco en la empleabilidad, por una profundización en líneas de investigación o incluso por desarrollar capacidades emprendedoras. Esta modularidad habilita un sistema formativo más inclusivo y adaptado a las realidades diversas de la comunidad estudiantil.

En paralelo, la iniciativa también promueve una innovación profunda en los contenidos y modalidades de enseñanza-aprendizaje. Se busca trascender los formatos tradicionales, incorporando propuestas pedagógicas más activas, basadas en proyectos, metodologías ágiles, colaborativas y mediadas por tecnologías digitales. El desarrollo de microcredenciales impulsa así un ecosistema educativo híbrido, que combina clases presenciales, entornos virtuales y experiencias reales del mundo del trabajo. Estas modalidades no solo enriquecen la experiencia formativa, sino que también contribuyen a preparar a los estudiantes para entornos laborales que hoy exigen habilidades digitales, flexibilidad y autonomía en el aprendizaje.

Otro objetivo esencial del proyecto es fomentar la construcción de un ecosistema colaborativo, que integre a múltiples actores vinculados con la educación, la ciencia, la producción y el desarrollo local y global. La implementación de microcredenciales no puede pensarse únicamente dentro de los límites institucionales de una carrera o universidad, sino que requiere articularse con empresas del sector tecnológico, organismos gubernamentales, organizaciones sociales, otras instituciones académicas y plataformas digitales.
Esta articulación permite validar de manera más robusta las credenciales emitidas y generar redes de confianza que potencien su reconocimiento tanto a nivel nacional como internacional.

Finalmente, uno de los beneficios más tangibles y urgentes de la iniciativa es su potencial para mejorar la inserción laboral de los egresados. Al ofrecer certificaciones claras, específicas y verificables sobre competencias que son altamente demandadas por el mercado (como programación, diseño de software, análisis de datos, metodologías ágiles, ciberseguridad, entre otras) se facilita la empleabilidad de los estudiantes, aumentando sus oportunidades y visibilidad profesional. En un contexto cada vez más competitivo, contar con microcredenciales

permite a los egresados destacar frente a otros perfiles, demostrando de forma concreta su experiencia y preparación para enfrentar los desafíos del mundo laboral actual.

En resumen, la iniciativa de microcredenciales de la UNRN no solo se propone adaptar la educación universitaria a los nuevos tiempos, sino también transformarla estructuralmente para que sea más flexible, pertinente, inclusiva, innovadora y alineada con las demandas reales de la sociedad y la economía del conocimiento.

6.3. Sustentación en Credenciales Verificables (VCs) de W3C

Para sustentar el proyecto de microcredenciales en la Universidad Nacional de Río Negro (UNRN), se ha optado por adoptar el estándar internacional de Credenciales Verificables (Verifiable Credentials, VC), definido por el World Wide Web Consortium (W3C). Esta elección no es arbitraria: las VCs representan una solución tecnológica avanzada que permite garantizar aspectos fundamentales como la fiabilidad, seguridad, interoperabilidad y portabilidad de las credenciales digitales, todos ellos requisitos esenciales para un sistema de certificación moderno, robusto y alineado con las necesidades del siglo XXI.

El modelo propuesto por el W3C describe una arquitectura en la cual las credenciales son emitidas en formato digital y están firmadas criptográficamente, lo que permite verificar su autenticidad de forma automática y segura. Este proceso elimina la necesidad de contar con intermediarios centralizados para validar la información, reduciendo la carga operativa de las instituciones educativas y aumentando la confianza en el sistema. Gracias a este enfoque descentralizado, cualquier verificador autorizado (ya sea un empleador, otra universidad o una agencia gubernamental) puede comprobar de manera autónoma si una credencial es legítima, si proviene efectivamente de la UNRN y si ha sido emitida al titular correcto.

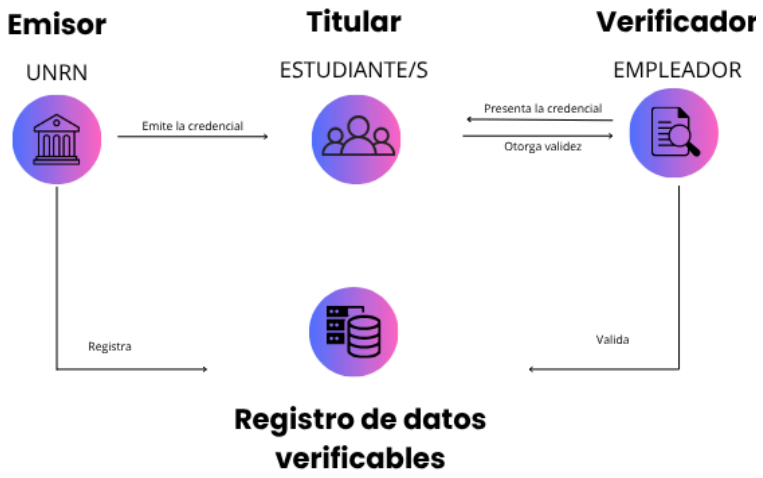
Una de las principales fortalezas del modelo de VCs es que están diseñadas para ser portables: los estudiantes o egresados pueden almacenar sus microcredenciales en billeteras digitales personales, disponibles desde sus dispositivos móviles o

plataformas online, y utilizarlas en distintos contextos a lo largo de su vida académica y profesional. Otro aspecto central del diseño es que están centradas en el usuario: es decir, el titular de la credencial tiene el control total sobre su información y puede decidir en cada caso qué datos compartir, con quién y bajo qué condiciones. Esta capacidad de divulgación selectiva permite proteger la privacidad del estudiante, al tiempo que facilita el intercambio ágil y confiable de información relevante para cada situación.

En el contexto específico de la UNRN, el uso de VCs permite construir una infraestructura tecnológica confiable, automatizable y escalable. Las microcredenciales pueden ser emitidas digitalmente desde las propias plataformas institucionales, almacenadas por los estudiantes en sus billeteras virtuales, y luego presentadas en múltiples escenarios: postulaciones laborales, admisiones a programas académicos, solicitudes ante organismos públicos, entre otros. Este flujo se realiza sin fricciones, y con la posibilidad de integrarse con sistemas externos que también adopten los estándares abiertos del W3C, promoviendo la interoperabilidad a nivel nacional e internacional. La validación puede ser instantánea, segura y transparente, lo que representa una mejora significativa respecto de los procesos tradicionales de verificación manual, lentos y propensos a errores o fraudes.

El proyecto de microcredenciales en la UNRN se apoya también en los desarrollos realizados por el Digital Credentials Consortium (DCC), una iniciativa impulsada por el Massachusetts Institute of Technology (MIT) junto a otras universidades líderes a nivel global. El DCC promueve una arquitectura descentralizada, abierta y basada en estándares internacionales, que ofrece herramientas y marcos de implementación concretos para la gestión de credenciales verificables en el ámbito académico. Al adoptar esta infraestructura, la UNRN no solo garantiza la calidad técnica y la seguridad de su sistema de microcredenciales, sino que también fortalece su proyección internacional, abriendo la posibilidad de integrarse a redes globales de validación y reconocimiento académico y profesional. Este enfoque estratégico coloca a la universidad en una posición de liderazgo regional en la adopción de tecnologías emergentes aplicadas a la educación superior.

6.4. Funcionamiento del Ecosistema VC en la UNRN



Ecosistemas credenciales verificables W3C.

Elaboración propia realizada en Canva

El funcionamiento del ecosistema de credenciales verificables en la Universidad Nacional de Río Negro (UNRN) se basa en el modelo conceptual del "triángulo de confianza" propuesto por el World Wide Web Consortium (W3C), el cual define tres roles fundamentales y bien diferenciados: el emisor, el titular y el verificador. Esta estructura, sustentada por tecnologías criptográficas, permite establecer una red de intercambio de información educativa digital, segura y verificable, sin la necesidad de intermediarios manuales o sistemas centralizados.

En una primera instancia de este ecosistema, la UNRN, a través de sus diferentes unidades académicas o áreas institucionales, asume el rol de emisor. Es decir, la universidad es responsable de crear y emitir las microcredenciales que reflejan competencias específicas, certificaciones de participación, logros académicos o incluso constancias administrativas, como la condición de alumno regular. Cada una de estas credenciales se genera en un formato digital estándar y se firma criptográficamente utilizando la clave privada de la institución, lo que garantiza su autenticidad. Por ejemplo, un estudiante podría recibir un certificado digital titulado

“Certificado de Competencia en Desarrollo Full Stack” o bien una microcredencial que acredite su participación activa en un proyecto interdisciplinario sobre Inteligencia Artificial (IA).

Una vez emitida, la credencial pasa al segundo actor del modelo: el titular. En este caso, el estudiante o egresado que ha obtenido la microcredencial, la recibe y guarda en su billetera digital. A diferencia de los modelos tradicionales de certificación, donde la institución conserva el control sobre el acceso y la verificación de los datos, aquí es el propio estudiante quien administra sus credenciales. Tiene la potestad de decidir en qué momento, con quién y qué parte de su información desea compartir, lo que permite una lógica de divulgación selectiva. Por ejemplo, puede elegir mostrar sólo la credencial relacionada con una competencia técnica cuando aplica a un puesto de trabajo, sin exponer otra información personal o académica irrelevante.

El proceso culmina con el rol del verificador, que puede ser una empresa que busca validar habilidades de un postulante, una universidad que revisa antecedentes para un programa de posgrado, o incluso un organismo estatal que exige documentación académica. El verificador solicita al titular una presentación verificable. Esta presentación es luego verificada automáticamente mediante procesos criptográficos, que permiten confirmar que la información no fue alterada, que fue efectivamente emitida por la UNRN y que corresponde al titular que la presenta. Todo esto ocurre sin necesidad de comunicarse directamente con la universidad ni de realizar trámites presenciales, lo que acelera los procesos de validación y refuerza la confianza entre las partes.

Desde una perspectiva más estructural, el modelo de confianza de las VCs se basa en la eliminación de la autoridad central única. Esto significa que no es necesario que todas las partes se conecten con el emisor para verificar una credencial, sino que cada verificador puede validar por sí mismo la autenticidad e integridad de la información gracias al uso de claves criptográficas y registros descentralizados. Esto simplifica la construcción de confianza, elimina intermediarios y reduce costos asociados a la verificación, permitiendo una validación en tiempo real con mínimo riesgo de error o fraude.

El ecosistema de credenciales verificables implementado por la UNRN representa un cambio paradigmático en la gestión de la información académica. Al combinar descentralización, seguridad y autonomía, se fortalece la confianza institucional y se promueve una relación más transparente entre la universidad, los estudiantes y los diferentes actores sociales. Este modelo no solo optimiza los procesos administrativos, sino que también otorga a los estudiantes un control real sobre su identidad digital y profesional, consolidando un sistema moderno, eficiente y alineado con los estándares internacionales de la educación digital.

6.5. Análisis del Caso de Estudio

El proyecto de microcredenciales de la Licenciatura en Sistemas fue analizado como caso de estudio, destacando la adecuación de la tecnología de Credenciales Verificables del W3C a las necesidades institucionales. La integración del modelo VC ha permitido desarrollar un prototipo funcional que puede escalar a nivel de toda la universidad.

Se han diseñado credenciales de prueba, se han definido flujos de emisión y validación, y se ha trabajado en la compatibilidad con billeteras digitales y protocolos de verificación estándar. Este avance sitúa a la UNRN entre las primeras universidades argentinas en explorar la implementación de credenciales digitales descentralizadas como soporte para su oferta académica.

La incorporación de microcredenciales en el ámbito universitario, y en particular su implementación sustentada por tecnologías como las Credenciales Verificables (VCs), constituye una de las transformaciones más significativas de la educación superior en las últimas décadas. Este fenómeno responde a una realidad en la que el aprendizaje ya no puede circunscribirse a un trayecto formativo cerrado o lineal, sino que debe adaptarse a las exigencias de un mundo laboral cambiante, caracterizado por la innovación constante y la evolución acelerada del conocimiento. Las microcredenciales permiten precisamente eso: reconocer de manera formal, segura y flexible habilidades específicas desarrolladas a través de múltiples experiencias formativas, muchas veces por fuera del plan de estudios tradicional.

A diferencia de los títulos universitarios convencionales, que exigen largos períodos de cursado y que, en ocasiones, no reflejan con precisión las competencias adquiridas, las microcredenciales habilitan la certificación ágil de aprendizajes concretos, como el dominio de un lenguaje de programación, la participación en un proyecto de investigación aplicada, o la capacitación en herramientas tecnológicas emergentes. Algunas microcredenciales pueden incluso acumularse o “apilarse” (stackable), contribuyendo luego a la obtención de certificaciones más amplias o incluso titulaciones oficiales, mientras que otras funcionan de forma independiente, enfocadas en competencias muy puntuales. A su vez, dependiendo del modelo adoptado, pueden otorgar créditos académicos formales o simplemente funcionar como validaciones complementarias.

En este contexto, la tecnología desempeña un rol fundamental. Cada microcredencial puede emitirse de forma digital y firmarse criptográficamente, lo que garantiza que no pueda ser falsificada ni alterada. Esto contribuye directamente a reducir el fraude académico, protegiendo tanto al estudiante como a la institución emisora. Además, al no requerir validación manual, se eliminan procesos administrativos innecesarios, lo cual se traduce en una notable reducción de tiempos y costos.

Por otra parte, las microcredenciales permiten mejorar la calidad y precisión de la información académica. Al ser generadas en formatos estructurados, se facilita la interoperabilidad con diferentes sistemas digitales, tanto dentro como fuera de la universidad. Así, por ejemplo, una credencial emitida por una facultad puede ser fácilmente verificada por otra unidad académica, por un organismo gubernamental o por un empleador del sector privado, sin necesidad de acceder a bases de datos centralizadas o realizar trámites adicionales.

Esta interoperabilidad de borde, como se la denomina, permite que las microcredenciales fluyan entre sistemas institucionales de forma segura y controlada. Al mismo tiempo, el uso de VCs permite que el estudiante sea el verdadero dueño de sus logros, almacenándolos en su propia billetera digital (wallet), y decidiendo en cada caso qué información compartir, con quién y para qué propósito. Esta lógica se inscribe en el modelo de Identidad Digital Auto-Soberana

(SSI), que promueve el empoderamiento del individuo frente al control centralizado de la información.

Desde el punto de vista institucional, su implementación contribuye a fortalecer la integridad académica, al asegurar que toda certificación emitida esté respaldada por estándares verificables y difíciles de falsificar. Esto no solo protege la reputación de la universidad, sino que refuerza la confianza en sus procesos educativos. Además, las VCs, al estar basadas en estándares internacionales abiertos, amplían el horizonte de reconocimiento académico y profesional, haciendo que las competencias certificadas puedan ser aceptadas por instituciones y empleadores de todo el mundo.

Esta visibilidad internacional es clave para fomentar la movilidad académica y la cooperación transnacional. Gracias a iniciativas globales como las impulsadas por el MIT (a través del Digital Credentials Consortium) o por OpenEU en Europa, se avanza hacia un formato común de microcredenciales que facilite el reconocimiento mutuo entre universidades. Esto significa que un estudiante de la UNRN que obtenga una microcredencial podría, por ejemplo, utilizarla para postularse a una maestría en otro país o para validar su participación en un proyecto de innovación con impacto global.

El impacto de las microcredenciales también se observa en términos de empleabilidad. Diversos estudios, como el de *Coursera (2024)*, han demostrado que quienes obtienen microcredenciales tienen más oportunidades de inserción laboral, ya que estas permiten evidenciar habilidades precisas y alineadas con los perfiles requeridos en el mercado. Desde programación y análisis de datos hasta habilidades blandas o conocimientos en normativas específicas, las microcredenciales ofrecen un lenguaje común entre formación académica y mundo laboral.

Asimismo, el diseño modular que habilita el uso de microcredenciales promueve una mayor innovación en la oferta educativa. Las carreras pueden reconfigurar sus planes de estudio en base a rutas flexibles, acumulativas y adaptadas a las demandas del entorno productivo, social o científico. Esto permite construir

currículos más personalizados, ágiles y centrados en el estudiante, capaces de responder con rapidez a contextos en permanente transformación.

Finalmente, la adaptabilidad de este modelo al ámbito universitario es uno de sus grandes puntos fuertes. Cualquier actor puede ocupar los distintos roles del ecosistema (emisor, titular, verificador), incluso dispositivos del Internet de las Cosas (IoT), lo que abre la puerta a escenarios educativos más complejos y dinámicos. En este sentido, la UNRN podría ampliar esta estrategia a otras carreras, niveles y modalidades, generando un sistema universitario más abierto, digital, confiable y centrado en el estudiante.

La Licenciatura en Sistemas de la UNRN, por su perfil tecnológico y experimental, se posiciona así como proyecto piloto y caso de uso ejemplar para el despliegue de microcredenciales con VC. Su implementación inicial puede marcar el rumbo para una transformación institucional más profunda, en sintonía con los estándares internacionales y las necesidades del siglo XXI, consolidando a la UNRN como una universidad pública innovadora, inclusiva y preparada para los desafíos del futuro digital.

7. Conclusiones

El análisis realizado muestra que la implementación de microcredenciales sustentadas en el estándar de Credenciales Verificables (VC) del W3C constituye una estrategia innovadora y altamente pertinente para los desafíos actuales de la educación superior. En un contexto donde los métodos tradicionales de certificación resultan lentos, rígidos y poco adaptables a las demandas del mundo académico y laboral, las microcredenciales ofrecen un modelo ágil, modular y flexible para reconocer aprendizajes específicos y competencias adquiridas en trayectos diversos.

La incorporación de las VCs asegura que estas certificaciones no solo sean seguras, confiables e interoperables, sino también centradas en el usuario, al otorgar al estudiante el control de su información y la posibilidad de decidir qué datos compartir en cada situación. Este enfoque impulsa y fortalece la confianza

institucional, reduce los riesgos de fraude y facilita la verificación instantánea, a la vez que promueve la portabilidad global de credenciales y su reconocimiento en distintos contextos educativos y profesionales.

El caso de la UNRN evidencia que la articulación entre microcredenciales y estándares internacionales como las VCs permite innovar en la forma de acreditar saberes, potenciando la empleabilidad de los egresados, promoviendo trayectorias formativas personalizadas y contribuyendo a la construcción de un ecosistema académico más inclusivo, dinámico y conectado con las necesidades de la sociedad y la economía del conocimiento.

En definitiva, las microcredenciales basadas en credenciales verificables representan un puente entre la universidad y el mundo laboral, una herramienta estratégica para la educación del siglo XXI y un paso decisivo hacia un modelo de aprendizaje permanente, seguro e interoperable, alineado con las transformaciones digitales y sociales contemporáneas.

8. Referencias

Verifiable Credentials Data Model v2.0. (n.d.). www.w3.org. https://bit.ly/3L5dECb

Cambarieri, M., Viadana, C. A., Vivas, L., Rached, S., Jauge, M., Rizzo, A., Leder, J., Gonzalez, F., & Farra, C. (2025). **Microcredenciales en la Licenciatura en Sistemas, una carrera regulada por el Estado y el Rol del estándar W3C en el desarrollo de las Credenciales Verificables.** En *SIE - Simposio de Informática en el Estado (Jornadas Argentinas de Informática - JAIIO)*. Disponible en: https://bit.ly/3L2eqQu

Universidad Nacional de Río Negro. (2025). Resolución CDEyVE N° 004-25. Expediente 523-25 - Microcredenciales. Disponible en: https://bit.ly/47nwb44

Mateo-Berganza Díaz, M. M., Lim, J. R., Cardenas Navia, I., & Elzey, K. (2022). Un mundo en transformación: de las titulaciones tradicionales a las credenciales alternativas basadas en habilidades. https://bit.ly/47l2HE9

Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura (OEI). (2024). Panorama de las microcredenciales en la educación superior de Iberoamérica.
Coursera. (2024). El futuro de las microcredenciales en LATAM: Retos y oportunidades. Recuperado de: https://bit.ly/4ndtdoF

OECD (2021), "Micro-credential innovations in higher education: Who, What and Why?", OECD Education Policy Perspectives, No. 39, OECD Publishing, Paris, https://bit.ly/4ouzFsp

World Wide Web Consortium. (2020). Verifiable Credentials Data Model 1.0. Recuperado de https://bit.ly/4o7Fj49

Ministerio de Justicia y Derechos Humanos de la Nación. (2022). Ciberdelitos en pandemia. https://bit.ly/48KU0oS

Allende López, M. (2020). Identidad digital auto-gestionada: El futuro de la identidad digital: Auto-gestión, billeteras digitales y blockchain. https://bit.ly/48P7v7b

Universidad Nacional del Sur (UNS). (2019). [Noticia institucional sobre actividades académicas]. http://bit.ly/4nlPC3l

Infobae. (2024, 26 de noviembre). Alerta en las empresas de colectivos por los certificados de discapacidad truchos: la decisión que tomará el Gobierno. Recuperado de: http://bit.ly/3J21fhT

Identity.com. (n.d.). What are verifiable credentials? Recuperado de http://bit.ly/4oCvZVH

Brown, J., & Kurzweil, M. (2017). The complex universe of alternative and postsecondary credentials and pathways. American Academy of Arts and Sciences.
(Wikipedia, 2025 es.wikipedia.org).

Consejo de la Unión Europea. (2022, 2 de junio). Propuesta de Recomendación del Consejo relativa a un enfoque europeo de las microcredenciales para el aprendizaje permanente y la empleabilidad (ST 9237/22 INIT). http://bit.ly/4o8zqUi

W3C. (s.f.). World Wide Web Consortium. Recuperado de https://www.w3.org/

W3C Credentials Community Group. (2021, 17 de marzo). Use cases and requirements for decentralized identifiers (W3C Group Note). http://bit.ly/4o75WGo