UNRN Universidad Nacional de Río Negro

Licenciatura en Sistemas

Hacia una estandarización en los certificados digitales

European Learning Model

Autor: Gonzalez, Fernando Gabriel

Director: Cambarieri, Mauro German

Codirector: García Martinez, Nicolás

Viedma, Río Negro

2025

Introducción

En el marco del proceso de transformación digital que atraviesa la educación superior, las universidades enfrentan el desafío de modernizar sus mecanismos de certificación académica, garantizando mayor transparencia, interoperabilidad y reconocimiento internacional.
En este contexto, el presente trabajo final de carrera tiene como propósito analizar el European Learning Model (ELM) y evaluar su viabilidad de aplicación en la Universidad Nacional de Río Negro (UNRN) como modelo de lenguaje y referencia para la emisión de microcredenciales digitales verificables.

El eje central de este trabajo se orienta a comprender cómo la adopción del ELM, junto con las tecnologías y estándares propuestos por el World Wide Web Consortium (W3C), como el RDF (Resource Description Framework), JSON-LD (JavaScript Object Notation for Linked Data) y el modelo de Credenciales Verificables (Verifiable Credentials), puede contribuir a la modernización del proceso institucional de emisión de certificados académicos. La iniciativa busca no solo mejorar la interoperabilidad de los datos educativos, sino también fortalecer la confianza, seguridad y trazabilidad en la validación de títulos, diplomas y certificaciones emitidos por la universidad.

Actualmente, la UNRN, al igual que muchas instituciones argentinas, emite sus certificados y títulos en formatos tradicionales (PDF), con verificación manual y sin el respaldo de estándares internacionales. Esta práctica limita la movilidad académica y profesional de los estudiantes y egresados, además de dificultar la verificación automática de credenciales, generar cargas administrativas adicionales y aumentar el riesgo de fraudes o falsificaciones documentales.
Frente a este panorama, el ELM se presenta como una alternativa innovadora que propone un modelo de datos estandarizado, abierto y semántico, diseñado para describir elementos educativos y profesionales de forma estructurada y multilingüe, facilitando así el intercambio confiable de información entre distintas instituciones y sistemas.

El enfoque modular del ELM, sustentado en el concepto de credenciales verificables, favorece la certificación de trayectorias personalizadas de aprendizaje, el reconocimiento de microcredenciales y la validación del aprendizaje a lo largo de la vida. Su implementación podría representar un avance significativo para la UNRN, alineándola con estándares

internacionales de transparencia educativa y potenciando su integración en redes académicas globales.

Para alcanzar estos objetivos, el trabajo se estructura en una serie de etapas metodológicas. En primer lugar, se realiza una revisión bibliográfica y documental de los estándares propuestos por el W3C y del propio European Learning Model, con el fin de sistematizar los fundamentos teóricos y tecnológicos que los sustentan. Luego, se lleva a cabo un diagnóstico del estado actual de los procesos de emisión de certificados en la UNRN, identificando sus principales limitaciones frente a los nuevos modelos digitales. A partir de este análisis, se desarrolla un diseño conceptual que propone una estructura de datos compatible con el ELM y, posteriormente, se elabora un prototipo funcional capaz de convertir un certificado académico en formato PDF a un documento JSON-LD firmado digitalmente, conforme al modelo de credenciales verificables. Finalmente, se presenta un análisis de viabilidad que evalúa los beneficios, desafíos y posibles implicancias de la adopción del ELM en el contexto institucional, considerando dimensiones técnicas, administrativas y académicas, para concluir con una reflexión crítica y una serie de recomendaciones para su futura implementación.

En síntesis, este trabajo busca contribuir al debate sobre la innovación en la gestión de credenciales académicas dentro del sistema universitario argentino, proponiendo una mirada estratégica y sustentada en estándares internacionales que permita a la Universidad Nacional de Río Negro avanzar hacia una educación más abierta, confiable e interoperable en el escenario digital global.

1. Fundamentos teóricos y tecnológicos del ELM

1.1. ¿Qué es el ELM?

El European Learning Model (ELM) es un modelo de datos estandarizado y de código abierto desarrollado por la Comisión Europea, diseñado para describir de manera estructurada y semánticamente coherente información relacionada con el entorno educativo.

Este modelo actúa como un lenguaje común que permite a instituciones educativas, empleadores y organismos gubernamentales representar y compartir metadatos sobre el aprendizaje de forma interoperable, tanto a nivel nacional como internacional.

El ELM es una evolución del anterior modelo de datos del Marco Europeo de Cualificaciones (EQF) y constituye un componente esencial de iniciativas como Europass, facilitando la transparencia y el reconocimiento de habilidades y credenciales en toda Europa.

1.1.1. ¿Qué problema viene a solucionar?

El ELM viene a solucionar la falta de un lenguaje común y estructurado para describir elementos relacionados con el aprendizaje, las titulaciones, las competencias y la experiencia profesional en el ámbito europeo. Hasta su implementación, existía una gran fragmentación en la forma en que los distintos países, instituciones y plataformas digitales representaban esta información, lo que dificultaba su comprensión, validación y reconocimiento, especialmente a nivel internacional.

Entre los principales problemas que aborda se encuentra la escasa interoperabilidad entre los sistemas educativos y el mercado laboral, que dificultaba el intercambio confiable de datos entre países e instituciones. A esto se sumaban las barreras para el reconocimiento de credenciales académicas y profesionales, un obstáculo que limitaba la movilidad tanto estudiantil como laboral. Asimismo, la lentitud de los procesos manuales de verificación de títulos y competencias generaba una carga administrativa considerable. Finalmente, la falta de estandarización semántica obligaba a traducir y reinterpretar constantemente la información debido a diferencias idiomáticas y de contexto.

En pocas palabras, con el ELM se crea una forma unificada, digital y multilingüe de representar información educativa, lo cual facilita el intercambio de datos, garantiza la interoperabilidad y promueve una mayor transparencia y confianza en los perfiles formativos y profesionales en toda Europa.

1.1.2. ¿Cómo funciona el ELM?

El European Learning Model (ELM) funciona internamente como una ontología general, es decir, una representación semántica que organiza y define de manera precisa conceptos clave vinculados al aprendizaje, las competencias, los resultados formativos y las credenciales académicas o profesionales.
Esta ontología se estructura en cuatro niveles principales. En primer lugar, el modelo de información europeo, que establece las definiciones fundamentales sobre las cuales se construye todo el sistema.
Luego, la ontología del modelo europeo de aprendizaje, que organiza y conecta los distintos conceptos relacionados con la educación y el empleo, generando un marco semántico común. A continuación, los perfiles de aplicación, que especifican reglas particulares para distintos casos de uso, como la descripción de oportunidades de aprendizaje o la emisión de credenciales.
Finalmente, las extensiones, que permiten adaptar el modelo a necesidades concretas de un país, región o sector profesional, asegurando así su flexibilidad y aplicabilidad en diferentes contextos.

Además de esta estructura, el ELM incorpora una serie de componentes esenciales que hacen posible su implementación práctica. Entre ellos se encuentra la Learning Opportunity Specification, que permite describir de manera clara programas educativos, cursos o trayectorias de formación disponibles.
El Learning Outcome se centra en los resultados del aprendizaje, definiendo qué conocimientos, habilidades o competencias debe haber adquirido un estudiante al finalizar una experiencia educativa.
El componente de Qualification representa las credenciales formales obtenidas, tales como diplomas, títulos o certificaciones oficiales. A su vez, el Awarding Body identifica a la institución responsable de otorgar dichas credenciales, garantizando su validez y legitimidad.
Finalmente, el Assessment establece los mecanismos mediante los cuales se verifican y

evalúan los logros alcanzados por los estudiantes, asegurando la confiabilidad del proceso de aprendizaje.

En definitiva, el ELM ofrece una infraestructura semántica y tecnológica robusta que no sólo estandariza la manera en que se representan datos educativos, sino que también posibilita la interoperabilidad entre distintos sistemas, países e instituciones. Gracias a esta arquitectura, se promueve la transparencia, la confianza y el reconocimiento internacional de las credenciales académicas y profesionales, lo cual fortalece la movilidad estudiantil y laboral en un mundo cada vez más globalizado.

1.2. ¿Qué es el W3C?

El W3C (World Wide Web Consortium) es la organización global que define cómo debe funcionar la Web. Establece normas y buenas prácticas para que los contenidos, datos y aplicaciones en línea sean accesibles, seguros, interoperables y sostenibles a largo plazo.

1.2.1. ¿Cómo es el modelo de lenguaje de la W3C?

No existe un “modelo de lenguaje de la W3C” como tal, sino más bien que el W3C establece estándares relacionados con lenguajes y tecnologías web. Desarrolla especificaciones y guías para garantizar que las tecnologías web sean accesibles, interoperables y universales.

Para este caso, el modelo de lenguaje del ELM para credenciales se basa en el estándar de "Verifiable Credentials" (VC), que permite emitir, compartir y verificar credenciales digitales de manera segura y confiable. Este modelo es ampliamente utilizado para representar información verificable, como identificaciones, certificados académicos, licencias, entre otros.

2. El modelo de Verifiable Credentials

2.1. ¿Que es una Credencial Verificable?

Una Credencial Verificable es un documento digital emitido por una entidad confiable que certifica información específica sobre una persona, organización o dispositivo. A diferencia de las credenciales físicas, las credenciales verificables están firmadas

criptográficamente, lo que permite su autenticidad, integridad y verificación automática en entornos digitales.

Estas credenciales pueden representar licencias de conducir, títulos universitarios, identificaciones gubernamentales o cualquier otro documento que acredite una información específica.

Su diseño permite la divulgación selectiva de datos, mejorando la privacidad del usuario y garantizando la confianza en las interacciones en línea. Gracias a tecnologías como las firmas digitales[1] y blockchain, las credenciales verificables ofrecen mayor seguridad y fiabilidad que sus equivalentes físicos, facilitando su uso en la Web de manera interoperable y descentralizada.

2.1.1. Componentes principales:

Credential:

- Es un conjunto de datos que representa una afirmación verificable sobre un sujeto (por ejemplo, "Juan tiene un título universitario").
- Incluye metadatos como el emisor, el sujeto, y la información de la credencial.

Issuer (Emisor):

- Es la entidad que emite la credencial. Puede ser una universidad, una empresa, un gobierno, etc.
- Su firma digital garantiza la autenticidad de la credencial.

Holder (Titular):

- Es la persona o entidad que posee la credencial y puede compartirla con terceros.

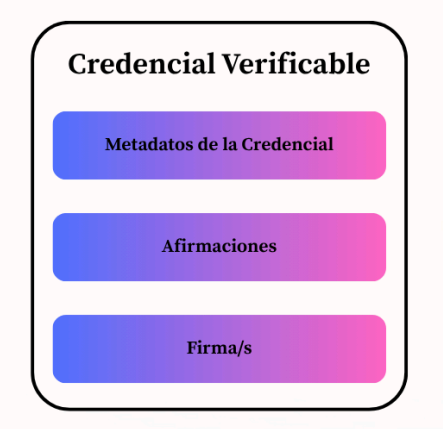
Verifier (Verificador):

- Es la entidad que recibe la credencial y verifica su validez y autenticidad.

[1] Firma Digital: Es una única, auténtica y verificable que permite saber que un documento digital corresponde a una persona determinada.

Proof (Prueba):

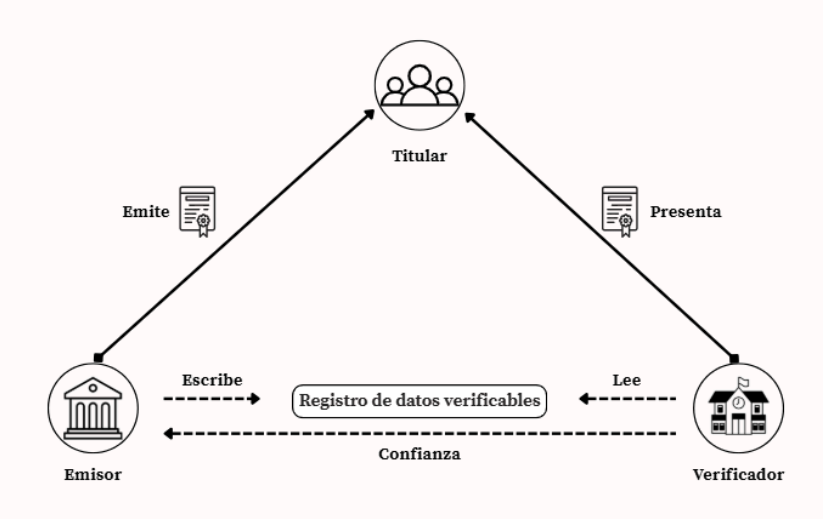
- Es un mecanismo criptográfico (como firmas digitales) que asegura que la credencial no ha sido alterada y que proviene de un emisor confiable.



Componentes de una Credencial Verificable.
Elaboración realizada en napkin

2.2. Sistema de emisión de credenciales

El esquema Holder–Issuer–Verifier describe la dinámica fundamental de las credenciales verificables: el *Issuer* (emisor) crea y firma la credencial, el *Holder* (titular) la recibe y almacena en su billetera digital, y el *Verifier* (verificador) valida su autenticidad e integridad sin necesidad de contactar directamente al emisor.



Ecosistema de credenciales verificables: triángulo de la confianza
Elaboración propia hecha en Canva

2.3. Beneficios del modelo:

Entre los principales beneficios de este modelo se destaca su interoperabilidad, ya que está basado en estándares abiertos que permiten su adopción a nivel global y facilitan el intercambio de credenciales entre diferentes sistemas e instituciones. También aporta mejoras significativas en términos de privacidad, dado que otorga a los usuarios la posibilidad de compartir únicamente la información estrictamente necesaria, como demostrar mayoría de edad sin revelar la fecha exacta de nacimiento. A su vez, garantiza un alto nivel de seguridad al emplear mecanismos criptográficos que preservan la autenticidad y la integridad de las credenciales. Gracias a estas características, el esquema Holder–Issuer–Verifier se posiciona como un pilar en la construcción de identidades digitales descentralizadas, siendo plenamente compatible con tecnologías emergentes como blockchain y los Decentralized Identifiers (DID).

3. ¿Cómo se relaciona el ELM con la W3C?

El European Learning Model (ELM) se relaciona estrechamente con el W3C a través del uso de los estándares abiertos y tecnologías web propuestas por esta organización. En particular, el ELM adopta como base el modelo de datos de Credenciales Verificables del W3C (VC-DM), lo que le permite garantizar que las credenciales educativas digitales emitidas sean interoperables, portables y criptográficamente seguras.

Esta conexión se expresa técnicamente mediante el uso de formatos estandarizados como RDF y JSON-LD, ambos promovidos por el W3C, que permiten representar de forma estructurada y semánticamente rica los datos sobre aprendizaje. Gracias a esto, las credenciales emitidas con ELM pueden ser comprendidas y verificadas automáticamente por diferentes sistemas, sin importar el país o proveedor, fomentando la integración, transparencia y confianza en el ecosistema educativo digital europeo.

Simbología de alianza entre el W3C y ELM

Elaboración propia hecha en Canva

3.1. ¿Qué es JSON-LD?

JavaScript Object Notation for Linked Data (JSON-LD) es un formato estándar del W3C que permite representar datos estructurados y enlazados usando JSON, el formato de datos ampliamente utilizado en aplicaciones web.

Su objetivo es hacer que los datos sean comprensibles tanto para humanos como para máquinas, facilitando su integración en la Web Semántica y el procesamiento automatizado.

Es clave para representar datos interoperables, seguros y verificables en aplicaciones web y sistemas digitales modernos.

3.1.1. ¿Qué lo diferencia del JSON tradicional?

Aunque visualmente es similar al JSON tradicional, JSON-LD agrega significado a los datos utilizando contextos y vocabularios estandarizados. Esto permite que los términos utilizados tengan definiciones precisas y universales, como por ejemplo "name", "date", "issuer", que pueden apuntar a definiciones oficiales como las del W3C o Schema.org.

3.1.2. Ejemplo de una credencial en formato JSON-LD:

En la imagen que sigue se puede ver un ejemplo de una credencial en formato JSON-LD:

```json
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://schema.org"
  ],
  "id": "urn:uuid:123e4567-e89b-12d3-a456-426614174000",
  "type": ["VerifiableCredential", "StudentCredential"],
  "issuer": {
    "id": "https://unrn.edu.ar",
    "name": "Universidad Nacional de Río Negro"
  },
  "issuanceDate": "2025-06-01T00:00:00Z",
  "credentialSubject": {
    "id": "did:example:lucia-gonzalez",
    "givenName": "Lucía",
    "familyName": "González",
    "dni": "12345678",
    "status": "Alumno regular",
    "program": "Licenciatura en Ciencias de la Computación"
  },
  "proof": {
    "type": "Ed25519Signature2018",
    "created": "2025-06-01T00:00:00Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "https://unrn.edu.ar/keys/1",
    "jws": "eyJhbGciOiJFZERTQSJ9..."
  }
}
```

3.2. ¿Qué es el RDF?

El Resource Description Framework (RDF) es un estándar desarrollado por el W3C que permite describir y estructurar datos de manera semántica en la Web. Es uno de los pilares fundamentales de la Web Semántica, cuyo objetivo es que los datos en la Web puedan ser comprendidos y procesados por máquinas, no solo por humanos.

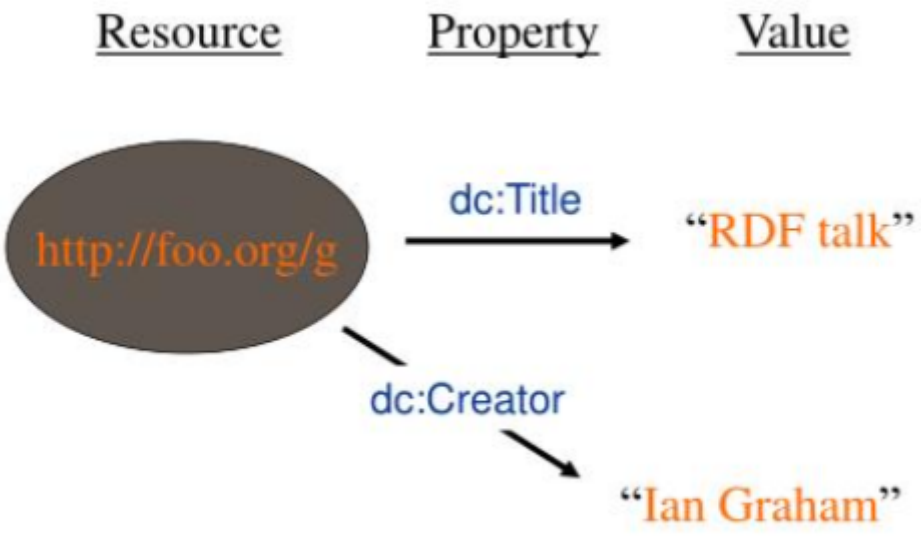
Representa información como tríadas de la forma:
Sujeto - Predicado - Objeto

Sujeto: la cosa de la que se habla (por ejemplo, una persona, documento o curso).

Predicado: la propiedad o característica (por ejemplo, nombre, autor, duración).

Objeto: el valor o entidad relacionada.

Estas tripletas pueden vincular datos entre sí en una red lógica que puede ser leída e interpretada por software.



Ejemplo del modelo RDF

Fuente: https://www.slideserve.com/ownah/an-introduction-to-rdf

Este gráfico muestra la relación establecida entre recursos, propiedades y valores. Las siglas "dc" hacen referencia a Dublin Core: es un conjunto de quince términos de metadatos que pueden utilizarse para describir recursos digitales, como sitios web, libros y artículos.

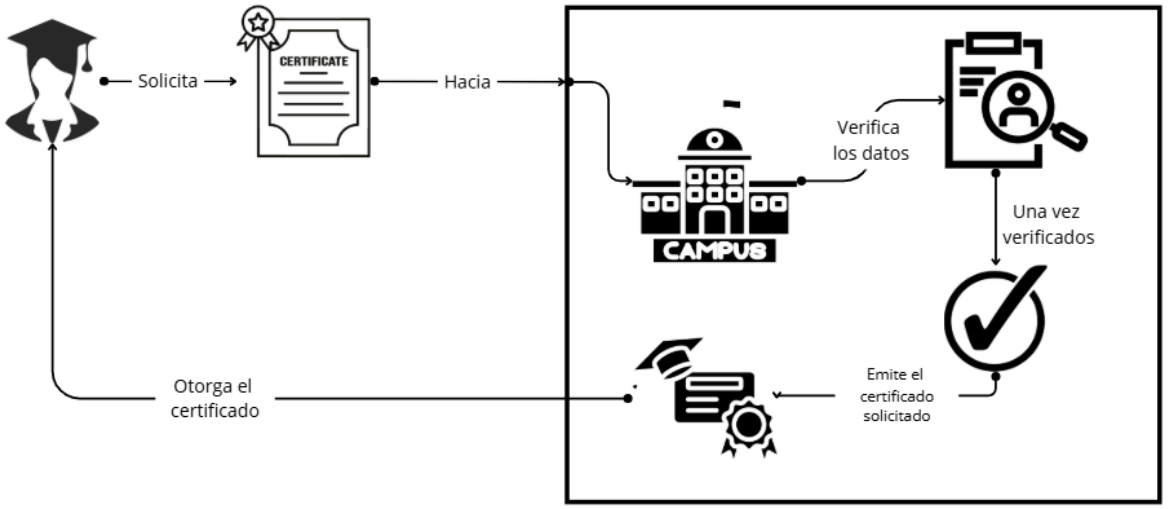
3.3. ¿Cómo se relacionan RDF y JSON-LD?

RDF y JSON-LD están estrechamente relacionados, ya que ambos forman parte del ecosistema de la web semántica promovido por la W3C, básicamente, se podría tratar al RDF como un modelo y al JSON-LD como un formato práctico que adopta dicho modelo y que lo representa en formato JSON.
Por eso, JSON-LD se ha convertido en la opción preferida para representar credenciales verificables, información educativa (como en el ELM) y datos semánticos en la Web moderna.

4. Análisis del estado actual de emisión de certificados en la UNRN

El proceso de emisión de certificados en la Universidad Nacional de Río Negro (UNRN) refleja prácticas tradicionales que combinan procedimientos administrativos manuales y soportes digitales en formato PDF. Este esquema, aunque funcional, presenta limitaciones en términos de eficiencia, seguridad e interoperabilidad. Los tiempos de emisión suelen variar según el tipo de certificado y la carga administrativa, lo que en algunos casos puede generar demoras de días o incluso semanas. En cuanto a la seguridad, la mayoría de los documentos carecen de mecanismos criptográficos avanzados como firmas digitales robustas o identificadores descentralizados, lo que restringe la verificación automática y obliga a depender del contacto directo con la institución para validar la autenticidad.

Además, el sistema actual no contempla de manera integral la automatización del ciclo de vida de los certificados, lo cual impacta en la agilidad de los procesos internos y en la experiencia de los estudiantes y egresados. La interoperabilidad también se ve limitada, ya que los documentos emitidos responden a un contexto local y no están diseñados para integrarse fácilmente con marcos internacionales de reconocimiento académico y profesional. Estos aspectos plantean un escenario donde resulta pertinente reflexionar sobre la adopción de nuevos modelos tecnológicos que puedan mejorar la eficiencia, la seguridad y la portabilidad de las credenciales académicas.



Circuito de emisión de certificados en la UNRN
Elaboración propia hecho en Canva

5. Modelo conceptual para la emisión de certificados con ELM

El modelo conceptual para la emisión de certificados digitales con ELM constituye un paso intermedio y fundamental entre el diagnóstico del estado actual de la UNRN y la posterior implementación de un prototipo tecnológico. Su finalidad es construir una representación abstracta y estructurada que permita comprender cómo deberían organizarse los procesos, actores, datos y relaciones necesarias para emitir certificados académicos bajo un estándar interoperable.

Este esquema conceptual no se centra aún en aspectos técnicos o de programación, sino en definir con claridad qué se emite, quién lo emite, quién lo recibe, bajo qué reglas, y cómo se garantiza la validez y trazabilidad de la información. En este sentido, el modelo busca alinear las prácticas institucionales de la UNRN con el ELM, y con las tecnologías recomendadas por el W3C (JSON-LD, RDF, Verifiable Credentials), con el objetivo de asegurar compatibilidad con los marcos internacionales.

De este modo, el modelo conceptual pretende:

- Representar formalmente los certificados académicos (diplomas, constancias, microcredenciales).
- Estandarizar los datos mínimos necesarios (identidad del estudiante, logro alcanzado, institución emisora, metadatos de validez).
- Definir los actores involucrados y sus roles, desde la universidad hasta los organismos verificadores externos.
- Plantear las relaciones entre dichos elementos, asegurando integridad, confiabilidad y verificabilidad.
- Servir como guía para el desarrollo del prototipo funcional, reduciendo ambigüedades y facilitando la adopción progresiva de la tecnología en la UNRN.

En síntesis, el modelo conceptual busca trasladar el proceso institucional actual de certificación académica a un marco estandarizado, verificable e interoperable, de manera que los certificados emitidos por la universidad sean reconocidos más allá del ámbito local, fortaleciendo la transparencia y la movilidad académica de sus estudiantes y egresados.

5.1. Elementos mínimos del modelo conceptual

Los elementos mínimos de un modelo conceptual son los siguientes:

1. Actores principales
    1.1. Emisor (Issuer): la UNRN como institución responsable de generar y firmar los certificados.
    1.2. Titular (Holder): estudiantes o egresados que reciben y almacenan la credencial digital.
    1.3. Verificador (Verifier): instituciones educativas, empleadores, organismos estatales u otros interesados que validan la credencial.

2. Objetos de certificación
    2.1. Certificados académicos tradicionales: títulos de grado, posgrado, constancias.
    2.2. Microcredenciales: logros parciales, cursos específicos, competencias puntuales.
        2.2.1. Metadatos asociados: fecha de emisión, validez, referencia normativa, identificadores únicos.

3. Estructura de datos (según ELM y W3C)
    3.1. Identificación única del estudiante.
    3.2. Información de la institución emisora.
    3.3. Descripción del logro o competencia alcanzada.
    3.4. Evidencias o resultados que justifican la credencial.
    3.5. Firma digital o mecanismo criptográfico de validación.

4. Relaciones y flujos de información
    4.1. Emisión: el emisor genera el certificado digital y lo entrega al titular.
    4.2. Almacenamiento: el titular conserva la credencial en un monedero digital o repositorio seguro.
    4.3. Verificación: el verificador accede al certificado y valida su autenticidad mediante la infraestructura de credenciales verificables.

5. Dimensiones transversales
    5.1. Interoperabilidad: compatibilidad con estándares internacionales (Verifiable Credentials, JSON-LD, RDF).
    5.2. Seguridad y trazabilidad: mecanismos de firma digital, protección de datos y auditoría.
    5.3. Usabilidad: facilidad de acceso y consulta por parte de estudiantes y empleadores.
    5.4. Escalabilidad: capacidad de extender el modelo a distintas facultades, programas o tipos de credenciales.

6. Desarrollo de un prototipo funcional para emisión de certificados con ELM

El desarrollo de un prototipo funcional constituye una etapa central del proyecto, al permitir trasladar los lineamientos del modelo conceptual a una implementación práctica que demuestre la factibilidad de adoptar el estándar European Learning Model (ELM) en la Universidad Nacional de Río Negro. Este prototipo no busca reemplazar de manera inmediata los sistemas institucionales vigentes, sino actuar como un entorno de experimentación y validación que permita observar el comportamiento real de la solución propuesta.

El prototipo contempla la conversión de certificados académicos tradicionales al modelo de datos definido por el W3C (JSON-LD y RDF), integrando los principios de credenciales verificables (VCs). De esta forma, cada certificado generado posee una representación digital estructurada, interoperable y apta para ser validada por terceros sin depender de verificaciones manuales.

Para garantizar su utilidad, el prototipo se diseñará con las siguientes características:

I. Automatización del proceso de emisión: implementación de un flujo que permita transformar datos de un certificado académico en una credencial digital conforme al ELM.

II. Uso de tecnologías estandarizadas: adopción de JSON-LD, RDF y esquemas de credenciales verificables, asegurando compatibilidad con prácticas internacionales.

III. Simulación de roles: incorporación de los actores principales (emisor, titular y verificador) en entornos controlados, para evaluar la circulación de credenciales desde su emisión hasta su validación.

IV. Interfaz de prueba: desarrollo de un módulo o script que permita visualizar la credencial en formato digital, así como su estructura interna en JSON-LD.

V. Validación de la autenticidad: inclusión de mecanismos criptográficos básicos (firma digital simulada) para mostrar la factibilidad de verificación descentralizada.

De este modo, el prototipo funcional cumple una doble función: por un lado, sirve como prueba de concepto para demostrar que la UNRN puede alinearse a los estándares internacionales de certificación; y por otro, como base técnica sobre la cual se podrán proyectar futuras implementaciones institucionales, más robustas y escalables.

6.1. Aspectos a tener en cuenta:

Al momento de diseñar un prototipo para la conversión de certificados académicos bajo el estándar del European Learning Model, es fundamental considerar ciertos elementos técnicos.
El primero de ellos es la extracción de los datos relevantes desde el PDF, ya que de la calidad de esta información dependerá la precisión de la credencial digital resultante.

Otro aspecto clave es la definición de un contexto JSON-LD (@context), que otorga significado semántico a los datos utilizando vocabularios y URIs estándar. En este punto, se pueden emplear directamente los vocabularios del W3C, incorporar los del ELM o incluso definir un contexto propio adaptado a las necesidades institucionales.
Además, es imprescindible garantizar que los datos se organicen en una estructura compatible con el modelo de Credenciales Verificables del W3C, lo que asegura la interoperabilidad y la posibilidad de verificación automática. Este diseño permitirá que la credencial pueda ser firmada digitalmente, fortaleciendo su validez y seguridad.

6.2. Metodología de trabajo

Para llevar a la práctica estos lineamientos, el proceso puede dividirse en cuatro etapas principales.
En primer lugar, es necesario extraer los datos del PDF: si el documento no está digitalizado se debe utilizar una herramienta de reconocimiento óptico de caracteres (OCR), mientras que si ya se encuentra en formato digital bastará con extraer directamente el texto.
Luego, esos datos deben ser modelados en una estructura JSON-LD, respetando los elementos básicos como el tipo de credencial, el emisor, el sujeto y la fecha de emisión.
A continuación, se debe incorporar el @context y el @type, especificando los vocabularios utilizados y definiendo la credencial como “VerifiableCredential”.
Finalmente, de manera opcional pero altamente recomendable, se puede proceder a firmar digitalmente la credencial mediante herramientas como Digital Bazaar, Veres One, EBSI Wallet o librerías como *vc-js*, lo que garantiza su integridad y verificabilidad automática.

6.3. ¿Qué tecnologías se pueden utilizar para el desarrollo?

Para el desarrollo del prototipo se pueden combinar distintas tecnologías. Por ejemplo, Python resulta muy práctico para realizar prototipos rápidos y conversiones de datos, ya que cuenta con librerías específicas para RDF y JSON-LD. En cambio, Java con Spring Boot puede ser una mejor opción si se busca mayor robustez, integración con la infraestructura institucional de la UNRN y un backend escalable.

Respecto al manejo de datos semánticos, existen varias librerías para RDF y JSON-LD que pueden ser de utilidad. En Python, RDFLib permite trabajar con grafos RDF y exportarlos en distintos formatos, mientras que pyld facilita la gestión de documentos JSON-LD. En el

ecosistema Java, las alternativas incluyen jsonld-java y el framework Apache Jena, este último ideal para RDF, SPARQL y modelos semánticos más avanzados.

Para garantizar la firma digital y el uso de identificadores descentralizados (DID), se pueden considerar herramientas como DIDKit (escrito en Rust, pero con bindings para Python, Java y Node.js), la librería w3c/vc-js en JavaScript para trabajar con credenciales verificables, o incluso frameworks más completos como Hyperledger Aries/Indy, pensados para la gestión de identidades descentralizadas y wallets, aunque su uso podría ser más avanzado en una primera etapa.

En lo referente al almacenamiento de datos, PostgreSQL es una buena opción para mantener registros tradicionales de la universidad y enlazarlos con las credenciales emitidas. Si se prefiere un modelo más flexible para trabajar con JSON-LD, MongoDB ofrece ventajas al no requerir un esquema rígido. Por otro lado, si se desea experimentar con consultas semánticas mediante SPARQL, un triplestore como Apache Fuseki o GraphDB puede complementar la arquitectura.

Para la interfaz y las pruebas, existen herramientas muy útiles como JSON-LD Playground (de la W3C) que permite validar la estructura de las credenciales, así como Postman o Insomnia para testear los endpoints de emisión y verificación. En caso de querer implementar una interfaz sencilla tipo “wallet” para estudiantes o usuarios finales, frameworks como Angular o React pueden facilitar el desarrollo.

Finalmente, dado que la universidad ya maneja certificados en formato PDF, conviene considerar herramientas de automatización y conversión. Por ejemplo, pdfminer.six o PyPDF2 en Python permiten extraer datos de los PDFs existentes, mientras que reportlab es una alternativa eficaz para generar nuevos certificados en PDF, incluyendo la incorporación de códigos QR o enlaces directos a la credencial verificable.

A continuación, se presenta el proceso de extracción, estructuración y firma de los datos que conforman la credencial verificable, a modo de ejemplo ilustrativo del funcionamiento general del sistema. Este desarrollo se implementó mediante un prototipo funcional que demuestra de manera práctica cómo se generan y protegen las credenciales dentro del modelo adoptado.

6.4. Selección de tipo de certificado

Para el desarrollo del prototipo fue necesario seleccionar un tipo de certificado real emitido por la Universidad Nacional de Río Negro con el fin de adaptar el proceso de extracción y estructuración de datos a un caso concreto. Se eligió el certificado correspondiente a la aprobación del curso “Introducción al Aprendizaje Profundo”, el cual se presenta en formato PDF y contiene una serie de campos con estructura relativamente estable: el nombre completo del estudiante, su número de DNI, la denominación exacta del curso, los organismos responsables, el período de cursada, la carga horaria y la disposición administrativa que lo avala.

Sobre esta base, se actualizó el script de extracción para identificar patrones textuales específicos presentes en el documento, tales como la frase “CERTIFICA QUE:” seguida del nombre del estudiante, la referencia explícita al DNI y el nombre del curso encerrado entre comillas. Mediante expresiones regulares adaptadas, el prototipo ahora es capaz de reconocer automáticamente estos elementos dentro del PDF y organizarlos posteriormente en una estructura coherente que servirá como insumo para construir la credencial digital.

Este ajuste permitió demostrar que es posible adaptar el proceso de conversión a distintos tipos de certificados institucionales, incluso cuando contienen textos extensos y formatos administrativos particulares. A partir de esta información extraída, el prototipo genera una credencial siguiendo los lineamientos del ELM y del modelo de Credenciales Verificables del W3C, manteniendo la coherencia semántica necesaria para su verificación automatizada. De esta manera, el caso seleccionado funciona como un ejemplo representativo y evidencia la viabilidad de extender el enfoque hacia otros certificados emitidos por la UNRN en el futuro.

UNRN Universidad Nacional de Río Negro

CERTIFICA QUE: **Fernando González,** DNI: **00000000**

Aprobó el Curso ***"Introducción al Aprendizaje Profundo"***, organizado por el Laboratorio de Informática Aplicada (L.I.A.) y la Dirección de la carrera Licenciatura en Sistemas, con el aval de la Subsecretaría de Extensión de la Sede Atlántica de la UNRN.

Docentes a cargo: Ing. Nicolás Garcia Martinez (docente coordinador), Lic. Patricio Nicolás Castro y Lic. Horacio Munóz Abbate. Coordinación: Ing. Mauro Germán Cambarieri.

Curso realizado en modalidad presencial y virtual entre el 23 de abril y el 23 de junio de 2025, con una carga horaria total de 48 (cuarenta y ocho) horas reloj, en la Sede Atlántica de la Universidad Nacional de Río Negro, en Viedma, Capital de la Provincia de Río Negro. Disposición ATL Nº 541/2025.

Dr. Daniel Barrio
Vicerrector Sede Atlántica
Universidad Nacional de Río Negro

Certificado de aprobación del curso Introducción al Aprendizaje Profundo
Fuente: Certificado del curso Introducción al Aprendizaje Profundo (obtenido por el autor)

6.5. Extraer datos del PDF (ejemplo)

Como primer paso del proceso de conversión hacia una credencial digital verificable, se requiere obtener la información relevante contenida en los certificados académicos emitidos por la universidad. Para ello, se desarrolló un procedimiento automatizado que permite leer y extraer los datos principales desde archivos en formato PDF, como el nombre del estudiante, su número de documento (DNI), la carrera o programa académico cursado y la fecha de emisión del certificado.

Este proceso se lleva a cabo mediante un pequeño programa desarrollado en Python, un lenguaje de programación ampliamente utilizado por su simplicidad y capacidad para el tratamiento de texto y datos. En términos generales, el programa abre el archivo PDF, recorre todas sus páginas y extrae el texto que contiene, buscando dentro de él los campos relevantes mediante patrones definidos (por ejemplo, palabras como "Nombre", "DNI", "Carrera" o "Fecha de emisión").

Una vez identificados esos datos, el sistema los organiza en una estructura ordenada, asignando cada uno a su respectiva categoría (por ejemplo, "nombre del estudiante" o

“fecha de emisión”), de modo que puedan ser utilizados posteriormente para generar una credencial digital en formato estructurado (como JSON-LD, según el estándar del ELM).

En síntesis, este procedimiento automatiza una tarea que, de realizarse manualmente, resultaría lenta y propensa a errores, permitiendo transformar certificados en papel o PDF tradicionales en fuentes de datos reutilizables y verificables, adecuadas para su integración en sistemas de credenciales digitales.

6.6. Mapear a estructura ELM / VC

Una vez obtenidos los datos desde el certificado en formato PDF, el siguiente paso consiste en estructurarlos siguiendo los lineamientos del ELM y del estándar de Credenciales Verificables definido por el W3C.

Para ello, se elaboró un procedimiento que transforma la información extraída, como el nombre del estudiante, el número de documento, la carrera y la fecha de emisión, en el formato digital estructurado llamado JSON-LD .

El proceso comienza generando un identificador único para cada credencial, garantizando que ninguna sea igual a otra. Luego, se incorporan los metadatos fundamentales: el contexto semántico (que define el significado de los datos), la identidad de la institución emisora (en este caso, la Universidad Nacional de Río Negro), la fecha de emisión y los datos del estudiante que recibe la credencial.

El resultado final es una representación digital del certificado académico que cumple con los estándares internacionales de interoperabilidad y verificabilidad, permitiendo su posterior firma digital y verificación automatizada por parte de otras instituciones o empleadores. En otras palabras, este paso convierte la información contenida en un documento tradicional en una credencial digital verificable, lista para integrarse a ecosistemas de reconocimiento académico y profesional más amplios.

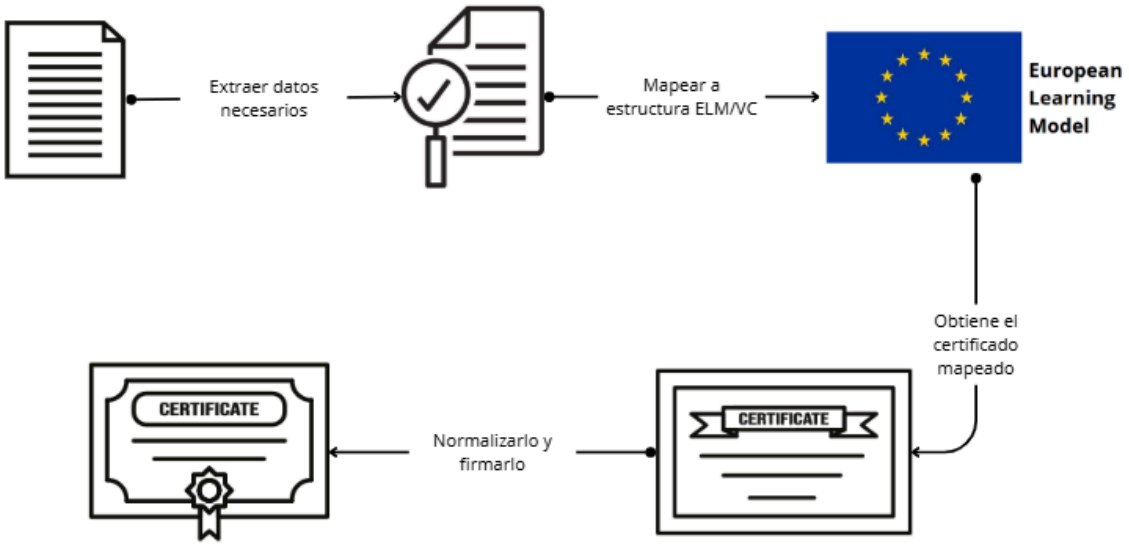
6.7. Normalizar JSON-LD y firmar (crear proof)

Una vez estructurada la credencial en formato JSON-LD, es necesario garantizar su integridad y autenticidad antes de su emisión. Para ello, el sistema implementa un proceso de normalización y firma digital, siguiendo las buenas prácticas recomendadas por el W3C para el manejo de credenciales verificables.

En primer lugar, se aplica un proceso denominado “normalización canónica” (basado en el algoritmo URDNA2015), cuyo propósito es transformar el documento JSON-LD en una representación estandarizada y única. Esta etapa es fundamental, ya que asegura que cualquier modificación, incluso mínima, en la estructura o el contenido del documento sea detectada posteriormente al momento de su verificación. De este modo, se garantiza que la credencial mantenga su integridad a lo largo del tiempo y en diferentes contextos de uso.

Posteriormente, sobre este documento normalizado, se realiza la firma digital de la credencial. Este proceso emplea un método criptográfico de tipo JSON Web Signature (JWS), que genera un código único llamado token. Dicho token se incorpora al documento dentro de un campo denominado proof, el cual contiene además información relevante como el tipo de firma, la fecha de creación, el propósito de la prueba y la clave pública del emisor utilizada para la verificación.

El resultado de esta operación es una credencial digitalmente firmada, que puede ser verificada por cualquier tercero sin necesidad de depender del sistema original que la emitió. Esto garantiza tanto la autenticidad del emisor (la Universidad Nacional de Río Negro) como la no alteración de los datos del estudiante, permitiendo su uso en entornos interoperables, seguros y confiables.



Circuito representativo de conversión de un certificado a ELM

Elaboración propia hecha en Canva

El producto del presente trabajo final es el prototipo funcional descrito anteriormente, que permite observar de forma integral las etapas de creación, normalización y firma de una credencial verificable.
Para una descripción más detallada y técnica de la implementación, incluyendo el código fuente y su explicación paso a paso, se recomienda consultar el Anexo 1.

7. Riesgos y posibles mitigaciones

La implementación de un sistema de emisión de certificados digitales con estándares como el European Learning Model (ELM) implica una serie de riesgos que deben ser previstos desde el inicio. Entre los principales riesgos técnicos se encuentran la compatibilidad con el estándar en sí, dado que su evolución constante puede invalidar implementaciones obsoletas, y la interoperabilidad con otras instituciones, donde errores en los metadatos podrían generar incompatibilidades en la validación de certificados. Asimismo, la integración con los sistemas actuales de la universidad (SIU, SIGE, entre otros) puede generar problemas de duplicidad o inconsistencias si no se gestiona correctamente la sincronización. Para mitigar estos riesgos, resulta clave utilizar bibliotecas oficiales y actualizadas, realizar pruebas de validación automáticas contra los esquemas de referencia, implementar validaciones cruzadas de interoperabilidad y diseñar una capa intermedia de integración que desacople al prototipo de los sistemas existentes.

En cuanto a los riesgos de seguridad, la falsificación o alteración de certificados es una amenaza central si no se aplican mecanismos de firma digital. A ello se suma la posible exposición de datos personales sensibles como, por ejemplo, nombre, DNI o carrera, y la gestión inadecuada de llaves criptográficas, que podría comprometer la integridad de todo el sistema. Para reducir estas vulnerabilidades, se recomienda firmar los certificados con estándares robustos (X.509, PKI nacional o institucional), garantizar cifrado tanto en tránsito como en almacenamiento, aplicar controles de acceso estrictos por roles y emplear sistemas seguros de gestión de claves, como módulos HSM o servicios de Key Management en la nube.

Otro aspecto a considerar son los riesgos de adopción institucional. Puede existir resistencia al cambio por parte del personal administrativo, habituado a los certificados en papel, así como desconfianza por parte de estudiantes y empleadores respecto al valor y legitimidad del nuevo formato digital. Para facilitar la transición, es recomendable ofrecer capacitaciones, manuales claros y un período híbrido que combine papel y digital, además de implementar estrategias de comunicación que destaquen los beneficios del modelo,

incluyendo campañas institucionales, demostraciones en ferias o acuerdos con empresas que validen estas credenciales.

También deben contemplarse los riesgos legales y regulatorios. En Argentina, aún pueden existir vacíos legales sobre la equivalencia plena de certificados digitales frente a los emitidos en papel. Asimismo, la protección de datos personales regulada por la Ley 25.326 (Habeas Data) implica un cumplimiento estricto para evitar sanciones o pérdida de confianza. Para mitigar estos riesgos, es fundamental realizar consultas con asesoría legal, respaldarse en la Ley de Firma Digital vigente y en convenios internacionales, además de diseñar el sistema bajo principios de minimización de datos, consentimiento informado, auditorías periódicas y políticas claras de retención de información.

Finalmente, aparecen riesgos vinculados a la sostenibilidad tecnológica. Una mala elección de frameworks o la dependencia excesiva de proveedores externos puede volver el sistema obsoleto o inservible en el mediano plazo. Por ello, se recomienda optar por tecnologías abiertas y con comunidades activas de soporte (por ejemplo, Spring Boot, Angular o Node.js), trabajar con estándares abiertos como JSON-LD y OAuth2, y diseñar una arquitectura modular que permita reemplazar fácilmente componentes externos sin afectar la continuidad del sistema

8. Conclusión: Beneficios, desafíos y viabilidad de la implementación

8.1. ¿Sería beneficioso aplicarlo en la Universidad Nacional de Río Negro?

La adopción del European Learning Model (ELM) podría traer importantes beneficios para una universidad como la Universidad Nacional de Río Negro (UNRN). En primer lugar, favorecería la interoperabilidad, ya que la información sobre programas de estudio, cualificaciones y credenciales emitidas sería comprensible y compatible con otros sistemas e instituciones. Esto permitiría simplificar el intercambio de datos con universidades, organizaciones educativas y empleadores, fortaleciendo la integración de la UNRN en un ecosistema académico más amplio.

Asimismo, el uso de un estándar reconocido internacionalmente aportaría una mayor visibilidad global, posicionando a la universidad en un nivel de mayor atractivo para

estudiantes y académicos extranjeros. La oferta educativa de la UNRN sería más accesible y fácilmente comparable con la de otras instituciones, incrementando su competitividad en el plano internacional.

Otro aspecto clave reside en la facilitación del reconocimiento de credenciales. Implementar el ELM simplificaría que los títulos y certificados emitidos por la UNRN sean reconocidos en el extranjero, lo cual beneficiaría directamente a los egresados interesados en continuar sus estudios o insertarse laboralmente fuera del país. Al mismo tiempo, haría más ágil el reconocimiento de credenciales extranjeras para aquellos estudiantes que deseen realizar sus trayectorias académicas en la universidad.

En esta misma línea, la transparencia en la descripción de cursos y cualificaciones abriría nuevas oportunidades para la movilidad estudiantil y académica, favoreciendo los programas de intercambio tanto de estudiantes como de profesores, y fortaleciendo la experiencia internacional que puede ofrecer la institución.

El ELM también constituye una herramienta clave para el desarrollo de credenciales digitales verificables, lo que permitiría a la UNRN emitir diplomas, certificados y otros documentos de manera electrónica, segura y fácilmente verificable. Esto no solo reduciría el riesgo de fraude, sino que también optimizaría los procesos administrativos.

A nivel interno, la implementación del modelo redundaría en una mejor gestión de la información académica, gracias a una estructura más organizada y eficiente de los datos vinculados a la oferta educativa, los resultados de aprendizaje y las credenciales emitidas. Esta modernización se complementaría con una alineación con estándares internacionales, lo que reforzaría el compromiso de la UNRN con la transparencia y la calidad en la educación superior.

Finalmente, adoptar el ELM abriría un potencial de colaboración con otras instituciones que también lo implementen, facilitando la creación de programas conjuntos, el intercambio de buenas prácticas y la consolidación de redes académicas.

En conjunto, estos beneficios evidencian que la incorporación del ELM no solo modernizaría los procesos de certificación de la UNRN, sino que también la proyectaría hacia una mayor integración internacional, fortaleciendo su prestigio y ampliando las oportunidades para su comunidad académica.

8.2. Desafíos para adoptar el ELM en la UNRN

La adopción de un modelo como el European Learning Model (ELM) en la Universidad Nacional de Río Negro presenta una serie de desafíos que deben ser cuidadosamente considerados. Uno de los principales se relaciona con la interoperabilidad de los sistemas actuales, ya que la universidad cuenta con plataformas administrativas y académicas propias, como la gestión de alumnos, expedientes y títulos, que no fueron diseñadas bajo estándares como RDF o JSON-LD. Esto implicaría la necesidad de adaptar o integrar dichas herramientas con nuevas arquitecturas capaces de soportar el modelo.

En paralelo, surgen exigencias vinculadas a la infraestructura tecnológica, dado que la implementación de credenciales digitales verificables requiere servidores especializados, repositorios seguros, registros públicos confiables y billeteras digitales para los estudiantes. En la actualidad, los certificados suelen emitirse como archivos PDF simples, lo que evidencia la necesidad de una transición hacia un esquema mucho más robusto y escalable.

Otro aspecto clave es la capacitación y la cultura organizacional. Tanto docentes como personal administrativo y técnico deberían adquirir competencias en estándares semánticos, identificadores descentralizados (DID), JSON-LD, blockchain y mecanismos de verificación digital. Este proceso se enfrenta al desafío cultural de superar la tradición del papel y los documentos PDF en favor de credenciales electrónicas verificables, un cambio que suele generar resistencia en instituciones educativas consolidadas.

En el plano normativo, la adopción del ELM debería contemplar el marco legal vigente, ya que en Argentina la validez de títulos y certificados se encuentra regulada por el Ministerio de Educación y organismos de acreditación. Sería necesario, por tanto, trabajar en adecuaciones legales que permitan reconocer oficialmente las credenciales emitidas bajo este modelo tanto en el ámbito nacional como internacional.

La seguridad y la confianza también representan un pilar esencial. La universidad tendría que garantizar la validez de las firmas digitales criptográficas, la correcta administración de claves privadas y la integridad de los datos, lo cual requiere políticas claras de ciberseguridad y un sistema de gestión de identidad digital sólido.

A ello se suma la necesidad de asegurar la compatibilidad internacional y local. Aunque el ELM está concebido en el contexto europeo, sería indispensable adaptarlo al marco argentino, teniendo en cuenta los marcos de cualificación, la terminología administrativa y

las regulaciones nacionales. Incluso, existe el riesgo de que se generen incompatibilidades con sistemas de educación superior de América Latina que todavía no adoptan estos estándares.

Por otro lado, se deben considerar los costos de implementación, que abarcan desde el desarrollo de prototipos y la capacitación hasta la integración de sistemas y el mantenimiento de la infraestructura. En una universidad pública, la disponibilidad de financiamiento puede convertirse en una barrera importante para llevar adelante este tipo de transformaciones.

Finalmente, la gestión del cambio para estudiantes y empleadores se presenta como un reto adicional. Los estudiantes tendrían que familiarizarse con el uso de billeteras digitales para administrar sus credenciales, mientras que los empleadores locales deberían contar con herramientas que les permitan verificar automáticamente la validez de los documentos. Esto implica un esfuerzo de difusión y de adopción que trasciende los límites de la propia universidad.

8.3. ¿Es viable adoptar un modelo como el ELM en el entorno de la UNRN?

La viabilidad de implementar un modelo estandarizado de credenciales digitales en una universidad como la UNRN depende de una combinación de factores tecnológicos, organizacionales y normativos. Si bien la adopción de este tipo de modelos ofrece claros beneficios en términos de interoperabilidad, transparencia, automatización y reconocimiento internacional de credenciales, su puesta en marcha requiere superar desafíos relacionados con la infraestructura tecnológica, la adecuación a los marcos legales nacionales y la capacitación del personal.

En este sentido, la viabilidad no puede considerarse absoluta, sino gradual: es factible avanzar mediante proyectos piloto y prototipos que permitan evaluar el impacto, identificar barreras y ajustar los procesos internos antes de una implementación a gran escala.

Bibliografía

RDF and XML tutorial (2019). Recuperado de: http://bit.ly/4nvFtkC

Hernandez, Margarita (S. F.) Las ventajas del Resource Description Framework: RDF. Recuperado de: https://acortar.link/svs6qj

An Introduction to RDF (2024). Recuperado de: https://acortar.link/uUBvXU

Gonzalez, Fernando (2025). Análisis sobre Modelos de Lenguajes para Microcredenciales. Informe final sobre Practica Profesional Supervisada: https://acortar.link/Vk2PQw

Europass. (s.f.). *European Learning Model for Stakeholders*. Recuperado el 19 de agosto de 2025, de https://europass.europa.eu/es/node/2128

European Commission. (s.f.). *European Learning Model Browser*. Recuperado el 19 de agosto de 2025, de https://europa.eu/europass/elm-browser/index.html

Europass. (s.f.). *Credenciales digitales europeas para el aprendizaje*. Recuperado el 19 de agosto de 2025, de https://europass.europa.eu/es/european-digital-credentials-learning

World Wide Web Consortium (W3C). (1999, 22 de febrero). *Resource Description Framework (RDF) Model and Syntax Specification* (W3C Recommendation). Recuperado el 19 de agosto de 2025, de https://www.w3.org/TR/1999/REC-rdf-syntax-19990222/ W3C

World Wide Web Consortium (W3C). (2020, 16 de julio). *JSON-LD 1.1: A JSON-based Serialization for Linked Data* (W3C Recommendation). Recuperado el 19 de agosto de 2025, de https://www.w3.org/TR/json-ld11/ W3C+1

Anexo 1: Implementación técnica del prototipo de credenciales verificables

El presente anexo tiene como objetivo describir en detalle los aspectos técnicos del prototipo desarrollado para la generación de credenciales verificables bajo el modelo del European Learning Model (ELM).

En las secciones siguientes se presentan los fragmentos de código implementados, junto con una explicación técnica sobre su funcionamiento, las librerías empleadas y las decisiones de diseño adoptadas.

Cada etapa corresponde a un componente clave del flujo de trabajo: extracción de datos, estructuración según el modelo ELM, y firma digital de la credencial.

Este anexo está destinado a lectores con formación técnica o interés en los aspectos informáticos del proyecto, complementando la descripción conceptual presentada en el cuerpo principal del informe.

Librerías Utilizadas

A continuación se mostraran el conjunto de librerías utilizadas en el desarrollo del prototipo:

```
import uuid, json, re, pdfplumber
from datetime import datetime
from pyld import jsonld
from jose import jws
import sys
import requests
```

Document Loader personalizado para JSON-LD

El prototipo incorpora un document loader personalizado para PyLD, necesario para resolver correctamente los contextos JSON-LD externos que se referencian mediante URLs. Por defecto, la librería PyLD podría bloquear ciertas solicitudes o no manejar adecuadamente documentos remotos. Para evitarlo, se implementó la función requests_document_loader, que utiliza la biblioteca requests para recuperar el contexto remoto y devolverlo en el formato requerido por PyLD.

Código:

```
def requests_document_loader(url, options=None):
    r = requests.get(url)
    r.raise_for_status()
    return {
        "contextUrl": None,
        "documentUrl": url,
        "document": r.json()
    }

jsonld.set_document_loader(requests_document_loader)
```

Este componente garantiza que los contextos utilizados, como por ejemplo, el contexto de las Credenciales Verificables o el de Schema.org, puedan ser descargados, interpretados y normalizados correctamente durante el proceso de canonicalización. Sin este módulo, el algoritmo URDNA2015 podría fallar o producir resultados inconsistentes.

Extraer datos del PDF

El primer paso del flujo técnico consiste en obtener los datos relevantes del certificado académico real.

Código:

```
def extract_fields(pdf_path):
    text = ""
    with pdfplumber.open(pdf_path) as doc:
        for p in doc.pages:
            page_text = p.extract_text()
            if page_text:
                text += page_text + "\n"

    m_nombre = re.search(r"CERTIFICA QUE:\s*([A-Za-zÁÉÍÓÚÑáéíóúñ\s]+),\s*DNI", text)
    m_dni = re.search(r"DNI:\s*(\d+)", text)
    m_curso = re.search(r"Curso\s*[“\"](.+?)[”\"]", text)

    return {
        "nombre": m_nombre.group(1).strip() if m_nombre else "",
        "dni": m_dni.group(1).strip() if m_dni else "",
        "programa": m_curso.group(1).strip() if m_curso else "Curso aprobado",
        "fecha_emision": ""
    }
```

Para ello, se utiliza la librería pdfplumber, la cual permite leer el contenido textual del PDF página por página. Una vez obtenido el texto completo, se aplican expresiones regulares diseñadas específicamente para este tipo de certificado emitido por la UNRN.

```
def extract_fields(pdf_path):
    text = ""
    with pdfplumber.open(pdf_path) as doc:
        for p in doc.pages:
            page_text = p.extract_text()
            if page_text:
                text += page_text + "\n"
```

El script busca patrones textuales característicos del documento:

- Nombre del estudiante: aparece inmediatamente después de la frase *"CERTIFICA QUE:"* y antes de la palabra *"DNI"*.

```
m_nombre = re.search(r"CERTIFICA QUE:\s*([A-Za-zÁÉÍÓÚÑáéíóúñ\s]+),\s*DNI", text)
```

- Número de DNI: detectado mediante la palabra clave *"DNI:"* seguida de una secuencia numérica.

```
m_dni = re.search(r"DNI:\s*(\d+)", text)
```

- Nombre del curso: aparece dentro de comillas rectas o comillas tipográficas (“ ”).

```
m_curso = re.search(r"Curso\s*[“\"](.+?)[”\"]", text)
```

El uso de estas expresiones hace que el prototipo esté adecuadamente adaptado al formato real del certificado, garantizando la extracción precisa de la información requerida.
El resultado se devuelve como un diccionario que servirá para construir la credencial JSON-LD:

```
return {
    "nombre": m_nombre.group(1).strip() if m_nombre else "",
    "dni": m_dni.group(1).strip() if m_dni else "",
    "programa": m_curso.group(1).strip() if m_curso else "Curso aprobado",
    "fecha_emision": ""
}
```

Este diseño permite extender el método para incorporar otros campos adicionales en el futuro.

Mapear a estructura ELM / VC

En esta fase, los datos extraídos se integran en un modelo estructurado compatible con las Credenciales Verificables y el ELM, empleando el formato JSON-LD.

Código:

```
def build_jsonld(datos):
    issuanceDate = datos.get("fecha_emision") or datetime.utcnow().date().isoformat()

    nombre = datos["nombre"]
    partes = nombre.split()
    given = partes[0]
    family = " ".join(partes[1:])

    credential = {
        "@context": [
            "https://www.w3.org/2018/credentials/v1",
            "https://schema.org/docs/jsonldcontext.json"
        ],
        "id": f"urn:uuid:{uuid.uuid4()}",
        "type": ["VerifiableCredential", "TrainingCertificate"],
        "issuer": {
            "id": "https://unrn.edu.ar",
            "name": "Universidad Nacional de Río Negro"
        },
        "issuanceDate": f"{issuanceDate}T00:00:00Z",
        "credentialSubject": {
            "id": f"did:example:{datos['dni']}",
            "givenName": given,
            "familyName": family,
            "dni": datos["dni"],
            "courseName": datos["programa"],
            "status": "Curso aprobado",
            "academicYear": "2025"
        }
    }
    return credential
```

@context: contiene las referencias necesarias para interpretar semánticamente la credencial. En este caso se incluyen:

- el contexto oficial de Verifiable Credentials,
- el contexto de Schema.org, útil para describir atributos comunes.

```
"@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://schema.org/docs/jsonldcontext.json"
],
```

id: se genera un UUID único por cada credencial usando la librería uuid.

```
"id": f"urn:uuid:{uuid.uuid4()}",
```

issuer: identifica a la UNRN como entidad emisora mediante una URL.

```
"issuer": {
    "id": "https://unrn.edu.ar",
    "name": "Universidad Nacional de Río Negro"
},
```

credentialSubject: contiene los datos de la persona titular, incluyendo:

- Nombre
- Apellido
- DNI
- Nombre del curso aprobado.

```
"credentialSubject": {
    "id": f"did:example:{datos['dni']}",
    "givenName": given,
    "familyName": family,
    "dni": datos["dni"],
    "courseName": datos["programa"],
    "status": "Curso aprobado",
    "academicYear": "2025"
}
```

El prototipo clasifica este documento como:

```
"type": ["VerifiableCredential", "TrainingCertificate"],
```

Lo cual indica que se trata de una credencial verificable de tipo certificado de formación.
La credencial generada está lista para ser firmada digitalmente.

Normalizar JSON-LD y firmar (crear proof)

La última etapa consiste en normalizar el documento JSON-LD y firmarlo digitalmente para garantizar su autenticidad e integridad.

Código:

```
def canonicalize(jsonld_doc):
    normalized = jsonld.normalize(
        jsonld_doc,
        {'algorithm': 'URDNA2015', 'format': 'application/n-quads'}
    )
    return normalized


def sign_credential(credential, key='secret-demo-key'):
    normalized = canonicalize(credential)
    token = jws.sign(normalized.encode('utf-8'), key, algorithm='HS256')

    proof = {
        "type": "LinkedDataSignature",
        "created": credential["issuanceDate"],
        "proofPurpose": "assertionMethod",
        "verificationMethod": "https://unrn.edu.ar/keys/1",
        "jws": token
    }

    credential["proof"] = proof
    return credential
```

Antes de firmar la credencial, es necesario convertir el documento JSON-LD en una representación canónica mediante el algoritmo URDNA2015, requerido por las firmas de Linked Data.

```
def canonicalize(jsonld_doc):
    normalized = jsonld.normalize(
        jsonld_doc,
        {'algorithm': 'URDNA2015', 'format': 'application/n-quads'}
    )
    return normalized
```

Este paso asegura que:

- La credencial tiene una estructura determinística.
- Cualquier modificación en sus datos pueda detectarse fácilmente, todos los verificadores obtengan exactamente la misma representación canónica.

Es un paso crítico para garantizar la integridad de la credencial.

Finalmente, la función sign_credential

```
def sign_credential(credential, key='secret-demo-key'):
    normalized = canonicalize(credential)
    token = jws.sign(normalized.encode('utf-8'), key, algorithm='HS256')

    proof = {
        "type": "LinkedDataSignature",
        "created": credential["issuanceDate"],
        "proofPurpose": "assertionMethod",
        "verificationMethod": "https://unrn.edu.ar/keys/1",
        "jws": token
    }

    credential["proof"] = proof
    return credential
```

Realiza la firma digital utilizando JSON Web Signatures (JWS).

```
token = jws.sign(normalized.encode('utf-8'), key, algorithm='HS256')
```

El resultado se incrusta dentro de un campo proof, que contiene:

- El tipo de firma.
- La fecha de creación.
- El método de verificación (una clave pública asociada a la UNRN).
- El token criptográfico resultante.

```
proof = {
    "type": "LinkedDataSignature",
    "created": credential["issuanceDate"],
    "proofPurpose": "assertionMethod",
    "verificationMethod": "https://unrn.edu.ar/keys/1",
    "jws": token
}
```

Esto produce finalmente una credencial completamente firmada y lista para ser verificada por terceros sin necesidad de contactar a la institución emisora.

```
credential["proof"] = proof
return credential
```

Flujo Completo

El bloque final del código integra todo el proceso

Código:

```
if __name__ == "__main__":
    ruta_pdf = sys.argv[1] if len(sys.argv) > 1 else "ejemplo_certificado.pdf"

    print("Extrayendo datos del PDF...")
    datos = extract_fields(ruta_pdf)
    print("Datos extraídos:", datos)

    print("\nConstruyendo la credencial JSON-LD...")
    cred = build_jsonld(datos)

    print("\nFirmando la credencial...")
    cred_firmada = sign_credential(cred)

    with open("credencial_firmada.json", "w", encoding="utf-8") as f:
        json.dump(cred_firmada, f, ensure_ascii=False, indent=4)

    print("\n¡Proceso completo!")
    print("Archivo generado: credencial_firmada.json")
```

1. Lectura de la ruta del PDF.

```
ruta_pdf = sys.argv[1] if len(sys.argv) > 1 else "ejemplo_certificado.pdf"
```

2. Extracción automatizada de datos.

```
print("Extrayendo datos del PDF...")
datos = extract_fields(ruta_pdf)
print("Datos extraídos:", datos)
```

3. Construcción de la credencial JSON-LD.

```
print("\nConstruyendo la credencial JSON-LD...")
cred = build_jsonld(datos)
```

4. Canonicalización y firma digital.

```
print("\nFirmando la credencial...")
cred_firmada = sign_credential(cred)
```

5. Guardado en un archivo credencial_firmada.json.

```
with open("credencial_firmada.json", "w", encoding="utf-8") as f:
    json.dump(cred_firmada, f, ensure_ascii=False, indent=4)

print("\n¡Proceso completo!")
print("Archivo generado: credencial_firmada.json")
```

Conclusión del anexo

La implementación presentada en este anexo demuestra la factibilidad técnica de generar credenciales verificables estandarizadas, aplicando los lineamientos del ELM y las recomendaciones del W3C.
El flujo completo, extracción, estructuración y firma, puede adaptarse fácilmente a distintos tipos de certificados académicos.

Este desarrollo constituye una base funcional para futuras ampliaciones, tales como la integración con sistemas de gestión institucional, validación descentralizada o publicación en redes de confianza académica.

Para la visualización completa del código fuente utilizado en este prototipo, se encuentra disponible el repositorio correspondiente en el siguiente enlace: https://bit.ly/3Mb64GI