



D6.1 Reporte de Recomendaciones Generales para la Implementación del Modelo de Centros de Emisión de Credenciales Digitales en las IEFP

T6.4 Desarrollo de documento de recomendaciones generales

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

D6.1 Reporte de Recomendaciones Generales para la Implementación del Modelo de Centros de Emisión de Credenciales Digitales en las IEFP

Título del documento	Reporte de Recomendaciones Generales para la Implementación del Modelo de Centros de Emisión de Credenciales Digitales en las IEFP	
Work package	WP6	
Fecha comienzo/fecha de finalización	02 de febrero 2024 / 30 de enero 2026	
Responsable WP	UC3M	
Entregable (título y número)	D6.1 Reporte de Recomendaciones Generales para la Implementación del Modelo de Centros de Emisión de Credenciales Digitales en las IEFP	
Fecha Límite	31 de julio 2026	
Autores	Alberto Jimenez, Carlos Alario Hoyos	
Colaboradores	Carlos Delgado Kloos	
Socios involucrados	UC3M, UG, KINAL, TUG	
Versión	1.0	
Estatus	Borrador ☐	Final ☒

Tabla de Contenido

Resumen ejecutivo	4
1. Introducción	5
1.1 Contexto del proyecto ECOCredGT	6
1.2 Objetivos del documento	7
2. Marco conceptual y tecnológico	9
2.1 Taxonomía y tipología de las credenciales digitales en el IEPF	10
2.2 Estándares internacionales de interoperabilidad	11
2.3 Seguridad, verificabilidad y tecnología mediante tecnología Blockchain	12
2.4 Marco ético y protección de datos	13
3. Recomendaciones para la infraestructura tecnológica	14
3.1 Modelos de gestión	15
3.2 Estrategias de integración con plataformas LMS y sistemas de gestión académica	16
3.3 Arquitectura técnica y protocolos de seguridad de los datos	16
4. Gobernanza y estructura organizativa del centro de emisión	18
4.1 Modelo operativo de centros de emisión para las IEPF	18
4.2 Definición de roles estratégicos, técnicos y académicos	19
4.3 Flujos de trabajo: diseño, emisión y de validación	20
5. Estrategia de formación, recursos humanos y gestión del cambio	22
5.1 El Plan de formación multinivel para adopción institucional.	22
5.2 Sensibilización y vinculación con el sector empresarial	23
5.3 Vigilancia tecnológica y actualización continua de competencias docentes	24
6. Aseguramiento de la calidad, sostenibilidad y mejora continua	26
6.1 Marco de calidad ECOCredGT.	26
6.2 Indicadores de impacto y métricas de éxito en la empleabilidad.	27
6.3 Hoja de ruta para la sostenibilidad técnica y financiera del ecosistema.	28
6.4 El papel del Observatorio ECOCredGT	29
7. Conclusiones y recomendaciones	31
7.1 Recomendaciones	31
7.2 Guía de replicabilidad para otras IEPF en la región	32
Referencias	34

Resumen ejecutivo

El presente entregable documenta y establece las recomendaciones generales para poner en marcha centros de emisión de credenciales digitales en las instituciones de educación y formación profesional (IEFP) que forman parte del proyecto ECOCredGT. El informe corresponde al paquete de trabajo 6 (WP6) y responde a una necesidad de ofrecer a los centros una guía que les ayude a revisar sus procesos de certificación académica y a adaptarlos a un contexto en el que las competencias, la empleabilidad y el reconocimiento de aprendizajes requieren formatos más flexibles y verificables.

El informe no se limita a describir una solución tecnológica. A partir de la revisión del estado del arte y de la experiencia obtenida en los pilotos locales, se identifican los aspectos que las instituciones deben preparar antes de adoptar este modelo. Entre ellos están la infraestructura técnica, la organización interna, la formación de los equipos implicados y los mecanismos de calidad que deben acompañar la emisión de credenciales.

Una conclusión importante del informe es que las credenciales digitales no pueden considerarse una simple sustitución del certificado tradicional. La transición de un documento en papel a un archivo digital es solo una parte del proceso. Lo relevante es definir cómo se diseñan las credenciales, quién las valida, con base en qué criterios se emiten y cómo pueden ser reconocidas por otros agentes, especialmente por el sector productivo. Por esta razón, el informe recomienda utilizar estándares abiertos de interoperabilidad, como Open Badges y el Modelo Europeo de Aprendizaje, así como soluciones que refuercen la integridad de los registros y la protección de la información.

El modelo propuesto también requiere ordenar la toma de decisiones dentro de cada institución. Para ello, se plantea una gobernanza híbrida, con responsabilidades diferenciadas en los niveles estratégico, técnico y académico. Esta organización permite que el profesorado mantenga un papel activo en el diseño académico de las credenciales, pero dentro de un proceso común de validación, seguimiento y control administrativo. De este modo se reducen los riesgos de fragmentación y se facilita que las credenciales emitidas respondan a criterios institucionales compartidos.

Otro componente del entregable se refiere a las capacidades necesarias para implementar el modelo. La puesta en marcha de centros de emisión exige que los equipos comprendan tanto el sentido académico de las microcredenciales como los procedimientos técnicos asociados a su emisión y verificación. Por ello, se proponen acciones de formación dirigidas a distintos perfiles de la comunidad educativa. También se incluyen orientaciones para reforzar la relación con empresas y empleadores, ya que su participación será clave para que las credenciales tengan utilidad más allá del ámbito institucional.

El informe también aborda la sostenibilidad del modelo. Las instituciones deberán prever cómo mantener la infraestructura, cómo actualizar los procesos y cómo asignar responsabilidades una vez finalizada la fase piloto. En este sentido, se recomienda vincular la oferta de credenciales digitales con el seguimiento de indicadores de empleabilidad. Esta información permitirá, con el tiempo, valorar si las insignias contribuyen a mejorar la visibilidad de las competencias adquiridas y su reconocimiento en las trayectorias profesionales de los graduados.

En resumen, el WP6 proporciona una base sobre la que las instituciones pueden avanzar en la implementación de centros de emisión de microcredenciales digitales con criterios comunes. El Observatorio ECOCredGT se plantea como un espacio de apoyo para recopilar aprendizajes, hacer un seguimiento del modelo y facilitar futuras acciones de réplica en otros contextos de Latinoamérica.

1. Introducción

El proyecto ECOCredGT parte de una necesidad a la que se enfrentan muchas instituciones de educación y formación profesional. Los certificados tradicionales siguen siendo necesarios, pero a veces no permiten mostrar con suficiente detalle qué sabe hacer una persona, qué competencias ha desarrollado ni cómo pueden ser verificados esos aprendizajes por terceros. Esta situación se hace más patente cuando la formación busca responder a perfiles laborales concretos y a cambios rápidos en el sector productivo.

Las credenciales digitales ofrecen una forma de atender esta necesidad. No sustituyen por sí solas a los títulos ni resuelven todos los problemas de reconocimiento, pero sí permiten describir los aprendizajes de manera más clara y verificable. También facilitan que una competencia pueda compartirse con empleadores, instituciones educativas u otros interesados, sin depender únicamente de documentos generales o de procesos manuales de verificación.

Para las instituciones de educación y formación profesional (IIEFP), la adopción de este tipo de credenciales no debe entenderse solo como un cambio tecnológico. Cambiar el formato del certificado es solo una parte del proceso. Lo más importante es revisar cómo se definen las competencias, qué evidencias las respaldan, quién participa en su validación y qué condiciones deben cumplirse para que una credencial tenga valor dentro y fuera de la institución.

Este proceso exige cierto orden institucional. Si cada programa, área o equipo docente emite credenciales con criterios distintos, el modelo puede perder coherencia y resultar difícil de mantener. Por ello, además de contar con herramientas digitales, las IIEFP necesitan procedimientos comunes, responsabilidades claras y mecanismos de calidad que acompañen todo el ciclo de emisión. Esta es una condición básica para que las credenciales sean útiles y puedan ser reconocidas por agentes externos.

En el marco del proyecto ECOCredGT, esta tarea se organiza a través de los Centros de Emisión de Credenciales Digitales. Estos centros se conciben como unidades de coordinación dentro de las IIEFP. Su función es apoyar a los equipos académicos y técnicos en el diseño, la emisión, la validación y el seguimiento de las credenciales digitales. También ayudan a organizar la relación entre las áreas responsables de la calidad, la gestión académica y la infraestructura tecnológica.

La creación de estos centros busca evitar que la emisión de credenciales se limite a iniciativas aisladas o a decisiones tomadas caso por caso. Es posible que haya buenas experiencias piloto en una institución, pero estas no siempre se convierten en procesos estables. Para que el modelo avance, es necesario definir quién toma las decisiones, cómo se revisan las credenciales antes de emitirlas, qué estándares se utilizan y cómo se mantiene la información actualizada.

La puesta en marcha de un Centro de Emisión de Credenciales Digitales requiere abordar cuestiones prácticas que no pueden dejarse para el final. Las instituciones deben revisar la infraestructura disponible, formar a los equipos implicados, adaptar algunos flujos de trabajo y garantizar la interoperabilidad de las credenciales con marcos reconocidos. También deben prever cómo se dará seguimiento al modelo una vez finalizada la fase piloto, especialmente si se espera que las credenciales formen parte estable de la oferta formativa.

Este documento se ha elaborado dentro del paquete de trabajo 6, dedicado al aseguramiento de la calidad del proyecto. Su propósito es reunir recomendaciones que ayuden a las instituciones participantes a implementar los centros de emisión con criterios compartidos. No pretende imponer un único modelo de organización para todas las IIEFP, sino ofrecer una base común que cada

institución pueda adaptar a su realidad manteniendo unos criterios mínimos de calidad, trazabilidad y sostenibilidad.

Las recomendaciones se basan en el trabajo realizado en etapas anteriores del proyecto. En particular, se toma como referencia el modelo de emisión de credenciales desarrollado en el documento D3.1, liderado por la Universidad Galileo y la Fundación Kinal. A partir de este documento y de la experiencia acumulada durante los pilotos locales, este documento recoge elementos que pueden orientar la aplicación del modelo en condiciones reales.

La introducción del WP6 sitúa el alcance del informe y la razón de las recomendaciones que se presentan en los capítulos siguientes. El objetivo final es apoyar a las IEFP en la creación de procesos de certificación digital claros, verificables y sostenibles que puedan servir de base para acciones futuras de réplica en otros contextos de Latinoamérica.

1.1 Contexto del proyecto ECOCredGT

El proyecto ECOCredGT se desarrolla con la cofinanciación de la Unión Europea a través del programa Erasmus+, en la línea de Construcción de Capacidades en Educación y Formación Profesional. El proyecto trabaja con instituciones de educación y formación profesional de Guatemala para avanzar en el uso de credenciales digitales en sus procesos de certificación. Esta línea de trabajo responde a la necesidad identificada por las instituciones participantes de reconocer mejor las competencias adquiridas por los estudiantes y hacerlas más visibles para el sector productivo.

Las credenciales digitales permiten describir aprendizajes que a menudo no se detallan suficientemente en los certificados tradicionales. Esto resulta especialmente útil en la formación profesional, ya que muchas competencias están directamente relacionadas con tareas, perfiles ocupacionales o necesidades concretas de las empresas. El proyecto no plantea este cambio como una simple digitalización de documentos. La adopción de credenciales digitales requiere revisar los procesos internos, acordar criterios comunes y contar con equipos capaces de mantener la modelo una vez finalizada la fase piloto.

El consorcio reúne instituciones europeas y guatemaltecas con funciones complementarias. La Universidad Carlos III de Madrid (España) y la Universidad Tecnológica de Graz (Austria) aportan experiencia en tecnologías educativas, estándares digitales y metodologías relacionadas con las microcredenciales. Por su parte, la Universidad Galileo y la Fundación Kinal conocen el contexto local y han participado directamente en la aplicación del modelo en Guatemala. Esta combinación ha permitido revisar las propuestas técnicas a partir de condiciones reales de implementación.

El proyecto se ha desarrollado mediante paquetes de trabajo interconectados. En las primeras fases, se revisó el contexto de partida a través del estado del arte recogido en el documento D2.1 y del autodiagnóstico institucional incluido en el documento D2.2. Estos documentos permitieron identificar las necesidades tecnológicas, formativas y organizativas. Sobre esa base, se diseñó el plan de formación multinivel presentado en el documento D3.2 y se organizaron los talleres multisectoriales recogidos en el documento D4.1.

Estas actividades ayudaron a preparar al personal docente, administrativo y directivo para participar en el proceso de adopción de credenciales digitales.

Uno de los resultados principales fue el modelo de centro de emisión de credenciales digitales, desarrollado en el D3.1, en el que la Universidad Galileo y la Fundación Kinal tuvieron una

participación especialmente relevante, tanto por su conocimiento del contexto guatemalteco como por su implicación en la preparación de los pilotos. Posteriormente, los proyectos piloto descritos en el D3.3 sirvieron para probar la infraestructura, los flujos de validación y la organización propuesta. La experiencia obtenida en esa etapa es una de las bases en las que se han elaborado las recomendaciones de este informe.

El control de calidad ha estado presente durante todo el proceso, no solo al finalizar el proyecto. El Paquete de Trabajo 6 ha permitido revisar la coherencia entre los objetivos previstos, las actividades realizadas y los productos elaborados por el consorcio. También ha servido para introducir ajustes en momentos clave, especialmente en la formación, la preparación de los pilotos y las acciones de diseminación previstas en el D7.1, por lo que la calidad se entiende en este documento como una tarea de seguimiento continuo y no únicamente como una validación final.

Este informe se sitúa en la fase de cierre de ese proceso de revisión. Tras analizar el contexto, formar a los equipos, diseñar el modelo y desarrollar los pilotos, era necesario recopilar en un solo documento las recomendaciones que pueden orientar la implementación de centros de emisión en otras IEFP. El resultado es una guía de trabajo basada en la experiencia del proyecto, con orientaciones pensadas para apoyar la continuidad del modelo en Guatemala y su posible adaptación a otros contextos latinoamericanos.

1.2 Objetivos del documento

El objetivo principal de este documento es presentar recomendaciones para implementar centros de emisión de credenciales digitales en instituciones de educación y formación profesional. El informe está dirigido a equipos directivos, responsables tecnológicos, personal académico y unidades de calidad que puedan participar en este tipo de procesos. No propone una única forma de organización para todas las instituciones. Más bien, ofrece criterios de referencia para que cada institución pueda adaptar el modelo a su realidad manteniendo condiciones básicas de calidad, trazabilidad y sostenibilidad.

El documento también cumple una función en la gestión del proyecto. Al formar parte del paquete de trabajo 6, dedicado al control de calidad, recoge evidencias y aprendizajes que ayudan a valorar cómo se ha desarrollado el modelo y qué aspectos deben tenerse en cuenta para garantizar su continuidad. De esta manera, el informe contribuye al cierre del WP6 y muestra cómo se han revisado las actividades del proyecto a lo largo de su ejecución.

Otro de sus propósitos es ordenar el conocimiento generado por los socios guatemaltecos, en especial la Universidad Galileo y la Fundación Kinal. El informe se basa en el modelo presentado en el D3.1 y en los resultados de los pilotos incluidos en el D3.3, y a partir de estos elementos se formulan recomendaciones que pueden resultar útiles para otras instituciones interesadas en adoptar credenciales digitales. Dichas recomendaciones tienen en cuenta aspectos técnicos, organizativos y culturales, ya que la implementación no depende únicamente de la tecnología utilizada.

El documento organiza las recomendaciones en varios ejes de trabajo para facilitar su uso por parte de las IEFP. En él se abordan cuestiones relacionadas con el marco conceptual, la infraestructura tecnológica, la interoperabilidad, la seguridad de la información, la gobernanza, los flujos de trabajo, la formación de los equipos y la gestión del cambio. Esta organización permite que cada área institucional identifique con mayor claridad qué aspectos debe revisar y qué responsabilidades puede asumir durante la implementación.

Otro objetivo es apoyar la sostenibilidad del modelo una vez finalizada la fase piloto. Para ello, el informe plantea criterios de seguimiento e indicadores que pueden ayudar a las instituciones a mantener activos sus centros de emisión. También se considera importante vincular las credenciales digitales con información sobre empleabilidad y reconocimiento externo. Esta relación permitirá valorar, con el tiempo, si las credenciales aportan beneficios concretos a estudiantes, graduados e instituciones.

Por último, el documento sentará las bases para el trabajo futuro del Observatorio ECOcredGT. Este espacio puede contribuir al seguimiento del modelo, la actualización de recomendaciones y el intercambio de experiencias entre instituciones. Desde esta perspectiva, el documento no solo pone fin a una actividad del proyecto, sino que recopila conocimientos que podrán aprovecharse en futuras acciones de réplica, adaptación y mejora en educación y formación profesional.

2. Marco conceptual y tecnológico

La creación de un modelo de credenciales digitales en las instituciones de educación y formación profesional (IEFP) requiere algo más que digitalizar certificados en papel. Una credencial digital debe permitir describir un aprendizaje, vincularlo con pruebas, facilitar su verificación y ofrecer información comprensible a quienes la consulten. Por ello, el marco conceptual y tecnológico del proyecto ECOcredGT se centra en definir criterios que ayuden a las instituciones a emitir credenciales claras, verificables y útiles para estudiantes, empleadores y otras entidades educativas.

Este marco también permite ordenar decisiones que no son únicamente técnicas. Las IEFP deben revisar cómo describen los resultados del aprendizaje, qué información acompaña a cada credencial, qué estándares se utilizan y qué responsabilidades asume cada área institucional. Si estos elementos no se definen desde el principio, la emisión de credenciales digitales puede quedarse en un simple cambio de formato, sin aportar una mejora real en los procesos de reconocimiento.

La infraestructura tecnológica del modelo se apoya en varias capas de trabajo. Entre ellas se encuentran la definición de competencias, la estructura de los metadatos, la interoperabilidad entre plataformas, la seguridad de la información y los mecanismos de verificación. Todas estas capas deben funcionar de manera coordinada para que una credencial emitida por una IEFP pueda ser leída, comprendida y validada en otros entornos. Este aspecto es especialmente importante si se quiere que el modelo tenga continuidad más allá de los pilotos locales.

Para que el modelo pueda replicarse en otras instituciones, es necesario mantener una relación clara entre pedagogía y tecnología. Una taxonomía bien diseñada pierde su valor si no puede comunicarse mediante estándares reconocidos. Del mismo modo, un estándar técnico es insuficiente si no se vincula con criterios académicos y procedimientos de calidad claros. Por esta razón, el capítulo presenta los elementos conceptuales y tecnológicos en los que se basan las recomendaciones operativas del informe.

La arquitectura propuesta debe entenderse como un sistema abierto, capaz de adaptarse a los cambios tecnológicos y a las nuevas necesidades formativas. La incorporación de estándares de interoperabilidad, credenciales verificables e identidades digitales descentralizadas hace que las IEFP puedan trabajar con soluciones menos dependientes de plataformas cerradas. Esto facilita la movilidad de los estudiantes y aumenta la probabilidad de que sus logros sean reconocidos por diferentes entidades.

El uso de tecnologías digitales en los procesos de certificación también exige tener en cuenta aspectos éticos. La información educativa contiene datos sensibles que deben tratarse con criterios de privacidad, transparencia y control por parte del titular. En el enfoque de ECOcredGT, la tecnología debe apoyar el reconocimiento de los aprendizajes sin reducir la autonomía de los estudiantes ni aumentar el riesgo de exclusión. Por este motivo, la protección de datos y la soberanía del usuario forman parte del marco conceptual del modelo.

Este capítulo establece la base sobre la que se desarrollan las recomendaciones de los apartados siguientes. La taxonomía, los estándares, la seguridad y la protección de datos no se presentan como elementos separados, sino como componentes que deben funcionar de manera coherente. Esta coherencia es necesaria para que los centros de emisión puedan operar con criterios de calidad, sostenibilidad e interoperabilidad.

2.1 Taxonomía y tipología de las credenciales digitales en el IIEFP

La taxonomía de credenciales digitales permite organizar el sistema de reconocimiento dentro de las IIEFP. En el marco de ECOCredGT, esta taxonomía ayuda a descomponer los programas formativos en unidades más específicas que pueden certificarse mediante microcredenciales. Esta organización facilita que las instituciones identifiquen competencias concretas, habilidades técnicas y aprendizajes transversales que a veces quedan poco visibles dentro de un certificado general.

Definir una taxonomía no consiste solo en clasificar credenciales. También implica precisar qué se certifica, con qué evidencias, bajo qué criterios y para qué finalidad. Esta claridad aumenta el valor informativo de la credencial, ya que permite a un empleador, a otra institución educativa o al propio estudiante comprender mejor el alcance de lo que se ha certificado. En la formación profesional, esta precisión es especialmente útil, ya que muchas competencias están vinculadas con tareas y perfiles ocupacionales específicos.

En esta organización, es necesario distinguir diferentes tipos de credenciales según su propósito y nivel de exigencia. Algunas pueden registrar la participación en una actividad formativa, mientras que otras deben certificar el logro de una competencia evaluada según criterios establecidos. Esta diferenciación ayuda a los centros emisores a gestionar una oferta más ordenada y evita que todas las credenciales tengan el mismo peso o significado.

Un elemento importante del modelo es la posibilidad de acumular microcredenciales. El trabajo desarrollado por la Universidad Galileo y la Fundación Kinal plantea que las microcredenciales funcionen como unidades que el estudiante va reuniendo a lo largo del tiempo. En determinados casos, varias microcredenciales pueden integrarse en una certificación de mayor alcance o ser reconocidas dentro de trayectorias formativas más amplias. Esta flexibilidad resulta útil para las personas que necesitan actualizar competencias sin tener que completar necesariamente programas largos.

Cada credencial debe incluir metadatos suficientes para explicar su significado. Estos metadatos pueden describir los resultados de aprendizaje, los criterios de evaluación, el nivel de cualificación, la entidad emisora y las evidencias asociadas al logro. Cuando esta información se presenta de forma clara y estandarizada, la credencial deja de ser una imagen o un archivo aislado para convertirse en una evidencia verificable del aprendizaje alcanzado.

La taxonomía también debe relacionarse con las necesidades del sector productivo. Para ello, las credenciales pueden vincularse con ocupaciones, competencias o marcos de referencia reconocidos, como ESCO u otros modelos adaptados al contexto latinoamericano. Esta relación ayuda a acercar el lenguaje de la formación al del empleo. También permite que las IIEFP comuniquen mejor el valor de sus programas y de las competencias desarrolladas por sus estudiantes.

La tipología de credenciales no debe ser fija desde el principio. Los centros emisores deberán revisarla periódicamente, especialmente cuando surjan nuevas necesidades formativas, cambios tecnológicos o modalidades de aprendizaje no formal. Una taxonomía bien mantenida permite organizar el catálogo institucional, orientar a los estudiantes y facilitar a los empleadores la interpretación del valor de cada credencial.

2.2 Estándares internacionales de interoperabilidad

La interoperabilidad permite que diferentes sistemas puedan intercambiar información y utilizarla correctamente. En el caso de ECOcredGT, esto significa que una credencial emitida por una IIEFP puede visualizarse, almacenarse y verificarse en plataformas compatibles dentro y fuera del país. Para conseguirlo, el modelo debe basarse en estándares abiertos que reduzcan la fragmentación tecnológica y eviten la dependencia excesiva de proveedores específicos.

El uso de estándares es una condición importante para que las credenciales digitales tengan valor más allá de la institución que las emite. Sin una estructura común, cada plataforma podría interpretar los datos de forma distinta, lo que dificultaría la movilidad académica y profesional de los estudiantes. Por tanto, la interoperabilidad no debe considerarse un detalle técnico secundario, sino un requisito para garantizar la calidad y la sostenibilidad del modelo.

Uno de los estándares relevantes para el proyecto es Open Badges, especialmente en su evolución hacia la versión 3.0. Este estándar define la estructura de la información de una insignia digital y facilita que pueda ser almacenada y compartida por el estudiante en carteras o plataformas compatibles. Su uso permite que la credencial no dependa únicamente del sistema interno de una institución, sino que pueda acompañar al titular en diferentes contextos educativos y laborales.

El European Learning Model también ofrece una referencia útil para describir aprendizajes, cualificaciones y resultados formativos con una estructura común. Alinearse con este tipo de modelos ayuda a mejorar la transparencia de las credenciales y facilita su comparación con otras ofertas formativas. En un proyecto Erasmus+, esta conexión es relevante porque fomenta el diálogo con marcos europeos y con prácticas ya utilizadas en procesos de reconocimiento educativo.

El modelo también tiene en cuenta las credenciales verificables del W3C. Este estándar permite expresar credenciales en Internet de forma legible para máquinas y con mecanismos criptográficos de verificación. Su adopción puede facilitar los procesos en los que un tercero necesite comprobar la validez de una credencial sin tener que realizar trámites manuales con la institución emisora. Esto puede resultar útil para empleadores, plataformas de empleo o sistemas de gestión del talento.

La interoperabilidad también está relacionada con la identidad digital. Los identificadores descentralizados permiten asociar credenciales con titulares e instituciones de una manera verificable, sin depender de una única autoridad central. Este enfoque puede fortalecer el control del estudiante sobre sus credenciales y reducir los riesgos relacionados con la suplantación de identidad o la pérdida de acceso a los registros institucionales. Para las IIEFP, estos elementos deben analizarse junto con sus capacidades técnicas y sus políticas de protección de datos.

La adopción de estándares como Open Badges, ELM y W3C VC facilita la replicabilidad del modelo de centros de emisión. También permite que las recomendaciones desarrolladas por el proyecto sean compatibles con sistemas internacionales y con futuras actualizaciones tecnológicas. En este sentido, la interoperabilidad es una condición práctica para que las credenciales de ECOcredGT puedan circular y ser reconocidas en distintos contextos.

2.3 Seguridad, verificabilidad y tecnología mediante tecnología Blockchain

La confianza es un elemento central en cualquier sistema de certificación. En un entorno digital, esta confianza depende de la posibilidad de verificar que una credencial ha sido emitida por una institución autorizada, que no ha sido modificada y que corresponde a su titular. El proyecto ECOCredGT considera el uso de la tecnología blockchain como una opción para reforzar esta capa de seguridad y trazabilidad en los centros de emisión.

La tecnología blockchain puede funcionar como un registro distribuido en el que se almacena una prueba de la existencia y validez de una credencial. En la práctica, no es necesario guardar todos los datos personales en la cadena. Lo más habitual es registrar una huella criptográfica que permita comprobar si la credencial presentada coincide con la emitida originalmente. Este mecanismo ayuda a detectar modificaciones posteriores y reduce la necesidad de realizar verificaciones manuales.

Desde el punto de vista técnico, la seguridad se basa en algoritmos criptográficos que generan una huella única para cada credencial. Si se alteran datos como el nombre del titular, la fecha o la competencia certificada, la huella deja de coincidir con el registro original. Esta verificación permite identificar posibles manipulaciones y protege tanto al estudiante como a la institución emisora. También puede reducir los tiempos de comprobación para terceros autorizados.

La verificabilidad es una de las principales ventajas del modelo. En los procesos tradicionales, un empleador o una institución pueden necesitar contactar directamente con la entidad emisora para confirmar la validez de un certificado. Con un sistema basado en credenciales verificables, esta comprobación puede realizarse de forma más rápida, siempre que existan herramientas adecuadas y reglas claras de acceso. Esto facilita el uso de las credenciales en procesos de selección, movilidad académica o reconocimiento de competencias.

La tecnología blockchain también puede aportar resiliencia al sistema. Los registros académicos gestionados únicamente en bases de datos internas pueden verse afectados por cambios institucionales, errores, ciberataques o problemas de conservación a largo plazo. Un esquema distribuido puede ayudar a mantener pruebas de validez aunque cambien las plataformas utilizadas por la institución. No obstante, su implementación debe planificarse con cuidado, teniendo en cuenta los costes, el mantenimiento, la gobernanza técnica y la sostenibilidad.

El modelo debe evitar almacenar información personal sensible en redes públicas o entornos que no garanticen un control suficiente. Se recomienda trabajar con arquitecturas que separen los datos personales de las pruebas criptográficas de validez. De esta forma, los centros emisores pueden combinar la transparencia necesaria para verificar una credencial con la protección de la privacidad exigida por la normativa aplicable.

La adopción de la tecnología blockchain no debe presentarse como un fin en sí mismo. Su valor depende de si resuelve necesidades concretas de verificación, trazabilidad y confianza. Para las IIEFP, lo importante es que la tecnología elegida sea comprensible, sostenible y compatible con los estándares definidos por el modelo. En este sentido, la tecnología blockchain puede ser una herramienta útil siempre que se integre en una arquitectura más amplia de seguridad, gobernanza y protección de datos.

2.4 Marco ético y protección de datos

La implementación de centros de emisión de credenciales digitales también plantea responsabilidades éticas. La información educativa incluye datos personales, pruebas de aprendizaje y registros que pueden influir en la trayectoria académica y profesional de una persona. Por ello, el modelo de ECOCredGT debe garantizar que estos datos se gestionen conforme a criterios de privacidad, transparencia, proporcionalidad y control por parte del interesado.

Un principio importante es que el estudiante debe poder tomar decisiones sobre el uso de sus credenciales. La Identidad Soberana, conocida como SSI por sus siglas en inglés, se basa en la idea de que la persona pueda conservar, gestionar y compartir sus credenciales desde una cartera digital. Esto no elimina el papel de la institución emisora, pero sí modifica la relación tradicional en la que todos los registros quedan bajo el control exclusivo de la entidad educativa. El objetivo es que el estudiante pueda utilizar sus credenciales sin perder la autonomía sobre su información.

El diseño del sistema debe incorporar la privacidad desde el principio. Esto implica aplicar el principio de minimización de datos y registrar únicamente la información necesaria para emitir, validar y verificar la credencial. También se deben incluir mecanismos claros de consentimiento informado para que el estudiante sepa qué datos se utilizarán, con qué finalidad y qué implicaciones tiene compartir una credencial en entornos digitales. Estos criterios deben revisarse a la luz del Reglamento General de Protección de Datos de la Unión Europea y de la normativa aplicable en Guatemala, que se considera en el autodiagnóstico D2.2.

La ética del modelo también incluye la inclusión digital. Las IIEFP deben evitar que la adopción de credenciales digitales cree nuevas barreras para los estudiantes con menos acceso a la tecnología o con competencias digitales limitadas. Para ello, las recomendaciones del informe contemplan la necesidad de contar con interfaces accesibles, ofrecer acompañamiento técnico y proporcionar formación básica sobre el uso de carteras digitales y mecanismos de verificación. Un sistema de credenciales solo será útil si puede ser utilizado por todos los estudiantes a quienes va dirigido.

Otro aspecto relevante es la revisión de los criterios de evaluación asociados a la emisión de credenciales. Cuando parte del proceso se apoya en plataformas digitales o sistemas automatizados, los centros emisores deben garantizar que las normas utilizadas sean claras, justificables y no discriminatorias. La tecnología puede facilitar la gestión de las evidencias, pero no debe sustituir a la responsabilidad académica de validar que una competencia ha sido alcanzada. En las credenciales de mayor nivel, la supervisión humana sigue siendo necesaria para proteger la calidad pedagógica del modelo.

La sostenibilidad ética también requiere políticas de gobernanza de datos a largo plazo. Las instituciones deben definir cómo se conservarán los registros, quién podrá acceder a ellos, cómo se actualizarán las credenciales y qué ocurrirá si cambian las plataformas o las estructuras institucionales. Estas decisiones deben tomarse antes de ampliar el modelo, ya que afectan directamente a la confianza de estudiantes, egresados y empleadores.

El Observatorio ECOCredGT puede desempeñar un papel de apoyo en este sentido. Puede orientar su función al seguimiento de buenas prácticas, la actualización de recomendaciones y la revisión de riesgos emergentes en materia de privacidad, seguridad e inclusión. Al situar la ética y la protección de datos dentro del marco tecnológico, el éxito del proyecto no dependerá únicamente del número de credenciales emitidas, sino también de la confianza que estas generen en las personas e instituciones que las utilizan.

3. Recomendaciones para la infraestructura tecnológica

La puesta en marcha de un centro de emisión de credenciales digitales requiere una infraestructura tecnológica bien definida. No basta con instalar una herramienta de emisión ni con utilizar una plataforma aislada. Las instituciones de educación y formación profesional necesitan contar con sistemas que permitan diseñar, emitir, verificar, almacenar y hacer un seguimiento de las credenciales digitales de forma segura y coherente. La calidad técnica de esta infraestructura influye directamente en la confianza que estudiantes, empleadores y otras instituciones podrán tener en las credenciales emitidas en el marco de ECOCredGT.

Los requerimientos tecnológicos identificados durante el proyecto muestran que las soluciones deben cumplir dos condiciones. Por un lado, deben alinearse con los estándares internacionales de interoperabilidad, seguridad y verificación. Por otra parte, deben ajustarse a las capacidades reales de las instituciones participantes, incluida la conectividad, la infraestructura disponible, el personal técnico y las posibilidades de mantenimiento. Esta segunda condición es especialmente importante según la información recogida en el autodiagnóstico D2.2, ya que permite plantear una transición tecnológica no solo deseable, sino también viable desde el punto de vista técnico.

Una arquitectura de referencia para las IIEFP debe considerar varias capas que funcionen de manera coordinada. La primera capa se ocupa del diseño y la generación de credenciales, lo que incluye la definición de metadatos y plantillas comunes. La segunda capa se relaciona con la integración entre las plataformas de aprendizaje, los sistemas académicos y los registros institucionales. La tercera capa se centra en la verificación y protección de la integridad de los registros mediante mecanismos criptográficos y, cuando corresponda, tecnología blockchain. Estas capas no deben entenderse como componentes separados, sino como partes de un mismo flujo de trabajo.

La experiencia de los proyectos piloto recogida en el documento D3.3 muestra que la dificultad principal no siempre radica en la herramienta utilizada, sino en la conexión entre sistemas. Si los datos se duplican, se introducen manualmente o se almacenan en plataformas que no están comunicadas entre sí, aumentan los errores y se debilita la trazabilidad del proceso. Por ello, se recomienda avanzar hacia soluciones modulares basadas preferiblemente en estándares abiertos, que permitan adaptar el modelo a las condiciones de cada institución y reducir la dependencia de un único proveedor tecnológico.

Desde la perspectiva del WP6, la infraestructura técnica debe revisarse conforme a criterios de calidad, seguridad y sostenibilidad. No basta con que una credencial pueda emitirse. También debe poder verificarse, conservarse y revocarse cuando sea necesario. Los sistemas que sustentan el centro de emisión deben contar con controles de acceso, registros de auditoría, políticas de copia de seguridad y mecanismos de protección de datos. Estas condiciones permiten que los centros emisores operen con criterios comunes y con un nivel razonable de confianza institucional.

Este capítulo organiza las recomendaciones tecnológicas en tres ámbitos. En primer lugar, se revisan los modelos de gestión de la infraestructura. A continuación, se presentan estrategias para integrar el centro de emisión con plataformas LMS y sistemas de gestión académica. Por último, se describen elementos de arquitectura técnica y protocolos de seguridad que las IIEFP deberían tener en cuenta antes de ampliar el modelo.

3.1 Modelos de gestión

La definición del modelo de gestión tecnológica establece cómo se administrarán los recursos informáticos, las autorizaciones de emisión y las responsabilidades técnicas dentro de una IIEFP. Cada institución deberá decidir si le conviene más un modelo centralizado, distribuido, híbrido o apoyado parcialmente en servicios en la nube. Esta decisión no debe tomarse solo por criterios de coste o facilidad de instalación. También deben tenerse en cuenta el control institucional sobre las credenciales, la capacidad del equipo técnico, la protección de las llaves criptográficas y la posibilidad de mantener el sistema a lo largo del tiempo.

El modelo centralizado puede ser adecuado en las primeras fases de adopción. En este esquema, el motor de emisión y los componentes principales se gestionan desde una unidad central, normalmente vinculada al área de tecnologías de la información o a la dirección académica. Esta organización facilita la aplicación de políticas comunes de seguridad, la actualización de la plataforma con mayor control y la garantía de que las distintas áreas utilicen plantillas, metadatos y criterios de emisión compatibles. También se reduce el riesgo de que cada departamento cree soluciones distintas sin coordinación institucional.

Un modelo distribuido ofrece una mayor autonomía a las facultades, sedes o departamentos técnicos. Puede ser útil cuando la institución tiene varias unidades con necesidades formativas muy diferentes y equipos con suficiente capacidad técnica. Sin embargo, este enfoque requiere mecanismos sólidos de coordinación. Si no existen criterios comunes, pueden aparecer diferencias en la estructura de los datos, en los procesos de validación o en la forma de aplicar los estándares. Esto dificultaría la auditoría interna y podría afectar a la confianza en las credenciales emitidas.

La experiencia de la Universidad Galileo y la Fundación Kinal durante los pilotos indica que un modelo híbrido o federado sería conveniente para muchas IIEFP. En este modelo, los elementos críticos se mantienen bajo control central, como las llaves de firma, el catálogo institucional de competencias, las políticas de seguridad y las reglas generales de emisión. Al mismo tiempo, las unidades académicas o técnicas pueden gestionar ciertos procesos operativos, como la asignación de credenciales a estudiantes que han cumplido los requisitos. Esta combinación permite mantener el control institucional sin bloquear la actividad diaria.

Para elegir el modelo más adecuado, las IIEFP deberían revisar su nivel de madurez digital según los resultados del autodiagnóstico D2.2, teniendo en cuenta la disponibilidad de personal técnico, la estabilidad de la conectividad, la capacidad de financiar infraestructura propia y la experiencia previa en integración de sistemas. Las instituciones con recursos técnicos limitados pueden considerar soluciones de software como servicio, siempre que se definan claramente la propiedad de los datos, la custodia de las claves y las condiciones de acceso a los registros históricos.

Se recomienda que la gestión tecnológica del centro de emisión quede bajo la supervisión de un comité o unidad institucional con capacidad de decisión. Este grupo debería revisar los cambios en la arquitectura, autorizar las integraciones, validar las políticas de seguridad y coordinarse con las áreas académicas y de calidad. Una gestión ordenada evitará emisiones erróneas, reducirá los riesgos de fragmentación y preparará el terreno para una futura articulación con el Observatorio ECOcredGT.

3.2 Estrategias de integración con plataformas LMS y sistemas de gestión académica

El centro de emisión será más útil si se integra con los sistemas que ya utiliza la institución. En las IIEFP, los entornos virtuales de aprendizaje y los sistemas de gestión académica suelen contener información clave sobre los estudiantes, los cursos, las evaluaciones y los resultados del aprendizaje. Conectar estos sistemas con el motor de credencialización ayuda a reducir tareas manuales, evitar la duplicación de datos y disminuir los errores en la emisión de credenciales.

Para apoyar una integración técnica sostenible, se recomiendan las siguientes estrategias:

- **Automatización mediante interfaces web:** La arquitectura debería utilizar API seguras y protocolos de comunicación documentados. Cuando un estudiante completa una competencia o cumple un criterio de aprobación en el LMS, el sistema puede generar una solicitud de emisión hacia el motor de credenciales. Esta automatización debe incluir validaciones previas para evitar emisiones incompletas o no autorizadas.
- **Configuración de reglas pedagógicas:** Los centros deben definir criterios claros de aprobación dentro de las plataformas virtuales. Estos criterios pueden incluir la obtención de una nota mínima, la finalización de actividades, la validación de evidencias o la revisión de portafolios. La integración debe permitir recuperar esta información y asociarla a los metadatos de la credencial, siempre que exista autorización institucional y se cumplan las normas de protección de datos.
- **Unificación de la identidad digital:** Es habitual que un estudiante tenga un usuario diferente para el LMS, el sistema académico y otras plataformas institucionales. Para evitar inconsistencias, se recomienda avanzar hacia mecanismos de autenticación única, como SAML 2.0 u OpenID Connect. De este modo, se puede vincular la credencial con su titular de forma más segura y se reducen los errores en la asignación de insignias.
- **Resiliencia y manejo de excepciones:** La capa de integración debe tener en cuenta los fallos temporales de red, las interrupciones de servicio y los errores en el intercambio de datos. Para ello, pueden utilizarse colas de eventos, registros temporales seguros y mecanismos de reintento. Si se produce un fallo en la conexión, la solicitud de emisión no debe perderse ni duplicarse sin control.

Además de implementar estas estrategias, las instituciones deben documentar las interfaces desarrolladas, los datos intercambiados y las responsabilidades de mantenimiento. Esta documentación será necesaria cuando se actualicen las plataformas, cambien los proveedores o se incorporen nuevas unidades académicas. Una integración bien documentada no solo mejora la operación diaria, sino que también facilita la continuidad del modelo tras la fase piloto.

3.3 Arquitectura técnica y protocolos de seguridad de los datos

La arquitectura técnica de un centro de emisión de credenciales digitales debe organizarse en componentes diferenciados. Una estructura por capas facilita el mantenimiento, permite escalar el sistema y reduce el impacto de posibles fallos. En general, se puede considerar una capa de presentación para usuarios, una capa de lógica empresarial para procesar reglas y taxonomías, una capa de persistencia para datos institucionales y una capa de verificación criptográfica vinculada con los mecanismos de confianza definidos por el modelo.

La seguridad de los datos es una condición básica para la validez del sistema. Las comunicaciones entre usuarios, plataformas LMS, servidores de emisión y servicios de verificación deben estar cifradas mediante protocolos actualizados, como TLS 1.3 o los equivalentes aceptados por la institución. Las bases de datos que almacenan información de estudiantes, evidencias, calificaciones o registros de emisión deben contar con cifrado en reposo, controles de acceso y políticas de copia de seguridad. Estas medidas reducen el riesgo de accesos no autorizados y protegen la información académica sensible.

La arquitectura debe aplicar los principios de minimización y separación de datos. De acuerdo con el marco ético presentado en la sección 2.4, no se recomienda almacenar datos personales directamente en una cadena de bloques pública ni en registros distribuidos que no puedan modificarse. El sistema puede procesar la información de la credencial en un entorno controlado, generar un archivo compatible con estándares como Open Badges 3.0 y registrar únicamente una huella criptográfica con fines de verificación. Este flujo de trabajo permite comprobar la autenticidad de la credencial sin exponer información personal públicamente.

El acceso al motor de emisión debe controlarse mediante autenticación multifactor y permisos basados en roles. El personal técnico, los equipos académicos, los responsables de calidad y las autoridades encargadas de aprobar credenciales no necesitan los mismos privilegios. Cada perfil debe tener acceso únicamente a las funciones necesarias para su trabajo. Además, las acciones relevantes dentro del sistema, como modificar una competencia, emitir una credencial, revocarla o cambiar una plantilla, deben quedar registradas en un historial de auditoría protegido.

Las IIEFP también deben prever planes de continuidad empresarial y de recuperación ante incidentes. El centro de emisión depende de activos críticos, como bases de datos, plantillas, registros de emisión y llaves criptográficas institucionales. La pérdida o exposición de una clave privada podría afectar a la capacidad de emitir, verificar o revocar credenciales. Por ello, se recomienda utilizar mecanismos seguros de custodia, como bóvedas digitales, módulos de seguridad de hardware o servicios equivalentes que se ajusten a la capacidad técnica y financiera de cada institución.

Las copias de seguridad deben realizarse de manera periódica y probarse con regularidad. No basta con crear copias de seguridad si la institución no verifica que puedan restaurarse correctamente. También conviene definir quiénes son los responsables, cuáles son los tiempos máximos de recuperación y qué procedimientos hay que seguir ante incidentes de seguridad, fallos de infraestructura o cambios de proveedor. Estas medidas ayudan a que el centro de emisión pueda mantenerse operativo incluso en escenarios de interrupción.

El cumplimiento de estos protocolos permite que el WP6 valore la infraestructura tecnológica según criterios de calidad y sostenibilidad. La seguridad no debe considerarse un requisito añadido al final del proceso, sino una condición que debe incorporarse desde el diseño. Al proteger los datos, ordenar los accesos y garantizar la trazabilidad de las credenciales, las IIEFP aumentan la confianza en el modelo y crean una base técnica más sólida para su continuidad y posible conexión con el Observatorio ECOCredGT.

4. Gobernanza y estructura organizativa del centro de emisión

Para adoptar un modelo de certificación basado en microcredenciales es necesaria una base organizativa clara. No puede depender solo de iniciativas individuales de docentes, departamentos o equipos técnicos. Para que el sistema funcione de manera estable, las IEF deben definir una estructura de gobernanza que establezca las responsabilidades, los niveles de decisión, las normas internas y los procedimientos de seguimiento. Así, la emisión de credenciales pasa de ser una acción puntual de innovación a formar parte de una política institucional.

Una estructura bien definida ayuda a evitar diferencias excesivas en los criterios de evaluación y emisión. Cuando cada área aplica reglas distintas, las credenciales pueden perder coherencia y resultar más difíciles de verificar o reconocer para los actores externos. Por ello, el centro de emisión debe contar con procedimientos comunes, registros claros y mecanismos de revisión que permitan comprobar cómo se tomó cada decisión. Esto protege la credibilidad de la institución y facilita las tareas de auditoría interna.

La experiencia del consorcio muestra que surgen varios problemas operativos cuando no existe una separación suficiente entre las funciones académicas, técnicas y administrativas. El modelo propuesto busca organizar esas funciones sin limitar la autonomía académica del profesorado. Los docentes deben seguir siendo responsables de definir y evaluar los aprendizajes, mientras que las áreas técnicas y de gestión deben garantizar que los procesos de emisión, registro y verificación se lleven a cabo conforme a los criterios institucionales.

Para consolidar esta organización, las instituciones deberían contar con reglamentos internos que formalicen el funcionamiento del centro. Estos documentos deben explicar cómo se aprueban nuevas credenciales, qué instancias intervienen, cómo se resuelven las incidencias y qué condiciones deben cumplirse antes de emitir una insignia. La formalización de estos procedimientos ayuda a mantener el modelo, aunque cambien los equipos directivos o se incorporen nuevos responsables al proceso.

4.1 Modelo operativo de centros de emisión para las IEF

El modelo operativo define la ubicación del centro de emisión dentro de la estructura institucional y la forma en que se relaciona con otras áreas. Se recomienda que el centro no funcione como una unidad aislada de una carrera o departamento específico. Es más conveniente ubicarlo como una unidad transversal vinculada a la dirección académica, la rectoría o la instancia equivalente. Esta posición le permite coordinarse con el registro académico, el diseño curricular, las tecnologías de la información, la calidad institucional y la vinculación externa.

A partir de las enseñanzas extraídas de los pilotos locales, se propone un enfoque operativo híbrido. La institución mantiene de forma centralizada las normas generales, el catálogo de competencias, los criterios de calidad, la identidad visual de las credenciales y los elementos críticos de seguridad. Al mismo tiempo, las facultades, sedes o unidades técnicas pueden participar en la gestión diaria de las evaluaciones y en la preparación de solicitudes de emisión. Este esquema combina el control institucional con la capacidad de respuesta en los distintos contextos formativos.

Para apoyar este modelo, resulta conveniente crear un consejo o comité de certificación. Este órgano podría estar integrado por representantes de la dirección institucional, la coordinación del centro de emisión, las áreas académicas, de tecnología, de calidad y de vinculación con el sector productivo.

Su función principal sería revisar y aprobar nuevas propuestas de microcredenciales para garantizar que respondan a necesidades formativas reales, que estén alineadas con el catálogo institucional y que cumplan los procedimientos establecidos.

En las instituciones con varios campus o sedes, el modelo debe definir claramente qué tareas pueden delegarse y cuáles deben permanecer bajo control central. Las sedes pueden gestionar procesos operativos, recopilar pruebas y preparar solicitudes, pero la aprobación de nuevas credenciales, los cambios en las plantillas oficiales y la autorización final de emisión deberían mantenerse en una instancia institucional común. De este modo, se reduce el riesgo de que haya formatos inconsistentes o decisiones que no estén alineadas con la política general de certificación.

El centro de emisión también debe regular su relación con los actores externos. Esto incluye a empresas, cámaras de comercio, ministerios, entidades certificadoras y otras instituciones educativas. La firma de convenios, acuerdos de co-emisión o mecanismos de reconocimiento mutuo debería gestionarse desde una instancia central. De este modo, se evita que diferentes áreas establezcan acuerdos aislados que puedan generar interpretaciones distintas sobre el valor de las credenciales o afectar a la coherencia institucional del modelo.

En términos operativos, el centro debe actuar como una unidad de apoyo y no como una fuente de trámites innecesarios. Su función es facilitar el trabajo de los equipos académicos, garantizar la calidad del proceso y minimizar los errores en la emisión. Para ello, es necesario contar con procedimientos claros, tiempos de respuesta definidos y canales de comunicación accesibles. Un diseño organizativo equilibrado permite que el centro funcione con transparencia y se adapte a otros entornos de educación y formación profesional.

4.2 Definición de roles estratégicos, técnicos y académicos

El funcionamiento del centro de emisión depende de una distribución clara de las responsabilidades. Para evitar solapamientos o lagunas en la gestión, se recomienda organizar los roles en tres áreas principales: estratégica, técnica y académica. Estos son: el estratégico, el técnico y el académico. Esta separación no debe entenderse como una división rígida, sino como una forma de garantizar que cada fase del proceso sea atendida por el perfil más adecuado.

El ámbito estratégico está asociado a la dirección o coordinación general del centro. Esta persona actúa como enlace entre el equipo operativo y las autoridades institucionales. Entre sus funciones se encuentran coordinar la planificación del centro, proponer prioridades de crecimiento del catálogo de credenciales, administrar los recursos asignados y garantizar que las actividades estén alineadas con la estrategia académica de la IIEFP. También puede convocar reuniones de revisión y supervisar el cumplimiento de las normas internas.

El área técnica se encarga de mantener la plataforma, configurar los registros y garantizar el funcionamiento del sistema. En este departamento puede haber un administrador de catálogo, que se encargará de cargar estructuras de datos, mantener plantillas y revisar la consistencia técnica de las credenciales. También puede participar un responsable de validación administrativa, que se encargará de contrastar actas, listados de estudiantes y solicitudes de emisión antes de que pasen a la firma institucional. Esta revisión ayuda a reducir errores y a separar la validación documental de la evaluación académica.

El ámbito académico sigue siendo responsable del contenido formativo y de la evaluación de las competencias. En este grupo participan diseñadores curriculares, docentes y evaluadores. El diseñador curricular puede apoyar la redacción de los resultados de aprendizaje, los criterios de

evaluación y las descripciones de las credenciales. El docente o evaluador experto se encarga de verificar el desempeño del estudiante, aplicar las rúbricas correspondientes y registrar los resultados en los documentos académicos oficiales. Esta función no debería ser desempeñada por personal administrativo o técnico.

Para coordinar estos ámbitos, es útil trabajar con matrices de responsabilidades. Estas matrices permiten identificar quién ejecuta una tarea, quién la revisa, quién la aprueba y quién debe ser informado. Su uso ayuda a evitar confusiones frecuentes, como que el área técnica modifique los criterios académicos o que un docente expida una credencial sin pasar por los controles institucionales pertinentes. También facilitan la incorporación de nuevos integrantes al equipo.

La estructura de recursos humanos debe prever los cambios de personal. El conocimiento sobre el funcionamiento del centro no puede concentrarse en una sola persona. Por ello, cada rol debería contar con una descripción de funciones, procedimientos documentados y materiales de apoyo. De este modo, se conserva el conocimiento institucional, se facilita la incorporación de nuevos colaboradores y se reduce el riesgo de interrupciones en el servicio de certificación.

4.3 Flujos de trabajo: diseño, emisión y de validación

Los flujos de trabajo describen los pasos necesarios para convertir una competencia o resultado de aprendizaje en una credencial que se entrega formalmente al estudiante. Estos procesos deben estar documentados en manuales operativos y ser conocidos por las áreas que participan en su emisión. Un procedimiento claro reduce los errores, mejora los tiempos de respuesta y facilita la revisión posterior de cada credencial emitida.

A continuación, se presenta una secuencia de trabajo recomendada para el funcionamiento ordinario del centro, junto con el procedimiento de revocación para casos excepcionales.

- **Diseño y aprobación curricular:** Esta fase se lleva a cabo desde los departamentos académicos con el apoyo del centro de emisión. En ella, se identifican las competencias que se van a certificar, se redactan los resultados de aprendizaje, se definen los criterios de evaluación y se preparan los textos que acompañarán a la credencial. Cuando la propuesta está completa, se presenta al consejo o comité de certificación para su revisión. Una vez aprobada, la credencial puede incorporarse al catálogo institucional antes del inicio de la actividad formativa.
- **Validación académica:** Esta etapa se lleva a cabo después de que los estudiantes hayan completado la formación o actividad correspondiente. El docente responsable consolida las calificaciones, las evidencias y los resultados de la evaluación en un acta o registro oficial. Este documento debe ser revisado por la instancia académica correspondiente, como la jefatura de departamento o la coordinación del programa. Posteriormente, se remite al centro de emisión para su validación administrativa.
- **Revisión administrativa previa a la emisión:** El personal del centro verifica que la información recibida esté completa y sea coherente con los criterios aprobados. Esta revisión incluye la comprobación de nombres, identificadores, curso o módulo, competencia certificada, fecha de emisión y cumplimiento de los requisitos. Si se detectan inconsistencias, la solicitud se devuelve al área académica para su corrección antes de continuar. Esta etapa es importante para evitar errores que puedan afectar a la validez o comprensión de la credencial.

- **Emisión y firma institucional:** Una vez validada la información, el personal autorizado prepara el lote de emisión en la plataforma correspondiente. La autoridad académica o administrativa delegada realiza la firma institucional según el procedimiento definido por la IEFP. Esta firma otorga validez formal a la credencial y permite su registro en los sistemas de control y verificación del centro.
- **Distribución y entrega al estudiante:** El proceso ordinario finaliza cuando el estudiante recibe la notificación de que su credencial está disponible. La institución debe ofrecer instrucciones claras sobre cómo aceptar, almacenar y compartir la credencial en el espacio digital correspondiente. Durante esta fase, el centro debe mantener un canal de asistencia para resolver incidencias como errores en los datos personales, problemas de acceso o dudas sobre el uso de la insignia.
- **Revocación en casos excepcionales:** El marco de gobernanza debe incluir un procedimiento para anular o revocar las credenciales cuando exista una causa justificada. Esta medida solo debería aplicarse en las situaciones previstas en el reglamento interno, como el fraude académico comprobado, la utilización de documentación falsa o la emisión realizada por error. El procedimiento debe incluir la apertura de un expediente, la revisión por parte de la instancia competente, la notificación al titular y la actualización del estado de la credencial en los sistemas de verificación.

Estos flujos de trabajo deben revisarse periódicamente. La práctica puede mostrar pasos redundantes, tiempos excesivos o incidencias no previstas durante el diseño inicial. Por ello, el centro emisor debería recoger las observaciones de docentes, estudiantes, personal administrativo y responsables técnicos. Esta información permitirá ajustar los procedimientos sin perder trazabilidad ni criterios de calidad.

5. Estrategia de formación, recursos humanos y gestión del cambio

La transición hacia un sistema de certificaciones digitales no depende únicamente de la infraestructura tecnológica. Las plataformas, los estándares y los mecanismos de verificación son necesarios, pero no suficientes. Para que el modelo sea sostenible en el tiempo, el personal administrativo, docente y directivo debe comprender cómo funciona, qué cambios introduce y qué responsabilidades conlleva en el trabajo diario de la institución.

La gestión del cambio debe abordarse desde el principio. La incorporación de nuevos procedimientos para evaluar, emitir y verificar credenciales puede generar dudas entre los equipos, sobre todo si las instituciones han trabajado durante años con procesos más tradicionales. Por ello, los departamentos de recursos humanos y gestión académica deben apoyar el proceso con información clara, espacios de consulta y acciones formativas. La adopción será más viable si el personal entiende el sentido del cambio y no lo percibe solo como una carga administrativa adicional.

La formación debe plantearse como un proceso continuo y no como una actividad puntual. Las experiencias desarrolladas durante el proyecto muestran que el personal no solo necesita aprender a utilizar las herramientas, sino también comprender el valor pedagógico e institucional de las microcredenciales. Esto incluye conocer cómo se formulan los resultados de aprendizaje, cómo se relacionan las credenciales con las competencias profesionales y cómo se garantiza la calidad de la información que se facilita al estudiante y a terceros.

Desde el punto de vista de recursos humanos, también es importante reconocer el esfuerzo que supone esta actualización. La participación en actividades formativas sobre credenciales digitales puede incluirse en los planes de desarrollo profesional, en los procesos de evaluación interna o en las estrategias de carrera del personal académico y administrativo. Este reconocimiento ayuda a que la adopción del modelo no dependa solo de la buena voluntad de algunos equipos, sino que forme parte de una política institucional de mejora.

La estrategia de formación debe complementarse con acciones dirigidas al entorno externo. Las credenciales digitales tendrán más valor si los empleadores comprenden la información que contienen, cómo se verifican y la utilidad que pueden tener en los procesos de selección o promoción laboral. Por esta razón, las IIEFP deben colaborar también con empresas, cámaras de comercio, asociaciones profesionales y otros agentes del sector productivo. La comunicación con estos actores debe ser clara y práctica, evitando un lenguaje excesivamente técnico.

Este capítulo presenta recomendaciones para organizar la formación, gestionar los recursos humanos y acompañar el cambio institucional. En primer lugar, se describe el plan de formación multinivel para los distintos perfiles involucrados. A continuación, se revisan las acciones de sensibilización y vinculación con el sector empresarial. Por último, se plantean orientaciones para mantener actualizadas las competencias docentes y seguir la evolución tecnológica relacionada con las credenciales digitales.

5.1 El Plan de formación multinivel para adopción institucional.

El plan de formación multinivel permite organizar la capacitación según las funciones de cada grupo dentro de la institución. No todos los participantes necesitan el mismo nivel de conocimientos técnicos ni intervienen de la misma manera en el ciclo de emisión. Por ello, conviene diseñar

itinerarios formativos diferenciados para el personal administrativo y técnico, los docentes y los coordinadores académicos, los estudiantes y los responsables institucionales. Esta diferenciación permite aprovechar mejor el tiempo disponible y evitar formaciones demasiado generales que no se adapten a las tareas reales de cada perfil.

El primer nivel debe dirigirse al personal administrativo y técnico que participa en el funcionamiento diario del sistema. Este grupo necesita formación en gestión de usuarios, manejo de bases de datos, protección de información estudiantil, control documental, emisión de credenciales y atención de incidencias. También debe conocer los procedimientos internos para revisar solicitudes, corregir errores y mantener registros actualizados. Su papel es importante, ya que una parte significativa de la calidad del modelo depende de que los trámites se realicen con precisión y dentro de los plazos establecidos.

El segundo nivel corresponde al cuerpo docente y a los coordinadores académicos. En este caso, la formación no debe centrarse solo en el uso de la plataforma. Los docentes deben trabajar aspectos relacionados con el diseño de resultados de aprendizaje, la elaboración de rúbricas, la selección de evidencias y la relación entre competencias formativas y necesidades del sector productivo. Esta capacitación garantiza que las credenciales emitidas reflejen aprendizajes verificables y no se conviertan únicamente en reconocimientos formales de participación.

El tercer nivel debe orientarse a los estudiantes. En muchos proyectos de digitalización se da por hecho que los estudiantes sabrán utilizar las credenciales sin necesidad de apoyo, pero no siempre es así. Las IIEFP deberían ofrecer guías, sesiones breves de orientación y materiales de consulta que expliquen cómo aceptar una credencial, almacenarla en una cartera digital y compartirla en contextos académicos o profesionales. Esta formación también puede incluir recomendaciones sobre el uso responsable de la identidad digital y la presentación de logros en redes profesionales.

El plan puede combinar distintas modalidades de enseñanza. Los recursos asincrónicos, como guías, vídeos breves o cursos en línea, permiten que el personal avance a su propio ritmo. Las sesiones presenciales o virtuales ayudan a resolver dudas, revisar casos concretos y compartir experiencias entre áreas. Los talleres prácticos son especialmente útiles para tareas como configurar una credencial, revisar metadatos, validar evidencias o resolver incidencias frecuentes.

La eficacia del plan debe revisarse periódicamente. Los departamentos de recursos humanos o calidad pueden registrar la participación, el progreso en las actividades formativas y las dificultades que hayan podido surgir. También se pueden aplicar encuestas breves o ejercicios de verificación de aprendizajes. Esta información permitirá ajustar los materiales, reforzar los temas que no hayan quedado claros y preparar nuevas ediciones del plan cuando se incorporen personas o se actualicen las herramientas.

5.2 Sensibilización y vinculación con el sector empresarial

El valor de una credencial digital depende en parte de su reconocimiento fuera de la institución que la emite. En el caso de la formación profesional, este reconocimiento está estrechamente vinculado al sector empresarial. Si las empresas no comprenden qué es una microcredencial, qué información contiene o cómo se puede verificar, no servirá de mucho para mejorar la empleabilidad. Por ello, los centros de formación profesional deben complementar la implementación técnica con una estrategia de comunicación y sensibilización dirigida a los empleadores.

Una primera tarea consiste en explicar el funcionamiento de las credenciales con un lenguaje sencillo. Algunas empresas pueden interpretar las insignias digitales como imágenes o certificados

informales, sin conocer los metadatos, las evidencias y los mecanismos de verificación que las respaldan. Las acciones de comunicación deben mostrar cómo se comprueba la autenticidad de una credencial, qué tipo de información ofrece y de qué manera puede apoyar los procesos de selección, las prácticas profesionales o la identificación del talento.

La colaboración con empresas no debería limitarse a presentar el modelo una vez finalizado. Se recomienda involucrar al sector productivo en el diseño de algunas credenciales, especialmente las relacionadas con competencias técnicas o perfiles ocupacionales específicos. Las mesas de trabajo, las entrevistas con empleadores y los talleres de contraste pueden ayudar a identificar qué habilidades son más relevantes y cómo deberían describirse para resultar comprensibles en el ámbito laboral. Esta participación mejora la pertinencia de la oferta formativa y favorece una mayor aceptación posterior.

También es conveniente establecer relaciones con cámaras de comercio, asociaciones profesionales, clústeres industriales y empresas colaboradoras. Estos acuerdos pueden facilitar la difusión del modelo, la revisión de competencias, la participación en proyectos piloto y la generación de oportunidades para estudiantes y egresados. La formalización de estas relaciones debe gestionarse de manera institucional para evitar acuerdos aislados que no se ajusten a los criterios generales del centro emisor.

La estrategia de vinculación debe incluir mecanismos de retroalimentación. Las IIEFP necesitan saber si los empleadores entienden la información incluida en las credenciales, si consideran útiles los criterios de evaluación y si las competencias certificadas responden a sus necesidades. Esta información puede obtenerse mediante encuestas, reuniones periódicas o espacios de evaluación conjunta. Los resultados deben trasladarse a los equipos académicos para ajustar programas, rúbricas o descripciones de competencias, si es necesario.

A medio plazo, estas acciones pueden contribuir a que las credenciales digitales se reconozcan con mayor naturalidad en los procesos de contratación. Este cambio no se producirá de forma inmediata. Requiere constancia, comunicación clara y ejemplos concretos de uso. Si las empresas comprueban que las credenciales digitales les ayudan a interpretar mejor el perfil de los candidatos, será más probable que las incorporen a sus procesos internos y que participen en futuras iniciativas de certificación.

5.3 Vigilancia tecnológica y actualización continua de competencias docentes

La tecnología educativa y los estándares asociados a las credenciales digitales cambian rápidamente. Por esta razón, una formación inicial, aunque sea completa, no garantiza por sí sola la continuidad del modelo. Las IIEFP deben prever mecanismos para revisar periódicamente las herramientas, los estándares de interoperabilidad, las prácticas de protección de datos y las nuevas formas de documentar las evidencias de aprendizaje.

La vigilancia tecnológica se puede definir como una actividad organizada de seguimiento y análisis. Entre sus actividades se incluyen la revisión de los avances de organismos internacionales, la participación en redes o foros especializados, la consulta de documentación técnica y la observación de experiencias de otras instituciones. Esta información permite anticiparse a los cambios y tomar decisiones más informadas sobre la actualización de las plataformas, los ajustes en los procesos de emisión o la incorporación de nuevas prácticas pedagógicas.

Los resultados de esta vigilancia deben conectarse con la actualización continua del profesorado. A medida que el sistema avance, los docentes necesitarán fortalecer competencias relacionadas con la evaluación basada en evidencias, el diseño de rúbricas, el uso de herramientas digitales, la integración de portafolios y el seguimiento de trayectorias formativas. También se pueden explorar nuevas herramientas, incluidas aplicaciones de inteligencia artificial, siempre que su uso vaya acompañado de criterios pedagógicos, revisión humana y normas claras de privacidad.

Una práctica útil es crear comunidades de práctica internas. Estos espacios permiten que los docentes y coordinadores compartan experiencias, dificultades, materiales y soluciones utilizadas en sus programas. El intercambio entre iguales puede reducir la inseguridad frente a las nuevas herramientas y generar aprendizajes más cercanos a la realidad de cada institución. Además, ayudan a crear un repositorio interno de ejemplos, plantillas y recomendaciones que pueden utilizar los nuevos equipos.

Para que la actualización continua sea posible, la institución debe asignar tiempo y recursos. Diseñar nuevas microcredenciales, revisar los criterios de evaluación o adaptar las herramientas tecnológicas requiere un trabajo adicional. Si estas tareas solo se realizan fuera del horario laboral, el modelo puede depender en exceso del esfuerzo individual de algunos docentes. Reconocer estas actividades en la planificación académica ayuda a mantener la participación del profesorado y a mejorar la calidad de las credenciales.

La actualización del profesorado también debe incluir al personal técnico y administrativo cuando los cambios afecten a los procesos de emisión. Una modificación de los estándares, de la plataforma o de los requisitos de protección de datos puede alterar las tareas de varias áreas. Por ello, la formación continua debe planificarse de manera coordinada y no solo como una responsabilidad del profesorado.

En conjunto, la vigilancia tecnológica y la actualización permanente permiten que el modelo no se quede limitado a las herramientas utilizadas durante la fase piloto. Mantener al personal informado, revisar las prácticas y adaptar los procedimientos cuando sea necesario ayuda a conservar la pertinencia de las credenciales digitales. Esta capacidad de aprendizaje institucional será clave para que el centro de emisión siga siendo útil, confiable y sostenible en el tiempo.

6. Aseguramiento de la calidad, sostenibilidad y mejora continua

La implementación de centros de emisión de credenciales digitales no termina cuando la plataforma comienza a funcionar. Para mantener el modelo a largo plazo, las instituciones de educación y formación profesional deben contar con mecanismos de revisión, seguimiento y mejora. Esta tarea es especialmente importante en el marco del WP6, ya que el control de calidad no solo consiste en comprobar los productos finales, sino que también permite valorar si los procesos definidos pueden mantenerse después del periodo de financiación europea.

El aseguramiento de la calidad debe entenderse como una práctica continua. Las instituciones deben revisar el diseño de las credenciales, la validación de los resultados de aprendizaje, la protección de los datos y la utilización de las certificaciones por parte de estudiantes y actores externos. Esta revisión permite detectar problemas operativos, corregir errores y ajustar la oferta formativa cuando cambian las necesidades del entorno laboral.

La sostenibilidad también requiere planificación. Los centros emisores necesitan recursos técnicos, personal formado, mantenimiento de las plataformas, actualización de los estándares y procedimientos internos estables. Si estos elementos no se integran en la gestión habitual de la institución, existe el riesgo de que el modelo se quede limitado a la fase piloto. Por ello, las IEFP deben prever cómo financiar, administrar y actualizar el sistema una vez que finalice el apoyo directo del proyecto.

Para poder justificar la continuidad del modelo, también es necesario medir sus resultados. La utilidad de una credencial digital no debería evaluarse solo por el número de insignias emitidas. Es importante analizar si las credenciales ayudan a visibilizar competencias, si son comprensibles para los empleadores y si aportan información útil para la inserción laboral o la movilidad profesional de los egresados. Los indicadores de empleabilidad permiten conectar la innovación tecnológica con resultados observables.

El proyecto destaca la importancia de contar con un espacio de seguimiento a nivel regional. El Observatorio ECOcredGT puede contribuir a recopilar información, compartir experiencias, analizar tendencias y apoyar a las instituciones que deseen adoptar o mejorar sus propios centros de emisión. Su función no sustituye la responsabilidad de cada IEFP, pero sí puede facilitar la coordinación y la actualización del modelo con el tiempo.

Este capítulo presenta informaciones relacionadas con la calidad, la sostenibilidad y la mejora continua. En primer lugar, se describe el marco de calidad ECOcredGT. A continuación, se proponen indicadores para valorar el impacto de las credenciales en la empleabilidad. A continuación, se plantea una hoja de ruta para la sostenibilidad técnica y financiera. Por último, se explica el papel que puede desempeñar el Observatorio ECOcredGT en la continuidad y evolución del modelo.

6.1 Marco de calidad ECOcredGT.

El marco de calidad ECOcredGT establece criterios comunes para orientar el diseño, la emisión, la validación y el seguimiento de las credenciales digitales. Su objetivo es ayudar a las instituciones a trabajar con procedimientos claros, evitando que cada área emita credenciales con criterios diferentes. De esta manera, el modelo crea consistencia y resulta más fácil de explicar a estudiantes, empleadores y otras entidades educativas.

Un primer elemento del marco es la revisión de la pertinencia curricular. Antes de incorporar una nueva credencial al catálogo institucional, es conveniente comprobar que responde a una necesidad formativa identificada y que está relacionada con competencias relevantes para el sector productivo. Esta revisión puede apoyarse en consultas con docentes, empleadores, responsables académicos y documentos de referencia nacionales o internacionales. Lo importante es que la credencial no se cree solo por disponibilidad técnica, sino porque representa un aprendizaje con sentido dentro de la oferta formativa.

El marco de calidad también debe cuidar por la claridad de la información incluida en cada credencial. Los resultados de aprendizaje, los criterios de evaluación, las evidencias requeridas y el nivel de cualificación deben estar redactados de forma comprensible. Una credencial con información incompleta o ambigua pierde valor para quien la consulta. Por ello, los equipos académicos y de calidad deben revisar que la descripción de cada logro sea precisa y permita entender qué competencia se ha certificado.

Desde el punto de vista de la gestión de la información, la calidad exige controles internos sobre los datos utilizados para emitir credenciales. Las instituciones deben verificar que los registros enviados al sistema coincidan con las actas, los listados o los documentos académicos oficiales. También deben establecer revisiones para evitar errores en nombres, identificadores, fechas, competencias y evidencias asociadas. Estos controles reducen las incidencias administrativas y protegen la confianza en las credenciales emitidas.

Otro aspecto relevante es la revisión de los instrumentos de evaluación. Las rúbricas, pruebas, portafolios o evidencias utilizadas deben permitir comprobar que el estudiante ha alcanzado la competencia declarada. El equipo de calidad no debe sustituir el criterio académico del profesorado, pero sí puede revisar que existan criterios explícitos, trazabilidad en la evaluación y coherencia entre lo que se enseña, lo que se evalúa y lo que finalmente se certifica.

La opinión de los usuarios también forma parte del marco de calidad. Las instituciones pueden recopilar información de estudiantes, docentes, personal administrativo y empleadores sobre el uso de las credenciales, la claridad de los procesos y las dificultades encontradas. Esta información ayuda a detectar barreras de adopción, problemas de comunicación o aspectos técnicos que deben mejorarse. La calidad del modelo depende, en parte, de que estas observaciones se incorporen a los ajustes institucionales.

El cumplimiento documentado de estos criterios permite al WP6 sustentar el cierre del paquete de trabajo desde una perspectiva de aseguramiento. No se trata solo de mostrar que se realizaron las actividades, sino de evidenciar que el modelo cuenta con procedimientos revisables, responsabilidades definidas y mecanismos de mejora. Este marco proporciona una base para mantener la integridad académica de los centros emisores una vez finalizado el proyecto.

6.2 Indicadores de impacto y métricas de éxito en la empleabilidad.

Uno de los objetivos de las credenciales digitales es mejorar la forma en que los estudiantes comunican sus competencias al mercado laboral. Para evaluar si esto ocurre, las instituciones deben complementar los datos operativos del sistema con indicadores relacionados con la empleabilidad, el reconocimiento externo y el uso real de las credenciales. Esta medición permite saber si el esfuerzo realizado tiene efectos que van más allá de la mera emisión técnica de insignias.

En el ámbito cuantitativo, los centros pueden registrar cuántas credenciales se emiten, cuántos estudiantes las aceptan, cuántos las almacenan en carteras digitales y cuántos las comparten en redes

profesionales o portales de empleo. También resulta útil medir las verificaciones realizadas por terceros cuando la plataforma lo permita. Estos datos ofrecen una primera aproximación al nivel de uso y visibilidad de las credenciales.

Sin embargo, las cifras de emisión no son suficientes. También conviene analizar cómo perciben los estudiantes el valor de las credenciales. Las encuestas de seguimiento pueden recoger información sobre si los egresados consideran que las insignias les ayudan a explicar mejor sus competencias, a prepararse para las entrevistas de trabajo, a construir su perfil profesional o a acceder a nuevas oportunidades laborales. Esta información permite interpretar mejor los datos de uso y ajustar las acciones de orientación.

La opinión de los empleadores es otro indicador importante. Las IEPF deberían consultar a las empresas si comprenden la información contenida en las credenciales, si confían en los mecanismos de verificación y si consideran útiles los metadatos para procesos de selección o promoción interna. Esta información puede mostrar si las credenciales están redactadas en un lenguaje comprensible para el sector productivo o si necesitan ajustes.

El seguimiento de egresados requiere mecanismos de contacto estables y respetuosos con la protección de datos. Las instituciones pueden establecer encuestas periódicas, entrevistas o espacios de actualización voluntaria para conocer la evolución profesional de sus graduados. Aunque este tipo de seguimiento puede ser complejo, es necesario para analizar si las competencias certificadas guardan relación con las trayectorias laborales, la inserción en el empleo o la mejora de las oportunidades profesionales.

Los resultados obtenidos mediante estos indicadores deben utilizarse en la revisión curricular. Si determinadas credenciales muestran un alto nivel de uso, una buena comprensión por parte de las empresas y una relación con las oportunidades laborales, la institución puede fortalecer esas líneas formativas. Por el contrario, si algunas credenciales tienen baja visibilidad o generan poca comprensión, conviene revisar su diseño, descripción o relación con las necesidades reales del mercado laboral. La medición debe servir para mejorar el modelo, no solo para producir informes.

6.3 Hoja de ruta para la sostenibilidad técnica y financiera del ecosistema.

La finalización de la financiación del proyecto exige que las instituciones definan cómo mantendrán activos los centros de emisión. La sostenibilidad no puede depender únicamente de recursos externos o del esfuerzo puntual de los equipos que participaron en la fase piloto. Para que el modelo continúe, las IEPF deben incorporarlo progresivamente a su planificación académica, técnica y financiera.

Desde el punto de vista financiero, la institución debe identificar los costes que tendrá que asumir. Estos pueden incluir el alojamiento de plataformas, el mantenimiento de sistemas, el soporte técnico, la actualización de estándares, la capacitación del personal y la gestión de incidencias. Una recomendación básica es integrar estos costes en presupuestos ordinarios vinculados a la innovación, la calidad académica o la gestión tecnológica. De este modo, se evita que el centro de emisión funcione como una actividad temporal sin respaldo institucional suficiente.

También se pueden explorar mecanismos complementarios de financiación. Algunas instituciones podrían desarrollar credenciales especializadas para empresas, programas de formación continua o servicios de certificación vinculados a sectores específicos. Estos esquemas deben evaluarse cuidadosamente para no desviar el enfoque educativo del modelo ni crear barreras de acceso para los

estudiantes. Su utilidad dependerá de que contribuyan a sostener la operación sin afectar a la misión formativa de la IEFP.

La sostenibilidad tecnológica requiere una planificación periódica. Las instituciones deben revisar el estado de sus plataformas, su compatibilidad con estándares internacionales, la seguridad de los sistemas y la continuidad de los servicios de verificación. También deben programar actualizaciones, pruebas de copia de seguridad y revisiones de interoperabilidad. Estas tareas ayudan a evitar que las credenciales emitidas pierdan validez técnica o se vuelvan difíciles de verificar con el paso del tiempo.

El personal especializado es otro elemento clave. La salida de una persona que conoce el sistema no debería poner en riesgo la actividad del centro. Para evitarlo, las IEFP deben documentar procedimientos, perfiles de puesto, manuales de uso, políticas de seguridad y rutas de atención de incidencias. También conviene contar con procesos de inducción para los nuevos integrantes. De esta forma, el conocimiento operativo queda en la institución y no solo en personas concretas.

Las alianzas institucionales pueden reforzar la sostenibilidad del modelo. La coordinación con entidades públicas, cámaras empresariales, asociaciones profesionales y otras instituciones educativas puede favorecer el reconocimiento de las credenciales y abrir oportunidades de cooperación. En algunos casos, estas alianzas también pueden facilitar futuras fuentes de apoyo técnico o financiero. Para que resulten útiles, deben alinearse con la gobernanza del centro emisor y con los criterios de calidad definidos por el proyecto.

La hoja de ruta debe revisarse periódicamente. Las necesidades de mantenimiento, los costes, las herramientas y los estándares pueden cambiar. Por ello, la sostenibilidad debe entenderse como una planificación flexible, con responsables y mecanismos de seguimiento definidos. Si la institución asegura recursos, conserva el conocimiento técnico y actualiza sus procesos, el centro de emisión tendrá más posibilidades de mantenerse después de la fase piloto.

6.4 El papel del Observatorio ECOCredGT

El Observatorio ECOCredGT se plantea como un espacio de apoyo para dar continuidad a los resultados del proyecto y facilitar la evolución del modelo de credenciales digitales. Su función principal es reunir conocimientos, organizar la información y promover el intercambio entre instituciones interesadas en implementar centros de emisión. De esta manera, el observatorio puede contribuir a que la experiencia acumulada no se limite a las instituciones que participaron directamente en los pilotos.

Una de sus tareas puede ser la recopilación y difusión de recursos técnicos y metodológicos. Manuales, guías, ejemplos de flujos de trabajo, criterios de calidad y casos de aplicación pueden servir de referencia para otras IEFP. El acceso a estos materiales reduciría la curva de aprendizaje de nuevas instituciones y facilitaría una réplica más ordenada del modelo, siempre y cuando se respeten las condiciones y capacidades de cada contexto.

El observatorio también puede contribuir al seguimiento de los cambios tecnológicos y normativos. Los estándares de interoperabilidad, las soluciones de verificación, las políticas de protección de datos y los marcos de cualificaciones evolucionan con el tiempo. Contar con un espacio que revise estos cambios y los comunique a las instituciones participantes puede ayudar a mantener la compatibilidad técnica y la actualización del modelo.

Otro aporte importante es la formación continua. El observatorio puede organizar encuentros, talleres, seminarios o comunidades de práctica en los que participen docentes, responsables técnicos, equipos de calidad y gestores institucionales. Estos espacios permiten compartir problemas comunes, soluciones aplicadas y recomendaciones derivadas de la experiencia. También pueden fortalecer la cooperación entre centros emisores y evitar que cada institución tenga que resolver los mismos desafíos de forma aislada.

El observatorio puede apoyar, además, la medición agregada del impacto del modelo. A partir de la información proporcionada por los centros participantes (respetando las normas de protección de datos), sería posible elaborar informes sobre el uso de credenciales, su aceptación por parte de los empleadores, las tendencias de empleabilidad y las necesidades de actualización. Estos informes pueden aportar pruebas útiles a instituciones educativas, empresas y responsables de políticas de formación profesional.

Para funcionar de manera sostenible, el observatorio necesitará una estructura de gobernanza clara. Habrá que definir quién participa, cómo se toman las decisiones, qué información se comparte, qué responsabilidades asume cada institución y cómo se financian sus actividades. Sin esta organización, el observatorio podría quedarse en una iniciativa de difusión limitada. Con una estructura adecuada, en cambio, puede convertirse en un mecanismo de coordinación y mejora continua.

El papel del Observatorio ECOCredGT debe entenderse como complementario al trabajo de cada IEFP. Cada institución seguirá siendo responsable de la calidad de sus credenciales y de la gestión de su centro de emisión. El observatorio puede aportar orientación, seguimiento, intercambio de experiencias y actualización técnica. Desde esta perspectiva, contribuye a preservar la continuidad del modelo y a preparar futuras acciones de adaptación en otros contextos de educación y formación profesional.

7. Conclusiones y recomendaciones

Este informe recoge el trabajo realizado en el marco del paquete de trabajo de calidad y presenta las recomendaciones finales para la implementación de centros de emisión de credenciales digitales en instituciones de educación y formación profesional. A lo largo del documento se plantea que este proceso no debe entenderse solo como una actualización tecnológica. La creación de un centro de emisión implica revisar los procedimientos académicos, administrativos, técnicos y de calidad que afectan a la forma en que una institución certifica y comunica los aprendizajes de sus estudiantes.

El análisis realizado muestra que el modelo funciona mejor cuando sus componentes se desarrollan de manera coordinada. La infraestructura tecnológica es necesaria, pero no suficiente si no existe una gobernanza clara, criterios comunes de emisión, flujos de trabajo documentados y personal preparado para operar el sistema. Del mismo modo, las normas internas pierden efectividad si no van acompañadas de formación, seguimiento y una relación activa con el sector productivo.

Desde la perspectiva del WP6, el aseguramiento de la calidad ha permitido revisar el modelo no solo por sus resultados técnicos, sino también por su capacidad para mantenerse en el tiempo. Las recomendaciones presentadas en este informe recogen criterios para diseñar, validar, emitir, verificar y mejorar las microcredenciales. Estos criterios ofrecen una base para que las IIEFP puedan institucionalizar el modelo de forma gradual, ajustándolo a sus capacidades y necesidades específicas.

La experiencia de los pilotos desarrollados por la Universidad Galileo y la Fundación Kinal ha sido especialmente relevante para este proceso. Su trabajo permitió contrastar las propuestas iniciales con las condiciones reales de implementación, incluidos los aspectos relacionados con la conectividad, la infraestructura, la organización interna y la adopción por parte de los equipos. Los hallazgos encontrados ayudaron a ajustar los flujos administrativos, las recomendaciones formativas y los mecanismos de validación propuestos en el documento.

La continuidad del modelo también dependerá del papel que pueda desempeñar el Observatorio ECOCredGT. Este espacio puede ayudar a conservar y actualizar el conocimiento generado por el proyecto, facilitar el intercambio entre instituciones y apoyar futuras acciones de réplica. Su función resultará especialmente útil si logra recopilar información sobre buenas prácticas, cambios tecnológicos, necesidades de formación e indicadores de impacto relacionados con la empleabilidad.

Este capítulo presenta dos subcapítulos. El primero resume las principales recomendaciones derivadas de los capítulos anteriores. El segundo propone una guía de replicabilidad para otras IIEFP interesadas en adaptar el modelo de centros de emisión a sus propios contextos institucionales.

7.1 Recomendaciones

Para facilitar la utilización de los resultados de este informe, se presentan a continuación las principales recomendaciones para la implementación de centros de emisión en las IIEFP:

- **Adopción de estándares abierto:** Se recomienda dar prioridad a los formatos de datos normalizados, como Open Badges y el Modelo Europeo de Aprendizaje, para facilitar la portabilidad, la interoperabilidad y la lectura automática de las credenciales por parte de sistemas externos.
- **Formalización de la gobernanza:** Las instituciones deben oficializar la estructura del centro de emisión mediante normas internas, procedimientos aprobados y el respaldo de la

dirección. Esto incluye definir roles, responsabilidades, perfiles de puesto y un comité o consejo encargado de revisar las propuestas de nuevas credenciales.

- **Diseño basado en evidencias:** Las credenciales deberían estar vinculadas a resultados de aprendizaje verificables, y no solo a la asistencia a una actividad. Se recomienda utilizar rúbricas, evidencias de desempeño y descripciones claras que permitan relacionar la credencial con competencias relevantes para el entorno productivo.
- **Gestión del cambio y formación continua:** La adopción del modelo requiere planes de formación para el personal técnico, docente, administrativo y los estudiantes. También conviene promover comunidades de práctica que permitan compartir experiencias, resolver dudas y actualizar conocimientos a medida que evolucionen las herramientas y los estándares.
- **Sostenibilidad financiera:** Los costes de mantenimiento, alojamiento, asistencia técnica y actualización deben incorporarse progresivamente al presupuesto ordinario de la institución. Las IIEFP también pueden explorar fuentes complementarias de financiación, siempre que estas no comprometan el acceso de los estudiantes ni la misión formativa del modelo.
- **Medición del impacto laboral:** Las estadísticas internas de emisión deben complementarse con información sobre uso, verificación externa, percepción de los empleadores y seguimiento de los egresados. Estos datos ayudarán a determinar si las credenciales contribuyen a aumentar la visibilidad de las competencias y a facilitar el acceso a oportunidades laborales.

7.2 Guía de replicabilidad para otras IIEFP en la región

La réplica del modelo en otras instituciones requiere una implementación progresiva. Las siguientes fases ofrecen una ruta de referencia que cada IIEFP podrá adaptar en función de su tamaño, recursos, normativa interna y nivel de madurez digital.

1. **Preparación y autodiagnóstico:** La institución interesada debe revisar su situación inicial. Dicha revisión incluirá la infraestructura tecnológica, la conectividad, las plataformas existentes, las competencias digitales del personal, los procesos de certificación actuales y la capacidad de mantenimiento. El objetivo es identificar las condiciones favorables, las brechas y los riesgos antes de iniciar el diseño del centro.
2. **Diseño institucional y alineación normativa:** En esta fase se define la ubicación del centro de emisión dentro de la estructura institucional. También se elaboran reglamentos internos, se constituye el comité responsable, se adapta la taxonomía de credenciales y se selecciona un primer catálogo de competencias. Se recomienda comenzar por áreas técnicas con una demanda laboral clara y con equipos académicos dispuestos a participar en la prueba piloto.
3. **Configuración técnica e integración de sistemas:** La institución despliega una arquitectura modular, preferiblemente basada en estándares abiertos y soluciones que puedan mantenerse en el tiempo. El equipo técnico configura el motor de emisión, revisa la integración con las plataformas LMS o los sistemas académicos y valida los mecanismos de seguridad y verificación. Esta fase debe incluir pruebas internas antes de expedir credenciales a los estudiantes.
4. **Capacitación y pilotaje operativo:** Antes de ampliar el modelo a toda la institución, se recomienda realizar una prueba piloto con un programa, curso o área técnica específica. Durante esta etapa, se capacita a docentes, personal administrativo, responsables técnicos y

estudiantes. La prueba piloto permite comprobar los flujos de diseño, validación, emisión y entrega, así como identificar incidencias que deban corregirse en los manuales de procedimiento.

5. **Vinculación externa y sensibilización:** La institución debe comunicar el modelo a empresas, cámaras de comercio, asociaciones profesionales y otros agentes del sector productivo. Las acciones pueden incluir reuniones informativas, talleres para contrastar el currículum y espacios para revisar las competencias prioritarias. Esta vinculación ayuda a que las credenciales sean comprendidas y valoradas en procesos de selección, prácticas profesionales o formación continua.
6. **Institucionalización y adhesión a la red regional:** Una vez validado el proyecto piloto, el centro de emisión puede incorporarse a la actividad ordinaria de la institución. Esto implica asignar presupuesto, definir responsables permanentes, actualizar procedimientos y ampliar progresivamente el catálogo de credenciales. La incorporación al Observatorio ECOcredGT puede facilitar el intercambio de buenas prácticas, la actualización técnica y la alineación con estándares internacionales de calidad.

Referencias

- 1EdTech Consortium. (2024). Open Badges Specification, Version 3.0. 1EdTech Standards. <https://www.1edtech.org/standards/open-badges>
- Alario-Hoyos, C., & Delgado Kloos, C. (2023). Experiences with Micro-Credentials at UC3M: Academic and Technological Aspects. In 2023 IEEE World Engineering Education Conference (EDUNINE) (pp. 1-6). IEEE. <https://doi.org/10.1109/EDUNINE57531.2023.10102861>
- Amado-Salvatierra, H. R., Morales-Chan, M., & Hernandez-Rizzardini, R. (2024). WIP: ECOCredGT Implementing Digital Credentials in Continuous Training for the Labour Market. In 2024 IEEE Frontiers in Education Conference (FIE) (pp. 1-5). IEEE.
- Amado-Salvatierra, H. R., Rizzardini, R. H., & Chan, M. M. (2020). The rise of webinars: thousands of learners looking for professional development. A practical case study. In 2020 IEEE Learning With MOOCS (LWMOOCS) (pp. 191-194). IEEE. <https://doi.org/10.1109/LWMOOCS50143.2020.9234321>
- Chango, M. (2022). Building a credential exchange infrastructure for digital identity: A sociohistorical perspective and policy guidelines. *Frontiers in Blockchain*, 4, Article 629790. <https://doi.org/10.3389/fbloc.2021.629790>
- Council of the European Union. (2022). Proposal for a Council Recommendation on a European approach to micro-credentials for lifelong learning and employability. ST-9237-2022-INIT. <https://data.consilium.europa.eu/doc/document/ST-9237-2022-INIT/en/pdf>
- Delgado Kloos, C., Alario-Hoyos, C., Ibáñez, M. B., Moreno-Marcos, P. M., Muñoz-Merino, P. J., & Estévez-Ayres, I. (2023). Recognizing the Value of Recognition in Education. In 2023 IEEE Global Engineering Education Conference (EDUCON) (pp. 1-5). IEEE. <https://doi.org/10.1109/EDUCON54358.2023.10126781>
- European Commission. (2021). Digital Education Action Plan 2021-2027: Resetting education and training for the digital age. European Union. <https://education.ec.europa.eu/focus-topics/digital-education/action-plan>
- Grech, A., Sood, I., & Ariño, L. (2021). Blockchain, self-sovereign identity and digital credentials: promise versus praxis in education. *Frontiers in Blockchain*, 4, Article 616779. <https://doi.org/10.3389/fbloc.2021.616779>
- Kemcha, R., Alario-Hoyos, C., & Delgado-Kloos, C. (2024). Exploring Recognition in Digital Education through Open Badges and the European Learning Model. In 2024 IEEE Digital Education and MOOCS Conference (DEMOcon) (pp. 1-6). IEEE.
- Knoth, A., Soldo, E., Clancy, K., & Lucke, U. (2023). A Distributed Infrastructure for Secure Diplomas: Proof of Concept and First Experiences. *Proceedings of European University*, 95, 181-192.
- Lenarduzzi, V., & Taibi, D. (2016). MVP explained: A systematic mapping study on the definitions of minimal viable product. In 2016 42th Euromicro Conference on Software Engineering and Advanced Applications (SEAA) (pp. 112-119). IEEE. <https://doi.org/10.1109/SEAA.2016.56>
- Mah, D. (2016). Learning analytics and digital badges: potential impact on student retention in higher education. *Technology, Knowledge and Learning*, 21(3), 285–305. <https://doi.org/10.1007/s10758-016-9286-8>

- McGreal, R., & Olcott Jr., D. (2022). A strategic reset: Micro-credentials for higher education leaders. *Smart Learning Environments*, 9, Article 9. <https://doi.org/10.1186/s40561-022-00190-z>
- OECD. (2023). *Micro-credentials for lifelong learning and employability: Uses and possibilities*. OECD Education Policy Perspectives, No. 66, OECD Publishing, Paris.
- Schwarzthans, M. (2023). *Digital credentials in higher education: An exploratory prototype for TU Wien* (Doctoral dissertation, Technische Universität Wien).
- World Wide Web Consortium. (2022). *Decentralized Identifiers (DIDs) v1.0*. W3C Recommendation. <https://www.w3.org/TR/did-core/>
- World Wide Web Consortium. (2024). *Verifiable Credentials Data Model v2.0*. W3C Recommendation. <https://www.w3.org/TR/vc-data-model-2.0/>