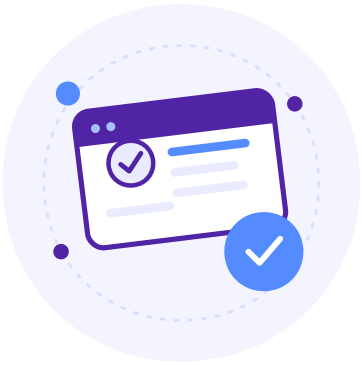
pok

GUÍA PARA DECISORES UNIVERSITARIOS

Cómo evaluar y elegir una plataforma de credenciales digitales

Marco completo de due diligence, auditoría técnica, validación funcional, pruebas de verificabilidad, checklist documental, formulario maestro y matriz comparativa para guiar la decisión institucional.



DESTINATARIOS

Rectores, vicerrectores, secretarías académicas, direcciones de TI y comités de selección de universidades, institutos y escuelas de negocio.

PROPÓSITO

Servir como documento institucional de circulación, base para RFI/RFP, evaluación de proveedores y comité de selección.

BASE NORMATIVA

Estándares 1EdTech y W3C, ecosistema Europass / ELM y prácticas de evaluación de infraestructura tecnológica crítica.

Una decisión de infraestructura, no una compra de herramienta

Esta guía está diseñada para que quien decide en una universidad pueda evaluar con rigor técnico, operativo, legal y funcional una plataforma de credenciales digitales antes de contratarla.

El documento puede utilizarse como guía de mercado, material interno de comité, checklist de due diligence, formulario de RFI/RFP, base para una prueba piloto y matriz de comparación entre múltiples proveedores. Está pensado para circular entre el equipo decisor y dar a todos los participantes un lenguaje común de evaluación.

IDEA CENTRAL

No alcanza con comparar demos, claims comerciales o listas de features. Una institución debe exigir evidencia verificable: estándares implementados, certificaciones vigentes, pruebas funcionales, integraciones comprobadas, arquitectura de datos, controles de privacidad, continuidad operativa y una auditoría real de verificabilidad de la credencial.

Quien decide no está comprando solamente una herramienta para emitir badges o certificados visualmente atractivos. Está eligiendo **infraestructura crítica** para la reputación digital de la institución, la verificación, la portabilidad, la trazabilidad, la privacidad, la empleabilidad de sus egresados, la integración académica y la continuidad futura.

Quién debería usar esta guía

La selección de una plataforma de credenciales rara vez es responsabilidad de una sola persona. Esta guía está pensada para alinear a todos los perfiles que intervienen en la decisión:

Rectorado y vicerrectorados

Definen el porqué institucional, el alcance estratégico y el impacto reputacional de emitir credenciales digitales.

Secretaría académica

Aporta los casos de uso reales: diplomas, microcredenciales, badges apilables y su articulación con la oferta académica.

Dirección de TI / sistemas

Evalúa arquitectura, integraciones con LMS y SIS, seguridad, APIs y continuidad operativa.

Áreas legal y de datos

Revisan cumplimiento, privacidad, DPA/DPSA, subprocesadores y obligaciones regulatorias.

Empleabilidad y vinculación

Valoran portabilidad, verificación pública y valor de la credencial en el mercado laboral.

Compras y administración

Conducen el RFI/RFP, el análisis económico total y las condiciones contractuales y de salida.

Cómo leer este documento

Cada sección puede leerse de forma independiente. El comité puede repartir los pilares según especialidad y consolidar al final con el formulario maestro y la matriz comparativa.

Contenido

Quince apartados que recorren todo el ciclo de evaluación: desde la definición interna de objetivos hasta la recomendación final y los anexos operativos.

1 Objetivo, alcance y principios de evaluación

El marco de criterios que ordena toda la decisión institucional.

La evaluación debe ir mucho más allá de una demo comercial. Quien decide debe recordar que la institución elige infraestructura crítica para reputación digital, verificación, portabilidad, trazabilidad, privacidad, empleabilidad, integración académica y continuidad futura.

1.1 Principios rectores

- **Priorizar interoperabilidad y portabilidad.** La institución debe evitar quedar atada a un proveedor o a un visor propietario.
- **Distinguir estándar, implementación y certificación.** Decir que una plataforma "soporta" un estándar no equivale a demostrar una implementación real y verificable.
- **Evaluar el producto completo, no solo la emisión.** Deben analizarse emisión, verificación, revocación, correcciones, experiencia del receptor, integraciones, analytics, gobierno operativo y salida futura.
- **Pedir evidencia y no solo afirmaciones.** Cada claim relevante debe venir acompañado de documentos, pruebas, sandbox, logs, certificados, reportes o referencias verificables.
- **Comparar con casos de uso reales de la institución.** La validación debe hacerse con escenarios concretos: diploma, microcredencial con skills, badge apilable, integración con LMS/SIS, verificación pública y revocación.
- **Tomar una decisión con criterios ponderados.** Debe existir scoring, umbrales mínimos y red flags de descarte.

1.2 Alcance mínimo de la evaluación

Una evaluación institucional madura debe cubrir, como mínimo, las siguientes diez dimensiones:

- Seguridad de la información.
- Estándares abiertos e interoperabilidad.
- Cumplimiento regulatorio y certificaciones.
- Blockchain, verificabilidad y auditoría de credenciales.
- Funcionalidades de producto y experiencia del usuario.
- Integraciones, APIs, LMS, SIS, SSO y webhooks.
- Privacidad, consentimiento y gobierno de datos.
- Infraestructura en nube, continuidad y resiliencia.
- Monitoreo, trazabilidad y auditoría operativa.
- Sostenibilidad operativa, soporte, roadmap y plan de salida.

Para el comité de selección

Si una de estas diez dimensiones queda sin responsable asignado, la evaluación tendrá un punto ciego. Conviene cerrar la asignación antes de contactar proveedores.

2 Proceso recomendado de selección

Un proceso por etapas evita compras basadas en discurso comercial.

La forma correcta de elegir una plataforma es mediante un proceso por etapas. Saltarse etapas suele generar compras basadas en discurso comercial, costos ocultos y migraciones traumáticas.

Fase	Objetivo	Entregable	Qué valida	Señal de avance
1. Definición interna	Alinear objetivos académicos, técnicos, legales y de empleabilidad	Casos de uso priorizados, criterios de éxito y responsables	Qué se quiere emitir y para qué	La institución sabe exactamente qué necesita
2. RFI inicial	Filtrar proveedores que no cumplen mínimos	Respuesta documental y evidencias	Seriedad, estándar, certificaciones, integraciones y soporte	Quedan solo proveedores viables
3. Demo guiada	Comparar flujos reales bajo el mismo guion	Acta de demo con observaciones	Claims comerciales y UX real	Se valida lo que el proveedor dice tener
4. Due diligence	Revisar seguridad, privacidad, arquitectura y cumplimiento	Checklist completo con semáforos	Riesgos ocultos no visibles en una demo	Se detectan debilidades estructurales
5. Piloto controlado	Probar con datos y procesos reales	Resultados del piloto y feedback	Operación real, tiempos y adopción	Se comprueba que funciona en contexto institucional
6. Evaluación económica y contractual	Entender costo total y salida futura	TCO, SLA, DPA, plan de salida	Costos ocultos, lock-in y continuidad	La comparación económica es realista
7. Decisión e implementación	Elegir y arrancar con gobernanza clara	Matriz final y plan de rollout	Madurez global del proveedor	Inicio con responsables, KPIs y alcance

Recomendación práctica para el comité

El proveedor no debería ver la ponderación completa antes de responder. Primero debe entregar evidencia; luego la universidad aplica el scoring. Esto evita respuestas "optimizadas" para un formulario sin sustento real.

3 Qué pedir obligatoriamente al proveedor

La carpeta mínima de evidencias con la que arranca toda evaluación seria.

Toda evaluación seria debe empezar con una carpeta mínima de evidencias. Si el proveedor no puede o no quiere entregarla, ya existe una señal de riesgo que el comité debe registrar.

Documento / evidencia	Por qué le importa a quien decide	Aceptable si...
Ficha técnica del producto y arquitectura	Permite entender alcance real, límites, módulos, dependencias y modelo de datos	Describe entornos, arquitectura, flujos principales, módulos, APIs y dependencias
Documentación de APIs + sandbox	Valida integrabilidad real	Incluye endpoints, autenticación, ejemplos, rate limits, versionado y ambiente de prueba
Matriz de estándares soportados	Evita claims vagos	Indica estándar exacto, versión, alcance y evidencia de conformidad
Listado de certificaciones vigentes	Comprueba madurez	Incluye organismo, vigencia, alcance y fecha de auditoría
DPA/DPSA y política de privacidad	Revisa obligaciones legales	Aclara roles, subprocesadores, transferencias internacionales y derechos del titular
Listado de subprocesadores	Muestra la cadena de tratamiento de datos	Incluye proveedor, función, país y medidas contractuales
SLA y esquema de soporte	Permite exigir servicio	Define tiempos, canales, severidades, escalamiento y cobertura horaria
Plan de continuidad / disaster recovery	Evalúa resiliencia	Indica backups, RTO, RPO y pruebas periódicas
Informe de pentest o carta ejecutiva	Mide seguridad real	Es reciente, de tercero independiente y con remediaciones documentadas
Clientes de referencia	Contrasta discurso con uso real	Hay casos comparables a la institución
Plan de salida	Evita lock-in	Explica exportación, continuidad de verificación, revocaciones y costos de salida

SEÑAL DE RIESGO TEMPRANA

La negativa, demora injustificada o respuesta evasiva ante esta carpeta mínima es, en sí misma, un dato de evaluación. Un proveedor maduro entrega estas evidencias sin fricción.

4 Dimensiones de evaluación y evidencia exigible

Diez pilares técnicos, cada uno con la evidencia que el comité debe exigir.

Esta sección desarrolla las diez dimensiones que estructuran la evaluación. Para cada pilar se indica qué debe cumplir la plataforma y, sobre todo, **qué evidencia concreta debe pedir y validar** quien decide. Una afirmación sin evidencia no debe puntuarse.

CÓMO USAR LOS DIEZ PILARES

Cada pilar puede asignarse a un perfil del comité según su especialidad. Las páginas siguientes presentan los diez pilares, cada uno con su cabecera identificable, para facilitar el reparto del trabajo y la lectura por partes.

Pilar	Dimensión	Foco principal de la evidencia
1	Seguridad de información	MFA, cifrado, logs auditables, pentests y respuesta a incidentes
2	Estándares abiertos e interoperabilidad	Open Badges 3.0, W3C VC, CLR, ELM / Europass con evidencia real
3	Cumplimiento regulatorio y certificaciones	ISO 27001, SOC 2, GDPR/FERPA, DPA/DPSA y subprocesadores
4	Blockchain y verificabilidad	Qué se registra on-chain, validador público y auditabilidad
5	Funcionalidades técnicas del producto	Emisión, skills, revocación, wallet del receptor y analytics
6	Integraciones y APIs	APIs documentadas, SSO, LMS/SIS, webhooks y LTI 1.3
7	Privacidad y gestión de datos	Mapa de datos, ubicación, retención, consentimiento y derechos
8	Infraestructura en nube	Región de hosting, redundancia, RTO/RPO y disaster recovery
9	Monitoreo y auditoría	Retención de logs, alertas, integridad y soporte forense
10	Sostenibilidad operativa	Roadmap, equipo, viabilidad de negocio y continuidad

01

PILAR UNO

Seguridad de la información

La base sobre la que descansa la confianza en toda credencial emitida.

La plataforma gestiona datos académicos sensibles y emite documentos con valor reputacional. Quien decide debe exigir controles de seguridad demostrables, no declarativos.

Qué debe cumplir la plataforma

- Autenticación multifactor obligatoria para perfiles administrativos y emisores.
- Gestión de roles con principio de menor privilegio y revocación inmediata de accesos.
- Cifrado en tránsito con TLS 1.2 o superior y cifrado en reposo, idealmente AES-256.
- Logs auditables de acceso, cambios de permisos, emisión, revocación, exportación y eventos críticos.
- Escaneos de vulnerabilidades, pentests externos, SDLC seguro, revisión de código y gestión de dependencias.
- Plan de respuesta a incidentes, responsables claros y SLA de notificación.

Cómo validarlo

Pedir demostración en vivo de alta, cambio de rol y revocación; solicitar logs; pedir evidencia de políticas de cifrado y un resumen ejecutivo de las auditorías de seguridad.

PILAR DOS

02 Estándares abiertos e interoperabilidad

La garantía de que la credencial sobrevivirá al proveedor y será portable.

Este pilar protege a la institución del lock-in y asegura que sus egresados puedan usar la credencial en cualquier ecosistema. Es uno de los de mayor peso en el scoring.

Qué debe cumplir la plataforma

- Open Badges 3.0 implementado de manera nativa, no solo mencionado comercialmente.
- W3C Verifiable Credentials cuando el producto afirma emitir credenciales verificables alineadas a ese modelo.
- CLR cuando el proyecto necesita un registro longitudinal o académico más amplio.
- LTI 1.3, OneRoster, CASE u otros marcos cuando la institución necesita integraciones académicas formales.
- European Learning Model (ELM) y compatibilidad con Europass cuando la institución necesita alineación con el ecosistema europeo, movilidad académica, portabilidad semántica o emisión de credenciales compatibles con European Digital Credentials for Learning.
- Capacidad de mapear resultados de aprendizaje, acreditaciones, organizaciones, calificaciones y metadatos académicos al modelo ELM, con evidencia de exportación, validación o interoperabilidad práctica con Europass.
- Posibilidad de exportación en formatos estándar y validación con herramientas independientes.

Qué pedir

Versión exacta del estándar, alcance concreto de implementación, ejemplos emitidos, documentación, validadores externos y, cuando exista, certificación o presencia en directorios oficiales.

COMPATIBILIDAD EUROPEA: EXIGIR PRUEBA

Cuando el proveedor afirme compatibilidad con Europass o con el European Learning Model (ELM), debe presentar mapeo explícito de campos, ejemplos reales de credenciales, validación semántica, documentación técnica y evidencia de interoperabilidad efectiva con el ecosistema Europass o con European Digital Credentials for Learning.

PILAR TRES

03 Cumplimiento regulatorio y certificaciones

El respaldo legal y de auditoría que protege a la institución.

Las áreas legal y de datos de la institución son las protagonistas de este pilar. Las certificaciones deben estar vigentes y cubrir el servicio efectivamente contratado.

Qué debe cumplir la plataforma

- ISO/IEC 27001 vigente para gestión de seguridad de la información.
- SOC 2 Type II cuando aplique, idealmente cubriendo Security, Availability, Confidentiality, Processing Integrity y Privacy según el alcance del servicio.
- Cumplimiento con GDPR, LGPD, CCPA, LFPDPPP, FERPA u otras normas relevantes para la operación institucional.
- DPA/DPSA claros, subprocesadores identificados y mecanismos de transferencia internacional.

NO ACEPTAR RESPUESTAS GENÉRICAS

No alcanza con un "cumplimos con GDPR". El comité debe pedir roles contractuales, políticas, flujos de derechos del titular, mapa de datos y mecanismos concretos de eliminación, exportación y respuesta a incidentes.

04

PILAR CUATRO

Blockchain y verificabilidad

Donde la promesa de verificabilidad se demuestra o se desmorona.

Es el pilar donde más se confunde narrativa con evidencia. La sección 6 lo desarrolla en profundidad con un procedimiento de auditoría completo.

Qué debe cumplir la plataforma

- Declaración precisa de qué blockchain se usa y qué función cumple.
- Explicación exacta de qué se registra on-chain y qué se mantiene off-chain.
- Confirmación de que no se almacenan datos personales en blockchain.
- Existencia de validador público y posibilidad de comprobación independiente en explorer.
- Capacidad de auditar hash, timestamp, estado y trazabilidad de una credencial.

Conexión con la sección 6

Este pilar no se puntúa solo con la respuesta del proveedor. Requiere la auditoría práctica de una credencial real descrita en la sección 6.

PILAR CINCO

05 Funcionalidades técnicas del producto

La capacidad real de la plataforma para emitir y dar valor a cada credencial.

Aquí la secretaría académica define qué necesita emitir realmente. La sección 5 explica cómo validar cada funcionalidad declarada.

Qué debe cumplir la plataforma

- Emisión individual y masiva.
- Templates, branding, múltiples idiomas, unidades académicas y permisos por rol.
- Skills, competencias, outcomes, evidencias, rúbricas, pathways, stackability y relaciones entre credenciales.
- Revocación, expiración, renovación, reemisión, corrección controlada y versionado.
- Wallet o locker del receptor, sharing, descarga, verificación pública, accesibilidad y experiencia móvil.
- Analytics operativos y reportes útiles para gestión académica y empleabilidad.

06

PILAR SEIS

Integraciones y APIs

La articulación con el ecosistema tecnológico ya existente en la universidad.

La dirección de TI evalúa este pilar. Una integración débil con el LMS o el SIS puede convertir una buena plataforma en una carga operativa.

Qué debe cumplir la plataforma

- APIs documentadas, autenticación clara, sandbox, ejemplos, límites, versionado y backward compatibility.
- SSO con SAML 2.0, OAuth 2.0 u OpenID Connect según el caso.
- LMS, SIS, CRM, ERP, HRIS, plataformas de assessment y mensajería.
- Webhooks o eventos para emisión, revocación, claim, expiración u otros flujos.
- LTI 1.3 y otros marcos edtech cuando corresponda.

07

PILAR SIETE

Privacidad y gestión de datos

El gobierno de los datos personales y académicos confiados a un tercero.

Este pilar tiene umbral mínimo alto en el scoring. La universidad sigue siendo responsable de los datos de sus estudiantes aunque la operación esté tercerizada.

Qué debe cumplir la plataforma

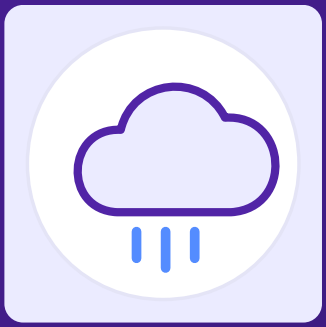
- Mapa exacto de datos personales y académicos: obligatorios, opcionales y derivados.
- Ubicación de datos por ambiente y por cliente.
- Retención, eliminación, corrección, anonimización, exportación y derecho de acceso.
- Consentimiento explícito cuando corresponda y registro auditable de ese consentimiento.
- Capacidad de separar continuidad de verificación de eliminación de datos personales.

PILAR OCHO

08

Infraestructura en nube

La resiliencia técnica que mantiene las credenciales disponibles en el tiempo.



La continuidad operativa de la verificación depende de una infraestructura sólida. Quien decide debe entender dónde viven los datos y qué pasa ante un fallo.

Qué debe cumplir la plataforma

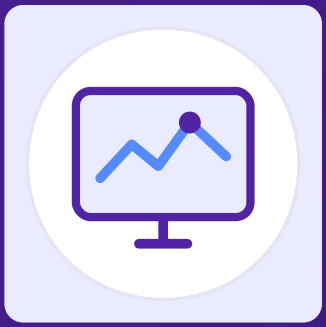
- Región o país de hosting.
- Redundancia, backups, alta disponibilidad y arquitectura multi-tenant o single-tenant según el modelo.
- RTO, RPO, continuidad operativa y pruebas de disaster recovery.
- Gestión de secretos, llaves y ambientes separados.

09

PILAR NUEVE

Monitoreo y auditoría

La capacidad de observar, registrar y reconstruir lo que ocurre en la plataforma.



Sin trazabilidad no hay rendición de cuentas. Este pilar habilita la respuesta de la institución ante incidentes y auditorías internas o externas.

Qué debe cumplir la plataforma

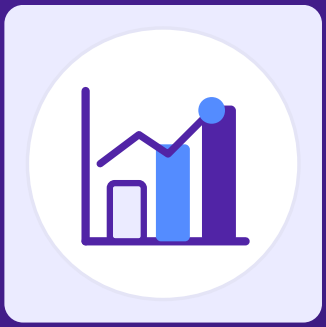
- Retención de logs y nivel de detalle.
- Alertas de seguridad y trazabilidad de acciones administrativas.
- Integridad de registros, exportabilidad y soporte a análisis forense.
- Paneles o reportes de monitoreo para la institución.

PILAR DIEZ

10

Sostenibilidad operativa

La probabilidad de que el proveedor siga existiendo y dando soporte a futuro.



Una credencial debe poder verificarse durante décadas. Quien decide evalúa aquí no solo el producto, sino la viabilidad del proveedor como organización.

Qué debe cumplir la plataforma

- Roadmap claro y consistencia del producto.
- Equipo de soporte y capacidad real de implementación.
- Viabilidad de negocio y continuidad del proveedor.
- Comunidad, alianzas, referencias y estabilidad del servicio.

Una pregunta clave para el comité

Si el proveedor cerrara mañana, ¿las credenciales ya emitidas seguirían siendo verificables? La respuesta separa una plataforma sólida de una apuesta arriesgada.

5 Cómo validar las funcionalidades declaradas

Una funcionalidad solo cuenta si fue documentada y demostrada de punta a punta.

Este punto es crítico. Dos proveedores pueden contestar "sí" a la misma funcionalidad y, sin embargo, ofrecer soluciones radicalmente diferentes. Una funcionalidad solo debe considerarse disponible si fue documentada y además demostrada end-to-end.

- Exigir una demostración sobre un guion común preparado por la universidad.
- Pedir acceso temporal a sandbox o tenant de prueba.
- Solicitar documentación, capturas, video corto o walkthrough por cada feature crítica.
- Usar un caso de prueba propio de la institución con datos reales o semi-reales.
- Verificar la funcionalidad de punta a punta: configuración, emisión, experiencia del alumno, verificación externa, corrección posterior y administración.
- Registrar evidencia en acta con semáforo: existe, existe parcialmente, requiere desarrollo adicional, depende de partner/servicio profesional o no existe.
- No puntuar roadmap, marketplace o dependencia de terceros como funcionalidad nativa disponible.

Feature crítica	Prueba exigida	Resultado esperado	Puntaje 0–5
Emisión masiva	Emitir lote real con archivo de prueba	Se emiten correctamente, con trazabilidad y errores controlados	
Verificación pública	Validar credencial sin login desde enlace externo	Verificación clara, pública y consistente	
Revocación	Revocar y volver a validar	El estado cambia correctamente y queda auditado	
Corrección / actualización	Editar dato permitido o reemitir según política	Se mantiene traza y coherencia del historial	
Skills / competencias	Mapear skill, nivel, evidencia y criterio	La estructura queda visible y verificable	
LTI / LMS	Lanzar desde el LMS y capturar contexto	El flujo funciona con el estándar declarado	
API de emisión	Emitir desde API con credenciales de prueba	La emisión funciona con auth y respuesta documentadas	
Analytics	Extraer dashboard o reporte útil	Los datos son utilizables para gestión	
Exportación	Descargar datos y credenciales	El formato es estándar y utilizable	

6 Auditoría técnica de la credencial y verificabilidad en blockchain

Cómo comprobar si la verificabilidad es real o solo una narrativa de marketing.

ADVERTENCIA CRÍTICA

La palabra "blockchain" se usa con frecuencia sin rigor técnico. Esta sección describe cómo auditar si una credencial realmente fue registrada de forma correcta y verificable, o si el proveedor solo exhibe una narrativa de marketing.

6.1 Preguntas fundacionales que debe responder el proveedor

- Qué blockchain utiliza exactamente: Ethereum, Polygon, LACNet, Bitcoin, Solana, Hyperledger, cadena privada, sidechain u otra.
- Quién opera los nodos y si la red es pública, permisionada o completamente privada.
- Qué dato registra on-chain: hash, identificador, prueba criptográfica, evento de contrato, metadata mínima o la credencial completa.
- Qué dato se guarda off-chain y dónde se aloja.
- Cómo se realiza la validación de integridad de una credencial y cómo se prueba la revocación.
- Cómo evita almacenar datos personales en blockchain.
- Cuál es la relación entre el viewer de la credencial, el botón de validación y la transacción que muestra el explorer.

6.2 Procedimiento obligatorio de auditoría de una credencial real

Además de revisar documentos, la auditoría debe hacerse sobre una credencial real del proveedor. No alcanza con que la plataforma muestre un hash o un ícono de blockchain. La institución debe comprobar que la credencial fue efectivamente registrada on-chain y que la transacción fue exitosa.

PASO CRÍTICO DE AUDITORÍA ON-CHAIN

La universidad debe entrar en una credencial real del proveedor, validar la credencial apretando el botón de validación, luego hacer click en el hashtag, ícono o enlace de blockchain que muestra la credencial, y recién allí verificar en el explorer que la transacción fue correcta. La transacción no puede estar en estado **failed, reverted, dropped** o similar. Además, la revisión debe cubrir todos los tabs relevantes del explorer para evitar falsos positivos visuales en los que no hay token transfers, aparecen failed internal transactions o, en términos prácticos, la credencial nunca quedó correctamente registrada on-chain.

PROCEDIMIENTO PASO A PASO

1. Entrar en una credencial real del proveedor, preferentemente una credencial pública emitida por un cliente o por el propio proveedor.
2. Usar el botón de validación de la credencial. El validador debe confirmar el estado de la credencial y exponer, directa o indirectamente, el vínculo con la prueba criptográfica o transacción.

3. Hacer click en el hashtag, ícono o enlace de blockchain que muestra la credencial o el validador. Ese link debería llevar a un blockchain explorer o a una referencia equivalente verificable públicamente.
4. Una vez en el explorer, verificar que la transacción exista y que su estado sea exitoso. No debe figurar como failed, reverted, dropped, cancelled ni con estados equivalentes según la cadena.
5. Revisar el hash de transacción, timestamp, bloque, dirección o contrato involucrado y consistencia con la fecha de emisión de la credencial.
6. Revisar todos los tabs relevantes del explorer. Dependiendo de la red, pueden existir pestañas como Overview, Logs, Token Transfers, Internal Transactions, Events o State. La revisión no debe quedarse solo en la portada de la transacción.
7. Confirmar que no exista una situación engañosa en la que el explorer muestre una transacción fallida, sin token transfers, o con failed internal transactions, porque eso puede significar que la credencial nunca fue registrada correctamente on-chain.
8. Verificar que el dato grabado o el evento emitido esté razonablemente conectado con la credencial auditada. Si el proveedor solo muestra un link genérico al explorer, sin forma de vincularlo a la credencial, la prueba no alcanza.
9. Repetir la validación en más de una credencial si es posible: una activa, una revocada y una recién emitida.
10. Documentar capturas, URLs, estado de transacción y cualquier inconsistencia detectada.

6.3 Qué revisar exactamente en el explorer

- **Estado de la transacción:** debe ser exitoso.
- **Hash de la transacción y bloque.**
- **Timestamp** y consistencia temporal con la emisión.
- **Contrato, método o evento** utilizado, cuando el explorer lo muestra.
- **Logs o eventos** relevantes.
- **Token Transfers,** si el modelo del proveedor efectivamente implica minting o transferencia. La ausencia de transfers no siempre invalida una credencial, pero sí obliga a entender qué prueba on-chain se registró realmente.
- **Internal Transactions,** cuando existan. Si aparecen fallidas, revertidas o inconsistentes, deben investigarse.
- **Coherencia** entre el dato mostrado en el viewer/validador y la evidencia on-chain.

Importante para quien decide

No todas las arquitecturas blockchain registran una credencial como token transfer. Algunas registran solo hashes, eventos o pruebas criptográficas. Por eso la verificación no consiste únicamente en "ver un NFT" o "ver una transferencia", sino en entender si la prueba on-chain real existe, fue exitosa y está vinculada de manera consistente con la credencial auditada.

MATRIZ OPERATIVA DE REVISIÓN DEL EXPLORER

Elemento	Qué debería verse	Red flag
Estado / Status	Success, confirmed o equivalente. Debe existir la transacción y haber sido procesada correctamente.	Failed, reverted, dropped, cancelled, pending indefinido o error sin explicación.
Token Transfers	Solo si el modelo del proveedor realmente implica minting o transferencia. Deben ser coherentes con la credencial auditada.	No hay transfers cuando el proveedor afirma minting/NFT; transfers inconsistentes con fecha, contrato o receptor.
Internal Transactions	Deben ser coherentes con la lógica del contrato, o no existir si la arquitectura no las usa.	Failed internal transactions, reverts o trazas inconsistentes sin explicación técnica suficiente.
Logs / Events	Eventos del contrato o logs que permitan vincular la evidencia on-chain con la credencial.	No hay forma de conectar la credencial con el evento, o los logs contradicen lo que dice el visor.
Timestamp, bloque y contrato	Deben ser consistentes con fecha de emisión, red y contrato declarados por el proveedor.	Diferencias temporales relevantes, contrato no identificado o red distinta a la declarada.

6.4 Pruebas prácticas mínimas de verificabilidad

1. **Generación de credencial test:** pedir una credencial de prueba, descargarla o verla en el viewer y extraer sus identificadores.
2. **Verificación independiente del hash o txid:** usar el explorer directamente y no depender solo del viewer del proveedor.
3. **Validación de firma criptográfica** o estructura verificable, cuando el estándar lo permita.
4. **Revocación:** revocar la credencial de prueba y comprobar que el estado cambia en el validador y, cuando aplica, en la evidencia on-chain.
5. **Validador público:** comprobar que una tercera parte puede verificar la credencial sin login y sin exponer datos innecesarios.
6. **Portabilidad:** exportar la credencial o sus metadatos en formato estándar y comprobar que siguen siendo utilizables.

6.5 Señales de alerta específicas de blockchain-washing

BLOCKCHAIN-WASHING · SEÑALES DE ALERTA

Las siguientes situaciones indican que la promesa de verificabilidad puede no tener sustento técnico real:

- No pueden explicar qué blockchain usan exactamente.
- No pueden mostrar una transacción real en un explorer público o verificable.
- La validación solo funciona dentro del visor propietario.
- El botón de validación no expone evidencia verificable independiente.
- El explorer muestra transacciones failed, internal transactions fallidas o inconsistencias temporales.
- No se puede vincular razonablemente la credencial con el dato on-chain.
- Guardan o parecen guardar datos personales directamente en blockchain.
- Cobran por verificar credenciales o la verificación depende enteramente de la continuidad comercial del proveedor.
- Hablan de "inmutabilidad" o "NFT" sin poder mostrar pruebas técnicas auditables.

7 Red flags y causales de descarte

Situaciones que, por sí solas, justifican detener o descartar una evaluación.

Las siguientes situaciones justifican, por sí solas, detener o descartar una evaluación salvo que el proveedor pueda remediarlas con evidencia fuerte y verificable. Quien decide debe tratarlas como criterios eliminatorios, no como simples puntos negativos del scoring.

	Causal de descarte
01	Ausencia de documentación técnica relevante.
02	Negativa a mostrar sandbox o pruebas funcionales.
03	Claims de estándares sin documentación, validadores ni ejemplos.
04	Falta de respuesta sobre subprocesadores, ubicación de datos o DPA/DPSA.
05	Ausencia de MFA para emisores y administradores.
06	Imposibilidad de exportar datos y credenciales en formatos útiles.
07	Falta de plan de salida o continuidad de verificación al terminar el contrato.
08	Uso ambiguo de blockchain sin prueba independiente.
09	Certificaciones vencidas, parciales o no aplicables al servicio ofrecido.
10	Roadmap presentado como producto disponible.

Regla de decisión

Ante cualquiera de estas red flags, el comité debería pausar la evaluación y exigir evidencia de remediación inmediata antes de continuar. Sin remediación, corresponde el descarte.

8 Formulario maestro de evaluación institucional

La batería de preguntas lista para usar como RFI/RFP o due diligence.

La siguiente batería puede utilizarse como formulario de RFI/RFP o de due diligence. Se recomienda pedir respuestas con evidencia adjunta y marcar cada ítem como **Documentado, Demostrado, Certificado, Pendiente o No disponible**.

IDENTIFICACIÓN DE LA EVALUACIÓN

Nombre de la plataforma	
Proveedor / empresa	
Fecha de evaluación	
Evaluador	
Alcance del caso de uso evaluado	

8.1 Producto y alcance funcional

Pregunta	Tipo de evidencia	Evaluación
¿Qué tipos de credenciales emite y gestiona la plataforma?	DOC DEMO CERT LINK	
¿Soporta emisión individual y masiva, renovación, expiración, revocación, reemisión y versionado?	DOC DEMO CERT LINK	
¿Permite skills, competencias, resultados de aprendizaje, evidencias, rúbricas o alineaciones?	DOC DEMO CERT LINK	
¿Soporta pathways, stackability, equivalencias o relaciones entre credenciales?	DOC DEMO CERT LINK	
¿Permite múltiples marcas, unidades académicas, campus, idiomas y permisos por rol?	DOC DEMO CERT LINK	

8.2 Estándares e interoperabilidad

Pregunta	Tipo de evidencia	Evaluación
¿Qué estándares soporta exactamente? Indicar versión y alcance: Open Badges, W3C Verifiable Credentials, CLR, European Learning Model (ELM), Europass / European Digital Credentials for Learning, LTI, OneRoster, CASE u otros.	DOC DEMO CERT LINK	
¿El proveedor puede demostrar compatibilidad semántica y/o interoperabilidad práctica con Europass o con el European Learning Model (ELM)? Adjuntar mapeo de campos, ejemplos emitidos, validación y evidencia funcional.	DOC DEMO CERT LINK	
¿Qué partes del estándar están implementadas nativamente y cuáles requieren desarrollo adicional?	DOC DEMO CERT LINK	
¿Existe certificación externa, validación o presencia en directorios oficiales?	DOC DEMO CERT LINK	
¿Cómo se maneja la verificación criptográfica, la revocación y la portabilidad entre sistemas?	DOC DEMO CERT LINK	
¿Qué dependencia existe de viewers o wallets propietarias?	DOC DEMO CERT LINK	

8.3 Integraciones

Pregunta	Tipo de evidencia	Evaluación
¿Qué APIs ofrece? Adjuntar documentación, autenticación, rate limits y versionado.	DOC DEMO CERT LINK	
¿Cuenta con webhooks, colas, exportaciones programadas o conectores nativos?	DOC DEMO CERT LINK	
¿Qué integraciones tiene con LMS, SIS, CRM, ERP, HRIS, assessment platforms y SSO?	DOC DEMO CERT LINK	
¿Puede operar con SAML, OAuth 2.0, OpenID Connect o SCIM donde corresponda?	DOC DEMO CERT LINK	
¿Cómo se sincronizan alumnos, cursos, resultados, cohortes y cambios?	DOC DEMO CERT LINK	

8.4 Seguridad

Pregunta	Tipo de evidencia	Evaluación
¿Requiere MFA para perfiles administradores y emisores?	DOC DEMO CERT LINK	
¿Cómo se gestiona el acceso privilegiado, la segregación por tenant y la revocación inmediata de usuarios?	DOC DEMO CERT LINK	
¿Qué cifrado utiliza en tránsito y en reposo?	DOC DEMO CERT LINK	
¿Conserva logs auditables? ¿Por cuánto tiempo? ¿Cómo garantiza integridad y monitoreo?	DOC DEMO CERT LINK	
¿Con qué frecuencia realiza escaneos de vulnerabilidades y pentests externos?	DOC DEMO CERT LINK	
¿Qué prácticas de SDLC seguro, revisión de código, gestión de dependencias y CI/CD aplica?	DOC DEMO CERT LINK	
¿Cuál es su proceso de gestión de incidentes y notificación a clientes?	DOC DEMO CERT LINK	

8.5 Privacidad y datos

Pregunta	Tipo de evidencia	Evaluación
¿Qué datos personales y académicos almacena exactamente? Separar obligatorios, opcionales y derivados.	DOC DEMO CERT LINK	
¿Dónde se alojan los datos por ambiente y por cliente? Indicar país o región.	DOC DEMO CERT LINK	
¿Quiénes son sus subprocesadores y qué rol cumplen?	DOC DEMO CERT LINK	
¿Cómo se gestionan retención, borrado, anonimización, corrección y exportación?	DOC DEMO CERT LINK	
¿Qué mecanismos usa para transferencias internacionales de datos?	DOC DEMO CERT LINK	
¿Cómo aborda GDPR, FERPA y legislación local aplicable?	DOC DEMO CERT LINK	

8.6 Operación y servicio

Pregunta	Tipo de evidencia	Evaluación
¿Cuál es el SLA estándar y qué incluye el soporte?	DOC DEMO CERT LINK	
¿Qué idioma y huso horario cubre el soporte?	DOC DEMO CERT LINK	
¿Cómo se implementa, cuánto dura y qué depende del cliente?	DOC DEMO CERT LINK	
¿Qué formación ofrece a administradores, emisores y soporte interno?	DOC DEMO CERT LINK	
¿Qué referencias comparables puede compartir?	DOC DEMO CERT LINK	

8.7 Contrato, costos y salida

Pregunta	Tipo de evidencia	Evaluación
Describir el modelo de pricing y todos los componentes facturables.	DOC DEMO CERT LINK	
Indicar límites de uso, storage, emisores, templates, integraciones, wallets, analytics y ambientes.	DOC DEMO CERT LINK	
¿Qué ocurre al terminar el contrato con verificación, hosting y exportación de datos?	DOC DEMO CERT LINK	
¿Existe costo por migración, salida o continuidad de verificación?	DOC DEMO CERT LINK	
¿La universidad conserva propiedad y control sobre sus datos y metadatos?	DOC DEMO CERT LINK	

Sugerencia de uso

Este formulario puede enviarse tal cual al proveedor como RFI. Conviene pedir que cada respuesta venga numerada y con su evidencia adjunta identificada, para facilitar la consolidación posterior en la matriz comparativa.

9 Guion de demo, piloto y pruebas

El recorrido común que todo proveedor debe ejecutar para una comparación justa.

Para que la comparación entre proveedores sea justa, todos deben ejecutar el mismo guion sobre escenarios reales de la institución. Este guion sirve tanto para la demo guiada como para el piloto controlado.

1. Configurar una credencial con branding institucional, metadatos, criterios y evidencias.
2. Emitir una credencial individual y un lote masivo.
3. Asignar skills o competencias y mostrarlas en la credencial o en su detalle.
4. Realizar claim por parte del receptor y compartirla externamente.
5. Verificar la credencial desde fuera de la plataforma.
6. Auditar el botón de validación y el enlace a blockchain/explorer cuando exista.
7. Revocar una credencial y verificar el cambio de estado.
8. Corregir un dato permitido y revisar la trazabilidad.
9. Consumir una API o webhook de ejemplo.
10. Mostrar permisos por rol y segregación por unidades académicas.
11. Exportar datos, metadatos y evidencias relevantes.
12. Probar accesibilidad, experiencia móvil y multilenguaje cuando sea requisito.

Recomendación para el comité

Conviene que el mismo grupo de personas observe todas las demos con este guion en mano y registre las observaciones en un acta común. Eso reduce el sesgo y hace comparables las evaluaciones.

10 Metodología de scoring y matriz comparativa

Cómo convertir la evidencia recogida en una decisión ponderada y defendible.

Se recomienda usar una escala de 0 a 5 por criterio. El scoring debe aplicarse solamente a funcionalidades o controles documentados y demostrados. El roadmap no se puntúa como disponibilidad actual.

Score	Significado	Interpretación	Aceptación
0	No cumple	No implementado o explícitamente no soportado	Rechazo
1	Muy débil / roadmap	Prometido o parcialmente conceptual	No contar como feature disponible
2	Parcial	Existe con limitaciones significativas	Requiere investigación adicional
3	Adecuado	Implementado correctamente y con evidencia suficiente	Cumple mínimo
4	Sólido	Implementado robustamente y con auditoría o madurez comprobable	Muy buen nivel
5	Excelente	Implementación excepcional, transparente y líder	Fortaleza clara

Pesos sugeridos por dimensión

Dimensión	Peso sugerido	Umbral mínimo
Estándares e interoperabilidad	20%	No menos de 3/5
Funcionalidad del producto	20%	No menos de 3/5
Seguridad	15%	No menos de 4/5
Privacidad y datos	15%	No menos de 4/5
Blockchain y verificabilidad	10%	No menos de 3/5
Integraciones y APIs	10%	No menos de 3/5
Operación y soporte	5%	No menos de 3/5
Economía total	3%	No menos de 3/5
Plan de salida / no lock-in	2%	No menos de 3/5

Fórmula e interpretación

Score ponderado final = suma de (score de cada dimensión × peso). Interpretación sugerida: 4.0 o más = recomendado; 3.0 a 3.9 = aceptable con reservas; menos de 3.0 = no recomendado.

REGLA DE GOBIERNO

Aunque el promedio general sea alto, un proveedor no debería aprobar si no alcanza los mínimos en seguridad, privacidad o verificabilidad.

10.1 Matriz resumida de comparación

Criterio	Peso	Proveedor A	Proveedor B	Proveedor C
Estándares	20%			
Funcionalidad	20%			
Seguridad	15%			
Privacidad	15%			
Blockchain y verificabilidad	10%			
Integraciones	10%			
Soporte	5%			
Economía	3%			
Salida	2%			
Score final	**100%**			

11 Evaluación económica, contractual y plan de salida

El costo total real, más allá del precio de lista, y las condiciones de continuidad.

La evaluación económica no termina en el precio de lista. Quien decide debe entender el costo total de propiedad, los costos ocultos y, sobre todo, qué ocurre el día que el contrato finalice.

- Revisar precio por emisor, por alumno, por credencial, por módulo, por integración o por storage.
- Identificar costos ocultos: implementación, branding, APIs, analytics, soporte premium, migración, wallet, templates, ambientes y training.
- Exigir SLA, DPA, límites de responsabilidad, subprocesadores, continuidad, backups y tratamiento de incidentes.
- Confirmar qué ocurre al finalizar el contrato: exportación de datos, revocaciones, continuidad de verificación, costos y formato de entrega.
- Verificar que la universidad conserve propiedad y control sobre datos, metadatos y evidencias que le pertenecen.

La pregunta del plan de salida

Antes de firmar, el comité debe poder responder: si cambiamos de proveedor en cinco años, ¿qué pasa con las credenciales ya emitidas y con su verificación? Si la respuesta no es clara, hay riesgo de lock-in.

12 Recomendación institucional final

El criterio que debería ordenar la decisión por encima de la estética y el discurso.

Una universidad no debería elegir una plataforma de credenciales digitales por estética, discurso comercial o lista de checks. Debería elegirla por **capacidad demostrada** para emitir, verificar, integrar, preservar, proteger y gobernar credenciales y datos con estándares abiertos, evidencia verificable y un costo total entendible.

La mejor práctica es combinar formulario documental, demo guiada, due diligence, piloto real, scoring ponderado y revisión contractual. Cuando un proveedor realmente tiene la capacidad que declara, este proceso lo fortalece. Cuando no la tiene, este proceso lo expone.

En especial, toda evaluación madura debería incluir la auditoría práctica de una credencial real y de su evidencia de validación. Si la credencial no puede validarse de manera confiable e independiente, la promesa de verificabilidad queda seriamente debilitada.

CONCLUSIÓN OPERATIVA

No compre declaraciones.
Compre evidencia.

Anexo A · Checklist rápida de descarte

Ocho preguntas de control para una primera filtración rápida de proveedores. Pensada para un cribado ágil antes de la evaluación a fondo.

- [ ] ¿Tiene ISO 27001 vigente y, si aplica, SOC 2 Type II?
- [ ] ¿Implementa estándares abiertos con versión exacta y evidencia real?
- [ ] ¿Puede demostrar, cuando lo declara, compatibilidad real con Europass y/o con el European Learning Model (ELM), con evidencia técnica y validación funcional?
- [ ] ¿Se puede verificar una credencial independientemente y auditar su evidencia técnica?
- [ ] ¿Tiene APIs documentadas, sandbox y logs auditables?
- [ ] ¿Cumple privacidad y evita almacenar datos personales en blockchain?
- [ ] ¿Permite exportar datos y credenciales en formatos utilizables?
- [ ] ¿Tiene plan de salida y continuidad de verificación?

CRITERIO DE DESCARTE

Si la respuesta es no a cualquiera de estas preguntas y el proveedor no aporta evidencia de remediación inmediata, la plataforma debería pasar a estado de descarte o pausa.

Anexo B · Plantilla resumida para RFI/RFP

Estructura mínima de contenidos que la institución debería incluir al armar su solicitud de información o de propuesta.

Contexto institucional
Descripción de la institución y casos de uso priorizados.

Volumen y usuarios
Volumen esperado de credenciales y perfiles de usuario.

Estándares
Estándares requeridos y versiones mínimas aceptadas.

Integraciones
Integraciones obligatorias y deseables.

Seguridad y privacidad
Requisitos de seguridad, privacidad y hosting.

Soporte e implementación
Requisitos de soporte, idiomas y plazos de implementación.

Evidencia
Evidencia obligatoria a presentar por el proveedor.

Piloto
Formato del piloto y criterios de aceptación.

Pricing
Modelo de pricing requerido y desglose completo.

Salida
Condiciones mínimas de exportación y salida.

Anexo C · Referencias de estándares y marcos utilizados

Fuentes oficiales que sustentan los criterios de esta guía. Se recomienda verificar siempre la vigencia directamente en las fuentes originales.

1. **1EdTech Consortium · Open Badges.** Página oficial del estándar y recursos de implementación. Consultado en abril de 2026. 1edtech.org/standards/open-badges
2. **1EdTech Consortium · Open Badges Certification Process.** Proceso oficial de certificación de conformidad para Open Badges. Consultado en abril de 2026. 1edtech.org/certification/open-badges
3. **1EdTech Consortium · TrustEd Apps Program Overview.** Directorio oficial de productos con certificación/interoperabilidad verificada por 1EdTech. Consultado en abril de 2026. 1edtech.org/program/trustedapps
4. **World Wide Web Consortium (W3C) · Verifiable Credentials Data Model v2.0.** Recomendación oficial publicada el 15 de mayo de 2025. w3.org/TR/vc-data-model-2.0
5. **European Commission / Europass · European Digital Credentials.** Infraestructura oficial para crear, emitir, almacenar, compartir y verificar credenciales digitales europeas. europass.europa.eu/en/european-digital-credentials
6. **European Commission / Europass · European Digital Credentials for Learning (EDC).** Definición oficial de credenciales digitales europeas para aprendizaje. europass.europa.eu/en/european-digital-credentials-learning
7. **European Commission / Europass · Information for Developers.** Documentación técnica del ecosistema Europass. europass.europa.eu/en/information-developers
8. **European Commission / Europass · European Learning Model (ELM) Browser.** Modelo oficial de datos europeo para aprendizaje y credenciales. europa.eu/europass/elm-browser
9. **European Commission / Europass · Latest developments to the European Learning Model.** europass.europa.eu/en/news/latest-developments-european-learning-model
10. **OWASP · Application Security Verification Standard (ASVS).** owasp.org/www-project-application-security-verification-standard
11. **OWASP · Authentication Cheat Sheet.** cheatsheetseries.owasp.org
12. **NIST · SP 800-218 Secure Software Development Framework (SSDF).** csrc.nist.gov/publications/detail/sp/800-218/final
13. **EUR-Lex · Regulation (EU) 2016/679 (GDPR).** eur-lex.europa.eu/eli/reg/2016/679/oj
14. **Etherscan Docs.** docs.etherscan.io

Nota sobre las referencias

Estas referencias complementan el material base aportado por la institución. La guía recomienda verificar siempre la vigencia de certificaciones, versiones de estándares y evidencias técnicas directamente en las fuentes oficiales al momento de la compra. Las referencias normativas y técnicas fueron consolidadas a partir de fuentes oficiales de 1EdTech, W3C y OWASP revisadas en marzo de 2026.

pok

¿Listos para tomar una decisión basada en evidencia?

En POK acompañamos a las universidades en la evaluación, implementación y gobierno de credenciales digitales verificables, con estándares abiertos y verificabilidad real. Si su comité está evaluando proveedores, hablemos.

CONTACTO

pok.tech · contacto@pok.tech