GUÍA 2026 · EDICIÓN TÉCNICA

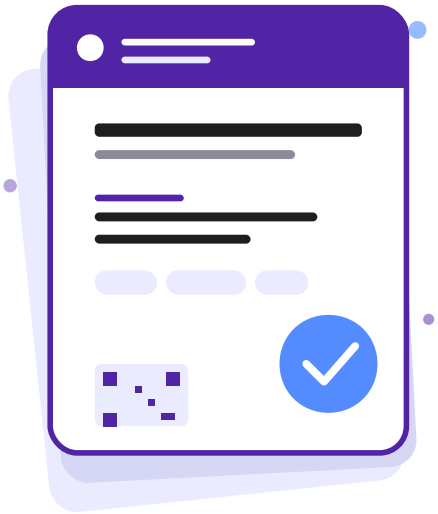
Guía Integral de Evaluación de Plataformas de Credenciales Digitales

MARCO EXHAUSTIVO PARA EVALUACIÓN TÉCNICA, SEGURIDAD, CUMPLIMIENTO, BLOCKCHAIN Y AUDITORÍA DE VERIFICABILIDAD

ABRIL 2026

pok

Una guía para decidir con criterio técnico, no con marketing.



Las plataformas de credenciales digitales se han convertido en infraestructura crítica para instituciones educativas, empleadores, gobiernos y organizaciones de capacitación. Pero no todas ofrecen el mismo nivel de seguridad, transparencia, interoperabilidad y capacidad técnica verificable.

Esta guía consolida estándares internacionales, marcos regulatorios y prácticas reales de selección utilizadas por instituciones líderes a nivel global. Refleja procesos de **due diligence aplicados en contextos reales** de adopción tecnológica en educación superior y organismos públicos.

¿Qué encontrarás dentro?

- ✓ Un **framework de 10 pilares** para evaluar cualquier plataforma sin omisiones
- ✓ Protocolos paso a paso para validar reclamaciones de blockchain
- ✓ Matrices de scoring ponderado y umbrales mínimos no negociables
- ✓ Red flags de descarte inmediato y red flags críticas
- ✓ Un formulario maestro de auditoría técnica listo para imprimir

¿Para quién es esta guía?

Universidades, escuelas de negocios, organismos públicos, entidades certificadoras, áreas de RRHH corporativo y equipos de compras tecnológicas que necesitan tomar decisiones informadas sobre plataformas de credenciales digitales.

Cómo usarla

La guía está diseñada para acompañar todo el ciclo de selección: desde la definición del marco interno, pasando por el RFI, la due diligence técnica, el piloto controlado y la decisión final con scoring ponderado. Cada pilar incluye preguntas críticas, métodos de validación y red flags a vigilar.

ÍNDICE

Tabla de contenidos

01 CAPÍTULO UNO Introducción

¿Por qué esta evaluación es crítica?

Las credenciales digitales representan **identidad verificable** en el mercado de trabajo. Una credencial débil o no verificable no tiene valor real. La privacidad y seguridad de datos de estudiantes, profesionales y empleados son responsabilidad institucional crítica: una brecha en una plataforma de credenciales afecta toda la vida profesional del titular.

Riesgos concretos que esta guía te ayuda a evitar

- ✓ **Blockchain-washing:** proveedores que usan la palabra sin implementación real
- ✓ **Vendor lock-in:** credenciales atrapadas en plataformas cerradas sin portabilidad
- ✓ **Costos ocultos:** integraciones deficientes que generan fricción operativa
- ✓ **Violación regulatoria:** incumplimiento de GDPR, LFPDPPP, LGPD o FERPA
- ✓ **Pérdida de credenciales:** imposibilidad de verificar tras el fin de contrato

Principios fundamentales de evaluación

1. Priorizar interoperabilidad y portabilidad

La institución debe evitar quedar atada a un proveedor único. Una credencial robusta debe poder circular, verificarse y preservarse más allá de una sola interfaz o portal. El proveedor no debería ser el único validador de sus credenciales.

2. Distinguir estándar, implementación y certificación

No es lo mismo "decir que soporta" un estándar que demostrarlo con documentación técnica, validadores funcionales, certificaciones externas vigentes y pruebas de intercambio reales.

3. Evaluar el producto completo

La plataforma debe cubrir emisión, gestión, evidencias, verificación, revocación, actualización, integraciones, analytics, experiencia del receptor, gobierno operativo y plan de salida.

Principios fundamentales (continuación)

4. Pedir evidencia, nunca solo afirmaciones

Cada claim relevante debe venir con prueba verificable: demostración en vivo, acceso temporal a sandbox, documentación técnica, certificado vigente de tercero independiente, informe de auditoría o cliente de referencia comparable. Un "sí" en un formulario sin evidencia no significa nada.

5. Validar con casos de uso reales

La comparación debe hacerse sobre **3 a 5 escenarios reales** de la institución: diploma académico, microcredencial con skills, badge apilable, integración LMS/SIS y verificación externa pública. No comparar sobre funcionalidades teóricas sino sobre lo que la institución realmente necesita emitir.

6. Tomar decisión con criterios ponderados

La compra no debe decidirse por afinidad comercial, presentación bonita o simpatía del equipo de ventas. Debe existir una **matriz de scoring objetiva** con pesos explícitos, umbrales mínimos no negociables y red flags de descarte inmediato.

> **IDEA FUERZA**
>
> Una institución educativa 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 con estándares abiertos, evidencia verificable y costo total transparente.

Estructura de esta guía

La evaluación de plataformas de credenciales digitales se estructura en **10 pilares críticos** que cubren toda la cadena de valor, desde seguridad hasta plan de salida sin lock-in. En las páginas siguientes encontrarás cada pilar desarrollado con sus preguntas críticas, métodos de validación y red flags, además de una matriz ponderada y un formulario de auditoría.

02 CAPÍTULO DOS

Marco de evaluación: 10 pilares clave

Este framework estructura la evaluación de plataformas de credenciales digitales en **10 dimensiones críticas** que cubren toda la cadena de valor, desde seguridad hasta salida sin lock-in.

01 Seguridad de la información
Cifrado, gestión de accesos, protección en tránsito y reposo, MFA, logs.

02 Estándares abiertos
Open Badges 3.0, 1EdTech, ELMS, W3C Verifiable Credentials, CLR.

03 Cumplimiento regulatorio
GDPR, LFPDPPP, LGPD, ISO 27001, SOC 2, certificaciones vigentes.

04 Blockchain y verificabilidad
Validación independiente, auditoría técnica, verificador público.

05 Funcionalidades técnicas
Generación, revocación, portabilidad, skills mapping, emisión batch.

06 Integraciones
APIs, OAuth/SAML, LTI, OneRoster, webhooks, sincronización.

07 Privacidad y datos
GDPR, consentimiento, eliminación, portabilidad, DPA.

08 Infraestructura cloud
Ubicación de datos, redundancia, backups, disaster recovery, SLA.

09 Monitoreo y auditoría
Logs de seguridad, alertas, retención, análisis forense.

10 Sostenibilidad
Roadmap público, comunidad, licencias abiertas, plan de salida.

CÓMO NAVEGAR LOS PILARES

- Pilares **1, 2, 3 y 4** son los críticos: si no aprueban, la plataforma se descarta.
- Pilares **5, 6 y 7** definen la usabilidad y operación del día a día.
- Pilares **8, 9 y 10** aseguran que la solución es sostenible en el tiempo.

01

PILAR UNO

Seguridad de la información

CRITICIDAD · ALTA

01 PILAR 1 · SEGURIDAD
Control de acceso y cifrado

¿Por qué este pilar es importante?

La seguridad es la base de una plataforma de credenciales. Sin controles rigurosos, la integridad y privacidad de credenciales y datos de estudiantes están comprometidas. Un incidente acá no es solo un incidente técnico: **es la pérdida de confianza de toda una comunidad académica.**

1.1 CONTROL DE ACCESO LÓGICO — PREGUNTAS CRÍTICAS

- ✓ ¿Se implementa MFA obligatoria para administrativos, emisores y validadores?
- ✓ ¿Qué factores se soportan? SMS, TOTP, push, biometría, hardware (U2F/FIDO2)
- ✓ ¿Cuál es el timeout de sesión inactiva por tipo de usuario?
- ✓ ¿Se revoca acceso inmediatamente al eliminar usuario o cambiar rol?
- ✓ ¿Existe historial detallado de cambios de permisos con trazabilidad?
- ✓ ¿Se aplica principio de menor privilegio (least privilege)?
- ✓ ¿Hay segregación clara entre emisor, revisor, aprobador y auditor?

Cómo validar

- ✓ Solicitar demo en vivo: crear usuario admin, activar MFA, validar bloqueo sin MFA
- ✓ Pedir acceso read-only temporal a logs de auditoría
- ✓ Ejecutar prueba de timeout en sesión inactiva
- ✓ Crear rol custom con permisos específicos y validar
- ✓ Reporte de usuarios activos últimos 90 días

1.2 CIFRADO DE DATOS

Ámbito	Requisito mínimo	Estándar deseado
Datos en tránsito	HTTPS/TLS 1.2 o superior obligatorio. Rechazo de HTTP sin cifrar.	TLS 1.3 + HSTS + PFS
Ciphersuites	Modernos. Evitar RC4, MD5, DES, 3DES.	SSL Labs rating "A" mínimo
Datos en reposo	AES-256 (no AES-128 para datos sensibles).	AES-256-GCM
Gestión de claves	KMS o HSM, no autogestión local.	HSM + rotación 90 días
Backups	Cifrados, con evidencia documentada.	Cifrado + integridad verificable

Pilar 1 · Seguridad (continuación)

1.3 DESARROLLO SEGURO (SECURE SDLC)

- ✓ ¿Se utiliza sistema de control de versiones con historial completo de cambios?
- ✓ ¿Es obligatorio code review por otro desarrollador antes de merge?
- ✓ ¿Se realizan escaneos automáticos de seguridad (SAST, SCA)?
- ✓ ¿Se escanean dependencias para vulnerabilidades? ¿Con qué frecuencia?
- ✓ ¿Se validan cambios de infraestructura (IaC) con igual rigor que código?
- ✓ ¿Se firman digitalmente artefactos de despliegue?
- ✓ ¿Se realiza testing de seguridad dinámico (DAST) en pre-producción?

1.4 VULNERABILIDADES Y PENTESTING

Práctica	Frecuencia mínima	Frecuencia ideal
Escaneos automáticos	Semanal	Diaria
Pentesting externo	Anual	Semestral
SLA patch crítico	< 7 días	< 48 horas
SLA patch alta	< 30 días	< 14 días
Programa bug bounty	Disponible	Activo y público

1.5 GESTIÓN DE INCIDENTES DE SEGURIDAD

- ✓ ¿Plan de respuesta a incidentes documentado?
- ✓ ¿Simulacros o tabletop exercises regulares?
- ✓ ¿SLA de notificación a clientes en incidente?
- ✓ ¿Se realizan post-mortems para mejorar?
- ✓ ¿Existe Security Officer designado?
- ✓ ¿Notificación a reguladores cuando aplica?

SLA recomendado

Notificación de breaches: 24 horas como objetivo, 72 horas como máximo (alineado con GDPR Art. 33). Cualquier ventana mayor es una red flag.

CONCLUSIONES DEL PILAR 1

- **Sin MFA obligatoria para administrativos**, la plataforma se descarta sin discusión.
- El cifrado en reposo con AES-256 y TLS 1.2+ en tránsito son el piso mínimo, no un diferencial.
- Pedir el reporte ejecutivo del último pentest externo es obligatorio. Si no lo comparten, red flag.
- Un Security Officer designado con contacto directo en caso de incidente es no negociable.

02

PILAR DOS

Estándares abiertos

CRITICIDAD · ALTA

02 Estándares abiertos

PILAR 2 · INTEROPERABILIDAD

¿Por qué este pilar es importante?

Los estándares abiertos son la base de la interoperabilidad y la portabilidad. Una plataforma que depende de formatos propietarios crea **vendor lock-in** y representa un riesgo estructural: tus credenciales podrían quedar atrapadas en un proveedor único, sin posibilidad de migración ni verificación externa.

2.1 OPEN BADGES 3.0

- ✓ ¿Implementación nativa de Open Badges 3.0 (no extensión custom)?
- ✓ ¿Exportación en formato Open Badge JSON-LD válido?
- ✓ ¿Incluye claim types estándar (issuer, recipient, criteria, evidence, achievement)?
- ✓ ¿Validación posible con herramientas independientes?
- ✓ ¿Soporte de extensiones estándar (alignment a frameworks)?
- ✓ ¿Compatibilidad con versiones anteriores?

¿Por qué importa?

Open Badges 3.0 es el **estándar de facto global** para credenciales digitales verificables. Una credencial Open Badge 3.0 válida puede ser verificada por cualquier institución con herramientas estándar, sin dependencia del validador propietario.

2.2 CERTIFICACIÓN 1EDTECH (IMS GLOBAL)

- ✓ ¿Certificación 1EdTech vigente? ¿Para qué estándares (Open Badges, CLR, LTI, xAPI)?
- ✓ ¿Fecha de vigencia y vencimiento de la certificación?
- ✓ ¿Verificable en el directorio público de **site.imsglobal.org/certifications**?
- ✓ ¿Cuál fue el alcance del proceso de certificación?

RED FLAG · CERTIFICACIÓN NO VERIFICABLE

Si el proveedor afirma estar certificado por 1EdTech pero no aparece en el directorio público, o la certificación está vencida, es **blockchain-washing aplicado a estándares**. Verificar siempre en la fuente oficial.

Pilar 2 · Estándares abiertos (continuación)

2.3 W3C VERIFIABLE CREDENTIALS (VC)

- ✓ ¿Soporte de W3C Verifiable Credentials Data Model 2.0 o superior?
- ✓ ¿Generación de VCs con firmas criptográficas verificables?
- ✓ ¿Incluye presentación de credenciales (Verifiable Presentation)?
- ✓ ¿Múltiples proof mechanisms (vc-data-integrity, vc-sd-jwt, otros)?
- ✓ ¿Documentación de alineación con estándar W3C?

2.4 ELMS (EUROPEAN LEARNING MODEL SPECIFICATION)

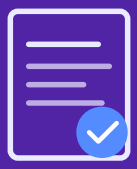
- ✓ ¿Alineación con ELMS para interoperabilidad en ecosistemas europeos?
- ✓ ¿Exportación en formato ELMS compatible?
- ✓ ¿Documentación de mapeos entre campos ELMS y credenciales?

2.5 RESUMEN COMPARATIVO: QUÉ EXIGIR SEGÚN CONTEXTO

Estándar	Aplicabilidad	Criticidad	Mínimo exigible
Open Badges 3.0	Universal	CRÍTICA	Implementación nativa, validable externamente
1EdTech	Universal	CRÍTICA	Certificación vigente verificable en directorio
W3C VC	Cross-sector	ALTA	Data Model 2.0 + firmas verificables
CLR	Educación superior	ALTA	Soporte para credenciales acumulativas
ELMS	UE / Bolonia	MEDIA	Mapeos documentados
LTI 1.3	Integración LMS	ALTA	Versión 1.3 certificada

CONCLUSIONES DEL PILAR 2

- "Soportar" un estándar no es lo mismo que estar **certificado** en él. Exigir prueba en el directorio público.
- Open Badges 3.0 nativo es el piso mínimo en 2026, no un diferencial.
- Si la credencial no puede validarse con un parser externo independiente, no es realmente abierta.



03

PILAR TRES

Cumplimiento regulatorio

CRITICIDAD · ALTA

03

PILAR 3 · COMPLIANCE

Cumplimiento regulatorio

¿Por qué este pilar es importante?

El cumplimiento regulatorio **no es negociable**. Una plataforma que viola GDPR, LFPDPPP, o estándares de seguridad expone a la institución a multas, sanciones y pérdida de reputación. La responsabilidad solidaria del controlador y procesador hace que este pilar sea crítico para la dirección legal y compliance.

3.1 CERTIFICACIONES INTERNACIONALES

Certificación	Alcance	Vigencia típica	Criticidad
ISO 27001	Sistema de gestión de seguridad de la información	3 años + auditoría anual	CRÍTICA
SOC 2 Type II	Confidencialidad, integridad, disponibilidad, seguridad, privacidad	1 año (renovable)	CRÍTICA
ISO 27017	Seguridad para servicios en nube	3 años	ALTA
ISO 27018	Protección de PII en cloud	3 años	ALTA

3.2 PREGUNTAS CRÍTICAS PARA CERTIFICACIONES

- ✓ ¿Cuál es la fecha de emisión y vencimiento del certificado?
- ✓ ¿Cuál fue el alcance (scope)? ¿Cubre toda la plataforma?
- ✓ ¿Se puede acceder a un reporte ejecutivo de auditoría?
- ✓ ¿Se realiza auditoría interna entre auditorías externas?
- ✓ SOC 2 Type II específicamente: ¿es auditoría de 1 año completo de operaciones?

Pilar 3 · Marcos regulatorios por región

Marco	Región	Exigencias clave
GDPR	Unión Europea	Derechos de acceso, eliminación, portabilidad. DPIA. Datos personales prohibidos en blockchain. DPA controlador/procesador. Subprocesadores documentados. Notificación breaches en 72 horas.
LFPDPPP	México	Derechos ARCO (acceso, rectificación, cancelación, oposición). Encargo de Tratamiento (DPA). Documentación de subencargados. Notificación de incidentes.
LGPD	Brasil	Consentimiento explícito y documentado. Derecho de portabilidad. Derecho de eliminación. Notificación en 72 horas. Termo de Processamento de Dados (TPCD).
CCPA / CPRA	California, USA	Derecho a saber, eliminar, opt-out de venta de datos. Notificación de prácticas de privacidad.
FERPA	USA · Educación	Protección de registros educativos. Consentimiento parental para menores. Restricciones de divulgación.

RED FLAG CRÍTICA · DATOS PERSONALES EN BLOCKCHAIN

Si el proveedor almacena datos personales (nombre, email, documento, calificación específica) directamente en blockchain: **viola GDPR/LFPDPPP/LGPD de forma flagrante**. Solo el hash o ID de credencial debería estar on-chain. Rechazo inmediato.

3.3 DOCUMENTACIÓN CONTRACTUAL OBLIGATORIA

- ✓ DPA / DPSA firmable que especifique roles de controlador y procesador
- ✓ Listado completo y actualizado de subprocesadores
- ✓ Evaluación de transferencias internacionales de datos (SCC, decisión de adecuación)
- ✓ Política de retención de datos documentada y vinculante
- ✓ Procedimiento de notificación de breaches con SLA explícito
- ✓ Plan de salida que preserve verificabilidad de credenciales emitidas

CONCLUSIONES DEL PILAR 3

- ISO 27001 **y** SOC 2 Type II vigentes son el piso. Una de las dos no alcanza.
- Sin DPA firmable, no se firma el contrato. Punto.
- La lista de subprocesadores debe ser pública o accesible bajo NDA. Si la ocultan, hay algo.

04

PILAR CUATRO

Blockchain y verificabilidad

CRITICIDAD · ALTA — AUDITORÍA TÉCNICA

04 PILAR 4 · AUDITORÍA TÉCNICA
Blockchain y verificabilidad

> ⚠ **ADVERTENCIA CRÍTICA**
>
> La palabra "blockchain" es ampliamente utilizada sin rigor técnico. Esta sección proporciona métodos prácticos y exhaustivos para validar de forma **independiente** las reclamaciones de blockchain. Sin validación técnica, es fácil caer en **blockchain-washing**.

4.1 PREGUNTAS TÉCNICAS FUNDACIONALES

- ✓ ¿Qué blockchain se utiliza exactamente? (Bitcoin, Ethereum, Solana, Hyperledger, Polygon, Hedera, privada, sidechain)
- ✓ ¿Quién opera los nodos? ¿Infraestructura pública, nodos privados del proveedor, red permisionada, mixta?
- ✓ ¿Qué datos exactos se registran en blockchain? ¿Credencial completa, solo hash, metadatos? ¿Qué se almacena off-chain?
- ✓ ¿Bajo ninguna circunstancia se almacenan datos personales? (Verificar explícitamente — GDPR lo prohíbe)
- ✓ ¿Cómo se verifica de forma independiente? ¿URL verificadora? ¿CLI? ¿Contrato inteligente? ¿Blockchain explorer?
- ✓ ¿El validador es público sin login, o depende de credenciales del proveedor?
- ✓ ¿La transacción se puede revisar directamente en explorer (Etherscan, Solscan, etc.) o solo a través del proveedor?

4.2 BLOCKCHAIN EXPLORERS POR RED — REFERENCIA RÁPIDA

Blockchain	Explorer público
Ethereum	etherscan.io
Solana	solscan.io
Polygon	polygonscan.com
Bitcoin	blockchain.com
Hedera	hashscan.io
Binance Smart Chain	bscscan.com

4.3 Protocolo exhaustivo de pruebas de verificabilidad

Este protocolo de 8 pasos permite validar de forma independiente si una plataforma cumple lo que promete en términos de blockchain. Es la prueba definitiva contra el blockchain-washing.

PASO 1 — GENERAR CREDENCIAL DE PRUEBA

1. Solicitar al proveedor que genere una credencial de prueba completamente válida en ambiente de producción con datos realistas.
2. La credencial debe incluir: nombre institución, nombre estudiante, título programa, fecha emisión, firma digital y datos blockchain.
3. Descargar en **todos** los formatos disponibles: JSON, JSON-LD, PDF, XML, HTML. Examinar estructura de cada formato.
4. Documentar el hash o ID único de credencial en blockchain (transaction ID, hash, credential ID).

PASO 2 — ACCEDER A LA CREDENCIAL EN PLATAFORMA

1. Loguear como usuario receptor (estudiante) en la plataforma.
2. Localizar la credencial emitida en el locker / wallet del usuario.
3. Verificar que la credencial está en estado "emitida" o "activa".
4. Buscar botón o enlace de "validar", "verificar", "detalles blockchain", "explorador".

PASO 3 — VALIDACIÓN EN PLATAFORMA

1. Presionar el botón de "Validar" o "Verificar" que ofrece la plataforma.
2. Observar resultado: ¿Muestra "Válida"? ¿"Verificada"? ¿Muestra detalles criptográficos?
3. Buscar hashtag de blockchain o link a transaction ID en los detalles.
4. Copiar el transaction ID, hash, o URL que se muestre.

Protocolo de verificabilidad (continuación)

PASO 4 — VERIFICACIÓN INDEPENDIENTE EN BLOCKCHAIN EXPLORER

1. Abrir una pestaña nueva del navegador.
2. Según la blockchain que use el proveedor, ir al explorer correspondiente (ver tabla anterior).
3. Pegar el transaction ID o hash en la barra de búsqueda.
4. Presionar "Buscar" y registrar el resultado.

PASO 5 — ANÁLISIS DETALLADO EN EXPLORER

Si la búsqueda encuentra la transacción, verificar sistemáticamente **todos** estos campos:

Campo	Qué validar
Status	Debe decir "Success" o "1". **NO** "Failed", "Reverted", "Error" o "0".
Transaction hash	Debe coincidir exactamente con el ID copiado de la plataforma.
From	¿Pertenece al proveedor o a un tercero?
To	¿Es un contrato inteligente o billetera personal?
Value	Cuánto valor se transfirió. Puede ser 0 si solo se registra hash.
Gas used	¿Costo razonable o anormalmente alto?
Timestamp / Block	¿Coincide con fecha de emisión de la credencial?
Confirmations	≥1 mínimo, ≥10 seguro.
Input data	¿Contiene hash de credencial? ¿Contiene datos personales? (No debería)
Method	Qué función se ejecutó (publish, register, store, transfer, etc.)

STATUS "FAILED" O "REVERTED"

Si el status es Failed o Reverted, **la credencial nunca fue registrada en blockchain exitosamente**. Es una red flag crítica. Rechazar.

TABS ADICIONALES A REVISAR EN EXPLORER

- ✓ **Token Transfers:** Debería estar vacío si solo se registra credencial
- ✓ **Internal Transactions:** Vacío salvo si se llamó funciones de contrato
- ✓ **Logs:** ¿Qué eventos se emitieron? ¿Qué información contienen?

Protocolo de verificabilidad (cierre)

PASO 6 — VALIDACIÓN DE FIRMA CRIPTOGRÁFICA

1. Si la credencial incluye firma digital (JWT, signature field), descargar en formato JSON.
2. Usar herramienta independiente para validar: **jwt.io** para JWT, OpenSSL para otras firmas.
3. Verificar que la llave pública del emisor está registrada públicamente y es correcta.
4. Confirmar que la firma es válida (no expirada, no falsificada, criptográficamente válida).

PASO 7 — PRUEBA DE REVOCACIÓN

1. Solicitar al proveedor que **revoque** la credencial de prueba.
2. En el locker/wallet: verificar que el estado cambió a "Revocada" o "Invalidada".
3. Volver al blockchain explorer: buscar si hay nueva transacción registrando la revocación.
4. Volver al botón "Validar": debería mostrar "Revocada" o "No válida".
5. Intentar compartir la credencial revocada: debería rechazarse o mostrarse como inválida.

PASO 8 — VALIDADOR PÚBLICO

1. ¿Ofrece validador público (sitio web) para que terceros verifiquen credenciales?
2. Si existe: acceder sin login, copiar URL pública de la credencial, pegar en validador.
3. El validador debería confirmar validez, mostrar información pública, **no** revelar datos personales.
4. Si no hay validador público: red flag crítica. La verificabilidad depende completamente del proveedor.

INTERPRETACIÓN FINAL DEL RESULTADO

Resultado	Veredicto
Transacción Success + datos consistentes	Credencial registrada exitosamente en blockchain. **VERIFICABLE.**
Status Failed o Reverted	Credencial NO fue grabada. **RECHAZAR.**
Transacción no encontrada	Blockchain-washing definitivo. **RECHAZAR.**
Blockchain privada sin acceso público	No hay verificabilidad independiente. **RED FLAG CRÍTICA.**
Sin validador público	Verificación atada al proveedor. **RED FLAG CRÍTICA.**

4.4 Las 6 red flags definitivas de blockchain-washing

Cualquiera de estas señales por sí sola debería ser motivo de descarte inmediato. Documentar cada hallazgo con captura de pantalla y anexarlo al expediente de evaluación.

RED FLAG #1 — NO PUEDEN DEMOSTRAR VERIFICABILIDAD INDEPENDIENTE

Si el proveedor no ofrece validador público o no permite acceder al blockchain explorer directamente: blockchain-washing definido. **Rechazar sin dudas.**

RED FLAG #2 — ALMACENAMIENTO DE DATOS PERSONALES EN BLOCKCHAIN

Si datos personales (nombre, email, documento, calificación) están on-chain: violación clara de GDPR/ LFPDPPP/LGPD. Solo hash o credential ID debería estar on-chain. **Rechazar inmediatamente.**

RED FLAG #3 — BLOCKCHAIN PRIVADA CERRADA

Si los nodos blockchain son operados únicamente por el proveedor y no se puede acceder públicamente: no ofrece verificabilidad independiente. Es centralizado con apariencia de blockchain.

RED FLAG #4 — NO PUEDEN MOSTRAR TRANSACCIONES EN EXPLORER

Si al buscar el transaction ID en blockchain explorer no aparece nada, o aparece "Failed", o "no token transfers, no internal transactions": no hay registro exitoso. **Rechazar.**

RED FLAG #5 — COBRAN POR VERIFICAR CREDENCIALES

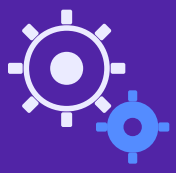
La verificación debe ser gratuita. Si cobran fee: el modelo es cuestionable y genera fricción. Rechazar.

RED FLAG #6 — NO PUEDEN MOSTRAR CERTIFICADO BLOCKCHAIN VIGENTE

Exigir link directo a blockchain explorer mostrando transacción real de una credencial. Si no pueden: hay blockchain-washing.

CONCLUSIONES DEL PILAR 4

- El protocolo de 8 pasos es el método más eficaz contra el blockchain-washing.
- Una transacción visible en explorer público **con status Success** es la única evidencia válida.
- Sin validador público de terceros, la "blockchain" del proveedor es marketing, no infraestructura.



05

PILAR CINCO

Funcionalidades técnicas

CRITICIDAD · MEDIA

05 PILAR 5 · OPERACIÓN
Funcionalidades técnicas clave

¿Por qué este pilar es importante?

No basta con que una plataforma "emita" credenciales: tiene que cubrir todo el ciclo de vida (emisión, revocación, portabilidad, visualización, skills) con la robustez y flexibilidad que exige una operación institucional real.

5.1 GENERACIÓN DE CREDENCIALES

- ✓ ¿Qué datos exactos se permiten? ¿Se permiten campos personalizados?
- ✓ ¿Se pueden incluir imágenes, logos, firmas digitales?
- ✓ ¿Emisión masiva (batch)? ¿Cuál es el límite? ¿Cómo se importan datos (CSV, Excel, API)?
- ✓ ¿SLA de emisión? (Inmediata, 1 hora, 24 horas, manual)
- ✓ ¿Workflows de aprobación? (Emisor propone, revisor aprueba, aprobador emite)

5.2 REVOCACIÓN

- ✓ ¿Se pueden revocar credenciales? ¿Quién tiene permiso?
- ✓ ¿Se registra motivo de revocación?
- ✓ ¿Es posible revocar múltiples credenciales simultáneamente?
- ✓ ¿Se puede revocar parcialmente?
- ✓ ¿Se actualiza inmediatamente el estado en blockchain (si aplica)?

5.3 PORTABILIDAD

- ✓ ¿Exportación en formatos estándar (JSON-LD, XML, PDF, HTML, Open Badge JSON)?
- ✓ ¿El usuario puede descargar todas sus credenciales en un archivo?
- ✓ ¿Importación desde otras plataformas?
- ✓ ¿Se mantienen firmas criptográficas intactas en exportación?

Pilar 5 · Funcionalidades (continuación)

5.4 VISUALIZACIÓN Y COMPARTIR

- ✓ ¿URL compartible por credencial?
- ✓ ¿Control sobre qué información es visible al compartir?
- ✓ ¿Integración con redes profesionales (LinkedIn)?
- ✓ ¿Badges digitales para sitios web?
- ✓ ¿Tracking de vistas y comparticiones?

5.5 SKILLS Y COMPETENCIAS

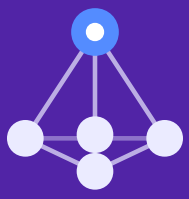
- ✓ ¿Mapeo de skills a frameworks estándar (ESCO, CASE, frameworks locales)?
- ✓ ¿Niveles de proficiencia?
- ✓ ¿Evidencias adjuntables (portafolios, videos, certificados)?
- ✓ ¿Soporte de rúbricas?

5.6 MATRIZ DE FUNCIONALIDADES — QUÉ EXIGIR SEGÚN CASO DE USO

Caso de uso	Funcionalidades imprescindibles
Diploma académico	Firma digital, revocación, exportación PDF + JSON-LD, branding institucional, verificador público.
Microcredencial con skills	Skills mapping a framework, evidencias adjuntables, niveles de proficiencia, badge apilable.
Badge apilable	Estructura jerárquica, relación entre badges, dashboard de progreso.
Certificación corporativa	Workflows de aprobación, expiración configurable, renovación, analytics de uso.
Emisión masiva	Importación CSV/Excel/API, validación previa, plantillas, emisión batch > 10.000 credenciales.

CONCLUSIONES DEL PILAR 5

- Una plataforma que emite bien pero revoca mal es incompleta. Probar el ciclo completo.
- La exportación en formato estándar con firmas intactas es la prueba real de portabilidad.
- Si los skills no se mapean a un framework reconocido, no son competencias verificables.



06

PILAR SEIS

Integraciones e interoperabilidad

CRITICIDAD · MEDIA

06 PILAR 6 · ECOSISTEMA
Integraciones e interoperabilidad

6.1 AUTENTICACIÓN

- ✓ ¿OAuth 2.0 / OpenID Connect? ¿Para administrativos y receptores?
- ✓ ¿SAML 2.0?
- ✓ ¿Proveedores de identidad soportados (Google, Microsoft, Okta, Shibboleth, Active Directory)?
- ✓ ¿SCIM para sincronización automática de usuarios?

6.2 APIS

- ✓ ¿Documentación pública con ejemplos de código?
- ✓ ¿Endpoints principales (emisión, revocación, búsqueda, validación)?
- ✓ ¿Autenticación soportada (API keys, OAuth, JWT, mTLS)?
- ✓ ¿Rate limits explícitos?
- ✓ ¿Versionado de APIs con compatibilidad hacia atrás?
- ✓ ¿SLA de disponibilidad ≥ 99.9%?
- ✓ ¿Sandbox / testing environment?

Prueba mínima

Exigir acceso temporal a un sandbox y validar al menos: emisión vía API, revocación vía API, consulta por filtros, recepción de webhook de emisión. Si el sandbox no existe, es red flag.

6.3 LMS / CAMPUS VIRTUAL

- ✓ ¿LTI versión 1.3 o superior?
- ✓ ¿Plataformas LMS soportadas (Moodle, Canvas, Blackboard, D2L, SAP SuccessFactors)?
- ✓ ¿Sincronización automática de datos académicos?
- ✓ ¿OneRoster para intercambio de roster?

6.4 WEBHOOKS Y EVENTOS

- ✓ ¿Configuración de webhooks por evento?
- ✓ ¿Payload detallado y documentado?
- ✓ ¿Verificación de webhook (firmas HMAC)?
- ✓ ¿Retry logic ante fallos?

CONCLUSIONES DEL PILAR 6

- Sin SSO empresarial, la plataforma genera fricción operativa permanente.
- Una API sin sandbox público es una API que no se puede integrar con seguridad.
- Webhooks con firma HMAC son requisito básico de seguridad en 2026.

07

PILAR SIETE

Privacidad y gestión de datos

CRITICIDAD · MEDIA

07 PILAR 7 · PRIVACIDAD
Privacidad y gestión de datos

7.1 DERECHOS DE DATOS

Derecho	Implementación esperada
Acceso	Usuario puede descargar todos sus datos en formato legible.
Rectificación	Usuario puede solicitar corrección con flujo documentado.
Olvido	Usuario puede solicitar eliminación. Excepciones explícitas y justificadas.
Portabilidad	Exportación de datos en formato estándar interoperable.
Oposición	Usuario puede oponerse a tipos específicos de procesamiento.

7.2 CONSENTIMIENTO

- ✓ ¿Consentimiento explícito y registrado con timestamp?
- ✓ ¿Consentimiento granular (por tipo de datos, propósito, duración)?
- ✓ ¿Revocación de consentimiento en cualquier momento?
- ✓ ¿Registro auditable de cuándo y cómo se otorgó cada consentimiento?

7.3 ANONIMIZACIÓN

- ✓ ¿Anonimización irreversible disponible?
- ✓ ¿Seudoanonimización en análisis y reportes?
- ✓ ¿Eliminación de identificadores manteniendo credencial válida?

7.4 RETENCIÓN DE DATOS

- ✓ ¿Política de retención exacta, documentada y vinculante?
- ✓ ¿Eliminación automática al cumplirse el período?
- ✓ ¿Diferenciación entre datos personales, credenciales y logs?
- ✓ ¿Posibilidad de mantener credenciales tras eliminar datos personales?

CONCLUSIONES DEL PILAR 7

- Una política de retención sin SLA de cumplimiento es solo una declaración de intenciones.
- El derecho al olvido debe ser ejecutable sin invalidar credenciales emitidas legítimamente.
- Consentimiento granular y revocable: piso mínimo bajo GDPR, deseable bajo cualquier marco.

08·09·10

PILARES OCHO, NUEVE Y DIEZ

Infraestructura, monitoreo y sostenibilidad

CRITICIDAD · MEDIA

08·09·10

PILARES 8, 9 Y 10 · CONTINUIDAD

Infraestructura, monitoreo y sostenibilidad

8.1 INFRAESTRUCTURA EN NUBE

Aspecto	Qué preguntar
Ubicación de datos	País, región y proveedor de nube. ¿Hay data residency?
Redundancia	¿Múltiples data centers? ¿Activo-activo o activo-pasivo?
Backups	Frecuencia, ubicación, encriptación, prueba de restauración.
Disaster recovery	RTO y RPO documentados. ¿Se prueba regularmente?
SLA disponibilidad	≥ 99.9% (downtime < 8.7 horas/año).
Monitoreo	24/7 con alertas y escalamiento documentado.

9.1 MONITOREO Y AUDITORÍA

- ✓ ¿Logs completos retenidos por al menos 12 meses?
- ✓ ¿Alertas configurables para eventos sospechosos?
- ✓ ¿Capacidad de análisis forense post-incidente?
- ✓ ¿Trazabilidad de cambios administrativos?
- ✓ ¿Integridad de logs garantizada (append-only, hash chain)?

10.1 SOSTENIBILIDAD OPERATIVA

- ✓ ¿Roadmap público de producto?
- ✓ ¿Comunidad activa? ¿Foro de usuarios?
- ✓ ¿Licencias abiertas donde es posible?
- ✓ ¿Viabilidad financiera del proveedor (rondas, runway, clientes)?
- ✓ ¿Plan de salida claro y sin lock-in?

CONCLUSIONES DE LOS PILARES 8, 9 Y 10

- RTO y RPO documentados, no aspiracionales: pedir el último informe de prueba de DR.
- Sin logs auditables, no hay forma de responder ante un incidente regulatorio.
- La sostenibilidad financiera del proveedor es parte del análisis: una startup sin runway es un riesgo.

CAPÍTULO ONCE

11 Proceso recomendado de selección

Un proceso estructurado en 7 fases permite combinar rigor técnico con velocidad de decisión. Cada fase produce un entregable concreto que alimenta la siguiente.

#	Fase	Objetivo	Entregable	Duración
01	**Definición interna**	Alinear stakeholders y objetivos del proyecto.	Casos de uso + criterios de éxito	2–4 sem
02	**RFI inicial**	Filtrar proveedores con respuestas documentales.	Respuestas documentales comparadas	2–3 sem
03	**Demo guiada**	Ver flujos reales en vivo con escenarios institucionales.	Acta de demo + preguntas pendientes	1–2 sem
04	**Due diligence**	Revisar en profundidad seguridad, blockchain, cumplimiento.	Checklist completa con scores	2–3 sem
05	**Piloto controlado**	Probar con 1 facultad o programa real.	Resultados + feedback usuarios	2–4 sem
06	**Evaluación económica**	Revisar costos completos (TCO), SLA, DPA.	TCO 3 años + DPA + SLA	2 sem
07	**Decisión y plan**	Elegir con scoring ponderado y arrancar rollout.	Matriz final + rollout plan	1–2 sem

TIEMPO TOTAL ESPERADO

Un proceso bien ejecutado toma entre **12 y 20 semanas**. Comprimir esto a 4 semanas es una receta para tomar una mala decisión. Extenderlo más de 6 meses suele indicar que la institución no tiene claros sus propios criterios de éxito.

12 CAPÍTULO DOCE
Matriz de evaluación ponderada

12.1 ESCALA DE EVALUACIÓN

Score	Nivel	Descripción
0	No cumple	No implementado o explícitamente no soportado.
1	En roadmap	Prometido pero no implementado aún.
2	Parcial	Implementado pero con limitaciones significativas.
3	Bueno	Implementado correctamente con documentación.
4	Muy bueno	Robusto, certificado o auditado externamente.
5	Excelente	Excepcional, líder de industria, transparencia total.

12.2 PESOS PONDERADOS SUGERIDOS

Criterio	Peso	Criticidad	Mínimo exigible
Seguridad	20%	CRÍTICA	Score ≥ 3
Cumplimiento normativo	20%	CRÍTICA	Score ≥ 3
Estándares abiertos	15%	ALTA	Score ≥ 2
Blockchain y verificabilidad	15%	ALTA	Score ≥ 2
Integraciones y APIs	15%	MEDIA	Score ≥ 2
Funcionalidades	10%	MEDIA	Score ≥ 2
Privacidad	5%	MEDIA	Score ≥ 2

12.3 FÓRMULA DE CÁLCULO

Score Ponderado = (Seguridad × 0.20) + (Normativo × 0.20) + (Estándares × 0.15) + (Blockchain × 0.15) + (APIs × 0.15) + (Funcionalidades × 0.10) + (Privacidad × 0.05)

12.4 INTERPRETACIÓN DE RESULTADOS

Score	Veredicto	Acción
≥ 4.0	Recomendado	Cumple estándares mínimos. Proceder con implementación.
3.0 – 3.9	Aceptable con reservas	Investigación adicional en áreas débiles.
< 3.0	No recomendado	Rechazar y evaluar alternativas.

13

CAPÍTULO TRECE

Formulario maestro de auditoría técnica

PARA IMPRIMIR Y COMPLETAR

13 AUDITORÍA TÉCNICA
Información general

Este formulario está diseñado para acompañar el proceso de due diligence técnica. Cada sección debe completarse con evidencia documental aportada por el proveedor. Sin evidencia, asignar score 0.

DATOS DEL PROCESO

Nombre de plataforma	_____
Proveedor / empresa	_____
Sitio web	_____
Contacto comercial	_____
Contacto técnico	_____
Fecha de evaluación	_____
Evaluador principal	_____
Institución evaluadora	_____

SECCIÓN 1 · DESCRIPCIÓN DEL PRODUCTO

Descripción en una frase	_____
Año de fundación	_____
Casos de uso principales	_____
Público objetivo	_____
Instituciones y usuarios globales	_____
Países donde opera	_____
Idiomas soportados	_____

Sección 2 · Seguridad de la información

Ítem	Score (0–5)	Evidencia	Observaciones
MFA obligatorio (admin)			
Cifrado TLS 1.2+ (tránsito)			
Cifrado AES-256 (reposo)			
Rotación automática de claves			
Code review obligatorio			
Escaneos de vulnerabilidades			
Pentesting externo			
ISO 27001 vigente			
SOC 2 Type II vigente			
Plan de respuesta a incidentes			
SLA de notificación de breaches			

Sección 3 · Estándares e interoperabilidad

Ítem	Score (0–5)	Evidencia	Observaciones
Open Badges 3.0 nativo			
1EdTech certificado (vigencia)			
W3C Verifiable Credentials			
CLR			
ELMS			
LTI 1.3			
OneRoster			
APIs documentadas			
OAuth 2.0 / OpenID Connect			
SAML 2.0			
Webhooks y eventos			

Sección 4 · Blockchain y verificabilidad (crítico)

PREGUNTAS FUNDACIONALES

¿Qué blockchain se utiliza? _____

¿Datos personales en blockchain? ☐ *NO (correcto)* ☐ *SÍ (RED FLAG · rechazar)*

PRUEBA DE AUDITORÍA — PROTOCOLO EN VIVO

☐ Paso 1 — Credencial de prueba generada exitosamente **SÍ** ○ **NO** ○

Transaction ID / Hash _____

☐ Paso 2 — Accesible desde interfaz de plataforma **SÍ** ○ **NO** ○

☐ Paso 3 — Botón de "validar" visible y funcional **SÍ** ○ **NO** ○

☐ Paso 4 — Muestra detalles de blockchain al validar **SÍ** ○ **NO** ○

Status de validación mostrado _____

PASO 5 · BÚSQUEDA EN BLOCKCHAIN EXPLORER

Explorer usado _____

☐ Transacción encontrada **SÍ** ○ **NO** ○

☐ Status = "Success" (no "Failed") **SÍ** ○ **NO** ○

Confirmations _____

From _____

To _____

Value / Data _____

PASO 7 · REVOCACIÓN

☐ Revocación ejecutada exitosamente

☐ Estado en plataforma cambió a "Revocada"

☐ Validación ahora muestra "No válida"

PASO 8 · VALIDADOR PÚBLICO

☐ Existe validador público sin login **SÍ** ○ **NO** ○

URL del validador _____

Veredicto blockchain

- ☐ **VERIFICABLE**— Transacción encontrada, status Success, datos consistentes.
- ☐ **FAILED**— Transacción mostrada pero status "Failed". Rechazar.
- ☐ **NO ENCONTRADA**— Blockchain-washing. Rechazar.
- ☐ **PRIVADA CERRADA**— Verificabilidad depende del proveedor. Red flag crítica.
- ☐ **SIN VALIDADOR PÚBLICO**— Red flag crítica.

Sección 5 · Cumplimiento regulatorio

Regulación	Estado	Evidencia / detalles
ISO 27001 vigente	Fecha: _____	
SOC 2 Type II vigente	Fecha: _____	
GDPR compliance (UE)		
LFPDPPP (México)		
LGPD (Brasil)		
CCPA (California)		
FERPA (USA · Educación)		
DPA / DPSA disponible	☐ Sí ☐ No	
Subprocesadores documentados	Número: ____	
Política de retención		
Derecho al olvido	☐ Sí ☐ No	
Portabilidad de datos	☐ Sí ☐ No	

Sección 6 · Funcionalidades y experiencia

Ítem	Score (0–5)	Evidencia	Observaciones
Emisión individual			
Emisión masiva (batch)		Límite: _____	
Revocación			
Portabilidad / exportación			
URL compartible			
Integración LinkedIn			
Skills y competencias			
Evidencias adjuntables			
Rúbricas			
Workflows de aprobación			
Analytics y reportes			
Multi-idioma			
Branding customizable			
Mobile / responsive			
Accesibilidad WCAG 2.1			

Sección 7 · Integraciones

LMS integrado	☐ Moodle ☐ Canvas ☐ Blackboard Otros: _____
SIS integration	Detalles: _____
SSO	☐ SAML ☐ OAuth ☐ OpenID
API REST documentada	☐ Sí ☐ No · Sandbox: ☐ Sí ☐ No
Webhooks	☐ Sí ☐ No
Rate limits API	_____ / minuto
SCIM	☐ Sí ☐ No
Conectores pre-construidos	Número: _____
Documentación	☐ Pobre ☐ Media ☐ Excelente

Sección 8 · Operación y soporte

SLA de disponibilidad	_____ %
SLA de respuesta (critical)	_____ horas
SLA de respuesta (high)	_____ horas
Soporte 24/7	☐ Sí ☐ No
Idiomas de soporte	☐ Español ☐ Inglés ☐ Portugués Otros: _____
Onboarding incluido	_____ horas
Capacitación incluida	☐ Sí ☐ No · Costo: $_____
Documentación	☐ Pobre ☐ Media ☐ Excelente
Plan de migración desde otra plataforma	☐ Sí ☐ No
Responsable de implementación	☐ Proveedor ☐ Cliente ☐ Mixto
Tiempo de implementación	_____ semanas

NOTAS SOBRE OPERACIÓN

Escribir observaciones sobre tiempos de respuesta, calidad del soporte, idiomas reales atendidos...

Sección 9 · Económico

MODELO DE PRECIOS

- ☐ Por usuario / año: $ _____
- ☐ Por institución / año: $ _____
- ☐ Por credencial: $ _____
- ☐ Por módulo / feature: $ _____
- ☐ Híbrido: _____

COSTOS ADICIONALES (POTENCIALMENTE OCULTOS)

Implementación	$ _____	**Branding**	$ _____
Integraciones	$ _____	**Wallets**	$ _____
Analytics premium	$ _____	**Soporte premium**	$ _____
Ambientes (test/stage)	$ _____	**Training**	$ _____

TCO — PRESUPUESTO TOTAL DE PROPIEDAD

Año 1	$ _____	**Año 2**	$ _____	**Año 3**	$ _____

PLAN DE SALIDA (CRÍTICO)

- ☐ Exportar todos los datos de usuarios — **SÍ** ○ **NO** ○
- ☐ Exportar todas las credenciales emitidas — **SÍ** ○ **NO** ○
- ☐ Verificación de credenciales post-salida — **SÍ** ○ **NO** ○

Costo de migración / salida *$ _____*

Período de transición _____ *días*

Formato de exportación ☐ *JSON* ☐ *XML* ☐ *Otro:* _____

Sección 10 · Scoring final y veredicto

Dimensión	Score (0–5)	Peso	Score × Peso
Seguridad		20%	
Estándares		15%	
Blockchain y verificabilidad		15%	
Cumplimiento regulatorio		20%	
Integraciones		15%	
Operación y soporte		10%	
Económico y salida		5%	

Score ponderado final

Suma de (Score × Peso) **____ / 5.0**

Interpretación · ≥ 4.0: **RECOMENDADO** | 3.0–3.9: **ACEPTABLE** con reservas | < 3.0: **NO RECOMENDADO**

VEREDICTO FINAL

- ☐ **RECOMENDADO**— Proceder con implementación.
- ☐ **ACEPTABLE CON RESERVAS**— Requiere mejoras en: _____
- ☐ **NO RECOMENDADO**— Rechazar y evaluar alternativas.

FIRMAS Y VALIDACIÓN

Evaluador principal	Nombre: _____ Firma: _____ Fecha: _____
Revisión técnica	Nombre: _____ Firma: _____ Fecha: _____
Revisión legal	Nombre: _____ Firma: _____ Fecha: _____
Revisión ejecutiva	Nombre: _____ Firma: _____ Fecha: _____

14

CAPÍTULO CATORCE

Checklist rápida

FILTRO INICIAL · 5 PREGUNTAS CLAVE

14

FILTRO RÁPIDO

5 preguntas que descartan el 80% de las plataformas

Cómo usar este checklist

Estas 5 preguntas funcionan como **filtro inicial**. Si la respuesta a cualquiera de ellas es NO, la plataforma se descarta antes de entrar en evaluación profunda. Esto te ahorra semanas de due diligence sobre proveedores que no pasarán las pruebas críticas.

1. **¿Tiene ISO 27001 o SOC 2 vigente?**
   Sin certificación de seguridad vigente y verificable: rechazo inmediato. No hay negociación posible.
2. **¿Soporta Open Badges 3.0 nativo?**
   Sin estándares abiertos hay vendor lock-in. Una credencial encerrada en formato propietario no es realmente tuya.
3. **¿Puedo verificar independientemente una credencial en blockchain explorer?**
   Sin verificabilidad pública es blockchain-washing. El protocolo del Pilar 4 lo demuestra en minutos.
4. **¿Tiene APIs documentadas y acceso a logs de auditoría?**
   Sin esto no hay transparencia operativa ni capacidad real de integración o auditoría.
5. **¿Cumple GDPR y NO almacena datos personales en blockchain?**
   Violación de privacidad: no negociable. La exposición regulatoria es inmediata.

RESULTADO DEL FILTRO

Si la plataforma responde **SÍ a las 5**, avanzar a la evaluación completa con el formulario maestro. Si responde **NO a una sola**, archivar y pasar a la siguiente candidata. Ninguna excepción.

Checklist práctica para imprimir

Una vez pasado el filtro inicial, usar esta checklist completa por dimensiones para acompañar la evaluación profunda. Marcar SÍ o NO en cada ítem para tener una vista rápida del estado.

SOBERANÍA Y CONTROL DE DATOS

- ☐ ¿Permite elegir ubicación de hosting en tu región preferida? **SÍ** ○ **NO** ○
- ☐ ¿Tus aprendices deben crear cuenta en la plataforma del proveedor? **SÍ** ○ **NO** ○
- ☐ ¿La plataforma recopila datos para servicios indirectos o publicidad? **SÍ** ○ **NO** ○
- ☐ ¿Hay DPA / DPSA firmable disponible? **SÍ** ○ **NO** ○
- ☐ ¿Los subprocesadores están documentados y son auditables? **SÍ** ○ **NO** ○

PERSONALIZACIÓN Y BRANDING

- ☐ ¿El diseño es totalmente personalizable (layout, branding, animaciones)? **SÍ** ○ **NO** ○
- ☐ ¿Se puede usar un dominio propio para las credenciales? **SÍ** ○ **NO** ○
- ☐ ¿El sender de los emails es personalizable? **SÍ** ○ **NO** ○
- ☐ ¿El diseño es responsive (mobile y desktop)? **SÍ** ○ **NO** ○
- ☐ ¿La credencial se puede mostrar sin referencias al proveedor? **SÍ** ○ **NO** ○

DURABILIDAD E INDEPENDENCIA

- ☐ ¿La plataforma retiene datos de aprendices al terminar el contrato? **SÍ** ○ **NO** ○
- ☐ ¿Backup de credenciales a largo plazo, independiente de la plataforma? **SÍ** ○ **NO** ○
- ☐ ¿Las credenciales siguen siendo verificables post-contrato? **SÍ** ○ **NO** ○
- ☐ ¿Existe plan de salida documentado y sin costo oculto? **SÍ** ○ **NO** ○

Checklist práctica (continuación)

SEGURIDAD TÉCNICA

- ☐ MFA obligatorio para usuarios administrativos — SÍ ○ NO ○
- ☐ Cifrado TLS 1.2+ en tránsito y AES-256 en reposo — SÍ ○ NO ○
- ☐ Pentest externo anual mínimo con reporte ejecutivo disponible — SÍ ○ NO ○
- ☐ SLA de notificación de breaches en 72 horas o menos — SÍ ○ NO ○

ESTÁNDARES E INTEROPERABILIDAD

- ☐ Open Badges 3.0 nativo (validable externamente) — SÍ ○ NO ○
- ☐ Certificación 1EdTech vigente verificable en directorio público — SÍ ○ NO ○
- ☐ W3C Verifiable Credentials 2.0 con firmas verificables — SÍ ○ NO ○
- ☐ Exportación con firmas criptográficas intactas — SÍ ○ NO ○

BLOCKCHAIN Y VERIFICABILIDAD

- ☐ Transacción visible y Success en blockchain explorer público — SÍ ○ NO ○
- ☐ Validador público sin necesidad de login — SÍ ○ NO ○
- ☐ Cero datos personales en blockchain (solo hashes) — SÍ ○ NO ○
- ☐ Revocación reflejada en blockchain y en validador — SÍ ○ NO ○

INTEGRACIONES Y ESCALABILIDAD

- ☐ API REST bien documentada y abierta — SÍ ○ NO ○
- ☐ Sandbox / ambiente de pruebas disponible — SÍ ○ NO ○
- ☐ Conexión sencilla a LMS y SIS existentes — SÍ ○ NO ○
- ☐ Soporte para automatización de emisión multi-programa — SÍ ○ NO ○

EXPERIENCIA DE USUARIO

- ☐ Se probó el flujo completo de aprendiz — SÍ ○ NO ○
- ☐ Compartir fácil (LinkedIn, QR, PDF) — SÍ ○ NO ○
- ☐ Verificable por recruiters sin crear cuenta — SÍ ○ NO ○
- ☐ Multilingüe y multi-formato (web + PDF) — SÍ ○ NO ○

15

CAPÍTULO QUINCE

Anexos y referencias

DOCUMENTOS · RED FLAGS · ESTÁNDARES

15 ANEXO A
Documentos a solicitar al proveedor

Esta es la documentación mínima exigible en un proceso serio de due diligence. Si el proveedor no puede entregar uno o más de estos elementos, registrar como hallazgo y evaluar el riesgo.

- ✓ Ficha técnica del producto y arquitectura detallada
- ✓ Documentación completa de APIs (Swagger / OpenAPI con ejemplos)
- ✓ Acceso a sandbox / testing environment
- ✓ Matriz de estándares soportados (versión exacta, alcance, evidencia)
- ✓ Listado de certificaciones vigentes (ISO 27001, SOC 2, 1EdTech, etc.)
- ✓ DPA / DPSA (Data Processing / Protection Agreement) plantilla
- ✓ Listado completo y actualizado de subprocesadores
- ✓ SLA y términos de servicio
- ✓ Plan de business continuity y disaster recovery
- ✓ Reporte de pentest o carta ejecutiva de seguridad (reciente, tercero independiente)
- ✓ Referencias de clientes comparables (3 mínimo)
- ✓ Plan de salida (cómo exportar datos, mantener verificación post-contrato, costos)
- ✓ Roadmap público de desarrollo
- ✓ Política de privacidad y retención de datos completa
- ✓ Especificaciones técnicas de blockchain: cuál, cómo se implementa, costos, reversibilidad

CÓMO GESTIONAR LA SOLICITUD

Estructurar la solicitud como un RFI formal con plazo de respuesta de 2 semanas. Documentar retrasos, omisiones y respuestas evasivas: son señales de alarma sobre la cultura del proveedor. Un proveedor maduro entrega esta lista sin fricciones.

15 ANEXO B
Red flags de descarte inmediato

Estas señales por sí solas justifican el descarte sin necesidad de evaluación adicional. Documentar el hallazgo, archivar y pasar al siguiente proveedor.

1. Ausencia total de documentación técnica.
2. Negativa a mostrar sandbox o ambiente de prueba.
3. Claims de estándares sin prueba de implementación verificable.
4. Falta de respuesta sobre subprocesadores.
5. Falta de DPA / DPSA firmable.
6. Ausencia de controles básicos de acceso (sin MFA para admin).
7. Imposibilidad de exportar datos o mantener verificación post-salida.
8. Datos personales almacenados en blockchain.
9. Blockchain privada cerrada sin verificabilidad independiente.
10. Transacciones fallidas (Failed/Reverted) en blockchain explorer.

Anexo C · Estándares y organismos de referencia

Estándar / organismo	URL oficial
1EdTech Open Badges 3.0	1edtech.org/standards/open-badges
1EdTech · Directorio de certificaciones	site.imsglobal.org/certifications
W3C Verifiable Credentials	w3.org/TR/vc-data-model-2.0
1EdTech CLR	1edtech.org/standards/clr
1EdTech LTI	1edtech.org/standards/lti
1EdTech OneRoster	1edtech.org/standards/oneroster
NIST SSDF (SDLC)	csrc.nist.gov/projects/ssdf
OWASP ASVS	owasp.org/www-project-application-security-verification-standard
GDPR guidance	gdpr-info.eu
FERPA guidance	studentprivacy.ed.gov
ISO/IEC 27001	iso.org/isoiec-27001-information-security-management.html

CIERRE

Conclusión

Elegir una plataforma de credenciales digitales no es una decisión estética ni comercial: es una **decisión estratégica de infraestructura** que define la reputación de tu institución, la seguridad de los datos de tu comunidad y la calidad de la experiencia que ofrecés a aprendices, recruiters y partners.

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

> *La mejor práctica es combinar formulario documental + demo guiada + due diligence técnica exhaustiva + piloto real + scoring ponderado + revisión contractual. Cuando el proveedor realmente tiene la capacidad que declara, ese proceso lo fortalece. Cuando no la tiene, el proceso lo expone de forma definitiva.*
>
> **— PRINCIPIO GUÍA DE ESTA GUÍA**

El proceso, en una línea

Filtro inicial de 5 preguntas → RFI → demo guiada → due diligence con formulario maestro → piloto controlado → scoring ponderado → revisión contractual → decisión.

RECORDÁ

- Pedir evidencia, no afirmaciones.
- Validar con casos de uso reales, no teóricos.
- Probar el ciclo completo, no solo la emisión.
- Asumir que blockchain-washing existe y aplicar el protocolo del Pilar 4.
- Decidir con criterios ponderados, no con afinidad comercial.

¿QUERÉS VER CON MÁS CLARIDAD?

Hablemos de tu proyecto de credenciales digitales.

En POK acompañamos a instituciones y organizaciones en la transición hacia credenciales digitales verificables. Creemos en un enfoque transparente, soberano y respetuoso de tu ecosistema.

Si querés tener una conversación constructiva o que evaluemos juntos las necesidades específicas de tu institución, nuestro equipo está listo.

Agendá una demo personalizada

pok.tech · contacto@pok.tech

pok