



ACTA DE SORTEO CERTIFICADO

SORTIVEN V1.4 — Sistema de Sorteo Auditable · Aleatoriedad Verificable (Provably Fair)

1. Identificación del Sorteo

ID del sorteo	cde3ddb1-fce2-4cee-82ea-bb80d51089a3
Nombre	sorteo prueba julio 1 triple falcon
Tipo de juego	Triple Falcón
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-07-13T02:18:22.562156+00:00
Ejecutado	2026-07-13T02:18:26.190354+00:00
Revelado	2026-07-13T02:18:35.422032+00:00

2. Resultado Oficial

Triple A: 818 (Terminal 18) · Triple B: 535 (Terminal 35) · Estado: Mérida

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	a7ef222f127b30b3aa1e487a72c2304ec9c4c54be11093daf3b5d87a12e5116d
Semilla del cliente (client seed)	1dcf40464ca5703b
Nonce	1
Semilla del servidor (revelada)	4f89d6100d4cf7a3ca2e091eee55475bf6b5ce8310522c15783fbe7fde1467ce

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	5
Hash anterior (prev_hash)	6debda5c40ad227ca6dc561309d52941507b071036593010b2882e47a49954f2
Hash del registro (record_hash)	a1dcca9e8876380d28246b3383c494f7841e0c8bb95b010654d2da4ce1620118

5. Cómo Verificar este Sorteo

Cualquier persona puede verificar la integridad de este sorteo: (1) Confirme que SHA-256 de la **semilla del servidor revelada** es igual al **compromiso** publicado antes del sorteo. (2) Recompute el resultado con (semilla servidor, semilla cliente, nonce) usando el algoritmo público **HMAC-SHA256** con muestreo por rechazo. (3) Verifique el **record_hash** recalculando SHA-256(prev_hash + datos canónicos). El portal público de verificación realiza estos pasos automáticamente.