



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	6425cbe2-0dd7-45b0-af84-df9db15e67d1
Nombre	[DEMO SENCAMER] Triple Falcón – Sorteo Digital — muestra 008
Tipo de juego	Triple Falcón
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:37:53Z
Ejecutado	2026-08-25T05:37:53Z
Revelado	2026-08-25T05:37:53Z

2. Resultado Oficial

Triple A: 801 (Terminal 01) · Triple B: 243 (Terminal 43) · Estado: Cojedes

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	7433e61a9553b17518c1ebea6136c93a4eea716ba6c84251256ec6158480fa38
Semilla del cliente (client seed)	sencamer-demo-triple-008
Nonce	8
Semilla del servidor (revelada)	3e6a8aeefaf2d5a7a24162e7b946d642de45684a984acd4e9414c556cc14839

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	14
Hash anterior (prev_hash)	15cedb8493c384d70f4eaaec2c43da83ca211ca585b731234f4201d03814350a
Hash del registro (record_hash)	45fba9c309c67eb05746771a26efc61a2cf50f5804dab8471c598690f0327352

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.