



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	313a5fcd-0a62-496e-b148-6e8d316bd989
Nombre	[DEMO SENCAMER] Triple Falcón – Sorteo Digital — muestra 007
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: 958 (Terminal 58) · Triple B: 339 (Terminal 39) · Estado: Bolívar

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	18fe15d72f0d7801c8860717b00cae3b75bbed4df28ed288e969e5149e142781
Semilla del cliente (client seed)	sencamer-demo-triple-007
Nonce	7
Semilla del servidor (revelada)	f6b90283d34fb5d0525be2575b02febe31ceec24c92181d7440091d869b66673

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	13
Hash anterior (prev_hash)	ef6e5dd05ed7f01c792cfcfeddb7fdbf9f5773256d6b55d9ea9d9e9e2b982e7b
Hash del registro (record_hash)	15cedb8493c384d70f4eaaec2c43da83ca211ca585b731234f4201d03814350a

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.