



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	feb5e267-47a4-433e-9df1-2ff25378f198
Nombre	[DEMO SENCAMER] Triple Falcón – Sorteo Digital — muestra 001
Tipo de juego	Triple Falcón
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:37:50Z
Ejecutado	2026-08-25T05:37:50Z
Revelado	2026-08-25T05:37:50Z

2. Resultado Oficial

Triple A: 816 (Terminal 16) · Triple B: 755 (Terminal 55) · Estado: Falcón

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	173267fe3b03f3f9cad899d00dd4f829c348dfcd4280366e4b2708c2f23b4557
Semilla del cliente (client seed)	sencamer-demo-triple-001
Nonce	1
Semilla del servidor (revelada)	a6f233b3a0f98dad93fe1b467e283194937d26e48c5a2e5172aa73f2c0a7416c

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	7
Hash anterior (prev_hash)	bf3e8f0ebbe9315fd5c05878d10d72125e790468ebf32f434e9c1aa8c8085cf3
Hash del registro (record_hash)	cb03971da580889c4bd41998a1dbe512efc6871bab740fc3792b40932e20abff

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.