



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	115b199d-1e69-4777-953d-ee0175f04a69
Nombre	[DEMO SENCAMER] Triple Falcón – Sorteo Digital — muestra 002
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: 492 (Terminal 92) · Triple B: 060 (Terminal 60) · Estado: Táchira

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	5c5f94bdbad1454a175c5be6c5574a0130e3e575db63229dc48605138d6bb268
Semilla del cliente (client seed)	sencamer-demo-triple-002
Nonce	2
Semilla del servidor (revelada)	e0ac385c0f2d0e77158a6bdc0815e399e1fb611bdcb2d65a77f8ed1182c52297

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	8
Hash anterior (prev_hash)	cb03971da580889c4bd41998a1dbe512efc6871bab740fc3792b40932e20abff
Hash del registro (record_hash)	3956e441dce736598c5bab59f00c2291a4d09f78cf712ef18f289ab3e433d7e4

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.