



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	aef5b114-f940-41e7-bd81-a8b56e5b867e
Nombre	[DEMO SENCAMER] Triple Falcón – Sorteo Digital — muestra 006
Tipo de juego	Triple Falcón
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:37:52Z
Ejecutado	2026-08-25T05:37:52Z
Revelado	2026-08-25T05:37:52Z

2. Resultado Oficial

Triple A: 708 (Terminal 08) · Triple B: 595 (Terminal 95) · Estado: Mérida

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	989806f03dc9c26d6dfa4196fc91b69456a85620adb0bab6d7a8813cde6e85d1
Semilla del cliente (client seed)	sencamer-demo-triple-006
Nonce	6
Semilla del servidor (revelada)	d84f81158a34c7775060524fbadaa494e513dee5305f2c86f02fc088b7e68b3a

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	12
Hash anterior (prev_hash)	640aac9e0640ca9df17f0cbe83c3df04fe96594e949db82b4a56d3f3d64a78d9
Hash del registro (record_hash)	ef6e5dd05ed7f01c792cfcfeddb7fdbf9f5773256d6b55d9ea9d9e9e2b982e7b

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.