



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	7b676843-0856-49f1-9248-dcda1493486a
Nombre	[DEMO SENCAMER] Triple Falcón – Sorteo Digital — muestra 005
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: 787 (Terminal 87) · Triple B: 545 (Terminal 45) · Estado: Distrito Capital

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	912695594eaed9ec18f92db746729f5ed6c6c1bf9b0a6a6ed5c5a0ce93e88b8c
Semilla del cliente (client seed)	sencamer-demo-triple-005
Nonce	5
Semilla del servidor (revelada)	9980cab3b942161e75627b6d69312fa56c4a2ab39564f97800821ee2d2260be8

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	11
Hash anterior (prev_hash)	f76719f0f0b22457b0ad636c6f67e0dfda3336d696e34487042c25c50d37cc8c
Hash del registro (record_hash)	640aac9e0640ca9df17f0cbe83c3df04fe96594e949db82b4a56d3f3d64a78d9

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.