



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	d36dfb69-62ea-4989-baf3-e61a12bf0e9c
Nombre	[DEMO SENCAMER] Triple Falcón – Sorteo Digital — muestra 017
Tipo de juego	Triple Falcón
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:37:57Z
Ejecutado	2026-08-25T05:37:57Z
Revelado	2026-08-25T05:37:57Z

2. Resultado Oficial

Triple A: 436 (Terminal 36) · Triple B: 053 (Terminal 53) · Estado: Lara

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	1fc16a6a40e7f8b75d88b62c6821208ba69da75b22ece432f33c1ce225072639
Semilla del cliente (client seed)	sencamer-demo-triple-017
Nonce	17
Semilla del servidor (revelada)	7749ce91a8b5ca8b820466aaeb4305d082cc99de2e21a79b4367e77aeb73969b

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	23
Hash anterior (prev_hash)	e1c385529614631365ba760ba06ceeffd93d29dfdc3184e8d45a314389845014
Hash del registro (record_hash)	f1589491284bc9f20df63e8019a610f064f08638842709990b2b52e1f10b2734

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.