



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	c82412f9-3dca-4123-90a1-26dee0ecba27
Nombre	[DEMO SENCAMER] Triple Falcón – Sorteo Digital — muestra 019
Tipo de juego	Triple Falcón
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:37:58Z
Ejecutado	2026-08-25T05:37:58Z
Revelado	2026-08-25T05:37:58Z

2. Resultado Oficial

Triple A: 332 (Terminal 32) · Triple B: 467 (Terminal 67) · Estado: Monagas

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	a17aa24635bc422be1c7d1f1df81ad478ae687d4867685853e93a0f400e66990
Semilla del cliente (client seed)	sencamer-demo-triple-019
Nonce	19
Semilla del servidor (revelada)	7fc78b487e7ec6c81b74e234091e0e6c3aca83ab7e25b0928b79f6180c4fe7d9

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	25
Hash anterior (prev_hash)	1761519e2e3addf1d2602c8037699cf9e69e47d7886a300a51eef7cb8af799f
Hash del registro (record_hash)	9ec30c8076f71c086f631c2957265b16783ddda316cec6129ff9978011524692

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.