



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	dbc3e3fc-11a4-4682-bf71-d182da9bb669
Nombre	[DEMO SENCAMER] Triple Falcón – Sorteo Digital — muestra 015
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: 559 (Terminal 59) · Triple B: 569 (Terminal 69) · Estado: Trujillo

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	9b1d176a95ce62f7f15ff18cd2cafd59513bf08cd025b01bfbe28d1fcd22c84d
Semilla del cliente (client seed)	sencamer-demo-triple-015
Nonce	15
Semilla del servidor (revelada)	1f6a7c26fec109abefbb71469d8cf9f61ad053ea63b644773713d57454935ec9

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	21
Hash anterior (prev_hash)	992122b005e93e0619e3f34b0a2d2f38cb84455cf947696e9131672a99f954ba
Hash del registro (record_hash)	1843155fcd2b6e6482a1fcf415dc9880387cfb893c77e8f295bfac930b4f33f8

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.