



# ACTA DE SORTEO CERTIFICADO

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

## 1. Identificación del Sorteo

|                       |                                      |
|-----------------------|--------------------------------------|
| ID del sorteo         | 35206095-e4bd-4338-a203-4b03a4b90404 |
| Nombre                | 11am                                 |
| Tipo de juego         | Triple Falcón                        |
| Estado                | revelado                             |
| Versión del algoritmo | rng-v1                               |
| Creado                | 2026-06-03T20:08:47.521721+00:00     |
| Ejecutado             | 2026-06-03T20:08:52.026970+00:00     |
| Revelado              | 2026-06-03T20:09:17.709184+00:00     |

## 2. Resultado Oficial

Triple A: 590 (Terminal 90) · Triple B: 892 (Terminal 92) · Estado: La Guaira

## 3. Evidencia Provably-Fair

|                                   |                                                                   |
|-----------------------------------|-------------------------------------------------------------------|
| Compromiso (SHA-256) — pre-sorteo | 6809744297b5e2e59117dcf6403341d0fa47ed00a1bcd666160c959a767926c0  |
| Semilla del cliente (client seed) | 1                                                                 |
| Nonce                             | 1                                                                 |
| Semilla del servidor (revelada)   | 4d5a5fccdd4848c024a08176e5b2b6d11741bfc6adcc82cf729b3142ea9dd4e2f |

## 4. Cadena de Auditoría (Ledger inmutable)

|                                 |                                                                  |
|---------------------------------|------------------------------------------------------------------|
| Índice en la cadena             | 2                                                                |
| Hash anterior (prev_hash)       | 72366232d58aa46f999cea688f186e87d717cef76d1044b3c9dace78c96e405f |
| Hash del registro (record_hash) | 5b759582af17d50a18a5f7fa8c3ae942e5adc85a7fad4753d84ee9b761fb0b46 |

## 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.