



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	75cf881d-a9b8-49ed-aa25-2689db05662e
Nombre	Triple Falcón – Sorteo Digital — 03/06/2026 20:10
Tipo de juego	Triple Falcón
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-06-03T20:10:52.225683+00:00
Ejecutado	2026-06-03T20:10:57.495586+00:00
Revelado	2026-06-03T20:11:05.020346+00:00

2. Resultado Oficial

Triple A: 351 (Terminal 51) · Triple B: 528 (Terminal 28) · Estado: Miranda

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	62a44cf896c94fec36b1c85525673eb2818d0d0a87d754b41127f6f1c733cc2c
Semilla del cliente (client seed)	1
Nonce	1
Semilla del servidor (revelada)	0693ccb527fbc14cd29a9a479013a0b3b40d4419f675bee548fe99e20deccac

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	3
Hash anterior (prev_hash)	5b759582af17d50a18a5f7fa8c3ae942e5adc85a7fad4753d84ee9b761fb0b46
Hash del registro (record_hash)	260fa5dbd3c7507356d16d20c469dd998fef2ff618a2ba15d378dc4e03227740

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.