



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	c8e92ba1-23c5-441a-b4e9-701653de3d01
Nombre	prueba 1 F
Tipo de juego	Triple Falcón
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-06-03T20:04:40.718433+00:00
Ejecutado	2026-06-03T20:06:06.131767+00:00
Revelado	2026-06-03T20:06:42.256356+00:00

2. Resultado Oficial

Triple A: 191 (Terminal 91) · Triple B: 375 (Terminal 75) · Estado: Aragua

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	2b29fc4a11c85e50170058e3349f50bc1b3c7c8dae3c396cb9de89046d99e0ae
Semilla del cliente (client seed)	c64593d022dff53f
Nonce	1
Semilla del servidor (revelada)	deb929377ec996d6fec08bb1d5776f735377da1e93646e1c6b201ddb295f278b

4. Cadena de Auditoría (Ledger immutable)

Índice en la cadena	0
Hash anterior (prev_hash)	00
Hash del registro (record_hash)	7c40c28afae532502ee65ef916c3c08477c5b1add31569ddf5f234e6f231f6c6

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.