SORTIVEN
Sorteador Integral

ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	7d0e3a01-e366-4415-bbc0-7e6c08da7963
Nombre	Loto Zumba — 10/11/2026 12:34
Tipo de juego	Loto Zumba
Ente supervisor	Junta de Beneficencia Pública y Asistencia Social del Estado Bolivariano de Mérida (Lotería de Mérida)
Operadora	Operadora Zumba, C.A.
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-11-10T12:34:25.260096+00:00
Ejecutado	2026-11-10T12:34:26.431274+00:00
Revelado	2026-11-10T12:34:27.390618+00:00

2. Resultado Oficial

55 · OSO HORMIGUERO

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`860cdc779e0e90befcef528feeb4d84bc9f308e82c077e82facf678903acc035`
Semilla del cliente (client seed)	`6e758a278af8298a`
Nonce	1
Semilla del servidor (revelada)	`5e2712a9f4f93cfb6b44b7ea069a9c7efe390dc52409f401f7adb2d1070a96d0`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	102
Hash anterior (prev_hash)	`9eecc6c4bd12e4fef58282527c25bf6f97eda5d37ea38ff8854d10ebd444a7e9`
Hash del registro (record_hash)	`f023ad5901c0b43131d95eb923d4e92cda9a4b6bc00ae4dff85f4cf706c2db0a`

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.

Documento generado automáticamente el 2026-11-23 10:50:09 UTC. Este acta es un artefacto de auditoría reproducible.