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	99be0506-a73a-4a59-8c31-16cbeb10b4aa
Nombre	Loto Zumba — 10/11/2026 12:33
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	2026-11-10T12:33:28.623834+00:00
Ejecutado	2026-11-10T12:33:29.561403+00:00
Revelado	2026-11-10T12:33:30.397235+00:00

2. Resultado Oficial

24 · IGUANA

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`8bfb4c90b4e635b0c66bdf14ba8bbd7b90c32e586e8c739d650ce9b4e9e5e69c`
Semilla del cliente (client seed)	`1728ef8af204daf8`
Nonce	1
Semilla del servidor (revelada)	`a4725cb174d1d0dbd29d35e0dd5508574098809d5b6fa3ee30f5bf8780c71e51`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	100
Hash anterior (prev_hash)	`d74b9d930fc09b5aec20519b80a7d72ffb374781752c51c2e0c20056b20d8702`
Hash del registro (record_hash)	`d41cc8765ad4767bc2ca71f5fb448153a3a7336a76d7303e37870fc7a479a270`

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 10:57:15 UTC. Este acta es un artefacto de auditoría reproducible.