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	913c9a0e-cff6-4e51-89b2-dfb16bd391c9
Nombre	TEST_espejo zoolo
Tipo de juego	ZooloFalcón Venezuela
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-10-22T17:13:10.148736+00:00
Ejecutado	2026-10-22T17:13:17.224430+00:00
Revelado	2026-10-22T17:13:24.204995+00:00

2. Resultado Oficial

60 · Camaleón

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`d0b9da545a4724fe5ad3207f8c80095b0a36f03b8ea76d2f0d6efea0cfb1c288`
Semilla del cliente (client seed)	`99e630fc4ac30463`
Nonce	1
Semilla del servidor (revelada)	`ae45735723e01211ab0da92186e368e94e97f43f4572bbd8609589b9c3bf2cd7`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	71
Hash anterior (prev_hash)	`8c2847600abfd04dc5fcaa74a373e890de2b635b3d92604784b99051b0b4d1c4`
Hash del registro (record_hash)	`ea7a6801842181d1a7af212b8cc7fd65b554106b50d4e8edf71f96f881e58375`

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.