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	7986966c-aff8-48d3-9670-3ba1afb54859
Nombre	ZooloFalcón Venezuela — 22/10/2026 16:55
Tipo de juego	ZooloFalcón Venezuela
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-10-22T16:55:40.190847+00:00
Ejecutado	2026-10-22T16:55:43.139231+00:00
Revelado	2026-10-22T16:55:45.850713+00:00

2. Resultado Oficial

18 · Burro

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`37cb42a52429ec94ce6bd52d30b64041b7d055a7d358bcc0c2411e80d5c9ad4b`
Semilla del cliente (client seed)	`e7b9834de4aa6006`
Nonce	1
Semilla del servidor (revelada)	`83c14f7505b235c7a2479ae479ae05599cf50af4149f11343ec61eae7d1e210a`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	64
Hash anterior (prev_hash)	`e6c0fcf56845928df7c13b290a488b00d81cf8a0f6c289668a85f6a6297dfd8c`
Hash del registro (record_hash)	`88c205f48c38894dacda79a79c3c9f67d564c2f4ca664c025021073cdf8c8a83`

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.