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	8955f4b4-79a3-4089-bc36-430868521473
Nombre	ZooloFalcón Venezuela — 22/10/2026 18:44
Tipo de juego	ZooloFalcón Venezuela
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-10-22T18:44:00.262347+00:00
Ejecutado	2026-10-22T18:44:01.355729+00:00
Revelado	2026-10-22T18:44:02.387543+00:00

2. Resultado Oficial

61 · Panda

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`e5f495e676eca3d77cffcc24aa980b40b700e4291b488659820f468858a8c33f`
Semilla del cliente (client seed)	`79ba6ba98e492726`
Nonce	1
Semilla del servidor (revelada)	`3cce6ab42bff3f168d1bc376432735e3e07d8d8b8e8520f1ac26bf6c62d71a66`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	82
Hash anterior (prev_hash)	`b691c1708e9b91b97c231936dca26f75e6a03de96da5eb71f6f688a1f1750bc0`
Hash del registro (record_hash)	`a2df1c1c8c3fe9dc5e7b6c33de8c314ef48207f8e99496f50cd26182d8b928c3`

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.