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	25ba5ef5-6dce-45ac-b921-9b0320153eb7
Nombre	ZooloFalcón Venezuela — 10/11/2026 13:10
Tipo de juego	ZooloFalcón Venezuela
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-11-10T13:10:43.240470+00:00
Ejecutado	2026-11-10T13:10:44.240155+00:00
Revelado	2026-11-10T13:10:45.243794+00:00

2. Resultado Oficial

11 · Gato

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`6e2bb158689507663026900 5a8e643b5928a7dfa475e59031108509cd4fb3a2d`
Semilla del cliente (client seed)	`7072df5b8072dd97`
Nonce	1
Semilla del servidor (revelada)	`66f5a6fd5f43dc227e5885e37b46ecde5ffae1aca8d27a6ca096307e7b31fd62`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	131
Hash anterior (prev_hash)	`129393fc242203d54aa1ec71a401dd75046ffb196f70ff6070acdb57c21a8052`
Hash del registro (record_hash)	`e9c3b1a4a4632d50ca00432d126a182cd7da274e43ada3961db7ee6065cfe4e6`

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.