



ACTA DE SORTEO CERTIFICADO

SORTIVEN V1.4 — Sistema de Sorteo Auditable · Aleatoriedad Verificable (Provably Fair)

1. Identificación del Sorteo

ID del sorteo	dcb14a6c-52d3-4cd3-b910-cefc24476c5e
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 011
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:38:06Z
Ejecutado	2026-08-25T05:38:06Z
Revelado	2026-08-25T05:38:06Z

2. Resultado Oficial

09 · Águila

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	777f928b6a3b561b92b89e23519bde6688ddee597a210c8246cb801559e5de4d
Semilla del cliente (client seed)	sencamer-demo-animalitos-011
Nonce	11
Semilla del servidor (revelada)	346d4259833a53715cf6c55be1a2a37cd1bdb138e679edd88f0cb8c3f14a9a2c

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	42
Hash anterior (prev_hash)	e2cc1109de9400336fcb0ffe6b03f8fa34bf930d5bf8e2a9fd00439263945026
Hash del registro (record_hash)	56e01ae286c44eff30147cff4c0dc7b9b56a9fba2edadf1a88e16355985732b6

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.