



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	3a5f2f6b-5cb3-4586-a2a7-d94f6928d1bc
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 012
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:38:07Z
Ejecutado	2026-08-25T05:38:07Z
Revelado	2026-08-25T05:38:07Z

2. Resultado Oficial

50 · Canario

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	f65bf0a79013ad72cc5a3413ac4333298704b54c398572d64339a4a9ce2d499d
Semilla del cliente (client seed)	sencamer-demo-animalitos-012
Nonce	12
Semilla del servidor (revelada)	a8f97a39f34973bacece21eef01c1e06bd63044c3ef758c2260f2fc00e0334c0

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	43
Hash anterior (prev_hash)	56e01ae286c44eff30147c7f4c0dc7b9b56a9fba2edadf1a88e16355985732b6
Hash del registro (record_hash)	f8e7d82248debe3617fc73d9bd434f3673c400a847e98781b3049031c28465d7

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.