



FACULTAD DE CIENCIAS EXACTAS Y NATURALES
Universidad Nacional de La Pampa



FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS Y NATURALES
Universidad Nacional de San Luis

OTP-Vote: Avances en Seguridad, Auditoría y Verificabilidad End-to-End hacia su Implementación

Silvia BAST, Germán MONTEJANO, Mario BERÓN

Resumen



Este trabajo detalla la evolución de OTP-Vote, un sistema de voto electrónico basado en el cifrado One Time Pad (OTP). Se centra en fortalecer la seguridad, la auditoría y la verificabilidad End-to-End (VE2E) para garantizar procesos electorales robustos y transparentes.

Líneas de Investigación y Desarrollo

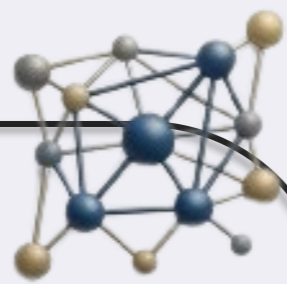


El desarrollo del modelo OTP-Vote se organiza en dos ejes principales:

- Optimización del modelo base: mejora de robustez, desempeño y confiabilidad.
- Extensión del modelo: incorporación de mecanismos de auditoría y VE2E.

Ambos ejes buscan consolidar un sistema de voto electrónico seguro, transparente e implementable.

Contexto



El trabajo se desarrolla en el marco del proyecto "Especificación Integral del Sistema OTP-Vote orientada a su Implementación" (FCEyN-UNLPam), que continúa la línea de investigación en voto electrónico basado en criptografía One Time Pad.

La investigación se realiza de forma conjunta entre UNLPam y UNSL, articulada con el proyecto PROICO 2020 de la UNSL, con el objetivo de avanzar hacia la implementación de un sistema de voto electrónico seguro, auditable y verificable.

Avances



Se lograron avances en:

- Profundización en la especificación de procesos del sistema electoral.
- Fortalecimiento del modelo de datos y estructuras críticas
- Sistema de auditoría con logs verificables.
- Mecanismos de VE2E preservando el secreto del voto.

Impacto. Los resultados consolidan OTP-Vote como una arquitectura que integra:

- Seguridad criptográfica
- Auditoría operativa
- VE2E
- Preservación del secreto del voto

Trabajos Futuros. Las próximas líneas incluyen:

- Validación mediante simulaciones
- Optimización para elecciones de gran escala
- Mejoras en los sistemas de auditoría

Formación de Recursos Humanos



En el marco del proyecto, Silvia Bast presentó en 2025 su tesis doctoral "Especificación Integral del Modelo OTP-Vote orientada a su implementación" (Doctorado en Ingeniería Informática, UNSL), que integra y amplía los resultados obtenidos en esta línea de investigación.

Contacto

silviabast@exactas.unlpam.edu.ar
gmonte@unsl.edu.ar
mberon@unsl.edu.ar