VINCULACIÓN ACADÉMICA EN AUDITORÍAS DE SOFTWARE ELECTORAL: FORMACIÓN DE TALENTO EN CALIDAD Y SEGURIDAD

ACADEMIC ENGAGEMENT IN ELECTORAL SOFTWARE AUDITS: TRAINING TALENT IN QUALITY AND SECURITY

J. Hernández Cabrera[1]
M. Pérez Medel[2]
A. Velasco Agustín[3]

RESUMEN

La auditoría de software electoral es crucial para asegurar la calidad y seguridad de los sistemas empleados en procesos democráticos. Este artículo expone una innovadora estrategia de vinculación académica entre la Facultad de Estudios Superiores Aragón de la UNAM e institutos electorales, donde estudiantes destacados de ingeniería en computación participan activamente en auditorías reales. A través de este modelo colaborativo, los alumnos no sólo aplican sus conocimientos técnicos en escenarios reales, sino que también adquieren habilidades profesionales críticas, como el análisis de vulnerabilidades, gestión de la seguridad informática y la elaboración de informes técnicos. Destacamos la metodología implementada, que incluye desde la selección de los estudiantes hasta su formación y asignación en roles específicos dentro de los proyectos de auditoría, como revisores de calidad en el proceso de desarrollo de software, analistas de seguridad, revisores de código y especialistas en infraestructura. Este enfoque no sólo ha fortalecido la seguridad y calidad de los sistemas auditados sino que también ha enriquecido la formación académica de los estudiantes, preparándolos de manera óptima para los desafíos del mercado laboral en tecnologías de la información y ciberseguridad.

ABSTRACT

Auditing electoral software is crucial to ensure the quality and security of the systems used in democratic processes. This article presents an innovative strategy of academic linkage between the UNAM Aragón School of Advanced Studies and electoral institutes, where outstanding computer engineering students actively participate in real audits. Through this collaborative model, students not only apply their technical knowledge in real scenarios, but also acquire critical professional skills, such as vulnerability analysis, computer security management, and the preparation of technical reports. We highlight the methodology implemented, which includes everything from the selection of students to their training and assignment in specific roles within audit projects, such as quality reviewers in the software development process, security analysts, code reviewers, and infrastructure specialists. This approach has not only strengthened the security and quality of the audited systems but has also enriched the academic training of students, optimally preparing them for the challenges of the labor market in information technology and cybersecurity.

ANTECEDENTES

El software electoral ha evolucionado como un componente esencial en la organización de elecciones modernas, facilitando desde la gestión del padrón electoral (Instituto Nacional Electoral [INE], 2025) hasta la publicación de resultados preliminares. Sin embargo, su correcta implementación y seguridad han sido objeto de preocupaciones constantes. En México, los sistemas de Programa de Resultados Electorales Preliminares (PREP) (INE, 2024) y Conteos Rápidos (CR) (INE, 2024) han estado en la mira de auditorías debido a la

[1] Profesor de tiempo completo Titular. FES Aragón UNAM. jesushc@unam.mx
[2] Técnico Académico Titular. FES Aragón UNAM. marcelo@unam.mx
[3] Profesor de asignatura. FES Aragón UNAM. aaronvelascovea@aragon.unam.mx

preocupación de posibles vulnerabilidades tecnológicas y fallos en la integridad de los datos. En este contexto, la vinculación académica ha permitido generar estrategias de auditoría que involucran a estudiantes universitarios bajo la guía de expertos en calidad y seguridad del software electoral.

En la revisión de la literatura sobre software electoral, se abordan las preocupaciones predominantes y se destaca la importancia que la industria asigna a la calidad y seguridad del software electoral, especialmente hacen énfasis en garantizar la integridad y confianza de los procesos electorales, por ejemplo Alex y Teague (2015) plantean algunas de estas preocupaciones en sistemas de votación, donde se ha comprobado que algunos sistemas de votación presentan fallas de seguridad que podrían ser explotadas para manipular votos o violar la privacidad de los electores. Es el caso del sistema iVote utilizado en Nueva Gales del Sur, Australia, se identificaron vulnerabilidades que permitían comprometer la integridad y confidencialidad de los votos.

Otra preocupación la plantea Jamroga et al. (2021) donde expresa que confianza excesiva en el software sin mecanismos de verificación independientes puede comprometer la transparencia electoral. Se ha propuesto el principio de "independencia del software", que sugiere que un sistema de votación debe proporcionar evidencia suficiente para convencer a los observadores de que el resultado es correcto, sin depender únicamente del software.

En la bibliografía, estas preocupaciones están relacionadas con el software de votación, el cual es un software vinculante en las elecciones, sin embargo, éste es un tipo de software diferente al PREP y a los sistemas de conteos rápidos (CR), ya que estos últimos son software no vinculante, diseñados únicamente para informar resultados preliminares y proporcionar tendencias electorales. Su función es exclusivamente informativa y sus datos no tienen validez oficial en la determinación del resultado final, sin embargo, las preocupaciones de seguridad y calidad es compartida.

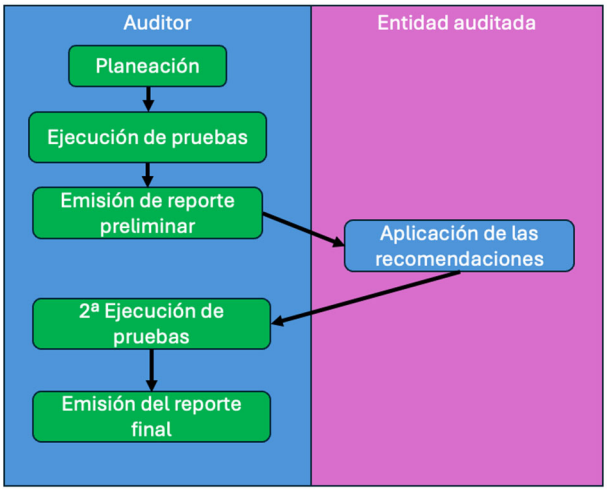
Abordar estas problemáticas requiere una colaboración estrecha entre autoridades electorales, expertos en seguridad informática y la comunidad académica para desarrollar e implementar soluciones que fortalezcan la integridad y confianza en los procesos electorales. Es aquí donde académicos y alumnos destacados de la carrera de ingeniería en Computación de la Facultad de Estudios Superiores Aragón (FES Aragón) de la Universidad Nacional Autónoma de México (UNAM) han participado activamente en el estudio y revisión de los sistemas PREP y CR desde el año 2015 en diferentes elecciones. A continuación, se presenta un resumen de la metodología adoptada por este grupo académico donde se privilegia la aplicación práctica de conocimientos de los alumnos en las áreas de Ingeniería de Software y Seguridad de la información.

METODOLOGÍA

La auditoría de software electoral se basa en un enfoque estructurado y metodológico que garantiza la evaluación exhaustiva de la calidad y seguridad de los sistemas utilizados en los procesos electorales. La implementación de esta metodología ha sido clave para detectar vulnerabilidades, evaluar la infraestructura tecnológica y proponer mejoras antes de su uso para la publicación de resultados de las elecciones. El proceso de auditoría que se muestra en la Figura 1 se desarrolla en diversas fases que incluyen la revisión de la calidad del software,

funcionalidad, la arquitectura, pruebas de penetración, pruebas de negación de servicio y validación de integridad de los datos.

Figura 1. *Metodología de pruebas de auditoría.*



1. Planeación

En esta fase, el equipo auditor, en coordinación con el ente auditado, establece los objetivos, fechas, requerimientos y alcance de las pruebas a implementar. Esta fase es crucial, ya que de ella depende la correcta ejecución de las siguientes etapas.

2. Ejecución de pruebas

Las pruebas para auditar el sistema informático del PREP y su infraestructura tecnológica se dividen en varias líneas de ejecución las cuales se resumen en la Tabla 1.

Tabla 1. *Síntesis de los tipos de pruebas que se deben llevar a cabo para garantizar tanto la seguridad como la calidad del software utilizado en el Programa de Resultados Electorales Preliminares.*

Categoría	Tipo de prueba	Descripción
Pruebas de Calidad de Software	Pruebas Funcionales de Caja Negra	Evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares, verificando el cumplimiento de las especificaciones funcionales usando (ISO/IEC, 2015).
	Validación del Sistema.	Asegurar que el software y bases de datos usados en el PREP correspondan a los previamente auditados y no contengan resultados electorales preliminares o de pruebas antes de su operación.
Pruebas de seguridad	Pruebas de Penetración (Pentest)	Evalúan las configuraciones de seguridad para identificar vulnerabilidades en infraestructura y aplicaciones. Se realizan tanto desde el interior como desde el exterior de la red.
	Análisis de Vulnerabilidades	Identificar debilidades de seguridad en la infraestructura tecnológica y en los servicios TI relacionados con el PREP, documentar las vulnerabilidades y recomendar medidas de mitigación (Chapple et al, 2018).
	Revisión de Configuraciones	Analizar las configuraciones de los dispositivos para garantizar que se ajustan a las mejores prácticas de seguridad informática.
	Pruebas de Negación de Servicio	Generar tráfico de red para simular ataques DDoS, evaluando la capacidad del sistema para mantener la disponibilidad del servicio (Amazon Web Services [AWS], 2023).

3. Elaboración de Informes

Tras la ejecución de las diferentes pruebas de auditoría, se elabora un informe técnico con carácter de preliminar el cual incluye:

- Lista de vulnerabilidades detectadas.
- Evaluación del impacto de cada hallazgo.
- Recomendaciones de mitigación.
- Acciones correctivas y plan de mejora.

4. Aplicación de Recomendaciones.

En esta fase, el ente auditado es el responsable de realizar los trabajos donde se implementan las medidas correctivas recomendadas. En esta actividad debe cubrir todas las recomendaciones hechas por el ente auditor y documentar como se trató el riesgo asociado.

5. Segunda fase de pruebas.
En esta fase el ente auditor ejecuta una segunda fase de pruebas donde se revisa que la aplicación de recomendaciones fueron realizadas correctamente y por tanto el hallazgo fue erradicado o en su defecto mitigado.

6. Entrega del Informe Final de Auditoría
El informe final documenta los resultados de la auditoría, las mejoras aplicadas y las conclusiones sobre la seguridad e integridad del sistema PREP, asegurando su confiabilidad antes de su operación.

Participación de alumnos en los proyectos: selección, capacitación y roles.
El modelo de participación académica en auditorías de sistemas PREP y CR sigue un proceso estructurado que garantiza la selección de los mejores talentos y su adecuada formación:

1. **Selección de estudiantes:**
- Se realiza una convocatoria abierta dentro de la FES Aragón, priorizando a alumnos con un alto desempeño en áreas de ingeniería de software, ciberseguridad y sistemas computacionales.
- Se aplican pruebas técnicas y entrevistas para evaluar sus conocimientos en auditoría de software y seguridad informática.
- Se busca diversidad de perfiles para cubrir distintos aspectos del proceso de auditoría.
2. **Capacitación y formación:**
- Se imparten cursos intensivos en seguridad de software electoral, basados en marcos como (Open Web Application Security Project [OWASP], 2024) y (National Institute of Standards and Technology [NIST], 2020).
- Los estudiantes reciben entrenamiento en el uso de herramientas de auditoría y metodologías de pruebas de penetración.
- Se realizan simulaciones y estudios de casos para preparar a los alumnos ante escenarios reales.
3. **Roles asignados dentro del proyecto:**
- **Analistas de seguridad:** Encargados de realizar pruebas de penetración y analizar vulnerabilidades en los sistemas electorales.
- **Revisores de código:** Responsables de examinar el código fuente en busca de posibles fallas de seguridad o calidad.
- **Especialistas en infraestructura:** Evalúan la arquitectura tecnológica del software electoral y su resistencia ante ataques.
- **Documentadores y reportadores:** Elaboran informes con hallazgos y recomendaciones para mejorar la seguridad y calidad del software auditado.

Este modelo de participación ha demostrado ser efectivo en la formación de talento, proporcionando a los estudiantes una experiencia práctica invaluable y generando impacto positivo en la seguridad de los sistemas electorales.

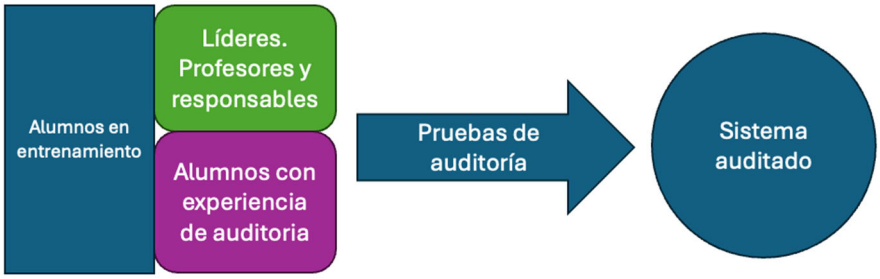
Esquema de Inclusión de Alumnos en Proyectos de Auditoría

El modelo de integración de alumnos en proyectos de auditoría tiene como objetivo complementar su formación académica en la carrera de Ingeniería en Computación mediante la participación en auditorías de sistemas reales con dos roles acotados:

- Alumnos en entrenamiento, quienes están en una etapa de aprendizaje inicial y adquieren conocimientos prácticos bajo supervisión.
- Alumnos con experiencia en auditoría, que han participado en proyectos previos y tienen un rol más activo en la ejecución de pruebas.

A lo largo del proceso, los profesores y responsables del proyecto actúan como guías, asegurando que los alumnos reciban el acompañamiento necesario y manteniendo un flujo continuo de integración y egreso de estudiantes como se muestra en el Figura 2. El trabajo en equipo permite que los alumnos desarrollen habilidades técnicas y metodológicas clave en auditoría de sistemas, realizando pruebas estructuradas que garantizan la seguridad e integridad del sistema auditado.

Figura 2. *Esquema de participación y aprendizaje de alumnos en proyectos de auditoría.*



Este enfoque asegura la formación de futuros profesionales con experiencia real en auditoría, fortaleciendo su preparación para el ámbito laboral.

Herramientas y estándares utilizados en las auditorías.
Para garantizar la calidad y seguridad de los sistemas de software electoral, las auditorías han hecho uso de herramientas especializadas y estándares internacionales que permiten evaluar con precisión la infraestructura, las aplicaciones y los protocolos de seguridad involucrados. La combinación de estos elementos ha sido clave para la detección de vulnerabilidades y la implementación de medidas correctivas antes de la jornada electoral.

1. Herramientas utilizadas en la auditoría de software electoral
Las auditorías de sistemas como el Programa de Resultados Electorales Preliminares (PREP) han requerido el uso de un conjunto de herramientas que facilitan el análisis de seguridad en distintos niveles del sistema: Burp Suite, Metasploit, Nessus, Wireshark, Nmap, OSSEC y Hashcat entre otros (Kali-Linux, 2025).

El uso de estas herramientas ha permitido a los auditores obtener un panorama detallado sobre el estado de seguridad del software electoral, garantizando que las vulnerabilidades sean detectadas y mitigadas de manera efectiva.

2. Estándares internacionales aplicados en la auditoría
Además del uso de herramientas especializadas, las auditorías han seguido metodologías y estándares reconocidos internacionalmente, asegurando que las evaluaciones se realicen con base en las mejores prácticas globales en materia de seguridad y calidad del software. Entre los principales estándares utilizados destacan:

NIST SP800-115 (NIST, 2020): Guía técnica del Instituto Nacional de Estándares y Tecnología de EE.UU., que proporciona lineamientos específicos para la ejecución de pruebas de seguridad en infraestructuras críticas.

OWASP Top Ten (OWASP, 2024): Marco de referencia en seguridad de aplicaciones web, utilizado para evaluar la exposición del software electoral a riesgos como inyección de SQL, configuración incorrecta de seguridad y exposición de datos sensibles.

OSSTMM (Open Source Security Testing Methodology Manual) (Institute for Security and Open Methodologies [ISECOM], 2010): Metodología de pruebas de seguridad aplicada a la infraestructura tecnológica del sistema electoral, enfocada en la identificación de vulnerabilidades y la evaluación de medidas de mitigación.

RESULTADOS

Impacto en la formación de estudiantes, aprendizaje y habilidades adquiridas.

La participación de estudiantes en auditorías de software electoral ha generado un impacto significativo en su formación, brindándoles conocimientos clave y fortaleciendo tanto sus habilidades técnicas como sus competencias profesionales.

En el ámbito técnico, esta experiencia les ha permitido desarrollar un dominio avanzado de herramientas y metodologías de auditoría de software, así como profundizar en conceptos de ciberseguridad y pruebas de penetración. Además, han adquirido la capacidad de analizar código y detectar vulnerabilidades, lo que les ha proporcionado una comprensión más sólida de los riesgos de seguridad en sistemas electorales.

A nivel profesional, la participación en estos proyectos ha fomentado el trabajo en equipo y la comunicación efectiva con expertos y autoridades electorales. Asimismo, ha impulsado el desarrollo del pensamiento crítico y la resolución de problemas, habilidades esenciales para la identificación y mitigación de amenazas en entornos tecnológicos. También han adquirido experiencia en la elaboración de informes técnicos y la presentación de hallazgos, lo que ha fortalecido su capacidad para documentar y comunicar resultados de manera estructurada.

En términos de crecimiento y oportunidades laborales, esta experiencia ha mejorado las habilidades laborales de los estudiantes, facilitando su acceso a oportunidades en el campo de la seguridad informática. Además, les ha permitido establecer redes de contacto con profesionales del sector, lo que amplía sus posibilidades de colaboración en futuros proyectos, esto se ve reflejado en el hecho de que todos los alumnos que participaron en

proyectos pasados se encuentren laborando en áreas afines a las que se desarrollaron durante los proyectos. Finalmente, ha incentivado su interés por continuar su formación en áreas de tecnologías de la información y ciberseguridad, promoviendo el desarrollo de talento especializado en la auditoría de sistemas críticos.

Aportaciones a la calidad y seguridad de los sistemas auditados.
Las auditorías realizadas en los sistemas PREP y CR han contribuido significativamente a la mejora de su calidad y seguridad. A través de la aplicación de metodologías estandarizadas y herramientas especializadas, se han identificado y mitigado vulnerabilidades críticas, fortaleciendo así la confiabilidad de los procesos electorales.

Uno de los principales aportes de las auditorías ha sido la identificación de fallas en la seguridad del software electoral. Se detectaron vulnerabilidades en la infraestructura tecnológica del Programa de Resultados Electorales Preliminares (PREP) y del sistema de Conteos Rápidos, lo que permitió su corrección antes de la jornada electoral. Se llevaron a cabo pruebas de caja negra y caja gris para evaluar la resistencia de los sistemas ante ataques cibernéticos, asegurando que la infraestructura fuera robusta y resistente a intentos de manipulación.

Las auditorías han incorporado estándares reconocidos internacionalmente, tales como:
- OWASP Top Ten, para evaluar riesgos en aplicaciones web.
- ISO/IEC 27001, para la gestión de seguridad de la información.
- OSSTMM, para la evaluación metodológica de pruebas de seguridad.
- NIST SP800-115, que proporciona guías técnicas para pruebas de seguridad.

El uso de estas normativas ha permitido garantizar que los sistemas auditados cumplan con las mejores prácticas en seguridad informática.

Se realizaron revisiones exhaustivas en los mecanismos de control de acceso y autenticación de los sistemas electorales. Se verificó que los permisos de usuario estuvieran correctamente configurados y que existieran registros detallados en los logs del sistema para rastrear cualquier actividad sospechosa. Asimismo, se aseguraron mecanismos de auditoría para detectar accesos no autorizados y prevenir ataques de escalamiento de privilegios.

Las auditorías implementaron mecanismos de validación de integridad de la información, asegurando que los datos electorales capturados en el PREP y en los Conteos Rápidos fueran consistentes, precisos y libres de alteraciones. Se verificó que todas las transacciones críticas generaran registros detallados en bitácoras, permitiendo la trazabilidad de cada acción dentro del sistema.

Se ejecutaron pruebas de rendimiento y estrés para evaluar la capacidad del sistema en condiciones de alta demanda, asegurando que pudiera soportar el volumen de información generado durante la jornada electoral. Se identificaron cuellos de botella en la infraestructura y se implementaron mejoras en la arquitectura del sistema para optimizar su desempeño.

A partir de los hallazgos de las auditorías, se han hecho recomendaciones para mejorar los lineamientos técnicos y operativos de los sistemas de software electoral. Esto ha permitido que organismos electorales adopten mejores prácticas en el desarrollo y mantenimiento de estos sistemas, alineándose con estándares internacionales de calidad y seguridad.

Otro de los aportes clave ha sido la formación de nuevas generaciones de especialistas en auditoría de software y ciberseguridad. Gracias a la vinculación con instituciones académicas, estudiantes universitarios han participado en estos procesos de auditoría, desarrollando habilidades técnicas avanzadas en pruebas de seguridad y evaluación de software crítico.

CONCLUSIONES

Las auditorías de software electoral han demostrado ser una herramienta fundamental para garantizar la calidad, seguridad y transparencia en los procesos electorales. A lo largo del estudio y aplicación de metodologías de auditoría en sistemas como el Programa de Resultados Electorales Preliminares (PREP) y los sistemas de Conteo Rápido, se han identificado áreas de oportunidad clave que han permitido mejorar la confiabilidad de estas plataformas antes de su despliegue en comicios oficiales.

Uno de los principales logros de estas auditorías ha sido la detección y mitigación de vulnerabilidades críticas, lo que ha permitido fortalecer la infraestructura tecnológica utilizada en el procesamiento de resultados electorales. La combinación de herramientas de pruebas de penetración, análisis de registros y evaluación de integridad de datos ha sido clave para identificar posibles amenazas y corregirlas de manera oportuna.

La implementación de estándares internacionales en seguridad informática, tales como NIST SP800-115, OWASP y OSSTMM, ha permitido que los sistemas electorales adopten mejores prácticas en ciberseguridad, mejorando la resistencia del software ante ataques y accesos no autorizados. Estas metodologías han brindado un marco sólido para la evaluación y mejora continua del software electoral, asegurando su correcto funcionamiento en escenarios de alta demanda y bajo estrictos requerimientos de confiabilidad.

Otro aspecto destacado ha sido el impacto en la formación académica de estudiantes universitarios, quienes han participado activamente en las auditorías, desarrollando habilidades avanzadas en seguridad informática, análisis de vulnerabilidades y gestión de infraestructura crítica. Este enfoque de vinculación académica ha permitido no sólo fortalecer la capacitación de futuros especialistas en ciberseguridad, sino también generar conciencia sobre la importancia de la integridad de los procesos electorales en la sociedad.

En conclusión, el desarrollo de auditorías de software electoral por parte de un equipo académico ha sido clave para garantizar la seguridad, calidad y confiabilidad de los sistemas utilizados en las elecciones. La combinación de metodologías técnicas rigurosas, herramientas especializadas y la vinculación con la comunidad académica ha permitido avanzar significativamente en la protección de la infraestructura electoral.

BIBLIOGRAFÍA

Alex, H., & Teague, V. (2015). The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election. arXiv (Cornell University)

AWS. (2023). ¿Qué es un ataque DDoS?. https://aws.amazon.com/es/shield/ddos-attack-protection/

Chapple, M., Stewart J. M., & Gibson, D. (2018). CISSP Certified Information Systems Security Professional Official. Sybex Inc

INE. (2024). Programa de Resultados Electorales Preliminares (PREP) del Instituto Nacional Electoral. https://ine.mx/voto-y-elecciones/prep/

INE. (2025). Estadísticasde la Lista Nominal y Padrón Electoral. Instituto Nacional Electoral. https://ine.mx/credencial/estadisticas-lista-nominal-padron-electoral/

ISECOM. (2024). Instituto Nacional Electoral, Conteo Rápido. https://ine.mx/voto-y-elecciones/conteos-rapidos-ine/

ISECOM. (2010). OSSTMM V3. isecom.org. https://www.isecom.org/OSSTMM.3.pdf

International Organization for Standardization. ISO/IEC. (2015). Software and systems engineering - Software testing. ISO/IEC/IEEE 29119-4:2015. https://www.iso.org/standard/60245.html

Jamroga, W., Ryan, P., & Schneider, S. (2021). A Declaration of Software Independence. In Protocols, Strands, and Logic. Springer, Cham.

Kali-Linux. (2025). Kali Tools, Tool documentation. https://www.kali.org/tools/

NIST. (2020). NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment. https://www.nist.gov/privacy-framework/nist-sp-800-115

OWASP. (2024). OWASP Top Ten. OWASP Project. https://owasp.org/www-project-top-ten/