

Auditoría al Programa de Resultados Electorales Preliminares (PREP) Elecciones Tlaxcala 2016

El Instituto Tlaxcalteca de Elecciones (ITE) de acuerdo a los lineamientos establecidos formó un Comité Técnico Asesor para el apoyo del proceso de auditoría.

El sistema PREP fue realizado por un desarrollo propio del ITE y de acuerdo a los lineamientos de la Auditoría de Sistemas Informáticos, la auditoría fue comisionada hacerla al Instituto Tecnológico de Morelia

La auditoría tiene el objetivo de verificación y análisis de los sistemas informáticos que son utilizados en la implementación del PREP, con la finalidad de evaluar la integridad en el procesamiento de la información y la generación de los resultados conforme a la normativa aplicable y vigente.

Los alcances de la auditoría abarcan los 7 puntos descritos en el artículo 33 del capítulo V del lineamiento de auditoría.

La funcionalidad del sistema se verificó en tres áreas siguiendo el flujo del procesamiento de información.

1. Centros de Acopio y Transmisión de Datos (CATD)
2. Publicación de Información

Centros de Acopio y Transmisión de Datos (CATD)

Se verificó que una vez recibidas las Actas de Escrutinio y Cómputo del PREP en un municipio en particular, estas sean procesadas correctamente para su publicación de acuerdo a las siguientes etapas:

1. Foliación
2. Captura
3. Verificación
4. Digitalización

Criterio	Hallazgo	Comentarios
Revisión que el personal del PREP siga de acuerdo a su manual de procedimientos el proceso de Acopio, Captura, Verificación y Digitalización de las Actas de Escrutinio y Cómputo que para su capacitación	Ninguno. Existe una buena documentación que es entregada a todo el personal. El personal está altamente capacitado en el proceso de acopio, captura, verificación y digitalización de actas ya que se realizan	Se pueden realizar videotutoriales para apoyar de mejor forma al personal que es más visual en su aprendizaje.



Departamento de
Sistemas y Computación



les sean proporcionadas.	diariamente simulacros	
Foliación (Verificación de actas recibidas en buena forma y validación de los siguientes datos: Tipo de Elección, Número de Sección, Tipo de Casilla, Domicilio, Funcionarios de la mesa de casilla)	Ninguno (las primeras revisiones se hicieron a través de actas prefabricadas).	Se verificó la existencia de un proceso de supervisión, en donde diversos supervisores apoyan al proceso de foliación en caso de que ocurra algún incidente, el cual se reporta al inspector de cada distrito
Foliación (verificación de la funcionalidad del aplicativo)	Ninguno, El sistema es fácil de usar, se tiene una administración de las cuentas de usuario. Solo las cuentas registradas en los equipos de cómputo pueden utilizarse.	Se sugiere que las contraseñas de los usuarios sean más robustas a fin de que sea más difícil que usuarios físicos no registrados puedan entrar (se comprobó que existe un protocolo de seguridad física a través de personal de seguridad).
Captura (verificación de asignación de actas a capturista)	Ninguno (la asignación de actas para capturas la realiza el supervisor de forma manual)	Se sugiere automatizar el proceso para que de forma automática se realiza la asignación de actas.
Verificación (comprobación de que la segunda captura sea coincidente)	Ninguno (la verificación se realiza por otra persona a través de la asignación por parte del supervisor. Una persona captura y otra diferente verifica)	Se verificaron los distintos escenarios de captura: <ol style="list-style-type: none">1. Cuando la segunda captura (proceso de verificación) es coincidente la captura se considera válida.2. Si la primera captura no coincide con la segunda (verificación) se deshecha la validación y se vuelve a realizar desde el principio el proceso de captura-verificación. El supervisor verifica los errores de capturistas y verificadores y

Rojas

Juan Carlos Olvera

		<p>en caso de fallas repetitivas puede cambiar de roles al personal involucrado.</p> <p>Se recomienda mejorar el proceso de captura-verificación a fin de hacerlo más automatizado y menos propenso a errores.</p>
Captura (publicación de resultados)	Ninguno	Se verificó que después de la correcta validación tanto la acta como los resultados de la acta se publican de forma adecuada.
Captura/Verificación (funcionalidad del aplicativo)	Ninguno	<p>El sistema maneja de forma adecuada validaciones de captura. Es de fácil uso pero un poco tardado en realizar las capturas y verificaciones.</p> <p>Se encontró que el personal está altamente capacitado en el proceso y en caso de duda siempre pregunta a sus supervisores.</p>
Verificar que las actas que se han digitalizado sean recibidas de forma correcta en el Sistema de Publicación.	Ninguno (las actas eran de prueba pero con el formato y datos de verificación correctos)	Se recomienda mejorar el proceso de digitalización ya que puede ser confuso al momento de nombrar los archivos y puede ser propensos a errores.
Verificación (se verificó que coincidan los datos del domicilio con la información del catálogo de casillas, además de los funcionarios anotados en el acta con los funcionarios de casilla contenidos en el catálogo del sistema.	Sin Catalogo	
Revisión de Infraestructura	Ninguno (Las capacidades del equipo de cómputo que lee y envía la imagen digitalizada, así como el escáner son de calidad, lo	Se revisó que existen protocolos para actuar en caso de contingencia generada por el equipo de digitalización o captura, así como protocolo de

Revisión

San Carlos Oaxaca

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]



Departamento de
Sistemas y Computación



	<p>que garantiza el correcto funcionamiento del sistema. Los equipos de cómputo para captura y verificación funcionan de forma adecuada. Se cuenta además con infraestructura adicional para usarse en caso de contingencia).</p>	<p>contingencia en enlaces de Internet (Plan de Continuidad) y de suministro de energía eléctrica así como que existen sistemas y procedimientos de monitoreo del correcto funcionamiento de la infraestructura.</p> <p>Se verificó la red de área local así como los equipos de cómputo utilizados en los CATO funcionando de forma óptima. Se detectó que la red de datos con respecto al cableado horizontal no cumple con requisitos de cableado estructurado, dado que se maneja red inalámbrica.</p> <p>Se cuenta con un site de telecomunicaciones con un servidor espejo rentado a TELCEL, el cual fue probado para llevar a cabo el último simulacro.</p> <p>Se cuenta con sistemas de redundancia de suministro de energía eléctrica, y con un plan de contingencia en caso de fallo, trasladarse a la central dado que el tiempo de arribo es poco debido a las cortas distancias de los distritos a la central de trabajo del ITE.</p> <p>Se cuentan con equipos de respaldo así como personal de soporte técnico cubriendo todo el estado.</p>
--	---	---

Publicación de Información

Se verificó que los datos mínimos obligatorios a publicar, derivado de su captura o cálculo cumplen con lo establecido en los lineamientos de la auditoría del PREP:

Criterio	Hallazgo	Comentarios
Seguridad (VER ANEXO TECNICO DE SEGURIDAD)	Se pudo verificar la robustez del sistema ante diferentes ataques de bombardeo de paquetes y saturación del servicio. No se encontró ninguna vulnerabilidad de nivel Alto o Medio, como resultado del escaneo y análisis de vulnerabilidades al sistema.	El equipo auditor al momento de realizar estas pruebas contaba únicamente con la liga de la publicación de resultados de un simulacro. La dirección proporcionada fue: http://simulacroprep.itetlax.org.mx/ El nombre de dominio para las elecciones quedo como http://prep.itetlax.org.mx El sistema no cuenta con vulnerabilidades de alto riesgo y responde eficazmente ante ataques de negación de servicio. De igual forma se recomienda activar el sitio al comenzar la jornada y sin mayor tiempo de anticipación como garantía para el mismo.
Se verificó que los votos respecto a los partidos políticos y los candidatos, sean estos independientes, por partido político o por coalición, según sea el caso fuera el correcto	Ninguno	Existe un solo sistema central de publicación garantizando la consistencia, integridad y disponibilidad de la información. Existe solo un mecanismos de respaldo (servidores espejo) que garantizan la integridad y consistencia de los datos antes una posible amenaza.
Se verificó que los datos del encabezado del Acta (entidad federativa, distrito, sección,	Ninguno	El sistema cuenta con mecanismos de respaldo para garantizar la consistencia, integridad y disponibilidad de la información.



casilla (número y tipo)) fueran correctos		
Se verificó el correcto funcionamiento de los estadísticos y sistema de seguimientos (como el porcentaje estimado de participación y el porcentaje y total numérico de avance en el registro de acta conforme a las actas recibidas y el total de actas);	Ninguno	El sistema cuenta con un módulo muy eficiente de reporte de estadísticas con gráficas.
Se verificó la hora y fecha de recepción del acta en el CATD;	Ninguna	Se guarda la hora exacta en que se recibió en el servidor de publicación.
Se verificó que la imagen del acta capturada que se publica es la correcta	Ninguna	Se sugiere guardar la imagen directamente en la base de datos (objeto BLOB).
Se verificó la correcta identificación de AEC con inconsistencias y su publicación	Ninguna	Se cumple con los lineamientos establecidos por el IEM.
Se verificó que los estadísticos finales (Total de votos, total de votos nulos y, en	Ninguno	El sistema muestra de forma amigable los resultados finales de la elección. Se verificó que los totales

Rafael

Juan Carlos Olvera

Se verificó

Se verificó

Se verificó

su caso, total de votos para candidatos no registrados.) fueran los correctos		subtotales corresponden a la sumas y promedios de sus datos individuales.
Funcionalidad del sistema de publicación	Ninguna	<p>El sistema cuenta con un diseño simple y funcional que muestra de forma clara y precisa los resultados de la elección.</p> <p>Se cuenta con muchas formas de ver la información partiendo de datos generales hasta alcanzar datos específicos de forma ágil.</p> <p>El sistema puede ser accedido desde diversos navegadores y dispositivos sin dificultad, incluyendo equipos ya algo antiguos.</p>
Infraestructura Tecnológica	Ninguna	<p>Los servidores se encuentran en la nube con TELMEX y altamente confiables que garantizan una alta disponibilidad, consistencia e integridad en la nube.</p> <p>El sistema en caso de falla al servidor al aplicar el plan de contingencia el tiempo de recuperación puede llevar mucho tiempo si no se cuenta con un técnico experto en el momento de la contingencia.</p> <p>Se cuenta con todo un protocolo establecido de seguridad física y lógica.</p>

Catálogos del Sistema PREP

Criterio	Hallazgo	Comentarios
Se revisaron cada una de las actas con sus datos	Ninguno	La información de los catálogos se encuentra



Departamento de
Sistemas y Computación



verificando su completo funcionamiento (Total de 5503 (1501 para gobernador, 1501 para diputados, 1506 para ayuntamientos, 1028 para comunidades) actas correspondientes a 15 distritos electorales, 60 municipios.)		<p>correctamente almacenada en la base de datos y se muestra de forma adecuada tanto en los sistemas de captura como de presentación de resultados.</p> <p>Se verificó que la captura de los datos se almacenará de forma adecuada en el catálogo adecuado así como que se mostrará de forma adecuada en los estadísticos individuales y grupales.</p>
Otros	Ninguno	<p>Se realizaron los simulacros donde se atendieron diferentes situaciones, como los fallos que se suscitaron por fallas de suministro eléctrico, las cuales fueron atendidas para proteger el evento el día de las elecciones situaciones que se pudieran dar durante la jornada electoral.</p> <p>Se cuenta con equipo humano capacitado para hacer captura, verificación y digitalización, el ambiente laboral se encuentra poco cordial pero comprometida con el proceso electoral.</p> <p>El tiempo promedio de procesamiento es de aproximadamente 6 a 8 horas considerando el tiempo de espera de las actas.</p>

Juan Carlos Oliveros

B

ANEXO TECNICO DE SEGURIDAD INFORMATICA

La metodología propuesta se basa en realizar una revisión sistemática de la dirección de Internet proporcionada, y donde se publican los resultados del Programa de Resultados Preliminares. Se utilizaron programas y herramientas especializadas para este tipo de análisis. El equipo auditor inicio la ejecución de diferente paquetería de software de escaneo, análisis de vulnerabilidades y generación de múltiples paquetes de tráfico hacia el sitio una vez que fue proporcionada la dirección URL por el Instituto Electoral de Tlaxcala a la fecha y hora señalada.

Para la generación de tráfico se utilizó un software propio que a través de múltiples instancias en ejecución, enviaba paquetes de datos de diversos tamaños hacia la dirección proporcionada, lo anterior con el objetivo de probar el comportamiento y la robustez del canal de comunicación, servidor y el servicio Web ante diferentes flujos de tráfico de datos.

Se hizo un escaneo de pruebas de vulnerabilidades sobre la dirección proporcionada, aplicándose las siguientes pruebas:

- Operating System Detected
- Open TCP Services List
- Web Server Version
- Firewall Detected
- SSL Web Server Version
- Host Names Found
- Traceroute
- Internet Service Provider
- IP ID Values Randomness
- SSL Certificate will expire within next six months
- Default Web Page
- SSL Server Information Retrieval
- ICMP Replies Received
- SSL Session Caching Information
- TLS Secure Renegotiation Extension Supported
- SSL Certificate - Information
- Host Scan Time
- SSL/TLS invalid protocol version tolerance
- DNS Host Name
- Target Network Information

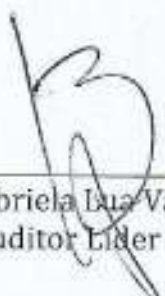
Para escaneo se realizaron las siguientes pruebas:

- Injection
- Broken Authentication and Session Management
- Security Misconfiguration




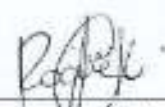
- Sensitive Data Exposure
- Missing Function Level Access Control
- Using Components with Known Vulnerabilities
- Unvalidated Redirects and Forward


En términos generales no se encontraron vulnerabilidades mayores que pudiesen afectar la seguridad del sistema.

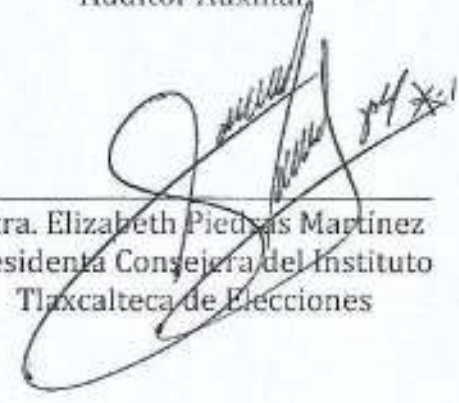

M.C. Gabriela Liza Vargas
Auditor Líder


M.C. Juan Carlos Olivares Rojas
Auditor Auxiliar


M.G.T.I. Salvador Jonathan Villagómez
Cárdenas
Auditor Auxiliar


Ing. Roque Trunfo Ramos
Auditor Auxiliar


Ing. Paulino Alberto Rojas Martínez
Director del Instituto Tecnológico de
Morelia


Mtra. Elizabeth Piedras Martínez
Presidenta Consejera del Instituto
Tlaxcalteca de Elecciones


M. D. Yareli Álvarez Meza
Presidenta de la Comisión de Informática y
Programa de Resultados Preliminares