

COMISIÓN ESPECIAL DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES Y CONTEOS RÁPIDOS DEL INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DEL ESTADO DE GUERRERO

Análisis del listado de candidatos a ente auditor. Presentado por el Comité Técnico del Programa de Resultados Electorales Preliminares

Para el presente análisis se consideraron las dos propuestas de los entes auditores con mayor solidez técnica, que además coincidieron con un menor costo, en este caso el Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) y la Universidad Autónoma Metropolitana (UAM), cabe mencionar que de origen la propuesta de la UAM ha sido la más detallada y explícita en cuanto a los procedimientos técnicos para efectuar la auditoría. En el caso del ITESM la propuesta original es general y en algunos casos no con la suficiencia especificidad, por lo anterior se solicitó a ésta institución que fuera mucho más explícita y específica en la propuesta. Con base en lo anterior, se presentan a continuación los puntos a considerar a favor y en contra de cada una de las propuestas:

1.- Respuesta a la solicitud del primer punto, *“Pruebas funcionales de caja negra al sistema informático del PREP y a la aplicación que se utilizarán para operar el mecanismo de digitalización de las actas desde las casillas.”*, los dos entes auditores realizan las pruebas de funcionalidad del sistema informático PREP, sin embargo, se tiene que:

1.1. La UAM, en su propuesta original, especifica los módulos a los que realiza las pruebas funcionales de caja negra, de los que resaltan; Módulos de Digitalización, Captura de datos y Verificación, así como el Módulo de Publicación de Resultados: todo esto bajo los lineamientos del ISTQB (*International Software Testing Qualifications Board*), en ese sentido, la UAM deja claro que aplicará hasta tres ciclos de pruebas al sistema informático para realizar las observaciones oportunas y éstas puedan corregirse.

1.2. Mientras que, en el primer documento emitido por el Tecnológico de Monterrey, únicamente confirma la realización de pruebas funcionales de caja negra, sin especificar módulos ni metodología; ya en su segundo informe, detalla tanto los módulos del sistema informático a aplicar las pruebas de caja negra, así como la metodología, la cual es ISO/IEC 29119.

Considerando las dos propuestas, este Comité Técnico, valora la importancia de definir desde un inicio alcances, límites y modo de trabajo, lo que sucedió desde un principio con la UAM, sin embargo, advirtiendo la aplicación internacional de las dos metodologías, se opina que la aplicación en cualquier de los dos casos en el PREP 2024, es válido.

2. Respuesta a la solicitud de *“Validación del sistema informático del PREP y/o servicios relacionados con TIC, así como sus bases de datos, ante un tercero con fe pública.”*

2.1. La UAM, en su propuesta Técnica especifica el alcance de lo que realizará, en ese sentido, ofrece la criptografía SHA-512, obteniendo las huellas criptográficas de todos los elementos que constituyen el sistema informático. Además, brinda lo mismo para la base de datos, de tal manera que otorga constancia de hechos de la validación previo al inicio, durante y posterior al cierre de operaciones PREP.

2.2. Por su parte, el Tecnológico de Monterrey, en su propuesta inicial sí ofrece huellas criptográficas, pero no es claro en especificar a detalle qué o cómo lo hará. En la sección “alcance”, en la propuesta ajustada, se especifica a detalle la metodología, resaltando el SHA-256.

Ahora bien, este COTAPREP, hace valoración que desde un inicio se señalará los objetivos y alcances sobre la validación tan importante del sistema informático PREP, y así, centrándose en los ofrecimientos técnicos, el ITESM detalla con mayor precisión la actividad que realizará; siendo las dos propuestas muy semejantes, por lo que nos centraremos en destacar los algoritmos en utilizar, siendo el SHA-256 el más común y rápido de aplicar, por otra parte, el SHA-512 es más seguro por su longitud; no obstante, ambos algoritmos son robustos y seguros, siendo la diferencia muy mínima.

En ese sentido, ambos ofrecimientos técnicos resultan favorables, sólo debe considerarse que el SHA-512, en su nivel de procesamiento, es un poco más lento: considerando este dato, debe extrapolarse ese nivel de procesamiento a la magnitud de información a validar, puesto que no es lo mismo generar una huella criptográfica a un archivo de 1 Gb a otro que tiene un tamaño de 10Gb, esto es solo por poner un ejemplo.

3. Respecto a la solicitud de *“Análisis de vulnerabilidades a la infraestructura y servicios relacionados con TIC donde se implemente el PREP”*, y para fines de un análisis

concreto, debe aclararse que, en las dos propuestas originales, sí muestran a detalle las metodologías de análisis de penetración: por su parte la UAM lo especifica en la página 7, apartado I.3, mientras que, el Tecnológico de Monterrey en la página 15, de ahí que puede señalarse lo siguiente:

Tanto la UAM como el Tecnológico de Monterrey utilizan la metodología PTES (*Testing Execution Standard*) y la complementan con los mismos marcos de referencia, así como ambas propuestas toman el catálogo de vulnerabilidades ya registradas de forma internacional como son CWE (*Common Weakness Enumeration*) o CVE (*Common Vulnerabilities and Exposures*). Las dos propuestas detallan las herramientas a utilizar para tal propuesta técnica, coincidiendo en: NMAP, METASPLOIT, NIKTO, NESSUS Y ZAP. Por lo que, en esta solicitud, los dos cumplen con lo requerido técnicamente.

Ahora bien, en este apartado el COTAPREP detecta que la UAM hace referencia en la página 10, en su apartado “Validación de los datos de entrada” y “Pruebas pasivas”, sobre el PREP 2021; por lo que es de vital interés conocer a que refieren exactamente la relación a dicho PREP 2021, toda vez que el documento de propuesta técnica debe responder a la solicitud de ofrecer la auditoría al PREP 2024.

4. Con relación a la solicitud “*Auditoría al Código fuente, considerando el sistema informático y componentes en el aplicativo móvil del PREP*”, tenemos lo siguiente:

4.1. La UAM, especifica la realización de auditoría al código fuente tanto del sistema Web como la aplicación móvil, utilizando como base lo que recomienda la organización OWASP (La Open Web Application Security Project), la cual proporciona herramientas y directrices para el desarrollo de aplicaciones web seguras.

4.2. Por su parte, el ITESM, menciona dos tipos de análisis a realizar, estático y dinámico, siendo los dos complementarios entre sí, es decir, se requiere que los dos se hagan para señalar posibles debilidades.

En este sentido, el COTAPREP identifica que las dos propuestas son aceptables, sin embargo, se propone que sean sumadas, es decir, la propuesta a elegir, sea la 4.1 o la 4.2, la que se elija se le sugiere aplique las dos formas de auditoría.

5. Para la solicitud “*Pruebas de negación de servicio al sitio de publicación del PREP y al sitio principal del IEPCG, considerando la complejidad de ejecutar este tipo de pruebas,*

éstas pueden llevarse a cabo directamente por el ente auditor, o a través de un tercero que cuente con los recursos de cómputo y ancho de banda necesarios para enviar un volumen de tráfico suficiente para simular las condiciones de saturación que se dan durante un ataque de este tipo.”, se tiene lo siguiente:

Para este punto, el COTAPREP observa que en las dos propuestas técnicas, tanto la UAM como el ITESM, tienen coincidencia en los tipos de ataque de negación de servicio, sin embargo, es de vital interés que en este tipo de pruebas se considere que la jornada electoral puede ocupar gran cantidad de transferencia de información, por tanto, realizar pruebas a una tasa de transferencia mucho mayor, ofrecerá seguridad de más resistencia del sistema informático PREP ante un posible ataque: en ese tenor, el ITESM en su propuesta inicial ofrece un ataque de 12Gbps, mientras que la UAM ofrece 400Mbps. Siendo el de 12Gbps la mejor propuesta.

6. Por último, para la solicitud de *“Revisión de las pantallas del sitio de publicación del PREP, verificando el apego a las plantillas base de la interfaz proporcionadas por el INE.”*

Ambas instituciones ofrecen el servicio de revisión de pantallas del sitio de publicación del PREP de acuerdo con las plantillas proporcionadas por el INE, por lo que el COTAPREP no tiene alguna observación en este punto.

Finalmente, con la finalidad de brindar una opinión técnica como COTAPREP, se advierte que es necesario considerar los planes de trabajo, propuestos por cada candidato para ente auditor, ya que esto define en gran medida los tiempos que tendrá la empresa desarrolladora del sistema a realizar los ajustes, cambios, actualización o demás, a fin de atender debidamente lo que resulte de cada fase de la auditoría.

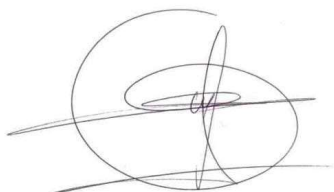
Es decir, un plan de trabajo que brinde tiempo suficiente para realizar pruebas y detectar problemas, y permita la corrección, siempre llevará a un mejor éxito del proyecto.

Con base en lo anterior se concluye:

1. Es importante que la UAM especifique a que se refiere cuando señala en la página 10, en su apartado “Validación de los datos de entrada” y “Pruebas pasivas”, sobre el PREP 2021.

2. Tanto la propuesta del ITESM, como la de la UAM cumplen con los requerimientos especificados por el INE y el IEPC del Estado de Guerrero. No obstante, desde el inicio la UAM ha sido mucho más explícita y contundente en la propuesta técnica. En el caso del ITESM fue necesario solicitarle que fuera más preciso en el planteamiento de los procedimientos y cómo utilizaría las herramientas.

A T E N T A M E N T E



Mtra. Marisol González Barragán



Dra. Celia Palacios Mora



Dr. Agustín Santiago Moreno