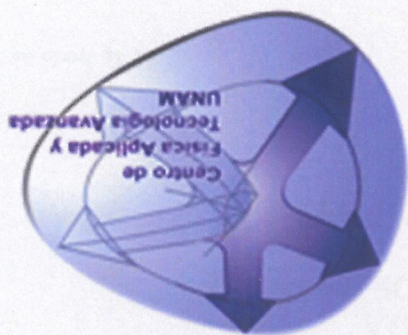


Informe Final 2016

AUDITORIA al Programa de Resultados Electtorales Preliminares del Instituto Estatal Electoral de Aguascalientes





M. en D. Luis Fernando Landeros Ortiz
Consejero Presidente del Consejo General del
Instituto Estatal Electoral de Aguascalientes
Presente
Estimado Maestro, a continuación se desglosa el informe de las actividades realizadas para la auditoría:

1. INTRODUCCIÓN

Como resultado de la entrada en vigor de las reformas en materia político electoral, se celebraron las elecciones locales en el estado de Aguascalientes bajo un nuevo modelo cimentado en un ambiente donde existirá una mayor coordinación entre el Instituto Nacional Electoral (INE) y el Instituto Estatal Electoral del Aguascalientes (IEE), lo anterior, con la finalidad de elevar los estándares de calidad en la organización y ejecución de los procesos electorales.

En este orden de ideas, la implementación del Programa de Resultados Electorales Preliminares (PREP), cuya atribución quedó a cargo de los Organismos Públicos Locales (OPL), tuvo un matiz distinto al conocido hasta entonces, y es que de acuerdo a lo que señala la Constitución Política de los Estados Unidos Mexicanos y las leyes en materia, fue la autoridad electoral a nivel federal quien emitió las normas bajo las cuales debe instrumentarse dicho mecanismo.

El Instituto Estatal Electoral optó por licitar el Programa de Resultados Electorales Preliminares (PREP) donde resultó adjudicada la empresa *PoderNet*. Con la finalidad de poder trabajar adecuadamente, se informaba de

los avances al Instituto y manera paralela a la empresa, para que las observaciones fueran atendidas lo más pronto posible.

En este documento se describen las actividades realizadas para dar cumplimiento a los lineamientos que señalan como puntos de la auditoría:

- El Análisis de vulnerabilidades en la infraestructura tecnológica del PRFP, incluyendo pruebas de negación de servicio, pruebas de inyección de código malicioso y pruebas de acceso a los diversos recursos del sistema informático.

- El análisis de caja negra

Los informes que fueron emitidos respecto a las vulnerabilidades y hallazgos detectados, tienen un carácter estrictamente confidencial y presentan recomendaciones que permitieron al Instituto atender el riesgo identificado durante las pruebas.

2. DESCRIPCIÓN DEL PROYECTO

2.1 Auditoría de Software y Análisis de vulnerabilidades de la infraestructura

2.1.1 Selección de activos para las pruebas y revisión de configuraciones.

El primer paso para el análisis de vulnerabilidades de la infraestructura de TIC (Tecnologías de la Información y Comunicación), es establecer los activos sobre los que se realizarán las pruebas y la revisión de configuraciones. Para lo cual deben tomarse en cuenta los siguientes aspectos:

- a. Clasificación de los activos por funcionalidad y aspectos técnicos como modelo y sistema operativo.

- b. Condiciones de operación actual de los activos a evaluar.

- c. Horarios de ejecución de las pruebas y revisiones.

A partir del listado total de activos de la infraestructura de TIC a evaluar y tomando en cuenta los puntos anteriores, se estableció la lista de activos tecnológicos sobre los que se realizaron las pruebas de penetración, así como

Después de la aplicación de las medidas de mitigación, se realizó una verificación enfocada específicamente a revisar cada hallazgo identificado y determinar si el impacto ha sido mitigado de forma parcial o total. Para este fin se volvió a realizar una segunda visita a todos los activos en las 5 zonas asignadas.

Se informó al IFE los nuevos resultados de la verificación de hallazgos y la implementación de medidas de mitigación. Se determinó que de forma interna no se presentaba ningún riesgo, pero de forma externa se recomendó revisar el certificado y utilizar un dominio diferente al de pruebas.

2.2 Límites de la Auditoría

La auditoría del PREEP es de carácter técnico y fue enfocada únicamente a lo que se refiere al funcionamiento del sistema informático, es decir, el software, programas de cómputo y a las vulnerabilidades que pueden presentarse en la infraestructura tecnológica.

2.2.1 Determinación de las líneas trabajo de la auditoría.

Las líneas de trabajo técnicas que se consideraron como parte de la auditoría al PREEP, fueron las siguientes:

- Análisis de vulnerabilidades en la infraestructura tecnológica del PREEP, incluyendo pruebas de negación de servicio, pruebas de inyección de código malicioso y pruebas de acceso a los diversos recursos del sistema informático.
- Aplicación de pruebas de penetración, revisión de configuraciones de seguridad y la realización de pruebas de denegación de servicio (DoS), con la finalidad de identificar posibles vulnerabilidades en la infraestructura tecnológica del PREEP.
- Pruebas funcionales de caja negra del sistema informático del PREEP.
- Monitoreo el día de la Jornada electoral

2.2.2 Requisitos funcionales de la auditoria

Se revisó que el sistema cumpliera con las funciones específicas y se encontró lo siguiente:

1. Datos mínimos obligatorios. El sistema publica los siguientes datos mínimos obligatorios:

- Los votos respecto a los partidos políticos y a los candidatos, sean independientes, por partido o por coalición, según sea el caso.
- El porcentaje estimado de participación.
- El porcentaje numérico de avance en el registro de actas recibidas y total de actas.
- Fecha y hora de recepción del acta en el CATD. Sólo se registra en la BD.
- Imagen del acta capturada.
- Identificación de AEC con inconsistencias
- Total de votos nulos y, en su caso, total de votos para candidatos no registrados.

2. Funciones mínimas del sistema.

- En cuanto a la funcionalidad del sistema es necesario garantizar y evaluar la integridad en el procesamiento de la información de las Actas de Escrutinio y Cómputo (AEC). En el caso del PRBP, se referirá a la información de las Actas de Escrutinio y Cómputo (AEC).
 - El sistema permite la captura, digitalización y publicación de los datos asentados en las Actas de Escrutinio y Cómputo que se reciben en los Centros de Acopio y Transmisión de Datos.
 - El sistema integra los procesos de captura, validación, transmisión, recepción, consolidación y difusión de los resultados electorales preliminares de las elecciones.
- El sistema apoya las siguientes funciones del CATD.

- Permitir al digitalizador realizar la captura digital de imágenes del acta

- de escrutinio y cómputo por medio de un equipo de captura de imágenes como escáner o multifuncional.
- Permitir al capturista registrar los datos plasmados en el acta de escrutinio y cómputo.
 - Permitir al verificador la revisión de los datos capturados en el sistema para corroborar que los datos coincidan con los datos plasmados en las actas de escrutinio, así como verificar que la imagen de dicha acta capturada corresponda a la casilla, por medio del encabezado del acta.
3. Integridad en el registro de la información.

- Generar una imagen digital a partir del acta en papel, que es una imagen completa y legible para ser almacenada sin alteraciones en su contenido y publicada para su consulta.
- La imagen del acta, así como los datos que en ella están plasmados manualmente, corresponden a la casilla, sección y distrito al que corresponda.
- Los resultados del acta son asociados al partido o coalición en cual se encuentran registrados.

4. Requisitos de desempeño. Validación de la información

- Las actas contabilizadas deben corresponder a alguna de las casillas autorizadas por la autoridad correspondiente, es decir, no se deben contabilizar actas que no existan en el catálogo oficial.
 - El catálogo fue cargado antes para hacer la validación.
5. Contabilización de actas y presentación de los resultados acumulados.

- El sistema acumula los resultados por distrito o entidad.
- Las actas inconsistentes son identificadas y tratadas de acuerdo a los criterios definidos por la autoridad electoral.
- Las actas contabilizadas deben ser las que cumplan con los criterios aprobados por la autoridad electoral.
- Los cálculos numéricos de porcentajes y sumas deben ser exactos, pero no mostraban todos los decimales en la página web.

- En el caso de las coaliciones, muestra los resultados preliminares para cada uno de los partidos que lo integran. Se realizó mediante diferentes combinaciones de captura.

3 METODOLOGÍA Y ANÁLISIS

Para establecer un procedimiento que garantice que las bases de datos no cuenten con información previa antes de su puesta en operación. Lo anterior fue realizado ante presencia de Notario Público y el COTAPREP el Día de la Jornada Electoral.

3.1 Verificación de los programas en el ambiente de producción.

Se tuvo participación como observador al momento de realizar la instalación de los programas. Las partes involucradas en la auditoría verificaron que los programas instalados con los que operará el PREP corresponden a los programas auditados, considerando aspectos como: la arquitectura tecnológica, la ubicación física de los servidores y equipos, la complejidad de instalación, entre otros.

Se verificó que dichos programas se encontraran instalados previo al inicio de operaciones del PREP.

3.2 Verificación de base de datos.

El contenido inicial de la base de datos es fundamental para la operación del sistema informático del PREP.

El día de la jornada electoral, previo a la operación del PREP, se verificó el contenido de dichas tablas, a través de la ejecución de scripts que permitan obtener datos estadísticos útiles entre otros datos que se consideren de valor

para transparentar el contenido inicial de la base de datos. La base de datos, fue verificada por Notario Público en el inicio del funcionamiento del Programa.

3.3 Selección de una opción

Una vez que se han expuesto las condiciones y requerimientos que demanda la auditoría en los sistemas del PRFP, se puede hacer la selección de las herramientas que se usarán para dicho propósito. Debido a que la auditoría hace referencia a la detección de vulnerabilidades en la infraestructura, a la negación de servicio y en caso dado detectar intrusos en la red, con este argumento se ha determinado que Nessus cubre una gran parte de lo que requiere la auditoría, por lo que será el software en el que estará basada la detección de vulnerabilidades y parte de la auditoría.

Para la parte de negación de servicio se ha determinado usar Kali Linux que es una herramienta especializada en este tipo de pruebas.

4 CONCLUSIONES

Si bien los resultados obtenidos fueron de beneficio para el IEF durante el proceso electoral 2015-2016, este documento sólo refleja una parte de la realidad que vivimos ya que los ataques son cada vez más sofisticados. Tomando en consideración los criterios de auditoría señalados, la inspección detallada de programas se enfocó en verificar el cumplimiento de los criterios generales de auditoría, en particular de aquellos criterios que son susceptibles de identificarse.

De manera primordial se determinó que no detectó algún módulo, programa, función, instrucción o variable que altere de manera injustificada la información de las Actas de Escrutinio y Cómputo que pudiera alterar los resultados preliminares.

El análisis se realizó en cada uno de los CATD instalados en los municipios del estado de Aguascalientes, entregando dos informes de las

vulnerabilidades encontradas en la infraestructura tecnológica del PRFP, dando también la información necesaria para hacer los ajustes y con ello elevar la seguridad en la infraestructura y aplicaciones de cada uno de los equipos.

Quedó exento como parte de la revisión el código, la evaluación de aspectos de seguridad (código seguro), disponibilidad, desempeño, el apego a estándares de programación y la optimización de código.

Las pruebas de caja negra mostraron que el programa es funcional para las elecciones de Diputados Locales, Ayuntamientos y Gobernador del Estado de Aguascalientes.

Las pruebas de análisis de vulnerabilidad de la infraestructura mostraron que el sistema mitigó todas las vulnerabilidades.

Durante la jornada electoral se atestiguó el ambiente de operación y se corroboró que el programa se mantuvo transmitiendo de manera constante durante las casi 18 horas de operación. Solamente se solicitó interrumpir, por aproximadamente quince minutos, la operación para que el COTAPREP revisara con los consejeros actas que consideraba ilegibles.

Atentamente

M. en C. Guillermo Vázquez Sánchez
Responsable de la Auditoría

Física Aplicada y Tecnología Avanzada
Director del Centro de



Recibido:
Entregado:
10 - JUNIO - 2016
12:28 HRS.
RAMIRO PÉREZ CAMPOS
Código de Postes
AGUASCALIENTES
ESTUDIO - ESTIM. ELECTORAL

Centro de Física Aplicada y Tecnología Avanzada
Universidad Nacional Autónoma de México

A.P. 1-1010
Querétaro, Qro. 76000, MEXICO

Fax. (01) 55-56 23 41 65
(01) 442-238 11 65

Tels. (01) 55-56 23 41 50
(01) 442-238 11 50