Informe Final

AUDITORIA al Programa de Resultados Electorales Preliminares

del Instituto Electoral del Estado de Queretaro

2015

1. INTRODUCCIÓN

Como resultado de la entrada en vigor de las reformas en materia político electoral, las elecciones locales en el estado de Querétaro se celebraron bajo un nuevo modelo cimentado en un ambiente donde existirá una mayor coordinación entre el Instituto Nacional Electoral (INE) y el Instituto Electoral del Estado de Querétaro (IEEQ), 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, será la autoridad electoral a nivel federal emitió las normas bajo las cuales debió instrumentarse dicho mecanismo.

El instituto electoral de Querétaro, ha utilizado diversos mecanismos para dar a conocer de forma inmediata y oportuna los resultados obtenidos por las fuerzas políticas que participan en cada una de las elecciones. En los años anteriores se requirió de la contratación de empresas con experiencia en el ramo.

Sin embargo a partir del año 2012 el Consejo General de IEEQ consideró viable que el diseño, construcción, implementación y operación del PREP quedara a cargo del propio institúto.

Para ello se consideró apropiado la suscripción de convenios de colaboración con el Centro de Física Aplicada y Tecnología avanzada (CFATA) de la Universidad Nacional Autónoma de México Campus Juriquilla, con el objeto de facilitar la cooperación tecnológica y contar con un informe técnico sobre las aplicaciones del PREP, y poeteriormente para realizar una auditoría informática y conformar un Comité Técnico Asesor.

En este documento se describen las actividades realizadas para dar cumplimiento los lineamientos que señalan como puntos de la auditoría: el Análisis de vulnerabilidades en la infraestructura tecnológica del PREP, incluyendo pruebas de negación de servicio, pruebas de inyección de código malicioso y pruebas de acceso a los diversos recursos del sistema informático. Los informes 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 Auditoria 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, tomando en cuenta los puntos anteriores, se determinó la lista de activos tecnológicos sobre los que se realizarán las pruebas de penetración así como aquellos que serán objeto de la revisión de configuraciones.

Por lo que se decidió realizar cinco secciones:

Sierra Gorda. Que incluye los municipios de Landa de Matamoros, Jalpan de Serra, Arroyo Seco, Pinal de Amoles y Peñamiller.

Semidesierto: Que incluye los municipios de Tolimán, San Joaquín, Cadereyta, Ezequiel Montes, y Colón.

Sur: Que incluye los municipios de Huimilpan, Amealco de Bonfil, San Juan del Río (con dos distritos), Tequisquiapan y Pedro Escobedo.

Zona conurbada: Que incluye los cinco distritos de Querétaro, y los municipios de Corregidora, y El Marqués.

Servidores: Que incluye los servidores Front End, Back End, el Centro Estatal de Computo y las Instalaciones del IEEQ.

2.1.2 Ejecución de pruebas de penetración (pentest) a activos seleccionados.

Se ejecutaron pruebas de seguridad informática de caja negra a los activos de información considerados en el alcance del *pentest*. Las pruebas consisten inicialmente en la ejecución de herramientas informáticas para identificar

potenciales vulnerabilidades y posteriormente en la aplicación de diversas técnicas para intentar explotarlas e identificar el impacto que tienen sobre la infraestructura.

El servicio de pruebas de penetración y análisis de vulnerabilidades para la infraestructura tecnológica tiene como objetivo obtener información relacionada con los activos tecnológicos evaluados, conocer el nivel de exposición de información sensible y documentar los hallazgos.

La primera etapa de las pruebas consisten en la identificación de vulnerabilidades en objetivos específicos, así como en otros que podrían proporcionar acceso a ellos, intentando explotar las vulnerabilidades identificadas para determinar el impacto potencial en caso de que alguna fuera aprovechada por un usuario malintencionado. Entre las vulnerabilidades que tratan de explotarse se encuentran:

- ✓ Errores o huecos de seguridad en el software.
- ✓ Configuraciones débiles o vulnerables.
- ✓ Vulnerabilidades que permiten a un atacante remoto acceder de forma no autorizada a información sensible.
- ✓ Vulnerabilidades que permiten a un atacante remoto modificar de forma no autorizada el contenido o la visualización del mismo en un activo de información.
- ✓ Vulnerabilidades que provoquen afectaciones a la disponibilidad de los recursos de TIC.
- ✓ Modificaciones no autorizadas en el contenido de los repositorios de documentos (bases de datos).

Para las pruebas de penetración se consideraron dos escenarios: pruebas externas y pruebas internas. En las pruebas externas se evalúan los objetivos que pueden ser accedidos desde Internet y se ejecutan a través de este mismo medio desde ubicaciones externas a la organización.

Las pruebas internas incluyen los objetivos que son accesibles sólo desde la red interna y se ejecutan en las instalaciones de la organización.

Para cada una de las vulnerabilidades documentadas y clasificadas por su impacto se hace una recomendación para su mitigación, misma que la entidad electoral administrativa debe evaluar para determinar su viabilidad o establecer otras medidas de mitigación.

2.1.3 Revisión de configuraciones en activos seleccionados.

Consiste en la evaluación de la configuración actual de los sistemas operativos de los dispositivos que conforman la infraestructura, a través de la comparación con buenas prácticas internacionales de seguridad informática. La revisión incluye servidores, consolas de administración de los servicios y servidores, así como dispositivos de telecomunicaciones.

Para la revisión de configuraciones de seguridad, se desarrollaron las siguientes etapas:

- ✓ Generación de listas de verificación para cada sistema operativo que se evaluó, con base en buenas prácticas de seguridad específicas para el mismo, recomendadas por entidades con reconocimiento internacional en materia de seguridad de la información.
- ✓ Muestreo discrecional para la selección de los sistemas a revisar, con base en la función y versión del sistema operativo de los servidores, consolas de administración, y dispositivos de telecomunicaciones.
- ✓ Revisión en sitio del estado actual de la configuración de sistemas operativos con respecto a las listas de verificación generadas.
- ✓ Informe de la revisión de configuraciones, que incluye la documentación de cada rubro verificado, los hallazgos y oportunidades de mejora clasificadas, así como el impacto ponderado.

La revisión de configuraciones se enfoca en el sistema operativo de servidores, consolas y dispositivos, por lo que no consideran servicios y aplicaciones que se ejecuten en los mismos. Los aspectos que se consideran son los siguientes:

Revisión de configuraciones Linux:	**Revisión de configuraciones Windows:**
Sistemas de archivos.	Cifrado de la unidad Bitlocker.
Actualizaciones.	Unidades de datos extraíbles.
Configuración de inicio del sistema.	Revisión de procesos no-maliciosos.
Aplicaciones en ejecución.	Configuración de las actualizaciones.
Firewall de host.	Gestión de comunicación en Internet.
Configuración de bitácoras.	Recursos compartidos sin permisos por defecto.
Cuentas de usuarios.	Procesamiento del inicio de sesión.
Privilegios de usuarios.	Opciones de seguridad locales.
Tareas programadas.	Asignación de permisos de usuarios.
Conexiones remotas.	Directivas de auditoria.
Permisos de archivos de sistema.	Revisión de firewall local.
Archivos o procesos maliciosos.	Gestión de archivos adjuntos.
Parámetros de red.	Actualizaciones aplicadas.
Servicios habilitados.	Existencia y actualización de Software antivirus.

Tabla 1: Revisión de configuración en Windows y Linux

Revisión de configuraciones de dispositivos de telecomunicaciones	
Autenticación.	Reglas de contraseñas.
Configuración de SNMP.	Configuración de reloj y NTP.
Reglas de servicio global.	Privilegios de usuarios.
Reglas de registro.	Reglas de ruteo.
Reglas de acceso.	Autenticación de grupos de trabajo.

Tabla 2: Revisión de configuraciones de dispositivos de telecomunicaciones

2.1.4 Análisis y clasificación de hallazgos de pruebas de penetración y revisión de configuraciones.

Todos los hallazgos y oportunidades de mejora que se obtienen como resultado de la ejecución del *pentest* y de la revisión de configuraciones se analizaron para identificar vulnerabilidades, se clasificaron de acuerdo con el sistema de calificación *Common Vulnerability Scoring System (CVSS-SIG)*, que está diseñado para proporcionar un método estandarizado para calificar vulnerabilidades de Tecnologías de la Información (TI). La clasificación de los hallazgos permite determinar su impacto en la infraestructura y proporciona elementos para definir prioridades para la aplicación de medidas de mitigación de los mismos.

2.1.5 Verificación de medidas de seguridad implementadas con base en los hallazgos.

A partir de los informes de pruebas de penetración y de revisión de configuraciones, se revisaron los hallazgos y las recomendaciones incluidas en los mismos para establecer las medidas de seguridad que se implementaron para mitigar el impacto de cada uno de ellos en la infraestructura de TI.

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 lo activos en las 5 zonas asignadas.

Se informó al IEEQ los resultados de la verificación de hallazgos posterior a la implementación de medidas de mitigación. Se determinó que de forma interna no se presentaba ningún riesgo, pero de forma externa sería necesario contar con la presencia in situ de los administradores de los servidores y los servicios de Backend y Frontend para mitigar los que se presentaran el día de la jornada.

2.2 Limites de la Auditoria

La auditoría del PREP es de carácter técnico y estará 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 considerarón como parte de la auditoría al PREP son las siguientes:

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

b. 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 PREP.

Dentro de la línea de trabajo también se consideran dos puntos importantes para la seguridad del PREP, estos puntos no están considerados inicialmente dentro del proyecto desarrollado pero se agregaron como requisitos de la UNAM.

- ✓ Revisión del código fuente del sistema informático del PREP.
- ✓ Pruebas funcionales de caja negra del sistema informático del PREP.

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:

a. El porcentaje estimado de participación.
b. El porcentaje numérico de avance en el registro de actas recibidas y total de actas.
c. Fecha y hora de recepción del acta en el CATD. Sólo se registra en la BD.
d. Imagen del acta capturada.
e. Identificación de AEC con inconsistencias
f. 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 PREP, se referirá a la información de las Actas de Escrutinio y Cómputo (AEC).

a. 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.
b. El sistema integra los procesos de captura, validación, transmisión, recepción, consolidación y difusión de los resultados electorales preliminares de las elecciones.
c. El sistema apoya las siguientes funciones del CATD.
    - ✓ Permitir al digitalizador que realice 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 toda los decimales en la pagina web.
- ✓ En el caso de las coaliciones, muestra los resultados preliminares para cada uno de los partidos que lo integran. Lo hizo mediante diferentes combinaciones de captura.

2.2.3 Bitácoras y pistas de auditoría.

El sistema informático creó un registro para generar y almacenar bitácoras y pistas de auditoría que faciliten los procesos de verificación, análisis y auditoría de los sistemas.

Los datos proporcionados deberán ser como mínimo, el registro de todos los movimientos de alta, modificación o baja de información de las AEC, indicando al menos: la fecha/hora, el usuario que hizo el movimiento y el tipo de movimiento.

Solo se registró un cambio a partir del día de la entrega del Código Fuente.

3 METODOLOGÍA Y ANÁLISIS

La metodología del Instituto Electoral del Estado de Querétaro propone que sea una metodología para detección de vulnerabilidades en redes, esto debido a que se iniciaron trabajos aún sin la entrega del código fuente para poder garantizar el adecuado funcionamiento del PREP el día de la jornada electoral por lo que fue necesario:

a. Establecer un procedimiento que garantice que los programas binarios o su equivalente que sean usados durante la operación del programa, sean construidos a partir del código fuente auditado, el cual fue elaborado por el Comité Técnico Asesor del PREP.
b. Establecer un procedimiento que garantice que las bases de datos no cuenten con información previa antes de su puesta en operación. El cual fue elaborado por el Comité Técnico Asesor del PREP y realizado ante presencia de Notario Publico el Dia de la Jornada Electoral.

3.1 Compilación y obtención de huella digital de los programas auditados.

- ✓ En el caso de los lenguajes compilados, los programas fuente auditados debieron ser compilados para generar los archivos ejecutables que se utilizaron.
- ✓ De los archivos y programas que resulten de la compilación, o bien de los archivos fuentes en el caso de los lenguajes interpretados, será obtenida una huella digital aplicando una función hash de tipo MD5, lo cual permitirá identificarlos. Se sugiere que en un futuro se utilice SHA-256 por su algoritmo mas robusto
- ✓ De los archivos y programas resultantes de este procedimiento debieron hacerse dos copias de esta información. Una copia de información la resguardó la autoridad electoral administrativa y fue a partir de la cual se instalaron los programas en los servidores de producción; otra copia la resguardó el ente auditor como fuente de cotejo para el procedimiento de verificación.
- ✓ Como resultado de este procedimiento se generó una constancia de hechos por los participantes de ambas partes ante Notario Público

3.2 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 verificarón 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.
- ✓ El procedimiento consideró, el cotejo de las huellas digitales de los archivos.
- ✓ Se verificó que dichos programas se encuentran instalados previo al inicio de operaciones del PREP.

3.3 Verificación de base de datos.

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

- ✓ Durante la auditoría, se identificaron aquellas tablas o catálogos que resultan críticos en el almacenamiento de la información de las AEC y el procesamiento de los resultados preliminares, así como la determinación de los datos válidos que deben ser precargados en éstas.
- ✓ 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. Procedimiento que

determinó el Comité Técnico Asesor del PREP y que fue verificado por Notario Público en el inicio del funcionamiento del Programa.

3.4 SELECCIÓN DE UNA OPCIÓN

Una vez que se han expuesto las condiciones y requerimientos que demanda la auditoria en los sistemas del PREP, 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

El analisis se realizó en cada uno de los 24 CATD instalados en los 18 municipios del estado de Querétaro, entregando tres informes de las vulnerabilidades encontradas en la infraestructura tecnológica del PREP, 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.

Si bien los resultados obtenidos fueron de beneficio para el IEEQ durante el proceso electoral 2014-2015, este documento sólo refleja una parte de la realidad que vivimos ya que los ataques son cada vez más sofisticados.

Bajo la técnica de revisión de código fuente de los programas, éstos no se encuentran en ejecución, sino como inicialmente fueron escritos por los programadores, y cada uno de los archivos que se encuentran en texto plano fue analisado línea por línea.

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 en el código fuente de los programas a través de una revisión estática.

De manera primordial se determinó que no existe 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.

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

Las pruebas de análisis de vulnerabilidad de la infraestructura mostraron que de forma interna, el sistema mitigó todas las vulnerabilidades y que de forma externa, sólo una obligó a generar un mecanismo que diera solución al riesgo en caso de que se presentara.

Durante la jornada electora se atestigüó el ambiente de operación y se corroboró que el programa se mantuvo transmitiendo de manera constante durante las 24 horas de operación.

Palabras clave

Vulnerabilidad: en la seguridad informática, hace referencia a una debilidad en un sistema, permitiendo a un atacante violar las propiedades de la información, como lo es la confidencialidad, integridad, etc. de las aplicaciones o datos del sistema.

Confidencialidad: que la información capturada viaje por la red sin que algún intruso tenga acceso a ella para modificar los datos, es decir, que sólo tengan acceso a dicha información las personas debidamente autorizadas, de tal manera que cuando el archivo sea enviado a su destino no contenga información de más o menos información de la que debería contener.

Disponibilidad: asegurar que la información esté disponible cuando se requiera.

Integridad: garantiza que la información no ha sido modificada por aquellos que no cuentan con los permisos apropiados. Con esta propiedad va relacionada la autenticidad.

Autenticidad: asegura que la información proviene de quien dicen provenir y que por lo tanto no ha sido modificada en su trayectoria.

No repudio: sirve a los emisores y receptores para probar que un mensaje transmitido ha sido recibido por la otra parte de la comunicación, es decir, cuando un mensaje es enviado, el receptor puede probar que el mensaje fue enviado por el emisor y viceversa.

Control de acceso: será establecido con el fin de que un usuario sea identificado y autenticado de manera exitosa para que entonces le sea permitido el acceso a la información.

Hash o función resumen: es la suma total del mensaje codificado.

Cifrado simétrico: es aquel en donde se utiliza una sola llave para cifrar y descifrar la información.

Cifrado asimétrico: conocido como "Criptografía de Llave Pública", es aquella que emplea dos llaves para las funciones de cifrado y descifrado de la información.