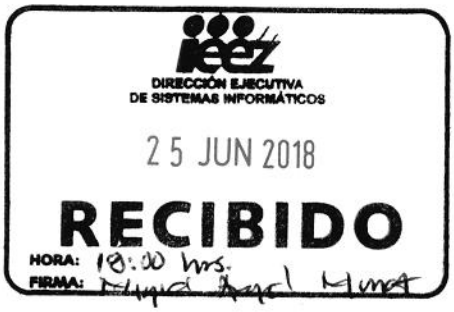
Informe

Auditoria al

Programa de Resultados Electorales Preliminares

Del Instituto Electoral del Estado de Zacatecas

Guadalupe Zacatecas 25 de Junio de 2018



Proceso Electoral 2017-2018

1. Introducción

El 19 de noviembre de 2014, el Consejo General del INE (Instituto Nacional Electoral) en uso de las facultades que la Constitución Política de los Estados Unidos Mexicanos y la Ley General de Instituciones y Procedimientos Electorales le confieren, en sesión extraordinaria emitió el acuerdo mediante el cual fueron aprobados los Lineamientos del Programa de Resultados Electorales Preliminares (LINPREP).

El 07 de septiembre de 2016, el Consejo General del Instituto Nacional Electoral aprobó mediante Acuerdo INE/CG661/2016, el Reglamento de Elecciones del Instituto Nacional Electoral del cual forma parte integral el Anexo 13, relativo a los Lineamientos del Programa de Resultados Electorales Preliminares.

El 22 de noviembre de 2017, el Consejo General del Instituto Nacional Electoral, mediante Acuerdo INE/CG565/2017, aprobó las modificaciones al Reglamento de Elecciones.

El 14 de febrero de 2018, el Consejo General del Instituto Nacional Electoral, mediante Acuerdo INE/CG90/2018, aprobó las modificaciones al Anexo 13 y 18.5 del Reglamento de Elecciones.

El Reglamento de Elecciones y su Anexo 13, relativo a los Lineamientos del Programa de Resultados Electorales Preliminares son de orden público de observancia general y obligatoria, en materia de implementación y operación del Programa de Resultados Electorales Preliminares (PREP), establecen las bases y procedimientos generales a los que deben sujetarse los Organismos Públicos Locales. El artículo 347 del Reglamento de Elecciones establece que se deberá de someter el sistema informático a una auditoria de verificación y análisis, con la finalidad de evaluar la integridad, disponibilidad y seguridad en el procesamiento de la información y la generación de los resultados conforme a la normatividad aplicable vigente.

En estricta observancia al Reglamento de Elecciones y al Anexo 13, relativo a los Lineamientos del Programa de Resultados Electorales Preliminares, el Instituto Electoral del Estado de Zacatecas, con fin de realizar la auditoria a su sistema informático PREP, suscribió convenio específico de colaboración con la Universidad Autónoma de Zacatecas.

En este documento se describen las actividades realizadas para dar cumplimiento a la citada norma que señalan como puntos de la auditoria: Pruebas funcionales de caja negra al sistema informático para evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares; y análisis de vulnerabilidades, considerando al menos pruebas de penetración y revisión de configuraciones a la infraestructura tecnológica del PREP, incluyendo pruebas de denegación 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. Para la ejecución de la auditoria aquí documentada se siguió el plan de Auditoria previamente remitido al Instituto Electoral del Estado de Zacatecas.

2. Auditoria

2.1 Pruebas de Caja Negra

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 Computo (AEC). En el análisis realizado se encuentra lo siguiente:

- 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 (CATD).
- El sistema integra los procesos de captura, validación, transmisión, recepción, consolidación y difusión de los resultados electorales preliminares.
- El sistema permite al digitalizador capturar digitalmente las imágenes de escrutinio y cómputo por medio de un escáner que identifica un código de barras y nombra el archivo automáticamente.
- El sistema permite la digitalización de Actas de Escrutinio y Cómputo de casilla a través de un dispositivo móvil, la cual es procesada en el Centro de Captura y Verificación instalado en oficinas centrales.
- El sistema permite al capturista registrar los datos plasmados en el acta de escrutinio y cómputo, ya sea identificando automáticamente el acta de escrutinio y cómputo o seleccionando directamente en el sistema el tipo de elección, distrito y/o municipio, sección y casilla.
- El sistema permite la distribución de las imágenes de las actas de escrutinio y cómputo a los verificadores disponibles o con menos carga de trabajo.
- El sistema permite al verificador la revisión de los datos capturados en el sistema para corroborar que los datos coincidan con los datos plasmados en la imagen de las actas de escrutinio y cómputo digitalizadas, así como corroborar que la imagen coincida con la elección, sección y casilla correspondiente.
- La imagen del acta, así como los datos que en ella están plasmados manualmente, corresponden a la casilla, sección y distrito al que corresponde.
- Las actas contabilizadas corresponden a alguna de las casillas autorizadas por el Instituto Nacional Electoral (INE), no se contabilizan actas que no existen en el catalogo revisado.
- El sistema cuenta con los catálogos cargados correctamente (partidos políticos, coaliciones, candidatos independientes donde registraron candidato en las dos elecciones, casillas aprobadas por el INE, Distritos y Municipios)
- El sistema permite el ingreso a personal autorizado y le permite acceder solo a las casillas correspondientes a su municipio o distrito.
- El sistema acumula los resultados por municipio, distrito y entidad.
- Las actas inconsistentes son identificadas y tratadas de acuerdo a los criterios definidos en el proceso técnico operativo.
- Los cálculos numéricos de porcentajes y sumas cuenten con el grado de exactitud especificados en los Lineamientos del Programa de Resultados Electorales Preliminares.

- En el caso de coaliciones los resultados se muestran de manera gráfica por partido político, coalición y candidato independiente y por candidato.
- El sistema publica automáticamente los resultados en un sitio web determinado para tal efecto.
- Los datos publicados en el sitio web para difusión a la ciudadanía en general coinciden con los registrados en el sistema de captura.
- Los datos publicados en el Consejo General, a través de graficas, coinciden con los registrados en el sistema de captura.
- El sistema informático crea un registro que facilita los procesos de verificación, análisis, y auditoria de los sistemas.
- El sistema registra todos los movimientos de alta, modificación o baja de información de las Actas de Escrutinio y Cómputo indicando fecha y hora así como que usuario realizo el movimiento y qué tipo de movimiento.
- El sistema publica los datos mínimos obligatorios en el al Anexo 13, relativo a los Lineamientos del Programa de Resultados Electorales Preliminares.

Es importante mencionar que en el procedimiento se establece que a demás de las bitácoras registradas por el sistema se llevarán bitácoras en formatos que requieren de la firma de quien efectúa los cambios.

2.2 Selección de activos para las pruebas y revisión de configuraciones

El primer paso para el análisis de vulnerabilidades de la infraestructura de tecnologías de información es establecer los activos sobre los que se realizarán las pruebas y la revisión de configuraciones.

A partir del listado total de activos a evaluar, se determino la lista sobre los que se realizarán las pruebas de penetración así como aquellos que serán objeto de la revisión de configuraciones.

Activo	Tipo de prueba
Servidor de publicaciones web	Vulnerabilidades y Configuraciones
Servidor de base de datos (centro de datos principal y centro de datos secundario)	Vulnerabilidades y Configuraciones
Servidor web de captura (centro de datos principal y centro de datos secundario)	Vulnerabilidades y Configuraciones

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

Se ejecutaron pruebas de seguridad informática a los activos de información considerados en la tabla anterior. 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 objetivo es conocer, de los activos seleccionados, el nivel de exposición de información sensible y documentar hallazgos.

La primera etapa consistió 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 se trataron de explotar se encuentran las siguientes:

- Errores o huecos de seguridad en el software
- Configuraciones 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 visualización del mismo en un activo de información
- Vulnerabilidades que provoquen afectaciones a la disponibilidad de los recursos TIC
- Modificaciones no autorizadas en el contenido de los repositorios de 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 medio desde ubicaciones externas de la Institución.

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

Para cada una de las vulnerabilidades identificadas se hizo la recomendación correspondiente para su mitigación, misma que la Institución evaluó su viabilidad y/o las medidas de mitigación.

2.4 Revisión de configuraciones en activos seleccionados.

Se realizo revisión en activos seleccionados evaluando la configuración actual de los sistemas operativos de los dispositivos que conforma la infraestructura, a través de la comparación con buenas prácticas de seguridad de informática.

Se verifico cada sistema operativo con base en las buenas prácticas de seguridad.

Revisión en sitio del estado actual de la configuración de sistemas operativos de activos seleccionados en sitio de respaldo.

Revisión a través de escritorio remoto de la configuración de sistemas operativos de activos seleccionados en sitio principal de captura de datos.

Revisión a través de escritorio remoto de la configuración de sistemas operativos de activos seleccionados para sitio de publicación en internet.

- Los aspectos que se consideraron en estas revisiones fueron las siguientes:
- Sistemas de archivos
- Actualizaciones
- Revisión de procesos no maliciosos
- Configuración de actualizaciones
- Recursos compartidos sin permisos por defecto
- Opciones de seguridad locales
- Permisos de usuario
- Firewall local
- Actualizaciones aplicadas
- Existencia de actualización de software antivirus donde se manejen carpetas con archivos subidos por usuario
- Configuración de servidores de bases de datos

2.5 Obtención de huella digital de los programas auditados

Los sistemas auditados, archivos y programas que resulten de la compilación, o bien de los archivos fuentes en el caso de lenguajes interpretados, será obtenida una huella digital aplicando una función hash de tipo SHA3 que permitirá identificarlos.

De los archivos y programas resultantes de este procedimiento se harán dos copias, una la resguardará la autoridad administrativa y la segunda copia la resguardará el ente auditor como fuente de cotejo para realizar un procedimiento de verificación.

Como resultado de este procedimiento se generará una constancia de hechos por los participantes de ambas partes ante notario público.

En caso de ser necesaria una modificación al código de alguno de los sistemas auditados, resultado de identificar algún funcionamiento no esperado deberá ser notificado al ente auditor y actualizar el código tipo hash correspondiente. Dejando debidamente documentado el cambio en la bitácora de cambios correspondientes.

2.6 Verificación de la base de datos

Durante la auditoria se identificaron las bases de datos en donde se efectúa el almacenamiento de la información de las actas de escrutinio y computo.

El día de la Jornada Electoral, previo a la operación del PREP, se verificara el contenido de dichas bases de datos, a través de la ejecución de la herramienta de administración de bases de datos que permita verificar que no se encuentra registrado ningún valor en la base de datos. Procedimiento que será verificado por notario público.

3. Conclusiones

Efectuado el análisis se entrego el presente informe al Instituto Electoral del Estado de Zacatecas, anexando, junto con el plan de trabajo, resultados documentados de las pruebas de caja negra efectuadas al sistema del Programa de Resultados Electorales Preliminares así como las vulnerabilidades encontradas en la infraestructura tecnológica del PREP, dando también la información para hacer los ajustes necesarios.

Tomando en consideración el plan de auditoría establecido, la inspección detallada de programas, la verificación del cumplimiento de los criterios generales de auditoría, incluyendo las pruebas de vulnerabilidad a los activos seleccionados, la revisión de la configuración de los mismos y el seguimiento a la operación del PREP se tiene lo siguiente:

- **Las pruebas de caja negra mostraron que el programa es funcional para las elecciones de Diputados Locales y Ayuntamientos del Estado de Zacatecas.**
- **Se determino que no existe algún modulo, programa, función, instrucción o variable que modifique de manera injustificada la información de las Actas de Escrutinio y Cómputo en los resultados electorales preliminares.**
- **Las pruebas de análisis de vulnerabilidad de la infraestructura mostraron que de forma externa e interna, el sistema mitigo todas las vulnerabilidades y que se subsanaron las observaciones realizadas a la configuración de los activos seleccionados.**
- **El sistema informático incluyendo cada uno de sus módulos opera correctamente.**
- **La infraestructura para captura, digitalización, verificación y publicación opera correctamente.**
- **La infraestructura para la publicación de los Resultados Electorales Preliminares en internet opera correctamente.**

A t e n t a m e n t e

Universidad Autónoma de Zacatecas, 25 de Junio de 2018.

M. en C. Miguel Omar Muñoz Dominguez
Responsable de la Auditoria

Ing. Jesus Alejandro Isais Torres
Personal académico, consultor y/o asesor

Ing. Alfredo González Saldaña
Personal académico, consultor y/o asesor

Ing. Carlos Miles Durón del Villar
Personal académico, consultor y/o asesor

Ing. Juan Luis Campos Barrera
Personal académico, consultor y/o asesor