INFORME EJECUTIVO DEL RESULTADO DEL SEGUIMIENTO DE LA AUDITORÍA AL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES HIDALGO 2024 ELECCIÓN EXTRAORDINARIA PARA SU PUBLICACIÓN EN SITIO.

- Introducción

El presente documento es el Informe Ejecutivo de Seguimiento de la Auditoria al Sistema Informático y a la Infraestructura Tecnológica del Programa de Resultados Electorales Preliminares, donde se muestran los resultados obtenidos de las pruebas realizadas durante este Seguimiento a la integridad en el procesamiento de la información y la generación de resultados preliminares que se utilizará en la elección local, el día de la Jornada Electoral.

Estas pruebas permiten conocer el conjunto de condiciones de entrada que ejerciten todos los requisitos funcionales del Programa de Resultados Electorales Preliminares (PREP). En ellas se ignora la estructura de control, concentrándose en los requisitos funcionales del sistema y ejercitándolos. Es decir, se basa en verificar que los datos de entrada plasmados en las Actas de Escrutinio y Cómputo (AEC) sean los que se reflejan en la publicación, Página Web Pública del PREP.

Simultáneamente al proceso de revisión de configuración de infraestructura y pruebas de penetración de la infraestructura del PREP, se realizó un escaneo de vulnerabilidades.

El acceso a los servicios de internet, ha permitido que más personas puedan obtener información para desarrollar ataques en la web. Esto ha generado amenazas entre las cuales, las cibernéticas, son un factor importante; por está razón es necesario que los datos contenidos en el PREP tengan una validación de disponibilidad.

El Seguimiento a la auditoría también tuvo como objetivo asegurar la correcta y continua disponibilidad del servicio web de los sitios de publicación de resultados del PREP, durante el período de operación.

- Resumen Ejecutivo

Se utilizaron los equipos instalados por la empresa Podernet en el Centro de Acopio y Transmisión de Datos (CATD), y se permitió acceso a los servidores para las pruebas de los módulos de Foliación, Captura, Validación y, de Publicación de Resultados.

Posterior a la revisión de los modelos de entrada y salida, fue necesario supervisar en las oficinas del Centro de Captura y Verificación (CCV), los módulos de Foliación, Captura y Validación.

Las pruebas realizadas consistieron en la ejecución de herramientas informáticas para identificar potenciales vulnerabilidades, posteriormente en la aplicación de diversas técnicas para intentar explotarlas e identificar así el impacto que tienen sobre la infraestructura y determinar el nivel de exposición de información sensible.

Se evaluó la configuración de los sistemas operativos de los dispositivos que conforman la infraestructura, a través de la comparación con buenas prácticas internacionales de seguridad informática.

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

Como parte de la auditoría se dio seguimiento al Pre-Simulacro y Simulacro desarrollados en conjunto con el IEEH y la empresa PoderNet, donde se atestiguó el manejo de las contingencias esperadas.

- Resultados

Se verificó la integridad en el registro de la información por el sistema, es decir: que a partir de un AEC en papel, se genere una imagen digital completa y legible de ésta y sea almacenada sin alteraciones en su contenido y publicada para consulta; **que la imagen digital del AEC, así como sus datos capturados manualmente sean debidamente asociados a la Casilla, Sección y Distrito que corresponda**; que los resultados del AEC capturados sean asociados fielmente al partido, coalición o rubro en el cual se registren.

Se atendieron los hallazgos de manera satisfactoria para la infraestructura, en materia de configuraciones de infraestructura y, las pruebas de penetración determinaron que **la infraestructura es adecuada para operar**.

Las aplicaciones web no pueden modificarse desde fuera de las instalaciones y el personal del PREP no tiene posibilidades de alterar el contenido de las mismas.

Se determinó que los servidores están protegidos adecuadamente.

Los equipos de telecomunicaciones sólo pueden fallar por desconexión física, pero la empresa cuenta con, al menos, una conexión de respaldo en el CATD; asimismo, resistieron

los ataques internos de negación de servicio.

Se revisaron las instalaciones del CCV y en las mismas se encontró que, a pesar de los ataques, las estaciones de trabajo de todo el personal siguieron operando sin problemas.

La página del PREP conservó su continuidad ante el ataque de negación de servicio, y fueron bloqueadas al detectarse.

La página, que se auditó es la misma que en su momento continuó respondiendo adecuadamente ante el tráfico de red, además se realizaron nuevos ataques a bases de datos y aun así, el servicio continuó operando adecuadamente.

Por lo que se considera **adecuado para operar el día de la Jornada Electoral**.

Juriquilla, Querétaro, a 28 de Noviembre de 2024

Atentamente

M en C Guillermo Vázquez Sánchez
Responsable Técnico

VoBo

Dr. José Luis Aragón Vera
Director del Centro de Física
Aplicada y Tecnología Avanzada