INFORME DE EVALUACIÓN DE LA AUDITORÍA AL SISTEMA INFORMÁTICO Y A LA INFRAESTRUCTURA TECNOLÓGICA DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES DEL IEPC

Julio de 2018

INFORME FINAL DE LA AUDITORÍA AL SISTEMA INFORMÁTICO Y A LA INFRAESTRUCTURA TECNOLÓGICA DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES DEL IEPC

De acuerdo con el convenio signado el pasado 27 de febrero entre el Instituto Tecnológico de Durango (ITD) y el Instituto Electoral y de Participación Ciudadana del Estado de Durango (IEPC) por parte de los representantes de ambas instituciones, cuyo objetivo fue llevar a cabo una auditoría al Sistema Informático y a la Infraestructura Tecnológica con la cual se llevó a cabo el proceso de elección estatal el pasado 1 de julio de 2018.

Cumpliendo con lo acordado entre las partes, se lograron garantizar las condiciones técnicas y de seguridad que permitirán un proceso con la transparencia y el buen funcionamiento tanto del sistema informático como de la infraestructura equipo de cómputo y de comunicaciones.

Para dar seguimiento a este convenio y los compromisos adquiridos, se realizaron reuniones de trabajo entre las partes quedando establecidos acuerdos, tiempos, recursos y compromisos para cada una de las cuatro etapas en el proceso de la auditoría.

ETAPAS

1ª. ETAPA. VISITA AL CATD DURANGO Y CATD NOMBRE DE DIOS

2ª. ETAPA. VISITA AL CATD GOMEZ PALACIO Y CATD CIUDAD LERDO

3ª. ETAPA. DENEGACIÓN DE SERVICIO Y VULNERABILIDAD

4ª. ETAPA. GENERACIÓN DE CÓDIGO HASH

1ª. ETAPA. VISITA AL CATD DURANGO Y CATD NOMBRE DE DIOS

La realización de esta visita se hizo el 7 de mayo de 2018 y se llevaron a cabo las siguientes pruebas:

Pruebas funcionales de caja negra al Sistema Informático del PREP,

- módulos de digitalización, captura y validación
- módulo de publicación de resultados

De donde se logró concluir que la ejecución del sistema, así como su comportamiento basado en las pruebas funcionales que se le aplicaron, reconociendo que el comportamiento de éste fue positivo y estable.

Análisis de Vulnerabilidad de la infraestructura tecnológica

Para llevar a cabo esta etapa se realizaron pruebas de penetración a la infraestructura tecnológica y una revisión de las configuraciones de infraestructura.

CATD NOMBRE DE DIOS.

Para este CATD se realizaron 8 recomendaciones, así como el análisis a 2 nodos de la red, con sus correspondientes equipos de cómputo y la conexión a internet.

CATD DURANGO.

Para este CATD se realizaron 11 recomendaciones, así como el análisis a 11 nodos de la red, con sus correspondientes 11 equipos de cómputo y la conexión a internet.

Este primer informe fue entregado a los 17 días del mes de mayo de 2018.

Todas las recomendaciones fueron corregidas por parte del IEPC y el proveedor del servicio, garantizando que al menos, en estos rubros se contara con la infraestructura puesta a punto para el proceso.

2ª. ETAPA. VISITA AL CATD GOMEZ PALACIO Y CATD CIUDAD LERDO

Esta segunda etapa se realizó el 29 de mayo, visitando la región de La Laguna para llevar a cabo 3 tareas:

1. **Evaluación de aplicación móvil y análisis de vulnerabilidad**: Debido al protocolo de comunicación del dispositivo móvil, la captura de información de los datagramas no pudo ser llevada a cabo a través del envenenando el dispositivo, ya que este protocolo evita esto, lo cual es bueno.

2. **Análisis de la vulnerabilidad de la infraestructura tecnológica:**

   CATD GOMÉZ PALACIO

   Se realizaron 6 recomendaciones, se revisaron 6 nodos de red y 6 equipos de cómputo, el acceso a internet y el sistema de respaldo de energía.

CATD LERDO

Se realizaron 6 recomendaciones, se revisaron 2 nodos de red y 2 equipos de cómputo, el acceso a internet y el sistema de respaldo de energía.

Todas las recomendaciones fueron corregidas por parte del IEPC y el proveedor del servicio, garantizando que al menos, en estos rubros se contara con la infraestructura puesta a punto para el proceso.

3. **Análisis de vulnerabilidad del sistema y servidores**

Se realizaron pruebas de penetración y vulnerabilidad por hardware y software, dejando como recomendación, habilitar el balanceador de carga, para evitar la vulnerabilidad a través del modem.

3ª. ETAPA. DENEGACIÓN DE SERVICIO Y VULNERABILIDAD

Esta etapa se realizó el 10 de junio del 2018 y el propósito fue realizar un ataque al sistema del PREP y al sitio web del IEPC, para simular como si fuera el día de la jornada electoral.

El ataque fue coordinado y dirigido durante 4 horas desde diferentes dispositivos geográficamente dispersos para que se realizaran accesos simultáneos con la finalidad de lograr vulnerar ambos sistemas, por medio de técnicas de DDoS (Denegación de Servicios).

Como resultado del ataque, se encontró que el sistema del PREP resistió de manera consistente manteniendo su operación ininterrumpidamente, no siendo el caso para el sitio web del IEPC.

Después de concluir este ejercicio, tanto el IEPC como el proveedor del servicio, trabajaron para corregir y fortalecer la infraestructura que garantizara el funcionamiento ininterrumpido del sitio web del IEPC, con base en la recomendación sugerida por este ente auditor.

El 24 de junio del 2018, se repitió este mismo ejercicio, encontrando que las recomendaciones fueron solventadas de manera efectiva, por lo que ambos sistemas funcionaron de manera satisfactoria, garantizando el correcto funcionamiento para el día de la jornada electoral.

4ª. ETAPA. GENERACIÓN DE CÓDIGO HASH

Esta etapa se llevó a cabo los días 29 de junio, el 1° y el 2 de julio del 2018 con el propósito obtener una huella digital del sistema consistentes en hash del sistema y hash de la

estructura de la base de datos, previo, durante y posterior al día de la elección que garantizara la integridad del sistema PREP.

Obteniendo los mismos resultados en la comparación de las tres huellas digitales obtenidas en tres momentos diferentes, mismos que fueron validados ante notario público.

CONCLUSIONES

Cada una de las etapas están respaldadas con un informe detallado, así como el oficio de entrega del mismo, signado por el ente auditor.

En importante hacer mención de la gran disponibilidad que se encontró por parte del personal del IEPC, así como por la empresa PROISI, para atender las recomendaciones que de manera propositiva siempre se presentaron, con el único propósito de lograr que la jornada electoral se realizara sin contratiempos de índole técnico.

Se hace entrega del este informe en la ciudad de Durango, Dgo. a los 18 días de mes julio de 2018.

AUDITORES

M.C. Sergio Valdez Hernández

M.C. José Antonio Gutiérrez Reyes

M.C. Salvador Ramos Collins

M.T.I. José Roberto López Quiñones

M.T.I. Marco Antonio Rodríguez Zúñiga