Informe Final de la Auditoría al Sistema e Infraestructura Tecnológica del Programa de Resultados Electorales Preliminares en Yucatán

PREP Yucatán 2021

Para dar cumplimiento a los Lineamientos del PREP 2021

Ernesto Guerrero Lara

2/junio/2021

Versión 1.0

Control de Documentación

Control de Configuración

Título:	Informe Final de la Auditoría al Sistema e Infraestructura Tecnológica del PREP en Yucatán
Autor(es):	Ernesto Guerrero Lara, Edwin León Bojórquez, Carlos Mojica Ruiz, Rodrigo Esparza Sánchez, Israel Novelo Zel, Wilberth Pérez Segura, Cristian Moisés Xool Catzin
Fecha:	2 de junio de 2021

Histórico de versiones

Versión	Fecha	Estado	Responsable	Nombre de archivo
1.0	2/junio/2021	A	Ernesto Guerrero	Informe Final Auditoría.docx

Estado: (B)orrador, (R)evisión, (A)probado

Histórico de cambios

Versión	Fecha	Cambios
0.1	2/junio/2021	Ninguna, primera versión borrador

Tabla de contenido

1. Antecedentes

El Instituto Electoral y de Participación Ciudadana de Yucatán (IEPAC) contrató los servicios de la empresa **GRUPO PROISI, S.A. DE C.V.**, para que ésta se haga cargo de brindar los servicios de cómputo, tanto de hardware como de software para llevar a cabo el conteo preliminar de votos de la jornada electoral del 06 de junio de 2021, es decir, montará los Centros de Acopio y Transmisión de Datos CATD en al menos 64 Municipios del Estado de Yucatán, además de montar el Centro de Captura y Verificación (CCV) y poner a disposición de la ciudadanía la información a través de internet.

En el anexo 13 "Lineamientos del Programa de Resultados Electorales Preliminares" del Reglamento de Elecciones emitido por el Instituto Nacional Electoral (INE) en su última modificación aprobada mediante acuerdo INE/CCOE004/2021 de fecha 11 de enero de 2021, en su Capítulo III "De la Auditoría del Sistema Informático" se indica que:

> *La auditoría de verificación y análisis del sistema informático que será utilizado en la implementación y operación del PREP, se deberá realizar 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 normativa aplicable y vigente.*

El IEPAC contrata a LA UADY por medio de su Facultad de Matemáticas para realizar la Auditoría al Sistema Informático y a la Infraestructura Tecnológica del Programa de Resultados Electorales Preliminares PREP, que se llevará a cabo en la jornada electoral del 06 de junio de 2021, de conformidad con lo establecido en los Lineamientos del PREP vigentes, aprobados mediante Acuerdo INE/CG661/2016 del Consejo General del Instituto Nacional Electoral de fecha 7 de septiembre de 2016 y su última modificación aprobada mediante acuerdo INE/CCOE004/2021 de fecha 11 de enero de 2021, para verificar los principios de certeza, legalidad, independencia, imparcialidad, máxima publicidad y objetividad del ejercicio de la función electoral relativa al diseño, operación e implementación del PREP dentro del Estado de Yucatán.

2. De la Auditoría

2.1. Objetivo General

El objetivo del proyecto fue auditar el Sistema Informático e Infraestructura Tecnológica que será utilizado en el PREP durante la jornada electoral del 6 de junio de 2021 en Yucatán 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 normativa aplicable y vigente.

La auditoría consideró las siguientes líneas de trabajo:

1. *Pruebas funcionales de caja negra al sistema informático y a la aplicación móvil del PREP.*
2. *Revisión de las pantallas de publicación del PREP.*
3. *Análisis de vulnerabilidades a la infraestructura tecnológica del PREP.*
4. *Pruebas de volumetría sobre el sitio de publicaciones del PREP y al sitio principal del IEPAC, para validar saturación, bloqueo de cuentas y caída sobre sus sistemas.*

El trabajo de auditoría concluyó el 29 de mayo de 2021 y el alcance de cada una de las líneas de trabajo se describe a continuación.

2.2. Pruebas funcionales de caja negra al Sistema Informático del PREP

Se auditó el sistema informático del PREP, mediante la ejecución de pruebas funcionales de caja negra, para evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares, conforme a lo establecido en el artículo 347, numeral 1, inciso a) del Reglamento de Elecciones.

Las pruebas funcionales consideraron los siguientes aspectos:

1. Analizar el funcionamiento del sistema informático en relación con las fases del proceso técnico operativo aprobado mediante acuerdo C.G.-002/2021 de Consejo General del IEPAC, considerando la digitalización, captura, verificación y publicación de resultados, mediante flujos completos e interacción entre los diversos módulos.
2. Analizar el funcionamiento de la aplicación móvil desarrollada para la digitalización de las Actas desde las casillas, y, en su caso, la captura de datos desde las casillas; mediante flujos completos e interacción entre los diversos módulos y fases del proceso técnico operativo.
3. Verificar el cumplimiento de las especificaciones funcionales y requerimientos contenidos en la documentación técnica y normatividad aplicable proporcionada por el IEPAC.

4. Verificar la correspondencia de la captura de los datos plasmados en las Actas PREP con los presentados en la publicación, mediante los distintos tipos de reportes desplegados por el PREP, considerando datos, imágenes y bases de datos.

Los módulos del sistema informático del PREP sujetos a pruebas funcionales de caja negra fueron los siguientes:

I. Módulo de Digitalización, Captura y Verificación
   - Obtención de la imagen digital del Acta PREP, considerando en este apartado el mecanismo que permita la digitalización.
   - Captura de la información contenida en las Actas PREP.
   - Verificación de la información capturada.

II. Módulo de Publicación de Resultados
   - Revisión de la obtención de los resultados, así como de la emisión de reportes y su despliegue, de acuerdo con la documentación técnica y la normatividad aplicable.

2.3. Revisión de las pantallas de publicación del PREP

Se revisó que el diseño del sitio de publicación del PREP cumpla las especificaciones definidas por el INE para la versión web y la versión móvil, tanto en la interfaz como en la usabilidad, a fin de lograr un mayor nivel de homologación de la información. Las actividades realizadas fueron:

- Revisar que los niveles de agregación de la información desplegada en las pantallas de publicación estén de acuerdo con los tipos de elección de Diputaciones y Ayuntamientos esto conforme a lo establecido en el numeral 30 del Anexo 13 del Reglamento de Elecciones.
- Revisar que las pantallas de publicación contengan los datos mínimos por publicar de acuerdo con lo establecido en el numeral 30, fracciones I a la X del Anexo 13 del Reglamento de Elecciones.
- Verificar que la distribución de los elementos gráficos de la interfaz del usuario esté conforme a las plantillas base proporcionadas por el INE.
- Verificar la funcionalidad de los elementos gráficos.
- Verificar los cálculos presentados en las tablas y gráficas y su correspondencia con los datos contenidos en las bases de datos.
- Revisar los elementos emergentes.
- Revisar el contenido del Centro de Ayuda.

2.4. Análisis de Vulnerabilidades a la Infraestructura Tecnológica

El alcance de esta línea de trabajo fue:

- Identificar debilidades de seguridad en la infraestructura tecnológica mediante la ejecución de pruebas de penetración y revisión de configuraciones de seguridad.

- Clasificar el impacto y documentar las vulnerabilidades identificadas con el propósito de recomendar al IEPAC y al PROVEEDOR las posibles medidas para la mitigación de las vulnerabilidades que previamente fueron identificadas y documentadas.
- Verificar que las medidas implementadas por el PROVEEDOR hayan atendido adecuadamente las vulnerabilidades reportadas.
- Se verificaron los siguientes componentes: Servidor para la Recepción, Captura y Verificación de Actas, Servidor para la Publicación de Resultados, Sistema de Digitalización PREP Tradicional, Sistema de Digitalización PREP Casilla, Sistema de Captura PREP, Sistema de Verificación PREP, Sistema de Publicación PREP, dos Centros de Captura y Verificación (CCV) implementados en Mérida y los siguientes ocho Centros de Acopio y Transmisión de Datos (CATD): Mérida, Progreso, Umán, Valladolid, Tizimín, Ticul, Tekax y Kanasín.

Esta línea se subdivide en dos sublíneas: pruebas de penetración y revisión de las configuraciones, las cuales se detallan a continuación:

2.4.1. Pruebas de Penetración

Se ejecutaron pruebas de penetración desde el interior y exterior de la red relacionada con la operación del PREP hacia los sistemas, servidores y dispositivos que conforman la infraestructura tecnológica del PREP con base en estándares y mejores prácticas de seguridad de la información como Application Security Verification Standard (ASVS), la Testing Guide de la OWASP y el Critical Security Controls (CSC) del Center for Internet Security (CIS), para identificar vulnerabilidades y emitir recomendaciones orientadas al fortalecimiento de ésta.

2.4.2. Revisión de Configuraciones

Se analizaron las configuraciones de los dispositivos que conforman la infraestructura tecnológica con base en mejores prácticas de seguridad informática para identificar oportunidades y emitir recomendaciones orientadas al fortalecimiento de ésta.

Las revisiones de configuraciones de seguridad de la infraestructura estuvieron basadas en guías de buenas prácticas.

2.5. Pruebas de denegación de servicio al sitio de publicación del PREP y al sitio principal del IEPAC

El alcance de esta línea de trabajo fue realizar ataques de denegación de servicio que permitieran identificar y evaluar la correcta operación y continua disponibilidad del servicio Web de los sitios de publicación de resultados del PREP y del sitio principal del IEPAC, durante la operación del PREP, así como documentar los hallazgos detectados durante la realización de las pruebas.

Se generó tráfico de red hacia el sitio de publicación de resultados del PREP (de los simulacros) y al sitio principal del IEPAC. Las pruebas de denegación de servicio se realizaron de manera concurrente y fueron de dos tipos:

- Tráfico no malintencionado que consiste en transacciones sintéticas que simulen el tráfico legítimo que se espera el día de la jornada.
- Tráfico de red malintencionado, consistente en paquetes de red malformados con las siguientes características:
  - Ataques volumétricos por protocolo TCP
    - Al menos de 400 Mbps de throughput
    - Al menos realizar SYN FLOOD
  - Ataques volumétricos por protocolo UDP
    - Al menos de 400 Mbps de throughput
    - Al menos realizar UDP FLOOD
  - Ataques volumétricos por protocolo ICMP
    - Al menos de 400 Mbps de throughput
    - Al menos realizar ICMP FLOOD
  - Ataques en la capa de aplicación (HTTP)
    - Al menos realizar SLOWLORIS ATTACK

2.6. Fuera del alcance

Las siguientes actividades relacionadas con la línea de trabajo *Análisis de Vulnerabilidades a la Infraestructura Tecnológica* quedaron fuera del alcance debido a que no se contó con el acceso a los equipos de telecomunicaciones, insumos requeridos o autorización para ejecutar alguna herramienta de auditoría.

Elementos	Fuera de Alcance
CCVs y CATDs	1. Análisis de eficiencia del Equipo Switch y Ruteador. 2. Verificación de posibles errores en la transmisión de datos en la red LAN y hacia Internet. 3. Verificación de planta de emergencia. 4. Verificación de redundancia en servicio de Internet (únicamente no se pudo en CATD).
Servidores	5. Pruebas de penetración y revisión de configuraciones de tipo caja gris o blanca en el Servidor para la Recepción, Captura y Verificación de Actas. 6. Pruebas de penetración y revisión de configuraciones de tipo caja gris o blanca en el Servidor para la Publicación de Resultados.

	7. Pruebas de penetración y revisión de configuraciones a servidores internos o intermedios a alguno a estos servicios, como, por ejemplo, servidor de base de datos o generador de contenido mencionados en la arquitectura del sistema.
Sistemas	8. Pruebas de penetración y revisión de configuraciones de tipo caja gris o blanca en el Sistema de Digitalización PREP Tradicional. 9. Pruebas de penetración y revisión de configuraciones de tipo caja gris o blanca en el Sistema de Digitalización PREP Casilla. 10. Pruebas de penetración y revisión de configuraciones de tipo caja gris o blanca en el Sistema de Captura PREP. 11. Pruebas de penetración y revisión de configuraciones de tipo caja gris o blanca en el Sistema de Verificación PREP. 12. Pruebas de penetración y revisión de configuraciones de tipo caja gris o blanca en el Sistema de Publicación PREP. 13. Pruebas de penetración y revisión de configuraciones a sistemas diferentes a los mencionados dentro del alcance, como sistemas administrativos para la creación de usuarios o reinicio de contraseñas, actualización de datos en la base de datos, sistemas de respaldo o monitoreo, por mencionar algunos.

3. Resultados

Al concluir los trabajos de Auditoría, con fecha 29 de mayo de 2021, se tienen los siguientes resultados.

3.1. Pruebas funcionales de caja negra al Sistema Informático del PREP

Los resultados son los siguientes:

1. Aplicación móvil para digitalización PREP Casilla, se considera aprobada en cuanto a la funcionalidad descrita en los casos de uso del aplicativo proporcionados por PROISI.
2. Aplicación de Digitalización y Transmisión PREP, se considera aprobada en cuanto a la funcionalidad descrita en los casos de uso del aplicativo proporcionados por PROISI.
3. Aplicación de Captura PREP, 1ª, 2ª y 3ª captura, se presenta un conjunto de defectos en el manejo de la inconsistencia "Excede Lista Nominal"
4. Aplicación para verificación, se presenta un conjunto de defectos en el manejo de la inconsistencia "Excede Lista Nominal"
5. Módulo de Publicación de Resultados, existen porcentajes por candidatura en los que el decimal de la cuarta posición no está truncado, por lo que no cumplen con lo establecido en el Capítulo II del Anexo 13 del Reglamento de Elecciones.
6. Módulo de Publicación de Resultados, existen porcentajes de participación ciudadana por Acta en los que el decimal de la cuarta posición no está truncado, por lo que no cumplen con lo establecido en el Capítulo II del Anexo 13 del Reglamento de Elecciones.
7. Módulo de Publicación de Resultados, el total de votos calculado por Partido Político y Candidatura Independiente no cumple con lo establecido en la Guía de Apoyo para la Distribución de Votos, debido a que en los partidos políticos participantes en candidaturas comunes la distribución de la fracción sobrante de votos (después la distribución igualitaria de votos) no está siendo asignada correctamente.
8. Módulo de Publicación de Resultados, los votos asentados en Actas PREP con la inconsistencia "Excede Lista Nominal" no son almacenados para su publicación en el sitio PREP y en la base de datos.

3.2. Revisión de las pantallas de publicación del PREP

Las pantallas de publicación del Programa de Resultados Electorales Preliminares cumplen con las especificaciones indicadas por el Instituto Nacional Electoral, a excepción de lo siguiente:

a) No está habilitado el hipervínculo al Centro de Ayuda de la palabra *Actas* en el apartado Estadística Entidad.
b) No está habilitado el hipervínculo al Centro de Ayuda en el texto *Participación ciudadana con base en la Lista Nominal de las Actas PREP Contabilizadas* en el apartado Estadística de Casillas.
c) Algunos nombres de etiquetas son incorrectos según el prototipo proporcionado por el INE.
d) En algunas pantallas, la gráfica de porcentaje de participación ciudadana por casilla no sigue las características de tipografía mostradas en las plantillas para los sitios de publicación PREP.
e) En algunas pantallas, en el menú migas de pan, el formato de la sección no tiene 4 dígitos.
f) Al seleccionar un partido con el botón *Ver detalle*, y luego presionar el botón *Agregar*, en la ventana que se despliega se muestra un botón con la etiqueta que dice "Cancelar" y debe ser "Agregar" según la normativa. El ente auditor considera que esta especificación podría mantenerse, ya que la forma de agregar partidos políticos es a través del botón "+" y no del botón "Agregar".

3.3. Análisis de Vulnerabilidades a la Infraestructura Tecnológica

Con respecto a las pruebas de penetración que se realizaron se tienen las siguientes fortalezas en los aplicativos y los servidores:

a. Las aplicaciones de Publicación de Resultados PREP y PREP Casilla cuentan con las correctas medidas de seguridad contempladas por el estándar de seguridad Application Security Verification Standard (ASVS) de la OWASP.
b. Las configuraciones y medidas de seguridad del Servidor de Recepción, Captura y Verificación, así como el Servidor de Publicación de resultados se encuentran robustas y altamente confiables.
c. Cuenta con un proceso de cifrado seguro entre las aplicaciones de escritorio Digitalización PREP Tradicional, Digitalización PREP Casilla, Captura PREP y Verificación PREP hacia el servidor de Recepción, Captura y Verificación de actas.

Con respecto a la revisión de configuraciones que se realizaron a la infraestructura tecnológica habilitada en los dos CCVs y ocho CATDs se tiene la siguiente fortaleza en los equipos de telecomunicaciones y las estaciones de trabajo:

a. La conectividad interna de las estaciones de trabajo hacia los equipos de telecomunicaciones principales de los CCV y CATD visitados presentan tiempos de respuesta adecuados.

b. Mejoró la seguridad de las estaciones de trabajo de los CCV y CATD con la aplicación de medidas de seguridad para la gestión y control de aplicativos que requieran ser instalados en el sistema operativo.

De acuerdo con el análisis de vulnerabilidades a la infraestructura tecnológica, se concluye que el sistema PREP se ha fortalecido atendiendo algunas recomendaciones realizadas por el ente auditor, sin embargo, presenta algunos riesgos que, aunque la posibilidad de que se materialicen es baja, pueden ser mitigados a través de buenas prácticas, contribuyendo con ello al aumento de la seguridad y correcta operación de los sistemas e infraestructura tecnológica del PREP.

3.4. Pruebas de denegación de servicio al sitio de Publicación del PREP y al sitio principal del IEPAC

Con respecto a las pruebas de denegación de servicio realizadas al sitio de Publicación del PREP y al sitio principal del IEPAC se concluye que ambos tienen los mecanismos de defensa necesarios para mitigar un ataque de este tipo en caso de que este se presente.

4. Recomendaciones

Con respecto a la línea de trabajo *Pruebas funcionales de caja negra al sistema informático y a la aplicación móvil del PREP* y la línea de trabajo *Revisión de las pantallas de publicación del PREP* se recomienda atender las observaciones señaladas para cumplir con los lineamientos del INE.

Con respecto a la línea de trabajo *Análisis de Vulnerabilidades a la Infraestructura Tecnológica* se recomienda aplicar en todo momento las buenas prácticas de seguridad como el Critical Security Controls o el Application Security Verification Standard, tanto en las configuraciones de servidores, infraestructura de red, equipos de trabajo y aplicativos para aumentar la seguridad y correcta operación de los sistemas e infraestructura tecnológica del PREP.

FIRMAS DE APROBACIÓN

Ing. José Gustavo Alberto Sánchez Cruz
Director de Tecnologías de Información
IEPAC

MC Ernesto Antonio Guerrero Lara
Coordinador del Proyecto
Facultad de Matemáticas - UADY