INFORME FINAL DE AUDITORÍA DEL SISTEMA INFORMATICO DEL PREP PARA LAS ELECCIONES EN EL EDO DE CAMPECHE 2018

Contenido

1. RESUMEN EJECUTIVO

El Instituto Tecnológico Superior de Calkiní (ITESCAM) en el estado de Campeche en el mes de febrero de 2018 recibió la invitación del Instituto Electoral del Estado de Campeche (IEEC) a través del comité técnico asesor del programa de resultados electorales preliminares (PREP), para realizar la auditoría del software que se utilizará en la jornada electoral del 1 de Julio de 2018 de las elecciones a Presidentes Municipales y Diputados locales y juntas municipales del Estado de Campeche.

Para dar cumplimiento a las normas y leyes vigentes de acuerdo con los Lineamientos del Resultados Electorales Preliminares (L.R.E.P.) emitidos por el Instituto Nacional Electoral (I.N.E.) y dar cumplimiento al artículo 33, el ITESCAM, trabajó en una Auditoria de Software al PREP desarrollando una revisión de auditoria de caja negra y blanca, que consiste en revisar la funcionalidad general del programa, inspección visual del código fuente e identificación de la trazabilidad del flujo en el programa para descartar el uso indebido de código que pueda realizar operaciones no reconocidas en el proceso electoral. El Trabajo de auditoria está basado en el estándar IEEE Standard for Software Reviews and Audits IEEE Std 1028™-2008 [1]

El ITESCAM participó en el desarrollo de la auditoria de software del PREP proporcionado por la empresa GRUPO PROISI S.A. de C.V. misma que fue convocada en base a la licitación número IEEC-LPN-O1-2017 del IEEC, así como el resultado de la licitación para la empresa, donde se dictaminó a la empresa responsable del PREP [2], misma que en fecha 14 de marzo durante sesión del comité técnico se realizó la entrega de la documentación ante notario a los funcionarios del ITESCAM para llevar acabo la auditoria al Programa PREP.

El alcance del PREP es un mecanismo de información electoral que recaba los resultados preliminares y no definitivos, de carácter estrictamente informativo a través de la captura de los datos asentados en las Actas de Escrutinio y Cómputo (AEC) de las casillas que se reciben en los Centros de Acopio y Transmisión de Datos (CATD) autorizados por el Instituto Electoral del Estado de Campeche (IEEC) en el ámbito de su competencia". [3]

El equipo auditor del ITESCAM al concluir la auditoría de software determinó que el flujo del aplicativo del programa de resultados electorales preliminares mantiene los lineamientos que solicita como mínimos el instituto nacional electoral para operar el día de la jornada electoral para el estado de Campeche. Se

realizaron pruebas de calidad a los aplicativos y al flujo de funcionamiento del sistema informático que generaron observaciones que estuvieron sujetas a consideración del IEEC para solventarlas.

Se realizó un análisis a la infraestructura tecnológica de publicación del sistema PREP en el que se determinó suficiente para los lineamientos solicitados por el Instituto Nacional Electoral(INE).

2. INTRODUCCIÓN

Con base al estándar IEEE Standard for Software Reviews and Audits de la IEEC se definió:

OBJETIVO DE LA AUDITORIA.

El objetivo general de la auditoría es revisar el proceso de aplicación de los sistemas informáticos de apoyo para la jornada electoral del Instituto Electoral del estado de Campeche y generar un informe imparcial que sirva para la mejora de dicho proceso.

ALCANCES DE LA AUDITORIA:

De acuerdo con las líneas de trabajo definidas por el Instituto electoral del estado de Campeche y para dar cumplimento al artículo 347, numeral 1, inciso a) del Reglamento de Elecciones el alcance de la auditoría aplicará para los módulos y las bases de datos del sistema informático del PREP, PREP CASILLA a utilizarse en las elecciones del 1ro de Julio de 2018 como se describe a continuación:

A. Pruebas funcionales de caja negra al sistema informático del PREP.

a. Se validará el proceso técnico operativo de los siguientes módulos:

i. Módulo de Digitalización, Captura y Validación que inicia con la obtención de la imagen digital del acta, captura de la información contenida en las Actas PREP y finaliza con la validación de la información capturada.

ii. Módulo de Publicación de Resultados que consiste en la 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 por el INE.

Las actividades de validación se realizan de acuerdo con el flujo completo establecido e interacción entre los diversos módulos identificando posibles alteraciones al proceso.

b. Se validará el cumplimiento de las especificaciones funcionales y requerimientos del sistema de acuerdo con la documentación técnica y la normatividad, inspeccionando el código en la búsqueda de posibles rutinas y/o código malicioso que pudiera alterar el resultado el día de las elecciones.

c. Se validará la correspondencia de los datos capturados 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.

B. Validación del sistema informático del PREP y de sus bases de datos.

a. Se verificará que los programas auditados se encuentren operando desde el inicio y hasta el cierre de operación del sistema informático PREP, así como que la base de datos se encuentre debidamente inicializada de acuerdo con el diagrama de flujo acordado conjuntamente entre el IEEC y el ITESCAM.

b. Se generarán y validará las huellas criptográficas utilizando el algoritmo SHA-256 del software PREP auditado contra los códigos generados del sistema instalado en el ambiente de producción que operará el día de la jornada electoral.

C. Pruebas a la infraestructura de los sistemas informáticos.

RESPONSABILIDADES DEL EQUIPO AUDITOR: Desarrollar la auditoria de Software del PREP para determinar la funcionalidad de este, así la inspección visual del código fuente para descartar algoritmos, módulos, rutinas o código que altere el resultado del conteo de los votos. Con el propósito de recoger, agrupar y evaluar evidencias para determinar si el sistema informático salvaguarda los activos, mantiene la integridad de los datos y lleva acabo eficazmente el proceso del PREP [10]

a) Auditoría de software al Sistema del Programa de Resultados Electorales Preliminares 2018, en adelante "PREP 2018", que en lo sucesivo se denominará "Auditoría de Software".

PARTICIPAR COMO OBSERVADORES EN LOS SIMULACROS

b) Participación del equipo de auditoría de Software como observadores en la Auditoría en materia de seguridad informática a la infraestructura de la Red del INSTITUTO ELECTORAL DEL ESTADO DE CAMPECHE “IEEC” y del "PREP 2018", así como monitoreo durante la jornada electoral del 1 de julio de 2018.

ENTRADA.

- Se requiere la versión final del programa de resultados electorales preliminares (PREP) desarrollada por la empresa Grupo PROISI S.A. de C.V.
- Documentación de la funcionalidad General del PREP y elementos que lo componen mismo que se definen por:
    - MÓDULO DIGITALIZACIÓN Y CAPTURA: donde se escaneará las actas de escrutinio y se realizará el montaje de Centros de acopio y Transmisión de datos

- MÓDULO DE VALIDACION. Que contiene la validación en dos momentos, Validador 1 y Validador 2, que verifican los datos capturados en el módulo de digitalización y captura.
- MÓDULO ADMINISTRACIÓN. Que considera la manipulación de la base de datos, inicialización de la jornada electoral y creación de usuarios y contraseñas.
- MÓDULO PUBLICACIÓN: Incluye la publicación de resultados, estadísticas en el entorno web para el público.

- Catálogo de documentos electorales, como son distritos, casillas, partidos políticos, candidatos, puestos.
- Código fuente del programa. No fue proporcionado por la empresa.

CRITERIOS DE INGRESO:

La empresa Grupo PROISI S.A. de C.V. autoriza al equipo auditor para realizar pruebas de caja negra de los módulos del programa de los que está compuesto el PREP, así como proporcionar todo el equipo necesario para el desarrollo de las pruebas funcionales para determinar el funcionamiento e integridad del programa. Aunque se requirió a la empresa el acceso al código fuente, solo se tuvo acceso remoto visual a los procedimientos de base de datos en donde se realizan los cómputos. En el ANEXO 1 se pueden observar los criterios de evaluación sobre los que se generaron las pruebas realizadas.

INICIO DEL PROCESO DE TRABAJO Y CRONOGRAMA DE ACTIVIDADES.

El día 15 de marzo se trabajó en la agenda de revisión de la funcionalidad del PREP misma que se desarrolló de acuerdo con la siguiente calendarización:

A. Del 22 de marzo al 18 de Abril revisión general de la funcionalidad de los módulos del PREP para identificar el flujo de funcionamiento de las clases del programa.
B. 23 y 26 de Abril, Realización de la documentación de los informes parciales por parte del Equipo Auditor.
C. 27 y 28 de Abril Revisión del Sistema Gestor de Base de datos y modelo de Base de datos desarrollado para la verificación y validación de los elementos a almacenar de forma permanente. Para determinar que las bases de datos no cuenten con información previa antes de su puesta en operación [5]

D. 29 y 30 de abril: Realización del Documento del Primer Informe de Auditoria

PROCEDIMIENTO DE LA REVISION E INSPECCIÓN.

A) Modelo

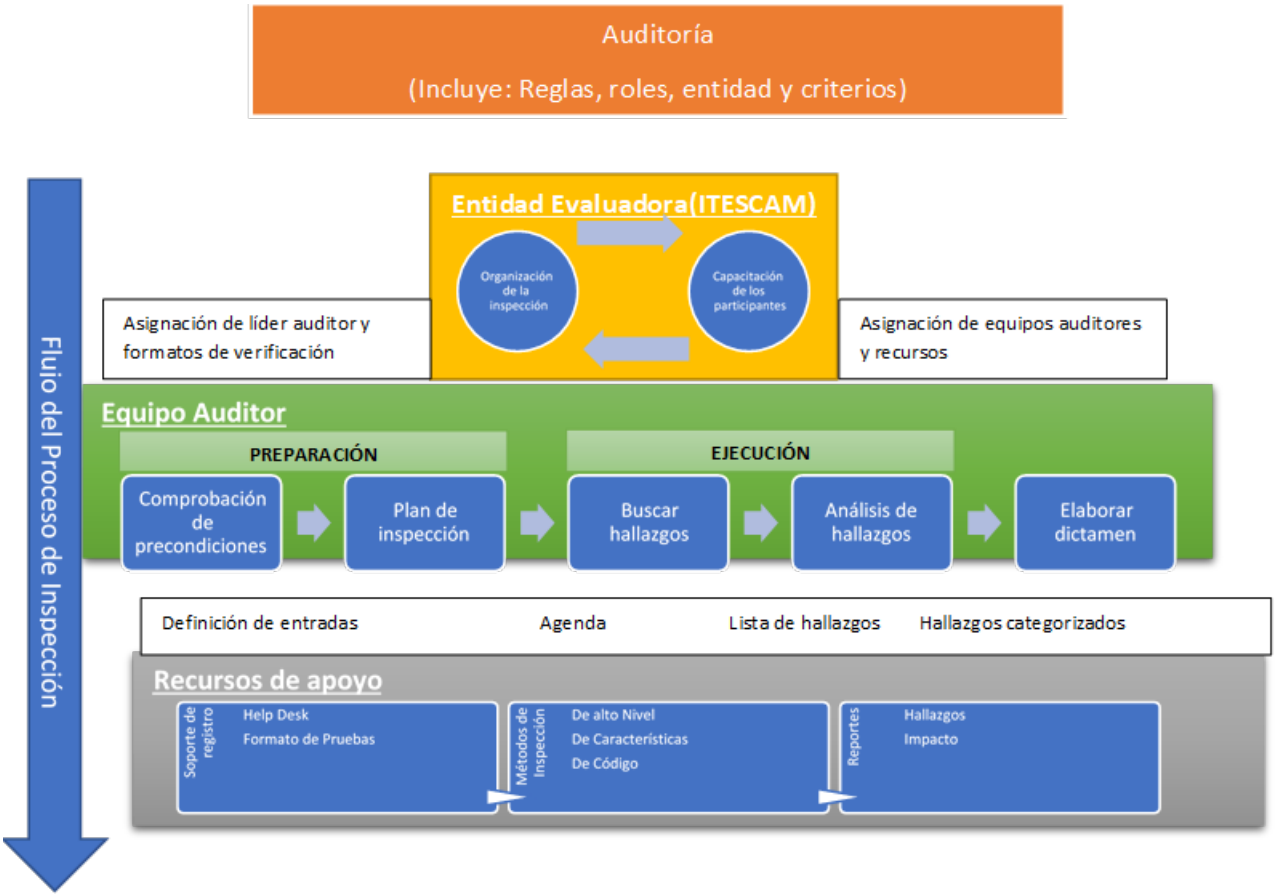


Figura 1 Modelo de flujo de actividades de auditoría

Para llevar a cabo el proceso de auditoría se ha planteado un modelo del proceso que engloba a los responsables y actividades que se llevarán a cabo durante el desarrollo de ésta. A continuación, se describe el modelo presentado en la Figura 1. La Entidad Evaluadora es la encargada de organizar la auditoría, determinar los roles de los participantes, y monitorear el cumplimento de los planes. Antes de iniciar se definen los formatos de acuerdo con los métodos de inspección que se utilizarán. Por último, se definen los equipos auditores considerando los roles y se capacitan para llevar a cabo las actividades.

Es responsabilidad del equipo auditor llevar a cabo las actividades de la auditoría y a través del auditor líder planear una agenda, darle seguimiento y generar un dictamen con los hallazgos encontrados y clasificados de acuerdo con su impacto.

Para la realización de la auditoría el modelo propone el uso de un conjunto de Recursos de Apoyo a través de aplicaciones de Help Desk para la comunicación de los hallazgos con el cliente y un Plan de pruebas para el proceso auditado, la definición de los métodos de inspección y un grupo de reportes que permitan monitorear los hallazgos durante y al final del proceso. Como se mencionó antes, el equipo auditor es el responsable de llevar a cabo las actividades propias de la auditoría, es por ello que se considera importante describir dichas actividades y para lo que se planteó un modelo a bloques que se detalla en la Figura 2. Ahí se pueden observar las tres fases que componen el proceso de auditoría: Preparación, ejecución y dictamen.

Durante la preparación es necesario tener un primer contacto con el ente a auditar para ello se agenda una visita preliminar cuyo propósito es el de conocer de manera general los aspectos del sistema que se va a auditar. En base a la visita se procede a generar la planeación de la auditoría para dar cumplimiento a los lineamientos de auditoría de verificación y análisis del sistema informático indicados en el anexo 13 capítulo III referente a la auditoría del sistema informático del reglamento de elecciones. En este punto se identifican los miembros que conformarán el equipo auditor, las actividades, fechas, horarios y responsabilidades necesarias para llevarla a cabo. Posteriormente se inicia la preparación de la auditoría durante la que, el Líder de auditoría elabora las listas de la documentación, las reglas, los estándares, programa reuniones con el equipo auditor, da instrucciones a los miembros del equipo, del material a ser asignado y asigna roles a cada integrante. Igualmente, cada miembro del equipo tendrá la tarea de estudiar el material y prepararse para desempeñar un papel satisfactorio. De acuerdo con la documentación presentada por las empresas, cada integrante tendrá asignado un conjunto de casos de uso del sistema, con lo que construirá un banco de pruebas a aplicar que permitan verificar la funcionalidad del aplicativo de acuerdo con lo establecido en las especificaciones. Se debe realizar una reunión donde cada participante entienda su función como parte del equipo y se acuerden los compromisos de entrega de sus reportes de actividad.

Durante la ejecución se deben realizar las acciones programadas, aplicando los instrumentos y herramientas identificando desviaciones a la funcionalidad establecida y registrándola en el Help Desk instalado para este propósito. Existen distintos métodos de inspección para un desarrollo completo o para un atributo de calidad [3], durante esta etapa se aplican tres métodos de inspección: a) de alto nivel: que utiliza los requisitos de software, las especificaciones de la interfaz y sobre estos realiza la inspección, b) de código: dirigida fundamentalmente a encontrar rutinas de código que puedan alterar la funcionalidad del producto de software. c) de características: que buscan analizar el conjunto de características determinadas del producto de acuerdo con los escenarios proporcionados por los usuarios, con la finalidad de obtener hallazgos

relacionados al uso de productos de software. Una vez que han sido revisados los sistemas y registrado los hallazgos en el HelpDesk se procede a realizar un análisis para asignarles su impacto y darle un seguimiento al estatus. Previamente antes del dictamen se realiza una reunión con el equipo auditor para identificar posibles situaciones no ligadas directamente al producto de software auditado pero que se pudieran dar durante la ejecución de la auditoría y que no tengan registro en el sistema. Con toda la información se realiza un resumen de los hallazgos de acuerdo con su impacto, se describen los mecanismos de seguimiento y se elabora los informes (Parciales y finales) según corresponda.

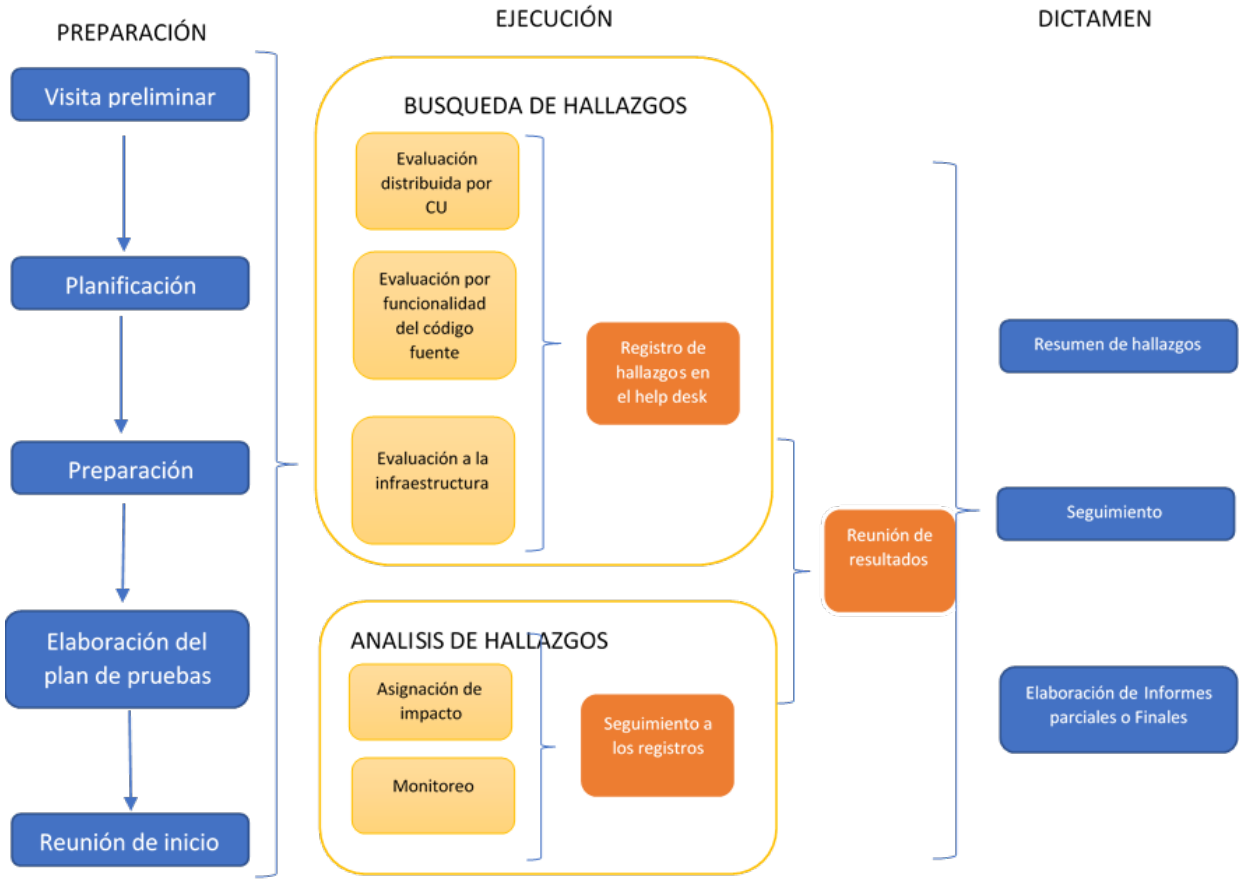


Figura 2. Modelo de desarrollo de actividades de la auditoría

3. PLAN DE AUDITORÍA

El plan de auditoría está dividido en tres partes: actividades de evaluación que van desde el 15 de marzo hasta el 30 de abril de 2018; actividades de simulacro comprendidos del 10 al 24 de junio y; actividades de la jornada electoral y poselectoral, del 1º al 15 de julio de 2018 como puede observarse en la Figura 3.

Figura 3. Plan de actividades

4. RESULTADOS

4.1. REVISIÓN DE MÓDULOS Y DE LA BASE DE DATOS

La auditoría del Sistema PREP 2018 consistió en una revisión de todos los módulos que lo componen, a través de la inspección a cada uno de sus procedimientos, con la finalidad de evaluar su estructura y lógica interna en relación con el tratamiento de la información. Se realizaron las pruebas funcionales de caja Negra y de caja Blanca por parte de la empresa Grupo PROISI S.A de C.V.

En dicha revisión se realizaron 84 pruebas correspondientes a los módulos de digitalización y captura, validación y publicación de resultados de las que se obtuvieron 26 observaciones distribuidas como se presentan en la Figura 4, sin embargo, no se levantaron incidencias sobre los módulos de control y administración de usuarios, monitoreo y control de capturistas, consulta de bitácoras y estadísticas de rendimiento de digitalizadores y capturistas por no estar disponibles.

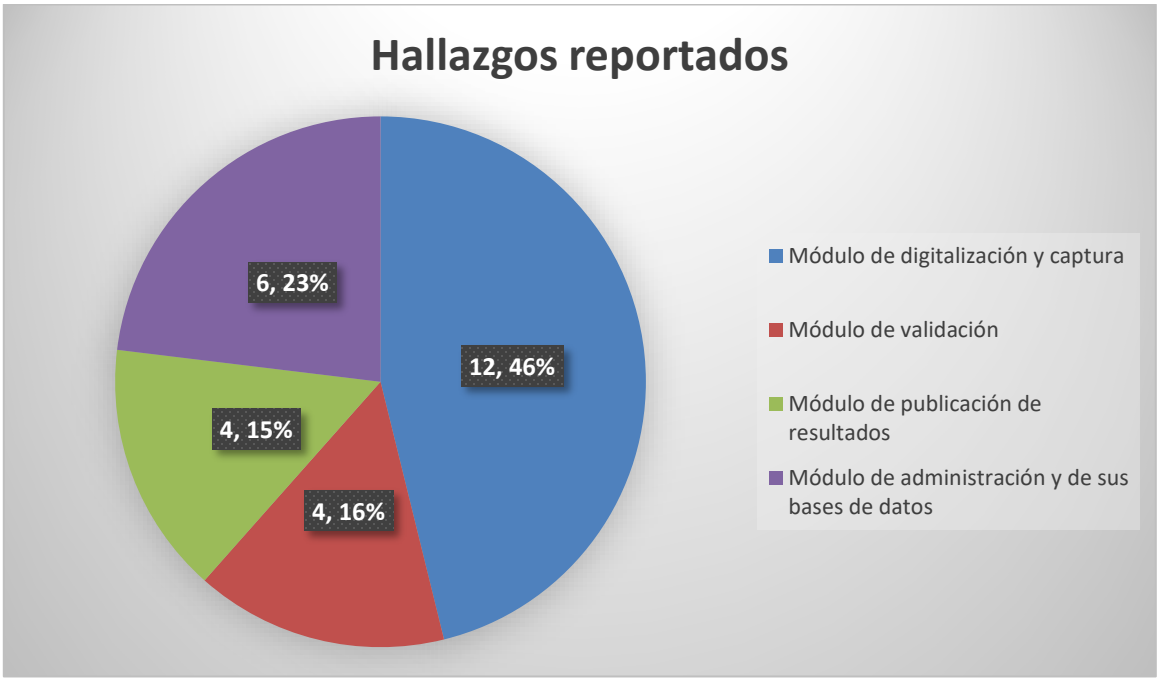


Figura 4. Hallazgos en los módulos del PREP Campeche

Todos estos hallazgos fueron clasificados de acuerdo con su nivel de impacto y enviados para su atención al IEEC.

a) Alto impacto. Afecta gravemente las características del software, la integridad de la información y/o la finalidad del PREP, lo que podría poner en riesgo el funcionamiento del sistema y/o la confiablidad.
b) Medio impacto. Afecta características importantes del software, sin poner el riesgo el funcionamiento del sistema del PREP 2018.
c) Bajo impacto. Afecta características que disminuyen la calidad global del software, pero no afectan su funcionamiento u operación.

Figura 5. Hallazgos clasificados por nivel de impacto.

Las pruebas funcionales de caja negra permitieron verificar que el sistema informático del PREP captura, transmite, procesa y despliega los resultados preliminares conforme a las especificaciones técnicas y normativas del IEEC. Para esto se utilizó una matriz de pruebas con un conjunto de datos de muestra de diferentes tipos definidos por los auditores, con los cuales se realizaron pruebas a cada uno de los sistemas descritos con anterioridad.

Con diferentes datos de entrada probamos que el resultado fuera el esperado.

Estas pruebas se realizaron en atención a lo señalado en los incisos III y IV del artículo 33° de los Lineamientos del programa de resultados preliminares (PREP), que indican como tareas de la

auditoria, realizar “La Revisión y las pruebas de Calidad del sistema informático y todos los aplicativos desarrollados específicamente para el PREP, en términos de funcionalidad.

Para la realización de las pruebas funcionales de caja negra, el equipo auditor de ITESCAM realizó un primer análisis de funcionalidad sobre el software del PREP con la finalidad de identificar el flujo de la información y la funcionalidad de los aplicativos, en base a ello diseño un plan de pruebas en el que se especificó los casos de prueba propuestos, los ciclos, los datos de entrada y de salida esperados para verificar el funcionamiento de la aplicación informática.

4.2. PRUEBAS DE SEGURIDAD

Las pruebas de seguridad se llevaron a cabo a solicitud del Comité Técnico y para evaluar el nivel de disponibilidad del servicio prestado por Grupo PROISI, con ello el PREP busca garantizar la confiabilidad y disponibilidad de la publicación y captura del sistema el día de las elecciones.

Utilizando diferentes aplicaciones se realizaron pruebas de carga del servidor solicitado http://prepcampeche2018.mx, para determinar el número de usuarios que soporta el servicio a través de análisis de soporte volumétrico por protocolos solicitados por el INE de hasta 400mbps. Durante esta prueba se pudo observar que el servicio de alojamiento utilizado por la empresa tiene soporte para los usuarios solicitados en el lineamiento del INE y se presentaron recomendaciones operativas sobre posibles vulnerabilidades sobre todo en respuestas de la aplicación.

Se debe considerar que el sitio presenta puertos abiertos que no son requeridos para el proceso de publicación de los resultados y aun cuando no se encontraron servicios con riesgo en ellos es una buena práctica cerrar los puertos para evitar cualquier problema de seguridad. El proceso y conclusiones se explican en el ANEXO 2 de este mismo documento

Una vez concluida la inspección visual y pruebas de caja negra a cada uno de los sistemas mencionados se firmaron digitalmente con la siguiente estructura y el Algoritmo de Hash Seguro (Secure Hash Algorithm SHA-256) de la versión final auditada tanto a la base de datos en ceros como al código fuente en producción.

Archivo	SHA-256
centrales_final.tar.gz	c52ea8d7c31bfca7fedeb3611fa780da5b0c8a6d6235831ab7f02a0b1cf16efc
prep_campeche2018_final.sql	fcc6d712cf5879c17438ce2640ba0533d4d9da4f106af263f1828bebd210aa03

5. CONCLUSIONES

Una vez que la empresa Grupo PROISI S.A. de C.V. atendió las observaciones reportadas y el ITESCAM verificó su correcta atención, se concluye que:

El sistema informático del PREP desarrollado, brinda la funcionalidad necesaria para apoyar en la digitalización, captura y publicación vía Internet de la información de las actas de escrutinio y cómputo de la elección de gobernador, diputados, presidentes y juntas municipales del estado de Campeche, procesándola de manera íntegra y confiable, y cumple con lo que señala la normativa aplicable y vigente.

Se identificaron oportunidades de mejora que se recomendaron durante la auditoría, relacionadas al proceso, a la logística de operación de la jornada electoral, así como al sistema informático que no alteran los resultados publicados por el IEEC pero es recomendable integrarla en futuras elecciones para garantizar un proceso más ágil.

6.- BIBLIOGRAFÍA.

[1] the Institute of Electrical and Electronics Engineers, «IEEE Standard for Software Reviews,» *IEEE Computer Society,* p. 52, 2008.

[2] Instituto Electoral del Estado de Campeche IEEC, «Notificación del fallo de la Licitación Pública IEEC-LP-02-2015,» Instituto Electoral del Estado de Campeche IEEC, Campeche Campeche, 2015.

[3] Comité Técnico Instituto Electoral del Estado de Campeche IEEC, «Procedimiento de Control de Cambios del Código Fuente y de las configuraciones del Sistema Informático,» Instituto Electoral del Estado de Campeche IEEC, Campeche, 2015.

[4] Instituto Nacional Electoral, «procedimiento de Control de Cambios del Código Fuente y de las configuraciones del Sistema Informático,» Instituto Nacional Electoral, Estados Unidos Mexicanos, México, 2015.

[5] Instituto Electoral del Estado de Campeche-ITESCAM, «Convenio de Colaboracion IEEC-ITESCAM,» de *Convenio de apoyo y Colaboracion IEEC-ITESCAM*, Campeche, 2015.

[6] IT Governance Institute, « COBIT, Herramientas de Implementación,» *IT Governance Institute,* vol. Tercera Edición, 2000.

[7] D. Cantone, « Implementación y debugging. USERSHOP.,» 2006.

[8] E. MÉNDEZ, M. PÉREZ y L. E. MENDOZA, « Aplicación de un Método para Especificar Casos de Prueba de Software en la Administración Pública.,» *Actas de Talleres de Ingeniería del Software y Bases de Datos,* vol. 1, nº 4, p. 47, 2007.

[9] I. N. Electoral, «Lineamientos del Programa de Resultados Electorales Preliminares,» *INE México,* vol. I, nº 1, p. 20, 2015.

[10] M. D. P. N. E. &. D. P. R. M. Piattini Velthuis, «Auditoría de tecnologías y sistemas de información.,» México., 2008.

ANEXO 1. CRITERIOS DE AUDITORÍAS

AUDITORÍA DE LOS REQUERIMIENTOS				
REQUERIMIENTO	CRITERIO	OBSERVACIONES	CONFORMIDAD	
			VERIFICACIÓN BASE DE DATOS	VERIFICACIÓN DEL PROCEDIMIENTO
1 digitalización	1. El sistema es capaz de digitalizar las AEC		SI	SI
	2. El sistema permite seleccionar el folio fecha y hora de la digitalización	Se validó que los valores aceptados en los campos son los esperados.	SI	SI
	El sistema almacena el acta digitalizada y la envía a captura.		SI	SI
2. captura de las AEC	1. El sistema permite la captura manual de los datos del acta.		SI	SI
	2. Marcar Inconsistencias en el AEC		SI	SI
	3. Transmisión de las AEC desde los CATD al validador		SI	SI
	4. Verificación de los valores ingresados en los campos	Se validó que los valores aceptados en los campos son los esperados.	SI	SI
	5. El sistema almacena la información capturada		SI	SI
3.2 Validación de las AEC	1. Recepción de las AEC en el sistema de verificación		SI	SI
	2. El sistema permite Aceptar, rechazar captura y rechazar digitalización.		SI	SI
	3. El sistema permita visualizar el acta, los datos capturados y/o las incidencias para su verificación.	Se verificó que todos los datos solo sean de visualización y no permitan la modificación de los mismos.	SI	SI
3.3 Procesamiento	1. Asignación de Perfiles de usuario en el sistema PREP	Se verificó la asignación de roles para cada uno de los usuarios y sus permisos requeridos	SI	SI
	2.Puesta en marcha e inicialización del PREP	Se implementó un sistema de borrado automático del sistema PREP y generación y generación de catálogos a partir de los datos proporcionados por el INE	SI	SI
	3. Manejo de Coaliciones	Se verificó el manejo del cómputo en las coaliciones para que cumpla con los lineamientos de INE	SI	SI
	4. Ingreso y validación de cuentas de usuario	Se verificó que el acceso al sistema cumpla con características de seguridad	SI	Si
	5. Transmisión entre los Distritos y el recinto	Se tomaron previsiones en las instalaciones con ups de	SI	SI

	central del IEEC	emergencia y una planta eléctrica, conectividad a internet dedicada, utilización de una VPN y servicios de ISP de Telmex.		
	6. Se verificó que las tablas no cuenten con campos en desuso para mejorar la integridad de los datos, igualmente que los campos tuvieran información consistente.		SI	SI
3.4 Publicación	1. Datos de salida en la publicación de resultados.		SI	SI
	2. Navegación y visualización de resultados		SI	SI
	3. Gráfica del PREP.		SI	SI
	4. Muestra de resultados estadísticos.		SI	SI
	5. Comportamiento de la publicación de resultados electorales.		SI	SI
	6. Indicador de avance de captura y publicación		SI	SI
3.5 Reportes	7. Generación de estadística.		SI	SI

ANEXO 2. AUDITORÍA DE VULNERABILIDADES Y DISPONIBILIDAD

Con el fin de reducir riesgos por posibles vulnerabilidades en la aplicación PREP Campeche 2018 de la empresa Grupo PROISI S.A. de C.V. se realiza una inspección de su protocolo y pruebas de DISPONIBILIDAD para medir el impacto en el servicio que proveerá en las contiendas electorales del 7 de junio de 2018.

Se realizarán validaciones que corroboren el protocolo que la empresa ha establecido.

Desarrollo

Como primera actividad el administrador cierra los puertos del servidor de recepción de AECs. Usando la herramienta nmap se validará que el puerto esté cerrado hasta antes del simulacro.

Análisis de Vulnerabilidades Externas – Infraestructura

Componentes con Vulnerabilidades Conocidas – Sin Riesgo

104.20.93.168

Summary

Critical	High	Medium	Low	Info	Total
0	0	3	0	19	22

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (5.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Medium (5.0)	42873	SSL Medium Strength Cipher Suites Supported
Info	10107	HTTP Server Type and Version
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	46180	Additional DNS Hostnames

Servicios Expuestos

Servicios Vulnerables – Sin Riesgo

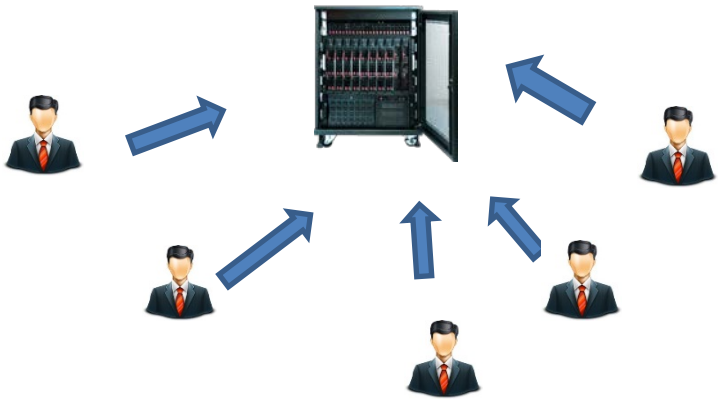
Puertos y Servicios Abiertos desde internet:

```
80/tcp   open  http       Cloudflare nginx
443/tcp  open  ssl/https    cloudflare
2052/tcp open  http       Cloudflare nginx
2053/tcp open  ssl/http     nginx
2082/tcp open  http       Cloudflare nginx
2086/tcp open  http       Cloudflare nginx
2087/tcp open  ssl/http     nginx
2095/tcp open  http       Cloudflare nginx
2096/tcp open  ssl/http     nginx
8080/tcp open  http       Cloudflare nginx
8443/tcp open  ssl/https-alt cloudflare
8880/tcp open  http       Cloudflare nginx
```

También se realizó la validación de disponibilidad del servidor prepcampeche2018.mx haciendo una revisión de puesta a cero de los datos contenidos en él.

Se pudo garantizar que prepcampeche2018.mx estuviera disponible y con valores iniciales del cómputo en cero.

Se realizó una validación de acuerdo con el siguiente esquema:



Ataque DDoS SynFlood/Slowloris

Análisis de Cifrados

Protocolos de Cifrado – Sin Riesgo

SERVER PREFERRED CIPHER SUITES

Preferred cipher suite for each protocol supported (except SSLv2). Expected configuration are ciphers allowed by PCI DSS and enabling PFS:

TLSv1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLSv1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLSv1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

```
Other addresses for prepcampeche2018.mx (not scanned): 2400:cb00:2048:1::6814:5ca8 2400:cb00:2048:1::6814:5da8 104.20.92.168
Not shown: 996 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 - unknown
|       TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 - unknown
|       TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256-draft - unknown
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 - unknown
|       TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 - unknown
|       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 - unknown
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (rsa 2048) - A
```

Se realizó el análisis de los protocolos en las aplicaciones encontradas y sobre las que se recomienda revisar el protocolo https.

Una vez validado que se realizó la apertura del puerto de recepción, en diferentes puntos se ejecutaron intentos de denegación del servicio distribuido (DDoS), a partir de las 10:30 A.M. y hasta las 5:00 pm., con diversas herramientas.

Aunque por momentos se observaba una disminución del tráfico hacia el servidor, éste se mantuvo disponible durante el tiempo reportado.

Conclusiones

Una buena práctica observada es la inhabilitación de las redes inalámbricas, por el riesgo que éstas representan.

Además, se recomienda contar con una página personalizada de errores mandando redireccionamiento al sitio de inicio.

Aunque el servidor se mantuvo disponible durante el tiempo que se le requirió, una recomendación del equipo auditor fue que dicho servidor no tenga abierto los puertos que no sean necesarios para reducir en lo posible los riesgos en los que se pueda comprometer la seguridad del sistema.