INSTITUTO TECNOLÓGICO SUPERIOR DE CALKINÍ

Auditoria informática al programa de resultados electorales preliminares (PREP) 2024 para el proceso electoral en el Estado de Campeche

INFORME FINAL

V 2.0

IEEEC- ITESCAM

1 de junio de 2024

Versión	**1.0**
Fecha de elaboración	01 de junio de 2024

HISTORIAL DE VERSIONES	
Número de versión	0.0
Fecha de actualización	12/04/2024
Responsable de la actualización	Dr. Yaqueline Pech Huh
Descripción de la actualización	Creación del formato
Número de versión	1.0
Fecha de actualización	16/04/2024
Responsable de la actualización	Dr. Jose Manuel Lira y Dra. Yaqueline Pech Huh
Descripción de la actualización	Anexo de fase 1 pruebas de caja negra
Número de versión	2.0
Fecha de actualización	30/05/2024
Responsable de la actualización	Dr. Yaqueline Pech Huh, Dr. José Manuel Lira Turriza, Dr. Jose Luis Lira Turriza.
Descripción de la actualización	Concentrado de la información final

RESPONSABLES	
Líder de proyecto	Dra. Yaqueline Pech Huh
Ejecución de las pruebas de seguridad. Jefe de auditoría	Dr. Jose Luis Lira Turriza
Ejecución de las pruebas de caja negra Jefe de auditoría	Dr. Jose Manuel Lira Turriza Dr. Gonzalo Miguel Quetz Aguirre
Documentador	Dr. Jose Manuel Lira Turriza

CONTENIDO

GLOSARIO 5

RESUMEN EJECUTIVO 6

INTRODUCCIÓN 8

DICTAMEN 11

PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES 13

OBJETIVO GENERAL 16

ALCANCE 17

METODOLOGÍA 18

A) MODELO 18
B) ROLES Y PARTICIPACIÓN 21

CRITERIOS UTILIZADOS PARA LA AUDITORÍA 23

METODOLOGÍA PARA CLASIFICAR LOS HALLAZGOS 25

RESULTADOS 27

A) PRUEBAS FUNCIONALES DE CAJA NEGRA 27

B) VALIDACIÓN DEL SISTEMA INFORMÁTICO PREP Y DE SUS BASES DE DATOS. 36

C) ANÁLISIS DE VULNERABILIDADES DE LA INFRAESTRUCTURA TECNOLÓGICA 40

ANEXOS 46

ÍNDICE DE FIGURAS

FIGURA 1 FLUJO PTO 2024 IEEC 15
FIGURA 2. MODELO DE FLUJO DE ACTIVIDADES DE AUDITORÍA 18
FIGURA 3 MODELO DE DESARROLLO DE ACTIVIDADES DE LA AUDITORÍA 21
FIGURA 4 MODELO DE RELACIÓN ENTRE CAUSAS Y EFECTOS PARA LA DETECCIÓN Y CORRECCIÓN DE ERRORES 25
FIGURA 5. CLASIFICACIÓN DE HALLAZGOS FASE 1 28
FIGURA 6 CLASIFICACIÓN DE HALLAZGOS FASE 2 30
FIGURA 7. SITIO DE PUBLICACIÓN SIMULACRO 19 DE MAYO 2024 32
FIGURA 8. GENERACIÓN DEL CÓDIGO HASH EN EL SIMULACRO DEL 19 DE MAYO 2024 33
FIGURA 9. TOTAL DE ACTAS CAPTURADAS EN EL SIMULACRO CORRESPONDIENTES A DIPUTACIONES 33
FIGURA 10 ACTAS CAPTURADAS PARA GUBERNATURA, DIPUTACIONES, AYUNTAMIENTOS Y JUNTAS MUNICIPALES SIMULACRO 3 35
FIGURA 11 HALLAZGOS IDENTIFICADOS (ATENDIDOS Y NO ATENDIDOS) 36
FIGURA 12 FLUJO BASE DE DATOS EN CEROS 37
FIGURA 13 FLUJO PARA LA VERIFICACIÓN DE HUELLAS CRIPTOGRÁFICAS 39
FIGURA 14 DISTRIBUCIÓN DE INFRAESTRUCTURA DEL PREP PROPORCIONADA POR INFORMÁTICA ELECTORAL EN SU ARQUITECTURA DEL SISTEMA INFORMÁTICO PREP 2024 FUENTE: INFORMÁTICA ELECTORAL. 41

ÍNDICE DE TABLAS

TABLA 1 ROLES Y ACTIVIDADES 22
TABLA 2 NIVEL CRITICIDAD 26
TABLA 3 SHA CÓDIGO FUENTE VERSIÓN FINAL 40

Glosario

Acta PREP: Primera copia del AEC destinada para el PREP, o en ausencia de ésta, cualquier copia del AEC.

AEC: Acta de Escrutinio y Cómputo.

Código QR: Imagen bidimensional que almacena, de forma codificada, la información que permite identificar cada Acta PREP a través de medios electrónicos (Este dependerá de la herramienta informática que para tal fin se destine).

Cotejo: Fase que permite corroborar que los datos publicados coincidan con los datos asentados en el Acta PREP, a través del registro del resultado en el sistema informático.

Coprep: Módulo de Cotejo de Actas

CVPREP: Captura y verificación PREP.

CRID: Centro de Recepción de Imágenes y Datos.

EA: Equipo auditor conformado

IEEC: Instituto Electoral del Estado de Campeche.

Lineamientos del PREP: Lineamientos del Programa de Resultados Electorales Preliminares correspondiente al Anexo 13 del Reglamento de Elecciones del Instituto Nacional Electoral.

MCAD: Monitor de Captura de Actas Digitalizadas. Software que permitirá revisar las imágenes de las Actas PREP digitalizadas, así como registrar, de forma manual o automática, la fecha y hora de acopio, así como los datos de identificación contenidos en el Código QR (en su caso).

MRI Se conformará por el personal que resolverá los casos de discrepancia en la captura de datos de las Actas PREP, una vez que hayan sido procesadas por dos o tres Capturistas/verificadores diferentes, así como las actas clasificadas por los capturistas/verificadores con estatus de "ilegible".

PREP: Programa de Resultados Electorales Preliminares del Proceso Electorales Estatal Ordinario 2021, en el Estado de Campeche.

PREP Casilla: Aplicación móvil que permite realizar la toma fotográfica del Acta PREP y su envío al CRID para su captura.

PTO: Proceso Técnico Operativo

Reglamento de Elecciones: Reglamento de Elecciones del Instituto Nacional Electoral.

SIPREP: Sistema de Información del Programa de Resultados Electorales Preliminares. (Sitio de Publicaciones)

Sistema informático: Conjunto de programas e infraestructura tecnológica que se utilizará para el acopio, digitalización, captura/verificación, cotejo y publicación de los datos asentados en las Actas PREP y las imágenes de estas.

Resumen ejecutivo

En el proceso electoral estatal Ordinario 2024, en cumplimiento a la normatividad se contrató a quien lleve a cabo el Programa de Resultados Electorales Preliminares (PREP), que está sujeto a los Lineamientos del Programa de Resultados Electorales Preliminares, emitidos por Consejo General del Instituto Nacional Electoral. En el diseño, instalación e implementación del PREP se deberá de cumplir con los principios de certeza, legalidad, independencia, imparcialidad, máxima publicidad y objetividad, en el ejercicio de la función electoral. De acuerdo con lo que establecen los Lineamientos, 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. Así mismo se deberán incorporar en el desarrollo de su sistema informático, la función requerida para la generación y el almacenamiento de bitácoras que faciliten los procedimientos de verificación, análisis y auditoría del sistema.

Para dar cumplimiento a las normas y leyes vigentes de acuerdo con los Lineamientos del Programa de Resultados Electorales Preliminares 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 llevando a cabo la auditoria de caja negra y de seguridad, que consiste en revisar la funcionalidad general del programa, validación del proceso técnico operativo, validación del sistema informático del PREP y de sus bases de datos, análisis de vulnerabilidades a la infraestructura tecnológica, pruebas de denegación del servicio, pruebas de calidad así como la verificación y seguimiento del procedimiento durante los simulacros basado en el estándar IEEE Standard for Software Reviews and Audits IEEE Std 1028™-2008 (the Institute of Electrical and Electronics Engineers, 2008) y en la metodología ISTQB.

El ITESCAM participó en el desarrollo de la auditoria de software del PREP proporcionado por la empresa INFORMÁTICA ELECTORAL, S. C. misma que fue convocada con base en la licitación número IEEC-LPN-001-2024 del IEEC, así como el resultado de la licitación para la empresa,

donde se dictaminó a la empresa responsable del PREP (Instituto Electoral del Estado de Campeche IEEC, 2024), misma que en fecha 16 de abril 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 ser 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". (Comité Técnico Instituto Electoral del Estado de Campeche IEEC, 2024)

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).

Introducción

El 2 de junio de 2024 se llevarán a cabo las elecciones en el estado de Campeche en donde se elegirán 35 diputaciones locales, 13 Ayuntamientos y 22 juntas municipales, donde el Instituto electoral del Estado de Campeche (IEEC) es el encargado de la organización de las elecciones.
En el proceso electoral estatal Ordinario 2024, en cumplimiento a la normatividad se contrató a quien lleve a cabo el Programa de Resultados Electorales Preliminares (PREP), que está sujeto a los Lineamientos del Programa de Resultados Electorales Preliminares, emitidos por Consejo General del Instituto Nacional Electoral. En el diseño, instalación e implementación del PREP se deberá de cumplir con los principios de certeza, legalidad, independencia, imparcialidad, máxima publicidad y objetividad, en el ejercicio de la función electoral. De acuerdo con lo que establecen los Lineamientos, 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. Así mismo se deberán incorporar en el desarrollo de su sistema informático, la función requerida para la generación y el almacenamiento de bitácoras que faciliten los procedimientos de verificación, análisis y auditoría del sistema.

De acuerdo con los lineamientos vigentes del instituto nacional electoral (INE) donde se establece los Requisitos Mínimos para la elaboración del anexo técnico para la contratación de servicios de auditoría al sistema informático y a la infraestructura tecnológica del Programa de Resultados Electorales Preliminares, se señala que se deben considerar al menos las siguientes líneas de trabajo:

- Validación del proceso técnico operativo
- Pruebas Funcionales de Caja Negra
- Validación del sistema informático del PREP y de sus bases de datos

Es por ello por lo que, en marzo de 2024, el Instituto Electoral del Estado de CAMPECHE (IEEC) y el Instituto Tecnológico Superior de Calkiní en el Estado de Campeche (ITESCAM) suscribieron un convenio específico de colaboración con el objetivo de realizar la Auditoría de software al Sistema del Programa de Resultados Electorales Preliminares (PREP) que se utilizará para las elecciones en el Estado de CAMPECHE de la cual se desprende este informe.

Para la realización de esta auditoría, participó por parte del IEEC el personal técnico del instituto electoral, por parte del ITESCAM, personal de la Dirección Académica de las Carreras de Ingeniería Informática y Sistemas Computacionales al que denominaremos Equipo Auditor.

La revisión debe realizarse desde el punto de vista de la calidad, consistente del grado en el que el software satisface una serie de requisitos de operación preestablecidos, los estándares de desarrollo especificados con anterioridad y las características inherentes a todo producto de software desarrollado de manera profesional, ante las expectativas del cliente en una solución, la auditoría debe validar que ésta cumpla con las especificaciones definidas generando certeza en los datos publicados. Para la ejecución de la auditoría es indispensable utilizar un conjunto de estándares, técnicas, métodos y tecnologías de la información que permitan lograr que los sistemas sean correctamente auditados.

El estándar para la revisión y auditoría de software IEEE 1028TM 2008 en el que se define cinco tipos de revisiones y auditorías de software, junto con los procedimientos necesarios para la ejecución de cada tipo. Los tipos de revisión incluyen revisiones de gestión, revisiones técnicas, inspecciones, y walk-throughs, siendo aplicada en cualquier modelo de ciclo de vida del software seleccionado y proporciona un estándar contra el cual se pueden preparar y evaluar los planes de revisión y auditoría de software (IEEE S. C., 2010).

El estándar de clasificación de anomalías de software IEEE1044-2009 1.1 proporciona el conjunto básico de atributos para la clasificación de fallas y defectos. Este estándar es aplicable a cualquier software (incluidos sistemas operativos, sistemas de administración de bases de datos, aplicaciones, software de prueba, firmware y software integrado) y a cualquier fase del proyecto, producto o ciclo de vida del sistema (IEEE S. C., 2010).

El estándar para desarrollar un proyecto de software en el proceso de ciclo de vida IEEE 1074 en el que se explica como el aseguramiento de calidad del software debe apoyarse o relacionarse estrechamente con las siguientes actividades (Dorado & Sanz, 2000):

- Verificación: Básicamente revisiones y auditorías de configuración y calidad.
- Validación: Todos los niveles y fases de prueba de ejecución de software.
- Gestión de Configuración: Como medio de control de los productos generados.
- Medición de software: Contempla la necesidad de marcar objetivos y asociar métricas a los objetivos.

En estas actividades se resalta la verificación o auditoría del software y la medición a través de objetivos. Esta auditoría debe ser planificada y llevada por las personas asignadas para tal fin, no puede olvidarse ningún detalle y siempre se deben tener en mente los siguientes objetivos:

- Encontrar tempranamente los defectos.
- Prevenir el mal funcionamiento.
- Proporcionar mejoras.

El presente informe contempla los resultados de la auditoria al software PREP, del cumplimiento del PTO, el cumplimento a los aspectos de seguridad, la validación de las bases de datos y la validación de los procesos durante los simulacros.

Dictamen

Como resultado de la revisión llevada a cabo en los meses de abril y mayo de 2024 de la implementación del Proceso Técnico Operativo para el Programa de Resultados Electorales Preliminares del Estado de Campeche para el proceso electoral 2024, el Ente Auditor hace constar que:

1. El sistema informático y sus bases de datos auditados cumplen con los requerimientos funcionales mínimos para la operación del PREP durante la jornada electoral del próximo 2 de junio de 2024.

2. Se ha definido un procedimiento para garantizar que el sistema informático auditado es el que se utilizará durante la jornada electoral del 2 de junio.

3. El procedimiento técnico metodológico también valida que las bases de datos a usar antes del inicio del PREP, el 2 de junio, estarán en un estado inicial con todos sus datos en 0.

4. La implementación del PTO cumple de manera general con los requerimientos de seguridad y operación siendo su nivel de riesgo bajo para su operación.

5. El sistema informático cumple con los requerimientos funcionales definidos en los casos de uso y no realiza actividad alguna fuera de las que están descritas en la documentación, en lo general cubre estándares de seguridad informática que permiten asegurar que está libre de las vulnerabilidades más conocidas.

6. La solución de infraestructura tecnológica y servidores asociados al PREP 2024 tiene niveles de riesgo bajos y están configurados de forma adecuada para la operación del servicio.

7. Se han revisado los sitios de publicación de resultados, validando que puedan resistir los ataques informáticos más conocidos incluidos los que se refieren a los ataques de denegación de servicio básicos.

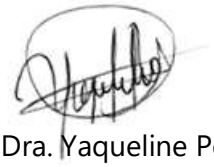
8. Es de observancia que, el que no exista un control de versiones puede llevar a presentar resultados de versiones anteriores que no cumplen con los requisitos establecidos, queda de la

empresa Informática Electoral, S. C. asegurarse que los datos sean extraídos y publicados de acuerdo con la versión auditada y validada durante cada actualización debido a que es un proceso interno del área de desarrollo que no fue auditado.

Considerando todo lo anterior, se constata que el sistema informático en la versión auditada del PREP 2024 se encuentra en condiciones suficientes para operar en la jornada electoral por celebrarse el día 2 de junio de 2024.

El presente dictamen se emite en la ciudad de Calkiní Campeche el día 31 de mayo de 2024.

ATTE



Dra. Yaqueline Pech Huh

Responsable del ENTE AUDITOR

Instituto Tecnológico Superior de Calkiní en el estado de Campeche

Programa de resultados electorales preliminares

En el artículo 339, párrafo 1, inciso c), del RE, en relación con el numeral 15 de los Lineamientos del PREP, se señalan las fases definidas por este Instituto para su ejecución en el proceso electoral estatal ordinario 2024 como se muestra en la figura 1.

El día 2 de junio se llevará a cabo la jornada electoral en el estado de Campeche y siendo las 18:00 horas –tiempo local-, se realizará el cierre de todas las casillas instaladas para la votación por parte de los ciudadanos, para que los funcionarios de casilla procedan a contar los votos uno por uno e inicien el proceso de elaboración de las actas de escrutinio. Una copia se guardará en un sobre transparente que permitirá observar su contenido sin necesidad de abrirlo y al que se denomina "Sobre PREP".

Una vez concluido el llenado del AEC, con base en lo establecido en el Programa de Asistencia Electoral 2023-2024, la o el CAEL solicitará el Acta PREP a la presidencia de la Mesa Directiva de Casilla, pegará el código QR correspondiente y, haciendo uso de PREP Casilla, realizará la toma fotográfica sin obstaculizar las actividades en el cierre de esta y se procederá al acopio que consistirá en la recepción de las Actas PREP en los CATD.

Posteriormente se iniciará la digitalización, esta fase consistirá en la identificación de las Actas PREP acopiadas en el CATD y, en su caso, se les asociará con un código QR. Posteriormente se llevará a cabo la captura digital de imágenes a través del equipo multifuncional. Finalmente, las actas digitalizadas, ya sea por este procedimiento o a través de PREP Casilla, se procesarán en el MCAD.

Seguidamente se registrarán y corroborarán todos los datos asentados y capturados de las Actas PREP, a través de la TCA. Y se realizará la publicación de resultados electorales preliminares que deberá iniciar a las 20:00 horas -Tiempo del Centro- del domingo 2 de junio de 2024. La divulgación de los datos, imágenes y bases de datos del PREP estarán a cargo del Instituto y, en su caso, de los difusores oficiales.

Se debe realizar un cotejo de actas que tendrá por objeto corroborar que los datos publicados coincidan con los datos asentados en el Acta PREP. El personal asignado al cotejo comparará los datos y la imagen publicados en el portal del PREP, o en su caso, con el Acta PREP física que posee el CATD y los datos que hayan sido publicados, registrando el resultado en el sistema informático.

La última fase, que corresponde al empaquetado de actas se archivarán las Actas PREP para su posterior entrega a la presidencia del Consejo Distrital que corresponda. Salvo la fase "Toma fotográfica del Acta PREP en la casilla", todas las demás fases descritas en el presente se realizarán en los CATD. Por otra parte, en los CCV, se podrán llevar a cabo actividades de digitalización de actas provenientes de PREP Casilla, captura, verificación y cotejo de las Actas PREP.

El cierre de la publicación de los resultados electorales preliminares concluirá, a más tardar, a las 20:00 horas -Tiempo del Centro- del lunes 3 de junio de 2024. La publicación del PREP podrá cerrar antes de las 20:00 horas -Tiempo del Centro- del lunes 3 de junio de 2024, siempre y cuando se logre el 100% de la publicación de las Actas PREP esperadas y se hayan agotado los recursos de recuperación de estas.

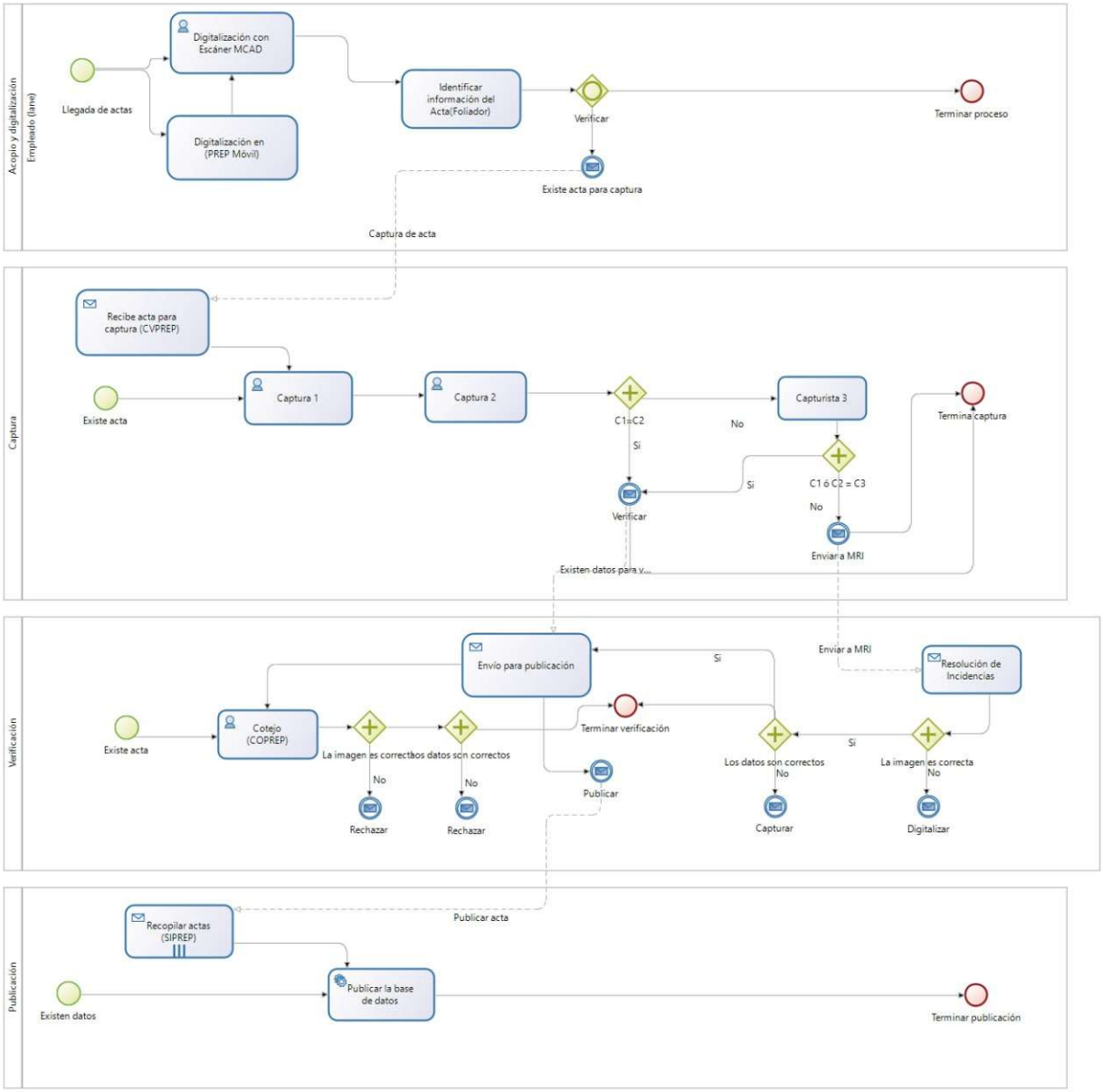


Figura 1 Flujo PTO 2024 IEEC

Objetivo General

El objetivo general de la auditoría es evaluar la integridad en el procesamiento de información y la generación de resultados preliminares, conforme a lo establecido en el artículo 347, numeral 1, inciso a) del Reglamento de Elecciones.

Objetivos específicos

1. Verificar el cumplimiento de las especificaciones funcionales y requerimientos contenidos en los lineamientos del Programa de Resultados Electorales Preliminares.
2. Revisar el cumplimiento de la aplicación en relación con el Proceso Técnico Operativo.
3. Evaluar la integridad y exactitud, del sistema informático del PREP en el procesamiento de información, generación y presentación de resultados.
4. Verificar la trazabilidad del proceso identificando la correspondencia desde la digitalización y captura hasta publicación.
5. Analizar vulnerabilidades a la infraestructura del PREP.
6. Ejecutar pruebas de denegación del servicio (DoS) al sitio web del PREP y al sitio principal del IEEC para comprobar su robustez y disponibilidad
7. Diseñar y ejecutar pruebas de penetración a
8. Elaborar un informe parcial y un informe final con los resultados de la auditoría
9. Elaborar recomendaciones relativas a las vulnerabilidades y riesgos detectados en la Auditoría

Alcance

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 de la que se desprende este informe aplica para **los módulos PREP Casilla, MCAD, CVPREP, MRI, SIPREP, COPREP del sistema informático PREP** a utilizarse en las elecciones del 2 de junio de 2024 considerando:

A. Analizar el funcionamiento de la aplicación en relación con las fases del proceso técnico operativo, considerando al menos, la digitalización, captura y publicación de resultados, mediante flujos completos e interacción entre el módulo de digitalización, captura y validación (obtención de imagen digital del acta, captura de la información contenida en las actas PREP, validación de la información capturada) y el módulo de Publicación de Resultados incluyendo la revisión de la obtención de los resultados, así como la emisión de reportes y su despliegue, de acuerdo con la documentación técnica y la normatividad aplicable.

Metodología

A) Modelo

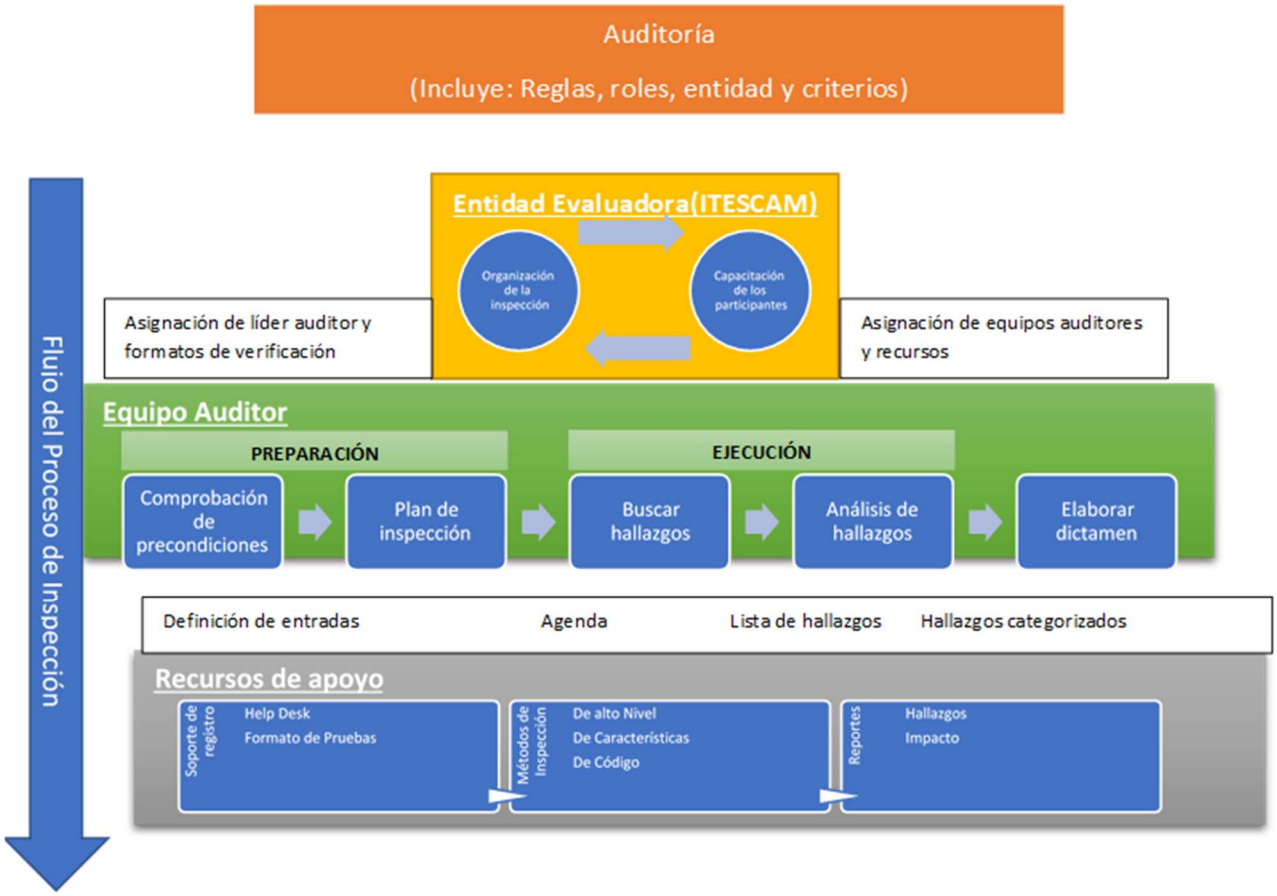


Figura 2. Modelo de flujo de actividades de auditoría

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 2. 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 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 por lo 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 para conocer los aspectos del sistema que se va a auditar. Con base en 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 (Plan de pruebas) identificando desviaciones a la funcionalidad establecida y registrándola a través de herramientas para este propósito. Existen distintos métodos de inspección para un desarrollo completo o para un atributo de calidad (ISTQB, 2021) (Peso, Velthuis, Gerardo, & Otros, 1998), durante esta etapa se aplican dos 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 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 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. (Sotés, 2004)

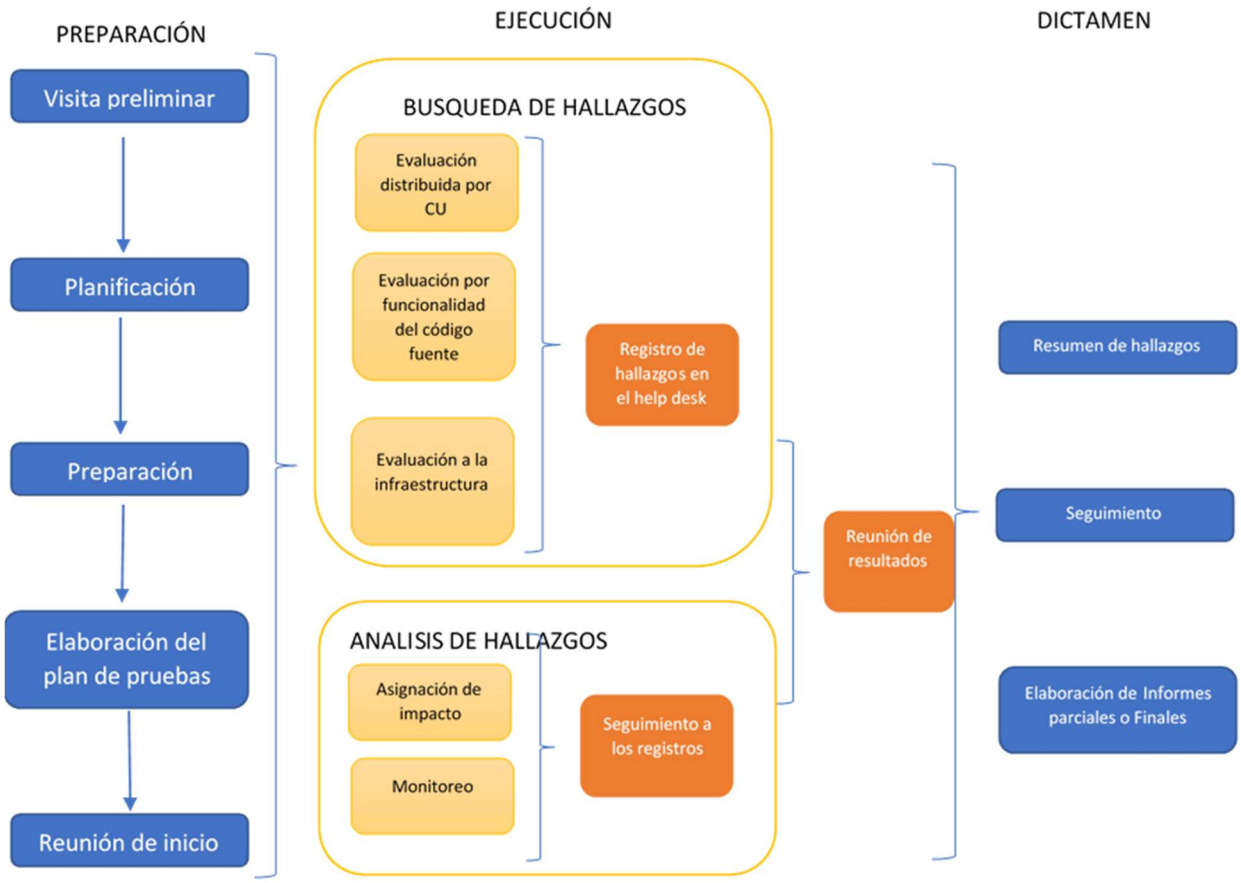


Figura 3 Modelo de desarrollo de actividades de la auditoría

B) Roles y participación

- Líder de auditoría: Es el responsable de las tareas administrativas relativas a la auditoría, la planeación y preparación, verificando que la auditoría se lleve a cabo de manera ordenada y que cumpla con los objetivos y de la recopilación de datos. Presenta los dictámenes al evaluado.
- Documentador: Es el responsable del registro y descripción de las anomalías, elementos de acción, las decisiones y recomendaciones formuladas por el equipo auditor. Registra los datos requeridos para el análisis de los procesos, el líder puede realizar esta función.

- Auditor: Tiene la responsabilidad de estudiar y comprender el material y la documentación de apoyo entregado por parte de la empresa auditada.

  Identificar y describir anomalías del producto

  Registrar en las herramientas de software los hallazgos encontrados de acuerdo con los formatos establecidos para este propósito.
- Jefe de auditores: Se encarga de llevar a cabo una reunión con el equipo de trabajo para acordar los elementos a auditar por cada integrante.

  Apoyar a los auditores en la detección de defectos

  Verificar que se siguen los estándares y reglas establecidas para la inspección

  Verificar que se cumpla la agenda planeada.
- Auditado: Tiene la responsabilidad de facilitar y distribuir la información y documentación al equipo auditor. Recomendar o no la realización de una sesión de presentación y explicación del sistema, este rol lo realiza una persona externa a la entidad evaluadora.

Cada uno de los integrantes del equipo auditor juega un rol importante dentro de la auditoría. En la tabla 1 se observa la participación de los actores en las distintas fases de la auditoría.

Etapas	Líder	Documentador	Auditor	Jefe de Auditoría	Auditado
Visita preliminar	X				X
Planificación	X	X		X	X
Preparación	X			X	
Elaboración del plan de pruebas	X	X	X	X	
Reunión de inicio	X	X	X	X	
Búsqueda de hallazgos		X	X	X	
Registro de hallazgos		X	X		
Análisis de hallazgos	X	X	X	X	
Seguimiento de hallazgos	X	X		X	
Integración de los hallazgos	X	X		X	
Elaboración de los informes parciales	X	X		X	

Tabla 1 Roles y actividades

Criterios utilizados para la auditoría

Para la finalidad de la auditoria que es detectar e identificar anomalías en los sistemas informáticos PREP, se utiliza la metodología ISTQB, el estándar para la revisión y auditoría de software IEEE 1028TM 2008 (IEEE, 2008), de los que se consideran los siguientes criterios:

4. Revisiones de Gestión

    4.1 Introducción

    4.2 Responsabilidades

    4.3 Entradas

    4.4 Criterios de entrada

    4.5 Procedimientos

5. Revisión técnica

    5.1 Introducción

    5.2 Responsabilidades

    5.3 Entradas

    5.4 Criterios de entrada

    5.5 Procedimientos

7. Recorridos

    7.5 Procedimientos

    7.7 Salidas

Así mismo se considerarán como criterios para la auditoría los contemplados en el PTO y los lineamientos del INE.

- Si el sistema cumple con las especificaciones descritas en la documentación.
- Si el sistema satisface las especificaciones y atributos de seguridad.
- Si el sistema se ajusta a los procedimientos, normas, directrices, planes y reglamentos aplicables por el INE y el IEEC.

Si el sistema no incluye códigos y/o software malicioso que pudiera afectar los resultados.

La medición de la criticidad de los hallazgos dependerá de si afecta a la información de los votos presentados en el módulo de publicación, que es la sección más importante debido a que será de consulta por toda la ciudadanía.

Todos estos elementos serán aplicados a los siguientes componentes:

- **Ingreso al sistema.** Se probará las diversas formas correctas e incorrectas de ingresar al sistema informático, así como para el módulo PREP Móvil.
- **Carga de imagen.** Simplicidad y tiempo requerido para anexar la imagen de las Actas PREP a la casilla correspondiente tanto para la versión MCAD del sistema como para la versión PREP Móvil.
- **Captura de datos.** Captura de valores aleatorios, verificando los totales obtenidos y concentrándolos. Aplicable solo al sistema de CVPREP.
- **Verificación de datos.** Verificación de datos capturados comparando con los datos concentrados de la captura. Esta verificación se realiza tanto en el módulo CVPREP como en el módulo MRI.
- **Publicación de resultados.** Verificación de resultados contra los datos capturados. Aplicable solo al sistema SIPREP.

METODOLOGÍA PARA CLASIFICAR LOS HALLAZGOS

Las anomalías se categorizaron basados en las especificaciones del estándar IEEE 1044-2009

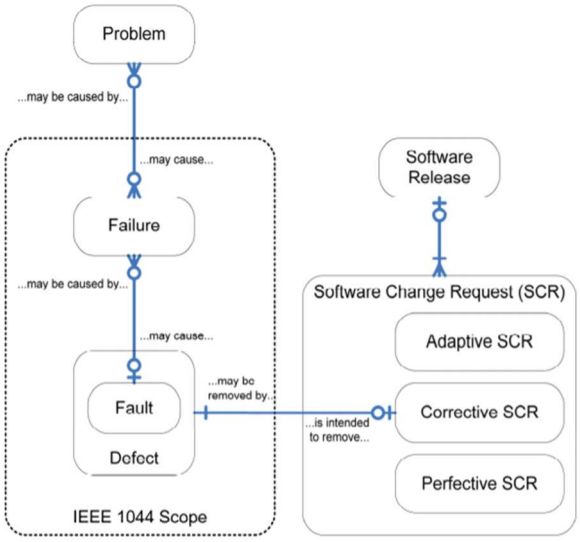


Figura 4 Modelo de relación entre causas y efectos para la detección y corrección de errores.

Las clases de anomalía proporcionan evidencia de inconformidad y las clasificamos:

a. ambiguo.
b. inconsistente.
c. mejora deseable.
d. no se ajusta a las normas.
e. propensa a riesgos.

Los hallazgos encontrados se agregan a una matriz y se clasifican de acuerdo con su nivel de criticidad que presenten en relación con el impacto y urgencia tabla 1.2, para esto se utilizarán los siguientes identificadores de riesgo:

Nivel	Simbología	Descripción
Alto		Anomalías que tienen como resultado una disminución considerable en la percepción de los usuarios finales, es decir que alteren los resultados publicados. Estas anomalías afectan al mayor grupo de usuarios (público en general) generados por uno o más procesos erróneos.

Medio		Anomalías de los sistemas que a pesar de presentarse y generar un fallo permiten la continuidad de las operaciones.
Bajo		Anomalías que difieran de las especificaciones pertinentes, pero no causará la falla de los sistemas de software o una salida observable en el rendimiento

Tabla 2 Nivel Criticidad

- Para dar seguimiento a los hallazgos encontrados se puso a disposición de la empresa la dirección electrónica: http://softmlx.com/issues al igual que se asignó usuarios y contraseñas de acuerdo con la lista proporcionada por el IEEC y la empresa Informática Electoral S. C. esto permite dar seguimiento al estatus de los hallazgos por parte de todos los involucrados.

Resultados

Una vez concluida la auditoría realizada durante el mes de abril en conformidad con el plan de pruebas entregado al IEEC y en cumplimento de los lineamientos establecidos y del proceso técnico operativo se presentan los resultados de la auditoría al software PREP 2024.

A) Pruebas funcionales de caja negra

Las pruebas funcionales de caja negra son una técnica de pruebas de software donde se verifica la funcionalidad sin considerar la estructura interna de código, detalles de implementación o escenarios de ejecución internos en el software, es decir se enfocan solamente en las entradas y salidas del sistema. Para obtener el detalle de cuáles deben ser esas entradas y salidas, se utilizan los requerimientos de software y especificaciones funcionales, estas pruebas se realizaron en dos fases utilizando las técnicas definidas por el ISTQB.

Durante estas fases se verificó que el software diera cumplimiento al PTO en sus fases de digitalización, captura, verificación y publicación. Estas pruebas se realizaron utilizando el estándar (IEEE, 2008), las técnicas de tablas de decisiones, partición de equivalencias, valores de frontera, entre otros.

La ejecución de las pruebas se realizó en el mes de abril de manera presencial en las instalaciones del CCV1, se contó con una réplica completa de todo el proceso: un escáner, un equipo de digitalización, 3 de captura, un equipo de verificación MRI y un módulo de cotejo, así como la ruta a la página de publicación desde un entorno denominado de auditoría.

El objetivo fue verificar que el software cumpla con los requisitos de integridad en el procesamiento de información y la generación de resultados preliminares, conforme a

lo establecido en el artículo 346, numeral 1, 347, numeral 1, inciso a) y numeral 9 del Anexo 13 del Reglamento de Elecciones.

Utilizando cada uno de los insumos proporcionados por el IEEC y la empresa Informática Electoral S. C. se definieron 136 casos de prueba, una lista de cotejo para validar que el módulo de publicación cumpliera con lo solicitado en el prototipo web y móvil proporcionado por el INE y una lista de cotejo para validar los elementos de PTO.

Fase 1.

Esta fase se realizó los días 18,19 y 20 de abril de 2024 de manera presencial, se revisaron los módulos de digitalización, captura y publicación de los que se desprendieron 12 hallazgos, como se muestra en la figura 4. Clasificación de hallazgos fase 1, cada uno de estos se registró en la plataforma de seguimiento (https://softmlx.com/issues) que se puso a disposición de la empresa y del IEEC.

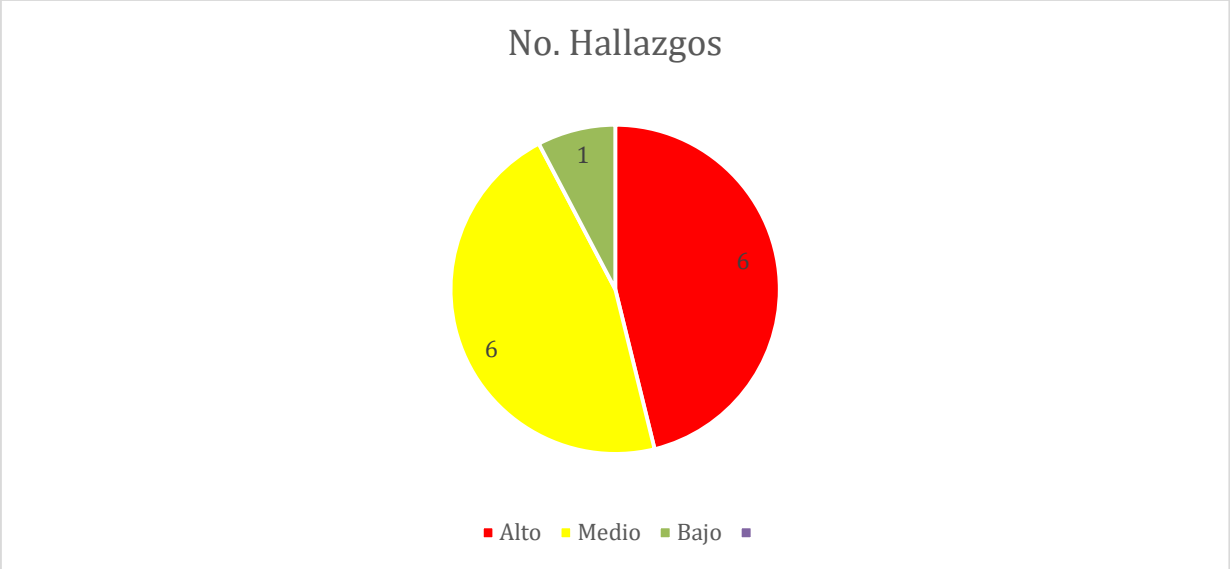


Figura 5. Clasificación de Hallazgos fase 1

Durante esta fase se observó la falta inicial de documentación tales como los manuales de operación, de usuario y demás documentación requerida para que los usuarios del software puedan realizar las operaciones y responder de manera adecuada a cualquier eventualidad.

Igualmente se hizo hincapié en la importancia de la implementación de un control de versione de manera que se pueda garantizar que la versión auditada es la misma que se está empleando en la versión en producción. El sistema de Issues que hemos puesto a su disposición solo contempla las observaciones realizadas por el equipo auditor y no los cambios hechos por requerimientos o fallas detectadas por el equipo de desarrollo. Tener este proceso definido minimizarán los riesgos de dañar módulos que ya hayan sido revisados

Para el caso de la publicación se revisó conforme a lo establecido en los manuales de la estructura para el sitio de publicación para el móvil y el web revisando que se cubran todos y cada uno de los aspectos de visualización definidos.

Todos los hallazgos se encuentran registrados en el anexo 1. Hallazgos. En esta fase no se pudo llevar a cabo la revisión del módulo prep móvil debido a que todavía se encontraba en revisión y no se había liberado. quedando pendientes para la siguiente revisión.

Fase 2.

La fase 2 se llevó a cabo durante los días 23, 24 de mayo de nueva cuenta se llevó a cabo una reunión de apertura, se revisó el contexto de la organización, la validación del PTO y la revisión a los módulos de digitalización, captura, PREP móvil, validación y publicación, igualmente se verificó el estado de los hallazgos identificados en la fase 1 modificando su estatus.

Durante esta fase se volvieron a aplicar todas las pruebas y las listas de cotejo identificando un nuevos hallazgo descritos en el anexo 1.

Los hallazgos fueron modificando su estatus conforme la empresa indico que aplicó los cambios requeridos, lo descrito fue solucionado y esto fue verificado con personal del equipo auditor.

La figura 5. Muestra los hallazgos identificados y clasificados de acuerdo con su impacto, es importante mencionar que durante la revisión no se registró un incremento significativo en los hallazgos aun cuando la revisión fue completa de todo el aplicativo y el proceso.

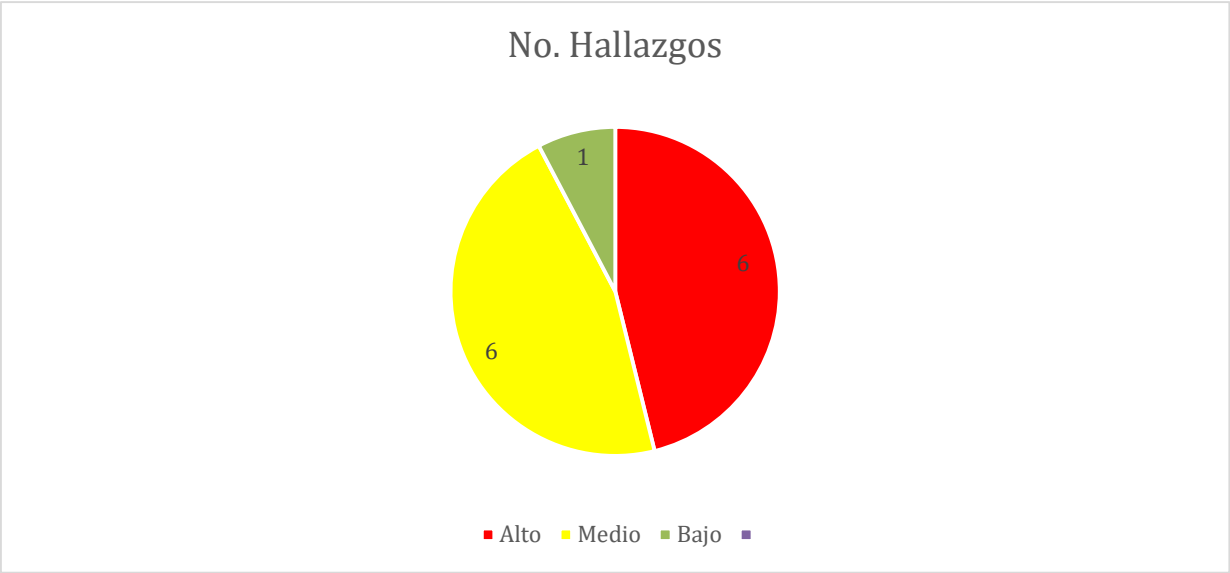


Figura 6 Clasificación de Hallazgos fase 2

Una vez terminada esta fase se dio tiempo a la empresa para la revisión y actualización de los hallazgos con la finalidad de cubrir cada uno de ellos.

Al término de ese tiempo se realizó una verificación de cada uno de ellos, en el anexo 1 se muestra una columna donde se presenta el estado de cada uno de los hallazgos.

Simulacros.

Se llevaron a cabo tres simulacros los días 12, 19 y 26 de mayo en donde se participó como observador del proceso, a continuación, se describen los hallazgos encontrados en cada evento.

Simulacro 12 de mayo de 2024.

Siendo las 8:00 AM el personal de IEEC, el personal de la empresa y el ente auditor dieron fe de la versión del software a utilizar en el simulacro bajo la siguiente agenda:

Se identificaron para la publicación la dirección https://simulacro836462.prepcampeche2024.mx/, el proceso inició las 8:30 AM momento en que se puso en ceros la base de datos previo a esto se observó que el aplicativo web de publicación se encontraba activo y con información precargada de algún evento de prueba anterior. Esto no afecto a los resultados del simulacro

sin embargo por percepción no debería estar activo para mostrar datos antes del inicio de la jornada electoral. Una vez iniciado las actas fueron entregadas para su digitalización y captura, y se procedió a seguir el protocolo.

Durante la jornada se observó la corrección de algunos hallazgos los cuales fueron documentados. Durante este evento destaca, la situación presentada en uno de los cortes pues se realiza la publicación de dos diferentes versiones del aplicativo, una que si corresponde con la versión auditada y que fue publicada en el portal https://simulacro836462.prepcampeche2024.mx/ y otra que corresponde a una versión que contenía errores que ya habían sido solventados por la empresa y que fue publicada en el portal https://prepcampeche2024.mx/ esto representa un elemento de seguridad grave y que queda fuera del ámbito de lo auditado debido a que es parte del proceso interno que el área de desarrollo de la empresa.

Debido a lo anterior se dio el caso de que cada uno de los equipos distribuidos en los CATD tenían diferentes versiones del aplicativo apuntando a espacios de almacenamiento distintos por lo que no se pudo observar el 100% de las actas capturadas debido a que, aunque estas ya habían pasado por todo el proceso no se visualizaron en su totalidad en ninguna de las dos direcciones web porque se almacenaron en lugares diferentes .

Otro hallazgo importante es el relacionado al formato de la base de datos descargable, debido a que no cumple con los requisitos de formato establecidos por el INE. Durante este evento solo se utilizó la aplicación de digitalización de escritorio para el escaneo, por lo que la aplicación PREP Móvil fue probada en ese momento.

Estos hallazgos se anexan en la plataforma puesta a disposición de la empresa para su atención inmediata.

Simulacro 19 de mayo de 2024.

Siendo las 8:00 se dieron cita en las oficinas del CCV1 personal del equipo auditor y el personal del IEEC para dar fe de la versión a utilizarse en el simulacro. Se pudo observar que el sistema de operación correspondía al auditado y con el de publicación en el sitio

https://simulacro836462.prepcampeche2024.mx/. Previo al arranque se verifica el inicio de la base de datos en ceros y con actualizaciones cada 20 minutos. Dando las 08:30 horas se verifica que se puede ingresar al sitio de publicación, se inició la captura y digitalización de las actas iniciando en los diferentes CATD como se puede observar en la Figura 7. De igual manera se realizo la validación del código Hash a través de la aplicación Figura 8 en donde se hizo la observación de que se podría generar en cualquier momento durante el simulacro para garantizar que en el proceso este siguiera sin alteraciones. En la agenda planeada para el simulacro del día 19 de mayo se establecieron 2 contingencias a verificar correspondientes al fallo del servicio del ISP en donde se haría un cambio al segundo servicio de ISP garantizando la continuidad del sistema PREP, por otro lado la segunda contingencia correspondía a una caída del firewall en donde se pudo constatar que la infraestructura de respaldo con la que cuenta la empresa proveedora del servicio solventaba la misma al entrar en funcionalidad al momento de haber una pérdida del primer firewall el segundo de manera ágil y al recuperarse del fallo devolver la operación al firewall principal.

Figura 7. Sitio de publicación simulacro 19 de mayo 2024

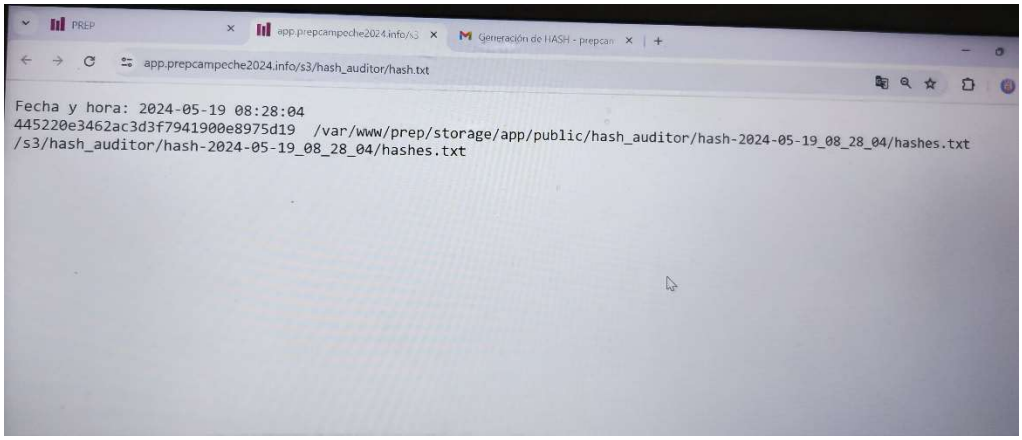


Figura 8. Generación del código Hash en el simulacro del 19 de mayo 2024

Durante el simulacro se pudo observar un flujo adecuado de la captura las actas desde todos los CATD de los diferentes municipios permitiendo observar tiempos satisfactorios de captura y comportamiento adecuado del sistema PREP en su operación, el proceso de captura y publicación de las actas finalizó con la captura de actas de diputaciones, ayuntamientos y juntas municipales alrededor de las 13:20 horas correspondientes al 100% de las actas establecidas para este segundo simulacro, en la Figura 9 se puede observar el correspondiente a la sección de Diputaciones.

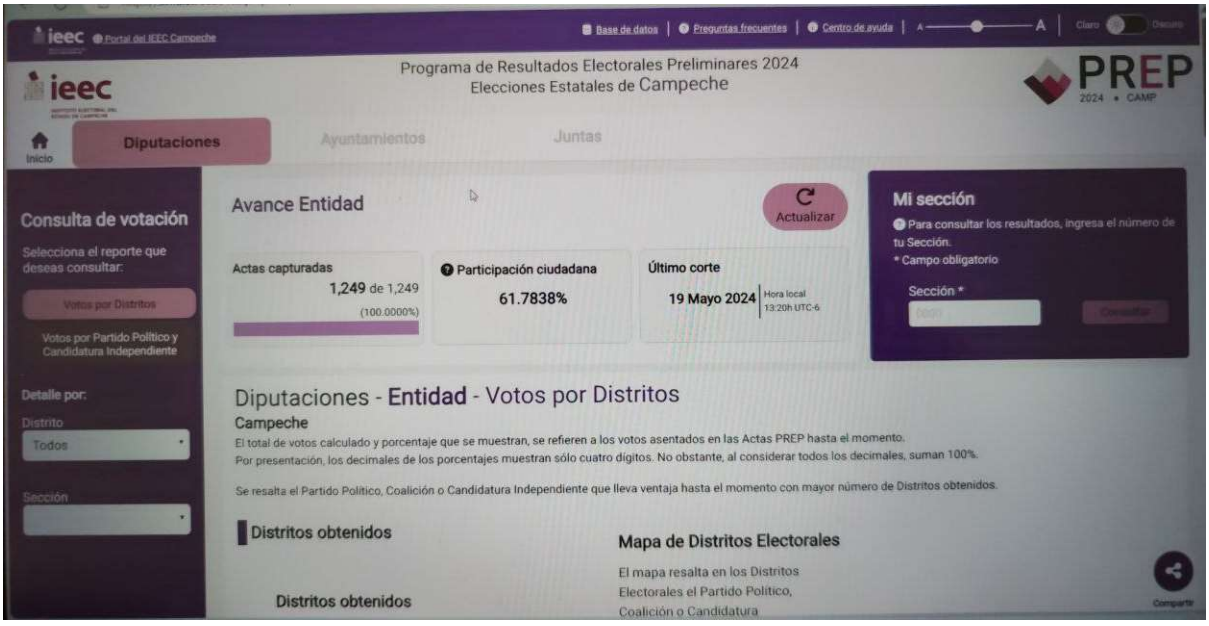


Figura 9. Total de actas capturadas en el simulacro correspondientes a Diputaciones

Simulacro 26 de mayo de 2024.

Durante el simulacro realizado el día 26 de mayo, se pudo observar que 11 de los hallazgos detectados en los ejercicios anteriores se han solventado, por lo que se actualizó el estatus en la plataforma de captura de hallazgos.

En la figura 10 se presenta el corte para cada una de las elecciones, identificando el avance de la entidad al último corte.

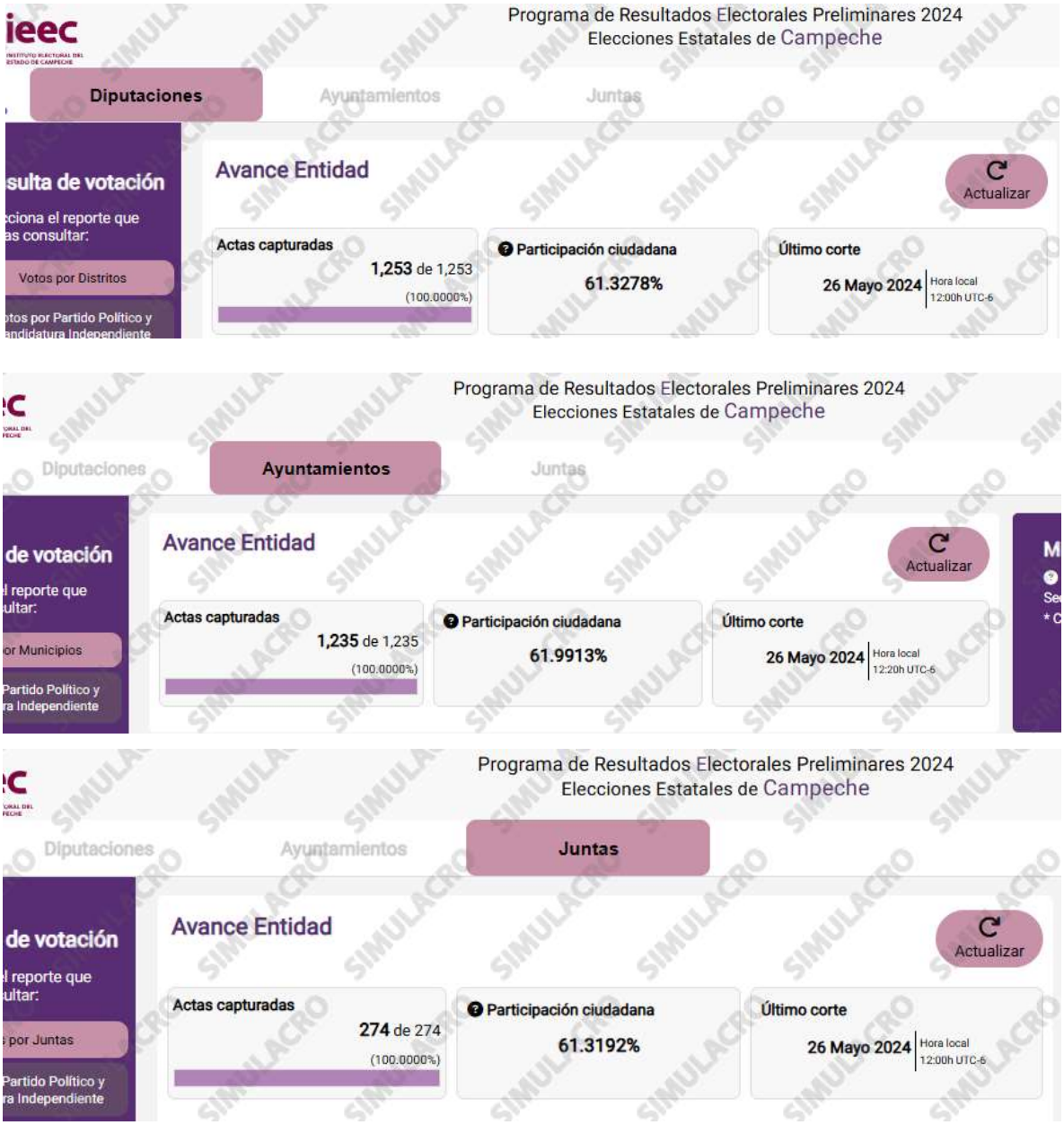


Figura 10 Actas capturadas para gubernatura, diputaciones, ayuntamientos y juntas municipales Simulacro 3

Al cierre de este simulacro todavía se encuentran 2 incidencias registradas como no atendidas, una de estas representa un cambio en la cantidad de votos asignada a cada partido para el tema de los votos que exceden la lista nominal.

Los hallazgos fueron modificando su estatus conforme la empresa indicó que aplicó los cambios requeridos, lo descrito fue solucionado y esto fue verificado con personal del equipo auditor.

La figura 11. Muestra la cantidad de hallazgos identificados y atendidos al cierre del tercer simulacro es importante mencionar que durante la revisión se registraron un incremento en los hallazgos debido a que se realizaron cambios durante cada uno de los simulacros.

Se observa que, de los 13 hallazgos, 11 fueron atendidos y 2 quedaron pendientes al cierre del 30 de mayo. De estos existen 6 de alto impacto que de no atenderse antes del 2 de junio pudieran representar problemas en la publicación relacionado a los aspectos visuales de la información.

Figura 11 Hallazgos identificados (atendidos y no atendidos)

Todos los hallazgos se encuentran presentados en el Anexo 1.

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

Este punto tiene como objetivo validar que el sistema informático del PREP que operará el día de la Jornada Electoral, corresponda al software auditado, así como que la base de datos se encuentre sin registros adicionales a los necesarios para que el sistema opere. Esta validación de la correspondencia del software auditado y el utilizado en la operación del PREP, se tendrá que realizar al inicio, durante y la final de la operación del sistema informático del PREP

El personal técnico que designe el ente auditor deberá llevar a cabo el proceso técnico para verificar que los programas auditados, así como la base de datos se encuentre debidamente

inicializada. Este procedimiento será validado por los miembros del Comité Técnico Asesor del PREP, así como por las personas que designe el IEEC.

Este procedimiento se llevará a cabo el domingo 2 de junio de 2024, a las 5:30 PM en las instalaciones que ocupe el Recinto Central, concluyendo el 3 de junio de 2024, y será atestiguado por la fe de un notario público que haya designado el IEEC, conforme a lo señalado en el inciso I del numeral 23, Capítulo I, Título III del Anexo 13 del Reglamento de Elecciones.

Para la validación este punto se estableció el procedimiento junto con los roles de cada usuario especificado a continuación:

La validación de la inicialización de las bases de datos y aplicaciones se realizar mediante huellas criptográficas generadas durante los simulacros y en la jornada electoral los flujos se presentan en las figuras 12 y 13.

Para la verificación de la base de datos en ceros se establece:

Se debe proporcionar un esquema de la base de datos identificando las tablas que contendrán los registros de votos.

Al inicio de la jornada electoral se verificará ante notario público que las tablas se encuentran vacías.

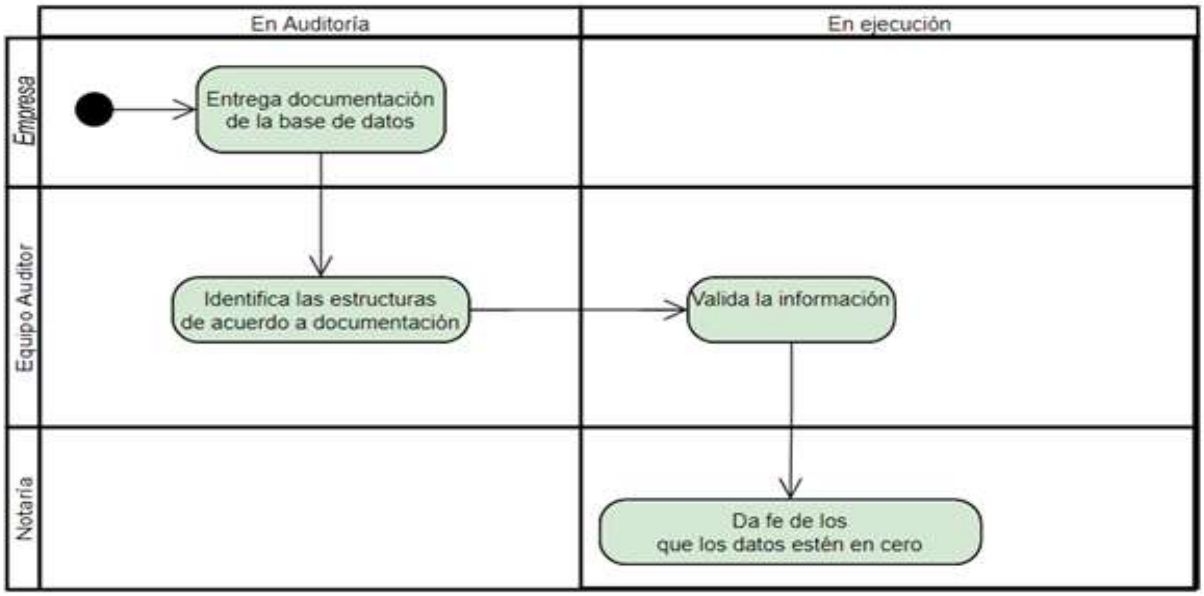


Figura 12 Flujo Base de datos en ceros

Para la verificación de las huellas criptográficas se establece:

Una vez que se tenga el software en la versión final y que haya sido aprobado por el ente auditor se crearán las huellas criptográficas de las bases de datos y aplicaciones del software inicializadas por personal de la empresa Informática Electoral S. C. y se firman mediante el algoritmo SHA256.

Para esto se requiere que la empresa Informática Electoral S. C. realice y entregue al ente auditor un inventario de todos los elementos que componen cada una de las aplicaciones y especifique su ubicación física de cada uno de ellos.

Se deberán considerar en el inventario y crear como mínimo las huellas criptográficas para los siguientes elementos:

a) Base de datos (script con la base de datos que se utilizará)
b) Página web del sitio de publicación
c) Aplicación para prep Móvil
d) Módulo de digitalización
e) Módulo de captura de datos
f) Módulo de verificación.

El proceso anterior se repetirá en el último simulacro y en la jornada electoral, durante el que se documentará cada elemento generado.

Posteriormente se realizará una validación de las huellas al principio, durante y al final de cada evento, comparando que coincida cada huella criptográfica generada.

Por último, se generarán las constancias de hechos, el ente auditor presentará el reporte detallando la coincidencia o no de las huellas realizado durante la validación. El proceso finaliza cuando el ente auditor presenta este reporte (sin incidencias) al notario y se procederá a firma la correspondiente constancia.

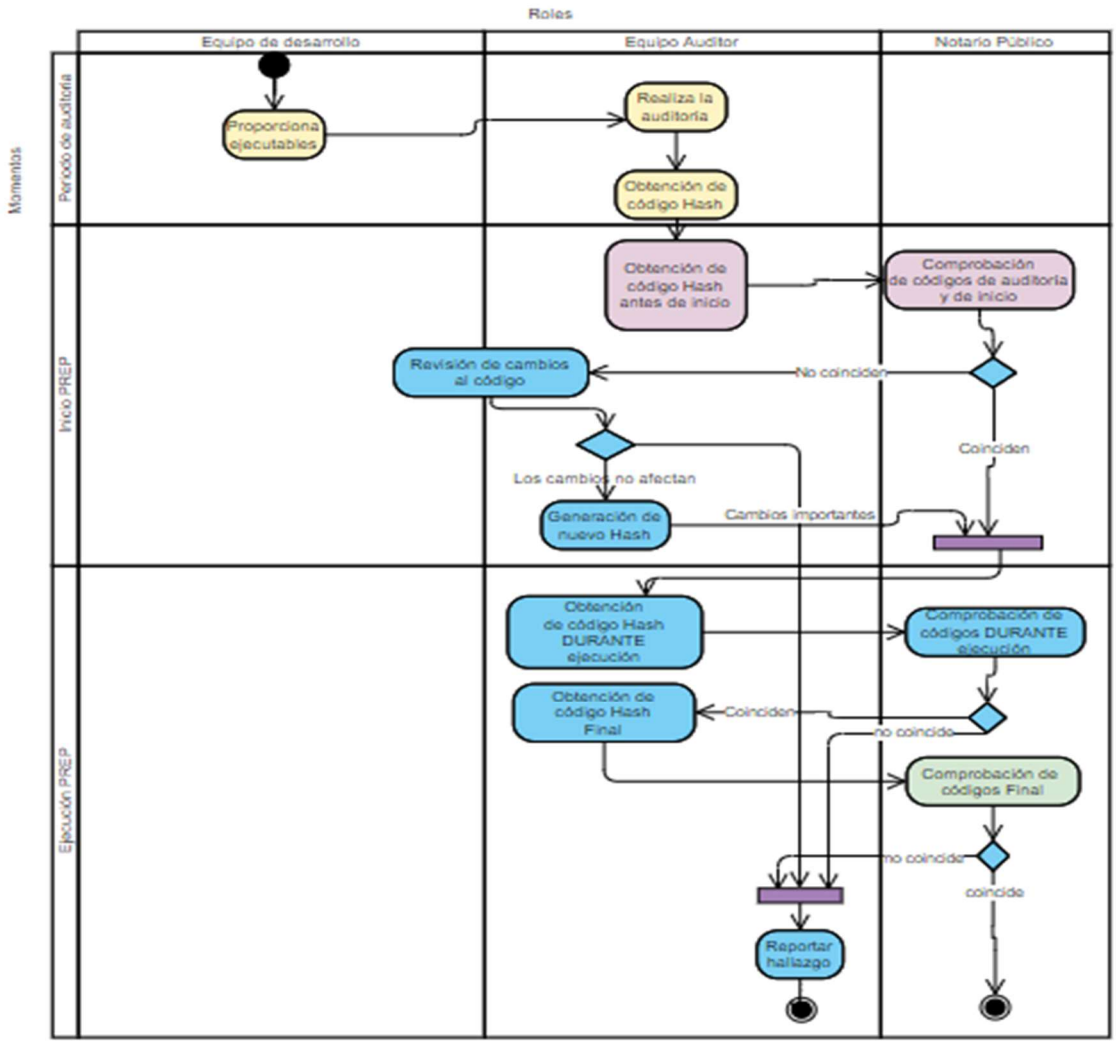


Figura 13 Flujo para la verificación de huellas criptográficas

Huellas criptográficas generadas en la última versión.

Una vez concluida la inspección visual y las pruebas de caja negra a cada uno de los módulos mencionados se firmaron digitalmente con los siguientes datos:

Archivo	Fecha y hora	SHA-256
hash 2024_05_31 v.txt	2024-05-31 11:13:50	acb3d78d7a2b14b98f99cec3d4fcbdb0962143d3ef2598e8468912b302e81d23

Tabla 3 SHA código fuente versión final

C) Análisis de vulnerabilidades de la infraestructura tecnológica

En este apartado se debe considerar tanto la infraestructura física como lógica de los diferentes subsistemas que componen el sistema PREP, así como la capacidad humana y estrategias que han sido seleccionadas para gestionarlos.

El principal objetivo de este análisis es identificar vulnerabilidades sobre los activos, documentarlos y minimizar o erradicar su impacto. Se determina que el proceso principal de riesgo para proteger es el que permite al sistema PREP llevar los datos recopilados en los diferentes centros de acopio a su publicación.

Descripción a bloques de la infraestructura física del sistema PREP

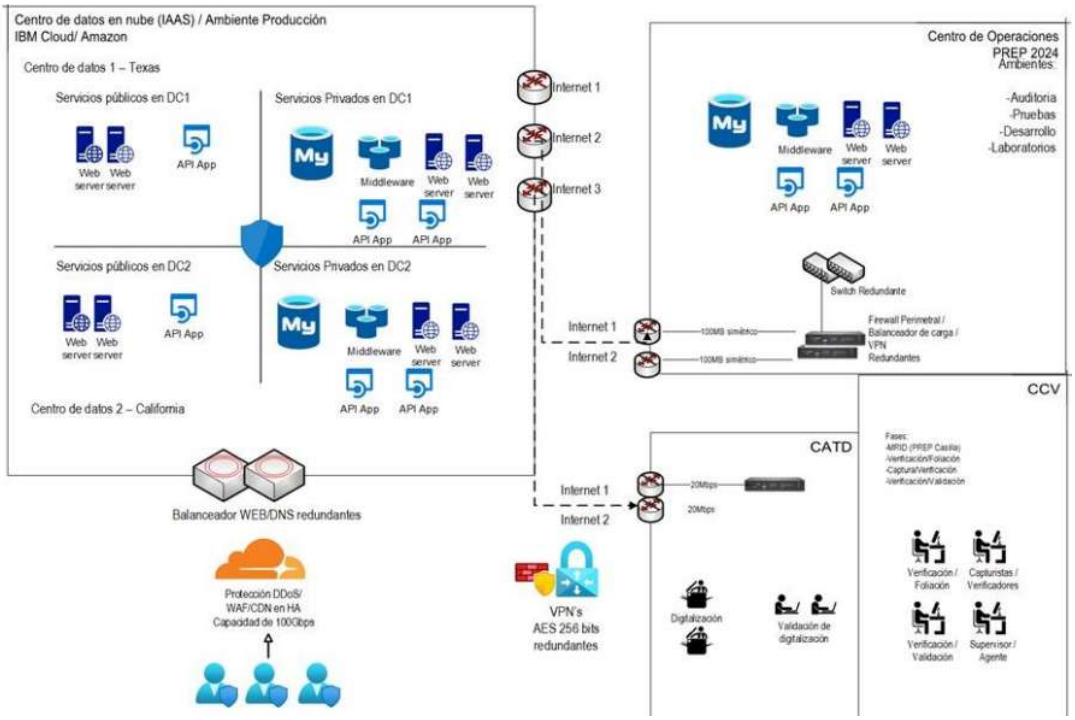


Figura 14 Distribución de infraestructura del PREP proporcionada por Informática Electoral en su Arquitectura del Sistema Informático PREP 2024 fuente: Informática electoral.

Objetivos

- Identificar debilidades de seguridad mediante la ejecución de pruebas de penetración, evasión de mecanismos de seguridad y pruebas de identificación de equipos(enumeración)
- Clasificar cada hallazgo de acuerdo con su impacto y urgencia para determinar una prioridad que permita al equipo PREP disminuir el riesgo.
- Verificar que las estrategias seguidas por el equipo PREP hayan atendido las vulnerabilidades reportadas

Alcance

Dentro del análisis se considerarán las redes tanto internas como externas que pueden afectar a la operación del sistema, además del sistema de recepción y publicación existente. El análisis de vulnerabilidades se realizó con base en tres etapas desde el

momento de implementación del centro de captura y verificación del equipo PREP(CCV) 1 y 2, así como a verificaciones en los CATD.

I. Presentación de hallazgos. Se presentó un informe previo con los hallazgos encontrados durante el análisis de vulnerabilidades, así como recomendaciones para atenderlos.
II. Validación de los hallazgos. El equipo PREP analizó y validó los hallazgos presentados por el equipo auditor con la finalidad de presentar estrategias y controles que minimicen el riesgo sobre los activos a proteger.
III. Atención de hallazgos. El equipo auditor validó los controles implementados para asegurar que los riesgos sobre las vulnerabilidades han sido minimizados.

Para realizar estas acciones se planearon dos aspectos a probar y evaluar: Las configuraciones de seguridad y Pruebas de penetración (Pentest).

Revisión de las configuraciones de seguridad.

Durante esta revisión se hicieron visitas a los CCV Principal y de respaldo, así como a algunos CATD para control. Se realizaron verificaciones de las configuraciones del Sistema Operativo, de las aplicaciones utilizadas, así como la infraestructura de continuidad de cada uno de ellos.

Hallazgos y recomendaciones

En este apartado se presentan los resultados de las visitas de control realizadas a cada una de las entidades arriba mencionadas.

Como es posible ver en la *Figura 14*, que se tienen 3 entidades principales por donde fluyen los datos hacia el servidor de concentración y posteriormente publicación.

CCV Principal o 1.

El acceso a esta área es restringido usando puntos de revisión a través de mecanismos de credencialización. Además, para cada visitante registrado se lleva una bitácora de entrada-salida.

El área de captura dentro de este lugar está protegida igualmente por un segundo punto de revisión.

Los equipos de comunicaciones se encuentran dentro del área de captura.

Existe una persona encargada de monitorear los accesos externos y permitir a visitantes dicho acceso. Además, un coordinador se encarga de monitorear el área de captura a través de cámaras de vigilancia.

El sistema operativo de los equipos de cómputo es instalado a través de una imagen y la configuración de hardware de cada uno de ellos es idéntico. El acceso a cada equipo es restringido a través de un usuario y una contraseña.

CCV Respaldo o 2.

El acceso a esta área es menos restringido, se encuentra un único punto de acceso a través de credenciales y una bitácora de registro en el mismo punto.

Al acceder se tiene acceso al área de captura, así como a los equipos de comunicaciones.

La imagen utilizada en los equipos de cómputo del CCV-1 también es utilizada en los del CCV-2 teniendo las mismas características.

CATD

Durante la revisión a siete centros de acopio se pudo acceder a las áreas PREP.

Las redes inalámbricas estuvieron activas todo el tiempo. Se puso a disposición, en ocasiones de continuidad, una red alterna para los casos de falla de internet. En una ocasión el responsable del CATD no conocía el procedimiento.

Tanto en el CCV-1 como en los CATD visitados se tienen plantas de energía para cualquier contingencia eléctrica. En una de las visitas se hicieron funcionar para garantizar el programa de continuidad.

Recomendaciones

Es recomendable que los equipos estén actualizados antes de la jornada electoral para evitar cualquier situación.

En todas las entidades mencionadas, es necesario que durante la jornada electoral las redes inalámbricas estén deshabilitadas, al menos en los CATD.

Es necesario que los responsables en las diferentes áreas, de acuerdo con su rol conozcan los procesos de continuidad del servicio para garantizar el funcionamiento de este.

Pruebas de Penetración (Pentest)

Estas pruebas se realizaron principalmente en los equipos de telecomunicaciones y servidores Web.

Como activo principal de análisis se tiene la publicación de datos a través de los medios propuestos: página web oficial, difusores, página del instituto electoral.

Hallazgos y recomendaciones

Pruebas a dispositivos de comunicación.

Se realizaron pruebas a los activos de telecomunicaciones encontrando redes inalámbricas próximas a los equipos de comunicación.

Los equipos conectados a la red de capturas utilizan direcciones estáticas para su conexión. Todos los equipos tienen acceso a internet limitados por el firewall. El acceso a internet se realiza a través de una línea dedicada, sin embargo, como se puede ver en la Figura 11, existe una línea de respaldo que permite la continuidad del servicio.

Se realizaron pruebas de DDoS a las direcciones https://simulacro836462.prepcampeche2024.mx/ en donde se simularon cargas similares a los de la jornada electoral propuestas por el INE, y cargas mayores a las propuestas. Los resultados determinaron que la dirección con IP asignada [104.22.15.177, 172.67.4.113, 104.22.14.177] responde de manera favorable a las pruebas realizadas.

Después de analizar la dirección se detectaron 4 puertos abiertos: 80, 443, 8080 y 8443.

Se realizó una prueba para tratar de acceder a datos en un CATD a través de ingeniería social. Se logró obtener a través de un digitalizador las cuentas de digitalización de un CATD y acceso a información sensible.

Recomendaciones

Es necesario revisar el tema de los difusores, el objetivo principal de tener difusores es tener repetidores de la información para cualquier eventualidad, hacer que toda la información sea consultada sobre la misma línea es un riesgo alto del sistema.

Es necesario trabajar cercanamente con los roles de más bajo nivel en dos aspectos: el primer aspecto es sobre lo que hay que hacer cuando se produce un evento que evite seguir con el proceso de digitalización/captura/validación; el segundo es sobre la seguridad de la información que manejan, es importante que dicha información no sea proveída a personas que no sean plenamente identificados dentro del sistema.

Anexos

Id	Descripción del hallazgo	Impacto	Estado	Fecha identificación	Módulo
1	El campo de usuario no es sensible a mayúsculas y minúsculas lo que representa un riesgo. Al hacer la prueba en el paso 2 nos dimos cuenta de que al cambiar el usuario a letras mayúsculas y con la contraseña correcta iniciaba sesión y dejaba entrar al sistema de capturista, se realizó la prueba con los 3 perfiles repetidas veces y presentando el mismo comportamiento.	**Bajo**	**No Atendida**	**17-04-2024**	**Todos**
2	Al ingresar al sistema con un usuario erróneo completamente diferente al correspondiente se da acceso al sistema	**Alto**	**Atendida**	**17-04-2024**	**Todos**
3	Durante el proceso de digitalización y captura de un acta, aquellas que llegan al módulo MRI por incidencia y esta requiera que el digitalizador vuelva a enviar la imagen del acta, no existe en el sistema una opción para que el digitalizador pueda consultar o identificar las actas que requieren esta acción.	**Medio**	**Atendida**	**19-04-2024**	**MCAD**
4	El sistema al momento de estar capturando un acta permite ingresar una fecha u hora fuera de la establecida para el acopio en PREP (18:00 horas del primer día hasta las 20:00 del segundo día). Para el caso de las pruebas las fechas disponibles eran desde el 17 de abril a las 18:00 hasta el 18 de abril a las 20:00 se realizan 6 casos para capturar entre el 16 y 17 de abril en horarios en un rango de 10:00 a 12:00	**Medio**	**Atendida**	**19-04-2024**	**Foliador**
5	Desde el inicio de la prueba el día 19 de abril, se intentaron forzar incidencias para su tratado en el módulo de verificación, sin embargo, se observó un tiempo prolongado desde su reporte hasta su visualización en el módulo. Este tiempo de retraso fue de aproximadamente 1 hora.	**Alto**	**Atendida**	**17-04-2024**	**MRI**

6	Al hacerse las pruebas de acta con un dato ilegible, no se visualizó la incidencia en el módulo MRI correspondiente para su resolución debido a un error en el flujo.	**Medio**	**Atendida**	**17-04-2024**	**MRI**
7	Se realizó la digitalización de un acta sin datos, en donde los capturistas 1, 2 y 3 no coincidieron en su captura por lo cual el acta se envía a módulo MRI. El usuario del módulo MRI recibe el acta y captura los campos con ceros y el acta se envía a COTEJO para su validación, el usuario de COTEJO rechaza el acta devolviendo al módulo MRI provocando que este usuario se mantenga bloqueado con el acta que recibió	**Medio**	Atendida	**19-04-2024**	**MRI**
8	Al digitalizar un formato de incidencia de acta (ausencia de acta PREP) esta debe llegar al MRI solamente, sin embargo, se observa que esta también pasa directamente a cotejo para su validación pudiendo generar inconsistencias entre el MRI y cotejo.	**Alto**	Atendida	**19-04-2024**	**MRI**
9	Actualmente, al seleccionar la opción de 'acta mal identificada' en el módulo MRI, se otorga un tiempo límite de un minuto para realizar las correcciones necesarias. Sin embargo, este periodo resulta insuficiente para que el verificador pueda realizar una revisión exhaustiva y precisa de los datos, lo que incrementa el riesgo de errores humanos durante el proceso.	**Medio**	Atendida	**19-04-2024**	**MRI**
10	En la sección de "Detalles de votos por casilla" no se debe visualizar las incidencias de las actas de los casos: Sin acta por paquete no entregado, Sin acta por casilla no instalada, Sin acta por paquete entregado sin bolsa, es decir, si un acta tiene alguna incidencia como por ejemplo "Sin acta por paquete no entregado" estas no se deberían visualizar.	**Alto**	**Atendida**	**17-04-2024**	**Publicación**
11	En los apartados "Diputaciones" no se visualiza el botón de votos anticipados de acuerdo con lo establecido en los cambios solicitados por el INE al prototipo navegable del día 28 de marzo.	**Alto**	**Atendida**	**17-04-2024**	**Publicación**
12	No se encuentra el apartado de Representación proporcional en el nuevo prototipo de la página web	**Alto**	**Atendida**	**19-04-2024**	**Publicación**

13	El sitio de publicación no muestra la etiqueta de Excede Lista Nominal en los casos en que se excede de 1 a 14 votos en donde se suman a la lista nominal 14 votos de manera fija correspondientes al campo de Personas y Representantes que votaron.	**Medio**	**No atendida**	**23-05-2024**	**Publicación**