CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS DEL INSTITUTO POLITÉCNICO NACIONAL

UNIDAD TAMAULIPAS

Servicios de Auditoría al Sistema Informático y a la Infraestructura Tecnológica del Programa de Resultados Electorales Preliminares de las elecciones locales del Estado de Tamaulipas para el año 2021

Informe Final de Auditoría al PREP 2021

V1.0

Ciudad Victoria, Tamaulipas. 5 de junio de 2021

Versión	1.0
Fecha de elaboración	Junio 5, 2021

HISTORIAL DE VERSIONES	
Número de Versión	1.0
Fecha de actualización	Junio 5, 2021
Responsable de la actualización	Javier Rubio-Loyola
Resumen de la actualización	Recopilación de información y revisión final

RESPONSABLES	
De la elaboración	José Luis González Compeán
Organización	Cinvestav Unidad Tamaulipas
Puesto	Líder de la capa 1: Datos
De la elaboración	Edwin Aldana Bobadilla
Organización	Cinvestav Unidad Tamaulipas
Puesto	Líder de la capa 2: Aplicaciones
De la elaboración	José Zapata Lara/Javier Rubio Loyola
Organización	Cinvestav Unidad Tamaulipas
Puesto	Líderes de la capa 3: Plataforma tecnológica
De la elaboración	José Zapata Lara/Javier Rubio Loyola
Organización	Cinvestav Unidad Tamaulipas
Puesto	Líderes de la capa 4: Infraestructura de comunicaciones
De la elaboración	Iván López Arévalo
Organización	Cinvestav Unidad Tamaulipas
Puesto	Líder de la capa 5: Nivel operativo

RESPONSABLES	
De la revisión	Javier Rubio Loyola
Organización	Cinvestav Unidad Tamaulipas
Puesto	
Firma	
De la aprobación	Javier Rubio Loyola
Organización	Cinvestav Unidad Tamaulipas
Puesto	Líder del Proyecto
Firma	

TABLA DE CONTENIDO

LISTADO DE TABLAS

LISTADO DE FIGURAS

ACRÓNIMOS Y ABREVIACIONES

AEC	Acta de Escrutinio y Cómputo.
CAEL	Capacitador-Asistente Electoral Local
CATD	Centro de Acopio y Transmisión de Datos.
CATD	Centro de Acopio y Transmisión de Datos
CCV	Centro de Captura y Verificación
CINVESTAV	Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional
CRID	Centro de Recepción de Imágenes y Datos.
IDS/IPS	Intruder Detection System/Intruder Protection System
IETAM	Instituto Electoral de Tamaulipas.
INE	Instituto Nacional Electoral
JSON	JavaScript Object Notation
ISP	Internet Service Provider
MCAD	Monitor de Captura de Actas Digitalizadas.
OPL	Organismos Públicos Locales
ORM	Mapeo Relacional de Objetos
PENTEST	Pruebas de penetración
PI-CATD-CCV	Planos de Instalación de CATD y CCV
PREP	Programa de Resultados Electorales Preliminares.
PREP 2021	Programa de Resultados Electorales Preliminares para el año 2021
PREP Casilla	Aplicación móvil que permitirá realizar la toma fotográfica del acta PREP y su envío para su captura.
PROVEEDOR	Desarrollador del PREP del IETAM
PTO	Proceso Técnico Operativo
SLA	Acuerdo de Nivel de Servicio
TCA	Terminal de Captura de Actas.
UML	Unified Modeling Language

Resumen

En este documento se presenta el Informe Final de Auditoría al Sistema Informático y a la Infraestructura Tecnológica del Programa de Resultados Electorales para el Proceso Electoral Ordinario Local 2020-2021 (PREP) encargado a la Unidad Tamaulipas del Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional. Este informe comprende las actividades desarrolladas por el Ente Auditor en el período comprendido entre el 5 de marzo y el 5 de junio de 2021. Los servicios de auditoría consideraron de forma general los siguientes aspectos:

i. Pruebas funcionales de caja negra al sistema informático para evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares.
ii. Análisis de vulnerabilidades considerando pruebas de penetración y revisión de configuraciones a la infraestructura tecnológica del PREP.

El proceso de revisión se llevó a cabo apegado a las líneas de acción establecidas por el Instituto Nacional Electoral y una quinta línea de acción agregada por Cinvestav:

LA1. Pruebas funcionales de caja negra al sistema informático del PREP 2021.
LA2. Validación del sistema informático del PREP y de sus bases de datos.
LA3. Análisis de vulnerabilidades a la infraestructura tecnológica.
LA4. Pruebas de denegación de servicio al sitio web del PREP y al sitio principal del OPL.
LA5. Pruebas de usabilidad y experiencia de usuario.

Para llevar a cabo todo el proceso de auditoría se siguió un modelo desarrollado por el Cinvestav organizado en 5 capas:

Capa 1. Datos y almacenaje de las actas de escrutinio e información capturada.
Capa 2. Aplicaciones que contiene el conjunto de herramientas y programas de cómputo para llevar a cabo el procesamiento y presentación de los resultados del PREP.
Capa 3. Plataforma tecnológica usada por todas las aplicaciones incluyendo dispositivos de cómputo y sistemas operativos.
Capa 4. Infraestructura de comunicaciones a desplegar para llevar a cabo la transmisión de información y la publicación de los resultados.
Capa 5. Operación integral de todos los procesos del PREP en los diferentes niveles.

En cada nivel se aplicó un análisis considerando los siguientes ejes transversales:

A) Requerimientos funcionales.
B) Requerimientos no-funcionales.
C) Aspectos de seguridad en la información.
D) Buenas prácticas de seguridad lógica y física.
E) Análisis de vulnerabilidades
F) Análisis de riesgos.

El proceso completo de auditoría al PREP se llevó a cabo en dos fases. La **fase 1** realizó los servicios de revisión del sistema completo y la entrega de informes parciales de acuerdo con las líneas de trabajo (LA1 a LA5). La **fase 2** incluye la revisión de la operación del PREP acorde con las líneas de trabajo identificadas por el INE durante una prueba celebrada el 21 de abril de 2021 y los tres simulacros realizados el 16, 23 y 30 de mayo de 2021.

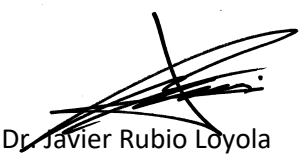
En la primera parte del documento, se revisa de manera breve el Programa de Resultados Electorales Preliminares. Posteriormente describe el alcance de los servicios de auditoría al PREP. Se procede a continuación a revisar las líneas de acción para los servicios de auditoría al PREP establecidos por el INE.

En la segunda parte del documento se presentan los resultados generales de la implementación del Proceso Técnico Operativo para el PREP.

En la tercera parte, se presentan los resultados de cada una de las líneas de acción establecidas por el INE y la quinta línea definida por Cinvestav. En la cuarta parte se presenta el resumen del análisis de riesgos para la operación del PREP y el dictamen de la revisión.

Este documento consta de 171 páginas y ha sido elaborado por la Unidad Tamaulipas del Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional, designado como Ente Auditor por el Instituto Electoral de Tamaulipas.

Ciudad Victoria, Tamaulipas, a 5 de junio de dos mil veintiuno.



Dr. Javier Rubio Loyola
Ente Auditor
Cinvestav-IPN
Unidad Tamaulipas

Dictamen

Con base en la revisión llevada a cabo entre el 5 de marzo y el 5 de junio de 2021 de la implementación del Proceso Técnico Operativo para el Programa de Resultados Electorales Preliminares del Estado de Tamaulipas para el proceso electoral 2020-2021, el Ente Auditor hace constar que:

1. El sistema informático y sus bases de datos auditados cumplen con los requerimientos funcionales para la operación del PREP durante la jornada electoral del próximo 6 de junio de 2021.
2. Se ha definido un procedimiento técnico metodológico para garantizar que el sistema informático auditado es el que se utilizará durante la jornada electoral del 6 de junio de 2021.
3. El procedimiento técnico metodológico también valida que las bases de datos a usar antes del inicio del PREP, el 6 de junio de 2021, estarán en un estado inicial con todos sus contadores en cero.
4. La implementación del proceso técnico operativo cumple en lo general con las buenas prácticas de seguridad y operación confiable.
5. El sistema informático cumple en lo general con los estándares de seguridad informática que permiten asegurar que está libre de las vulnerabilidades más conocidas.
6. Se han realizado las configuraciones necesarias y se han tomado las previsiones establecidas por las buenas prácticas de seguridad informática para que, el sistema informático del PREP, así como los sitios de publicación de resultados, puedan resistir los ataques informáticos más conocidos incluidos los que se refieren a los ataques de denegación de servicio básicos.

El presente informe se emite en Ciudad Victoria, Tamaulipas, el cinco de junio de dos mil veintiuno.

Dr. Javier Rubio Loyola
Ente Auditor
Cinvestav-IPN
Unidad Tamaulipas

Parte I

Informe Preliminar de Auditoría al PREP 2021

1. Introducción

El 6 de junio de 2021 se llevarán a cabo elecciones locales en el Estado de Tamaulipas como parte del Proceso Electoral Local Ordinario 2020-2021 en el Estado de Tamaulipas. El Instituto Electoral de Tamaulipas (IETAM) ha sido el encargado de la organización de las elecciones. Como parte de la normatividad aplicable, el IETAM ha sido encargado de instrumentar un Programa de Resultados Preliminares (PREP) mismo que el día de la elección tiene la función de difundir los resultados preliminares (no oficiales) de la elección. La instrumentación del PREP se debe iniciar con varios meses de anticipación al día de la jornada electoral y durante dicho periodo se debe llevar a cabo la implementación del PREP, una prueba, tres simulacros de su operación general, y su operación real en el día de la jornada electoral el cual concluye normalmente a las 20:00 horas del día siguiente al de la elección.

El reglamento del Instituto Nacional Electoral establece que los OPL deberán designar un ente auditor, preferentemente una institución académica con experiencia, para llevar a cabo la auditoría del PREP. La auditoría al PREP debe cubrir como mínimo las pruebas de caja negra a todos los procesos del sistema informático y el análisis de vulnerabilidades del sistema informático provisto para el PREP. El INE ha establecido las siguientes líneas de trabajo para llevar a cabo los servicios de auditoría al sistema informático y a la infraestructura tecnológica del PREP: 1) Pruebas funcionales de caja negra al sistema informático del PREP 2021, 2) Validación del sistema informático del PREP y de sus bases de datos, 3) Análisis de vulnerabilidades a la infraestructura tecnológica, y 4) Pruebas de negación de servicio al sitio web del PREP y al sitio principal del OPL. De manera adicional, Cinvestav ha evaluado una quinta línea de trabajo; 5) Pruebas de usabilidad y experiencia de usuario.

En este documento, la Unidad Tamaulipas del Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional (Cinvestav) presenta los resultados de los servicios de auditoría informática al PREP para el año 2021 para el Instituto Electoral de Tamaulipas (IETAM). Los servicios de auditoría han tomado como base la información presentada en el documento “Anexo Técnico para la Contratación de Servicios de Auditoría al Sistema Informático y a la Infraestructura Tecnológica del Programa de Resultados Electorales” emitido por el Instituto Electoral de Tamaulipas, así como también ha considerado las líneas de trabajo establecidas en el documento emitido por el INE “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”. Finalmente, los servicios de auditoría han tomado en consideración los “Lineamientos para la operación del Programa de Resultados Preliminares de las elecciones locales de 2021 en el estado de Tamaulipas”, en el que el IETAM ha descrito los alcances del PREP y las especificaciones funcionales de cada uno de los procesos que componen el programa.

En el Sistema PREP usualmente están involucrados tanto recursos humanos como herramientas de tecnologías de información y comunicaciones integrados en **procesos técnicos operativos** (PTO) que tienen como propósito dar certidumbre a los resultados de los procesos electorales. El proceso técnico operativo considera el flujo de información que inicia con la copia de un acta de escrutinio y termina hasta su procesamiento para contar los votos registrados en el acta en cada uno de los candidatos registrados en los procesos electorales. Este flujo de información pasa por varias etapas que incluye: 1) el acopio de actas de escrutinio, 2) la digitalización de las actas, 3) la captura, 4) validación, y 5) cotejo

de la información para su posterior publicación, 6) la publicación de los resultados agrupados en diferentes niveles, y 7) el empaquetado de todas las actas de escrutinio en los centros de acopio y transmisión de datos.

El Reglamento de Elecciones del INE, Sección Cuarta - Del Sistema Informático y su Auditoría, Artículo 347 establece que,

1. El Instituto y los OPL deberán someter su sistema informático a una auditoría de verificación y análisis, para lo cual se deberá designar un ente auditor. El alcance de la auditoría deberá cubrir, como mínimo, los puntos siguientes:
   a. Pruebas funcionales de caja negra al sistema informático para evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares.
   b. Análisis de vulnerabilidades, considerando al menos pruebas de penetración y revisión de configuraciones a la infraestructura tecnológica del PREP.

2. Para la designación del ente auditor se dará preferencia a instituciones académicas o de investigación y deberá efectuarse a más tardar, cuatro meses antes del día de la jornada electoral. El ente auditor deberá contar con experiencia en la aplicación de auditorías con los alcances establecidos en el numeral anterior.

El reglamento del Instituto Nacional Electoral establece que los OPL deberán designar un ente auditor, preferentemente una institución académica con experiencia, para llevar a cabo la auditoría del PREP.

Así también, con base en el documento generado por el Instituto Nacional Electoral, “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 han identificado cuatro líneas de acción mínimas requeridas por el INE, así como una quinta línea de trabajo que Cinvestav considera importante evaluar, de modo que para el PREP del IETAM se definen cinco líneas de acción:

LA1. Pruebas funcionales de caja negra al sistema informático del PREP 2021.
LA2. Validación del sistema informático del PREP y de sus bases de datos.
LA3. Análisis de vulnerabilidades a la infraestructura tecnológica.
LA4. Pruebas de negación de servicio al sitio web del PREP y al sitio principal del IETAM.
LA5. Pruebas de usabilidad y experiencia de usuario.

La metodología que siguió el ente auditor organiza todos los servicios de auditoría informática en actividades que se ubican de acuerdo a un modelo en capas organizado en los siguientes niveles:

1) Datos y almacenaje de las actas de escrutinio e información capturada.
2) Aplicaciones que contiene el conjunto de herramientas y programas de cómputo para llevar a cabo el procesamiento y presentación de los resultados del PREP.
3) Plataforma tecnológica usada por todas las aplicaciones incluyendo dispositivos de cómputo y sistemas operativos.
4) Infraestructura de comunicaciones a desplegar para llevar a cabo la transmisión de información y la publicación de los resultados.

5) Operación integral de todos los procesos del PREP en los diferentes niveles para completar el flujo de información de 7 pasos descrito anteriormente.

Así también, como parte de la metodología, en cada nivel se han clasificado las actividades para la revisión de los siguientes aspectos transversales:

A) Requerimientos funcionales
B) Requerimientos no-funcionales
C) Aspectos de seguridad en la información
D) Buenas prácticas de seguridad lógica y física
E) Análisis de vulnerabilidades
F) Análisis de riesgos.

El modelo de cinco capas con los seis aspectos transversales a cada capa permite identificar claramente a los diferentes actores, técnicos, informáticos, de infraestructura y comunicaciones que participan en cada línea de acción. Así también, permite dimensionar el esfuerzo en la realización de la auditoría informática.

El proceso completo de auditoría al PREP se llevó a cabo en dos fases. La **fase 1** realizó los servicios de revisión del sistema completo y la entrega de informes parciales de acuerdo con las líneas de trabajo (LA1 a LA5). La **fase 2** incluye la revisión de la operación del PREP acorde con las líneas de trabajo identificadas por el INE durante una prueba celebrada el 21 de abril de 2021 y los tres simulacros realizados el 16, 23 y 30 de mayo de 2021, el día de la jornada electoral (6 de junio de 2021) y la entrega del informe final (21 de junio de 2021).

2. El Programa de Resultados Electorales Preliminares

De acuerdo con el Instituto Nacional Electoral, el Programa de Resultados Electorales Preliminares es el mecanismo de información electoral encargado de proveer los resultados preliminares y no definitivos, de carácter estrictamente informativo a través del acopio, digitalización, captura, verificación y publicación de los datos asentados en las actas de escrutinio y cómputo de las casillas que se reciben en los Centros de Acopio y Transmisión de Datos autorizados por el Instituto Nacional Electoral o por los Organismos Públicos Locales.
El PREP está conformado por recursos humanos, materiales, procedimientos operativos, procedimientos de digitalización y publicación, seguridad y tecnologías de la información y comunicaciones. Las características, así como reglas de implementación y operación son emitidas por el Instituto Nacional Electoral a través los Lineamientos del Programa de Resultados Electorales Preliminares. Una organización típica de las diferentes organizaciones se presenta en la Figura 1.

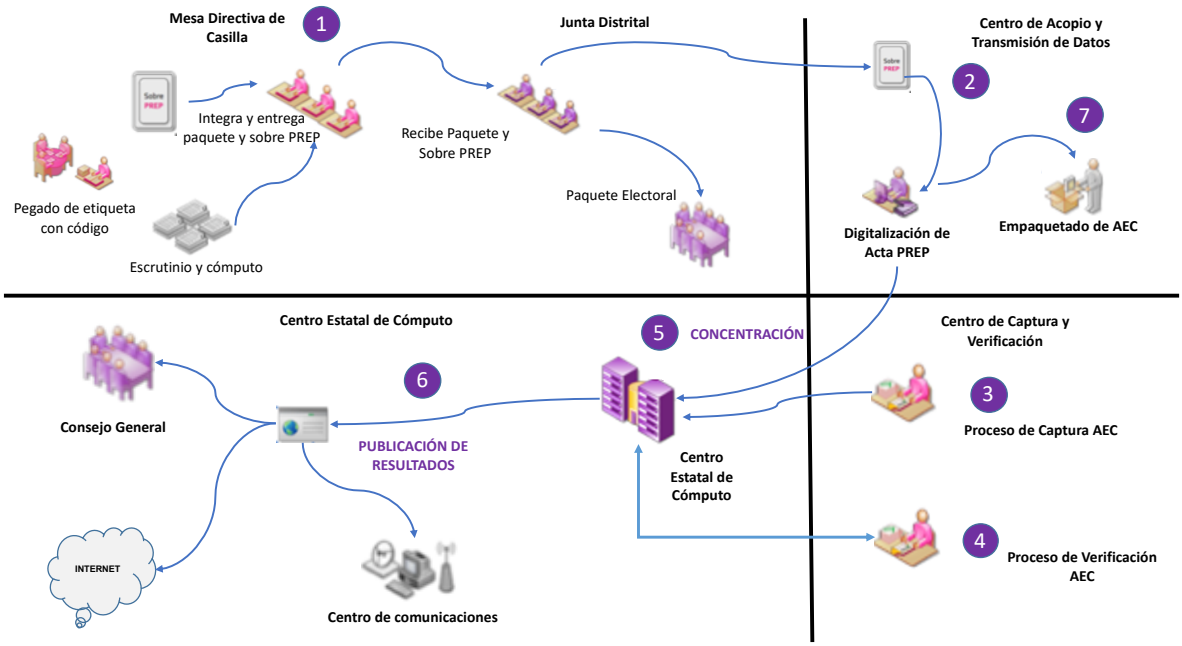


Figura 2.1. Centros de información típicos que participan en un PREP.

En la Mesa Directiva de Casilla se realiza el escrutinio y cómputo de los votos emitidos y se integra un paquete electoral, el cuál es entregado en el Consejo Electoral a que corresponde la casilla. En el Centro de Acopio y Transmisión se procede al acopio y digitalización (en algunos casos específicos se realiza captura) y se realiza el envío de la información a los centros de captura y verificación en donde se captura y verifica la información capturada con la imagen digital del Acta. Hecho lo anterior, se procede a su publicación.

La instrumentación del PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES (PREP) consiste de todos los elementos y requerimientos tecnológicos, de equipamiento, personal, capacitación, planeación y logística que sean necesarios para implementar el sistema informático. La infraestructura de procesamiento y comunicación juega un papel importante en el despliegue del PREP y los elementos más distintivos de una infraestructura típica para el mismo se pueden apreciar en la Figura 2. A través de una red de enlaces locales y remotos se integran los diversos centros de captura para transmitir la información obtenida en los centros de acopio hacia los servidores centrales en donde se almacena,

procesa, contabiliza y se generan los reportes correspondientes de la jornada electoral. Los resultados contabilizados son publicados hacia los servicios del propio OPL y hacia los difusores previamente autorizados por el OPL. Por la naturaleza de la información con los resultados de la jornada electoral, son esenciales los mecanismos de seguridad informática que aíslen los resultados de la jornada con posibles atacantes con el propósito de interferir en los resultados electorales. Los cortafuegos son uno de los mecanismos típicamente usados, pero no son los únicos. Adicionalmente se pueden incorporar, detectores de intrusos, mecanismos de control de acceso, herramientas para la protección de la información contra alteraciones maliciosas, cifrado de comunicaciones, por citar algunos de los más usados.

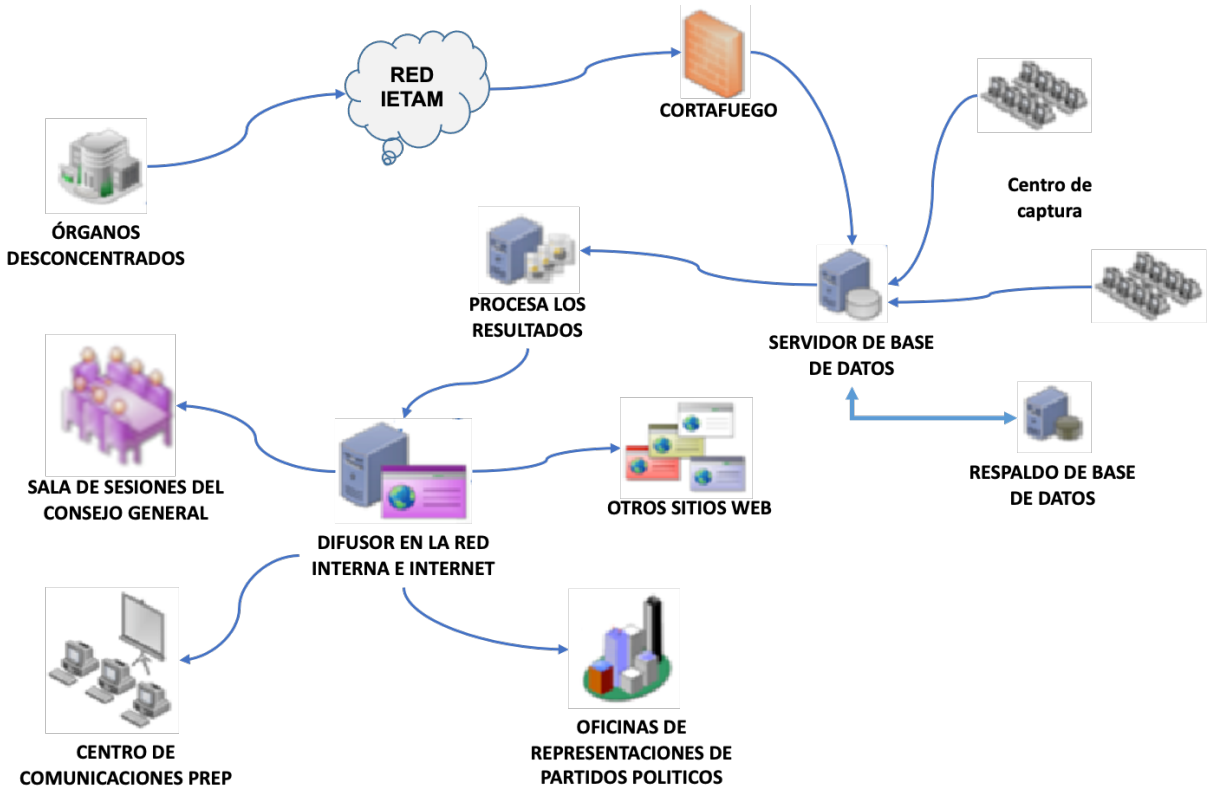


Figura 2.2. Infraestructura típica usada en un Sistema PREP.

Entre otros aspectos, la instrumentación del PREP considera al menos los siguientes elementos:

- Descripción detallada de la arquitectura de la solución propuesta.
- Detalle de la tecnología e infraestructura a utilizar.
- Detalle de la arquitectura de seguridad. Detalle de la solución propuesta para la publicación en Internet, específicamente el ancho de banda de los sitios en que se realizará la publicación y la justificación del por qué el ancho de banda seleccionado se considera suficiente.
- Detalle del esquema de tolerancia a fallas que tiene previsto el sistema.
- Descripción a detalle de los módulos del programa de computo, describiendo su arquitectura, funcionalidad, entradas y salidas.
- Requerimientos de espacio y su acondicionamiento para la ubicación del personal y la instalación del equipo.
- Estructura del personal requerido en la totalidad del proyecto.

- Plan y logística de implementación.
- Plan y logística de capacitación.
- Flujos de operación antes, durante y después del día de la elección.
- Normatividad a aplicar a los flujos del proceso.
- Método de captura a aplicar
- Diseño de los formatos de las pantallas preliminares del sistema.
- Diseño de los formatos de las pantallas preliminares de publicación.
- La información técnica, logística u operativa relevante.
- El análisis de riesgos en materia de seguridad de la información.
- Plan detallado de contingencias que garanticen la ejecución de los procedimientos de acopio, digitalización, captura, verificación y publicación, en caso de que se suscite una situación adversa o de contingencia.

3. Servicios de Auditoría al PREP

La auditoría externa al PREP permite la verificación y análisis de los sistemas informáticos utilizados en la implementación del Programa de Resultados Electorales Preliminares, con la finalidad de evaluar la integridad en el procesamiento de la información y la generación de los resultados preliminares conforme a los lineamientos establecidos para el mismo y a la normatividad aplicable.

El Reglamento de Elecciones del INE, Sección Cuarta - Del Sistema Informático y su Auditoría, Artículo 347 establece (entre otros aspectos) que:

1. El Instituto y los OPL deberán someter su sistema informático a una auditoría de verificación y análisis, para lo cual se deberá designar un ente auditor. El alcance de la auditoría deberá cubrir, como mínimo, los puntos siguientes:
   a) Pruebas funcionales de caja negra al sistema informático para evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares.
   b) Análisis de vulnerabilidades, considerando al menos pruebas de penetración y revisión de configuraciones a la infraestructura tecnológica del PREP.
2. Para la designación del ente auditor se dará preferencia a instituciones académicas o de investigación y deberá efectuarse a más tardar, cuatro meses antes del día de la jornada electoral. El ente auditor deberá contar con experiencia en la aplicación de auditorías con los alcances establecidos en el numeral anterior.

4. Líneas de Acción para los Servicios de Auditoría al PREP

Con base en el documento generado por el Instituto Nacional Electoral, “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” en el que se identifican cuatro líneas de acción mínimas requeridas por el INE, así como una quinta línea de trabajo que Cinvestav ha identificado, se han considerado cinco líneas de acción que se describen a continuación para el PREP del IETAM:

LA1. Pruebas funcionales de caja negra al sistema informático del PREP. El ente auditor analiza el sistema informático del PREP, mediante la realización de pruebas funcionales de caja negra, para evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares, conforme a lo establecido en el artículo 347, numeral 1, inciso a) del Reglamento de Elecciones.

LA2. Validación del sistema informático del PREP y de sus bases de datos. Se valida 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. La validación respecto a la correspondencia del software auditado y el utilizado en la operación del PREP, se realiza al inicio, durante y al final de la operación del sistema informático del PREP.

LA3. Análisis de vulnerabilidades a la infraestructura tecnológica. Se identifican debilidades de seguridad en la infraestructura tecnológica mediante la ejecución de pruebas de penetración y revisión de configuraciones de seguridad. Se clasifica el impacto y documentar las vulnerabilidades identificadas con el propósito de recomendar al IETAM las posibles medidas para la mitigación de las vulnerabilidades que previamente fueron identificadas y documentadas. Se verifica que las medidas implementadas por el IETAM hayan atendido adecuadamente las vulnerabilidades reportadas.

LA4. Pruebas de denegación de servicio a sitios web del PREP y al sitio principal del IETAM. El Ente Auditor realiza ataques de denegación de servicio que permitan identificar, evaluar y aplicar las medidas necesarias para asegurar la correcta y continua disponibilidad del servicio Web de los sitios de publicación de resultados del PREP y del sitio principal del IETAM, durante el periodo de operación del PREP.

LA5. Pruebas de usabilidad y experiencia de usuario. El ente auditor analiza la ergonomía de los aplicativos del PREP y analiza la experiencia de los usuarios de dichos aplicativos. Las pruebas de usabilidad y experiencia de usuario se realizan mediante un conjunto de pruebas no funcionales y análisis de buenas prácticas de aplicativos similares a los empleados por el PREP. Se diseñan y aplican cuestionarios para identificar y valorar el nivel de usabilidad y experiencia de usuario de cada uno de los aplicativos usados en el PREP. Se identifican y documentan aspectos a mejorar en la usabilidad y experiencia de los aplicativos. Se verifica que las medidas implementadas por los desarrolladores del PREP hayan sido atendidas.

Parte II

5. Resultados de la implementación del Proceso Técnico Operativo

5.1 Nivel 5: Operativo

En esta sección se describen las actividades realizadas en la revisión de la implementación del Proceso Técnico Operativo.

5.1.1 Justificación

El objetivo de esta auditoría es determinar el grado de cumplimiento del sistema informático PREP de acuerdo con el PTO del proceso PREP. La auditoría contempla todas aquellas actividades que los operadores del sistema informático pueden realizar con base en el PTO. Esto supone que los elementos de base de datos, aplicación, plataforma y comunicaciones funcionan adecuadamente de acuerdo con los lineamientos del INE e IETAM. Asumiendo esto último todas las indicaciones del PTO deben cumplirse.

5.1.2 Elementos considerados

Con base en las definiciones e indicaciones del PTO del proceso PREP, se identificó lo siguiente del sistema informático PREP:

a) Las tareas que se realizan. Esto contempla todas las operaciones que permite realizar el sistema informático.
b) Los roles de usuario. Esto contempla el tipo de operaciones que pueden realizar los operadores del sistema informático de acuerdo con el papel que juegan dentro del proceso PREP.
c) Los privilegios de los usuarios. Esto contempla las operaciones que tienen permitidas los operadores con base en el rol del usuario que desempeñan.
d) El flujo de información y datos. Esto contempla el flujo de los datos de las actas, desde su captura hasta su procesamiento para el conteo que se refleja en la publicación de resultados.
e) Los componentes tecnológicos. Esto contempla los dispositivos tecnológicos que se emplean durante todas las etapas del proceso PREP.

La capa de Nivel Operativo Integral incluye diversos criterios que se deben tomar en cuenta para llevar a cabo las actividades del Programa de Resultados Electorales Preliminares (PREP), tales como:

- Actividades propias del proceso PREP completo.
- Actividades para realizar mediante el sistema informático para el PREP.

Lo anterior involucra relacionar aspectos de recursos humanos, logísticos, tecnológicos y computacionales para llevar a cabo de forma transparente el proceso PREP.

Se identificó que las actividades a realizar se engloban en las siguientes 6 fases generales:

1. Toma fotográfica del Acta PREP en casilla.
2. Acopio de Acta PREP.
3. Digitalización de Acta PREP.
4. Captura y verificación de datos de Acta PREP.
5. Verificación de datos de Actas PREP.
6. Publicación de resultados.

Lo anterior se ha obtenido en colaboración con lo realizado para la Capa 2: APLICACIÓN. A partir de ello, de manera conceptual, se ha identificado:

- Las actividades que deben realizarse durante el proceso completo del PREP.

- Las actividades que deben realizarse mediante el sistema informático.
- Los roles de los usuarios.
- Los privilegios de los usuarios.
- El flujo de información durante el proceso PREP.

5.1.4 Procedimiento

Para llevar a cabo cada una de las actividades de la auditoría se generaron diversos cuestionarios para evaluar las tareas y subtareas de cada etapa del proceso PREP. Las actividades de la auditoría contemplaron diversas revisiones de la funcionalidad del sistema informático. Estas revisiones se realizaron en las siguientes fechas:

Tabla 5.A.1. Actividades detalladas de la etapa Toma Fotográfica de Acta PREP.

Fecha	Tipo de prueba	Actividades realizadas
Inicio auditoria a 21/abril/2021	Prueba 1	Revisión parcial al sistema informático
16/mayo/2021	Simulacro 1	Revisión parcial al sistema informático
23/mayo/2021	Simulacro 2	Revisión parcial al sistema informático
30/mayo/2021	Simulacro 3	Revisión parcial al sistema informático

5.1.5 Revisión de procesos realizados en las etapas del PREP

Con base en los casos de uso, flujo de información y actividades y diagrama tecnológico se analizaron las diversas etapas del PREP para identificar de manera más detallada, sin distinción del tipo de actividad, las actividades y eventos por cada una de las etapas del proceso PREP.

Tabla 5.A.2. Actividades detalladas de la etapa Toma Fotográfica de Acta PREP. Capa 5: Nivel Operación

Toma fotográfica del Acta PREP en casilla
1. El CAEL se encuentra en la casilla asignada 1.1. El CAEL no ha llegado a la casilla asignada 1.2. El CAEL se encuentra en una casilla incorrecta 2. Se ha llenado el AEC 2.1. El AEC tiene datos faltantes 2.1.1. El CAEL no tiene acceso a los datos faltantes 2.2. La AEC se llenó incorrectamente 3. El CAEL tiene acceso al Actas PREP 3.1. El CAEL no tiene acceso a las Actas PREP 3.1.1. El equipo de soporte no está disponible 3.1.2. El equipo de soporte no encuentra alguna solución para esta situación 4. El CAEL verifica que todos los datos de identificación del acta sean legibles 4.1. No se encuentran los datos de identificación del acta 4.1.1. El equipo de soporte no está disponible 4.1.2. El equipo de soporte no encuentra alguna solución para esta situación 4.2. Los datos de identificación del acta no son legibles

4.2.1. No se puede tener acceso a los datos de identificación del acta.
4.2.2. El equipo de soporte no está disponible
4.2.3. El equipo de soporte no encuentra alguna solución para esta situación

5. El CAEL tiene acceso al PREP Casilla
5.1. El CAEL no tiene acceso a la aplicación PREP Casilla

6. El CAEL cuenta con un manual de usuario para la aplicación PREP Casilla

7. El CAEL cuenta con dispositivo móvil para realizar la toma fotográfica
7.1. El CAEL no cuenta con dispositivo móvil
7.2 El dispositivo móvil se encuentra descargado
7.3. El CAEL no cuenta con cargador para el dispositivo móvil

8. El dispositivo móvil se encuentra en las condiciones necesarias para la toma fotográfica
8.1. El dispositivo móvil no cuenta con una cámara fotográfica
8.2. El dispositivo móvil tiene la cámara dañada
8.3. El dispositivo móvil no cuenta con una cámara apta para la toma fotográfica

9. El CAEL ingresa de manera manual los datos de identificación de la casilla en PREP Casilla
9.1. El CAEL no tiene acceso a los datos de identificación
9.2. No se pueden registrar los datos en la aplicación por una falla técnica.

10. El CAEL coloca el Acta PREP de tal forma que no presente dobleces
10.1 El acta sufrió un doblez al momento de acomodarla

11. El CAEL tiene acceso a la toma fotográfica en el PREP Casilla

12. El CAEL verifica que no se incluyan elementos ajenos al Acta PREP en la toma fotográfica
12.1. Es imposible omitir algún elemento ajeno al acta en la toma fotográfica

13. El CAEL realiza la toma fotográfica del Acta PREP
13.1. La cámara del dispositivo móvil no logra enfocar el acta.
13.2. El dispositivo móvil no permite realizar la toma fotográfica.

14. El CAEL verifica que la imagen tomada sea legible
14.1. El CAEL no tiene acceso a la fotografía
14.2. Algunos datos de la fotografía no se pueden apreciar correctamente

15. El CAEL confirma en la aplicación que la imagen es legible
15.1. El CAEL no tiene acceso a la imagen desde la aplicación
15.2. Algunos datos de la imagen no son visibles desde la aplicación

16. Se cuenta con servicio de datos para el envío de la imagen
16.1. Los datos para el envío de la imagen están disponibles, pero tienen señal pobre
16.2. Los datos para el envío de la imagen fallan constantemente

17. El CAEL realiza el envío de la imagen a través de PREP Casilla

17.1. Está deshabilitada la opción de enviar imagen en la aplicación 17.2. No se logra enviar la imagen correctamente 17.3. La calidad de la imagen es deteriorada significativamente al realizar el envío de la imagen 18. La calidad de la imagen se revisa en el MCAD del CATD correspondiente 18.1. El MCAD correspondiente a la revisión de su respectiva imagen no se encuentra disponible 18.2. La imagen no llegó al MCAD correspondiente 18.2.1. El equipo de soporte no se encuentra disponible 19. Se realizó el registro del proceso en la bitácora de actividades 20. El CAEL visita todas las casillas asignadas 20.1. El CAEL no logró visitar todas las casillas asignadas 20.2. El CAEL visitó alguna casilla errónea

Tabla 5.A.3. Actividades detalladas de la etapa Acopio de Acta PREP. Capa 5: Nivel Operación.

Acopio de Acta PREP
1. El acopiador recibe la Bolsa PREP 1.1. La bolsa PREP correspondiente no está disponible 2. El acopiador abre la Bolsa PREP para obtener el Acta PREP 2.1. La bolsa PREP no cuenta con algún acta 4. El acopiador deja constancia de la fecha y hora de acopio en el Acta PREP 5. El acopiador coloca las Actas PREP dentro de la bandeja de entrada del digitalizador en el mismo orden en que fueron recibidas 5.1. La bandeja de entrada no está disponible para las Actas PREP

Tabla 5.A.4. Actividades detalladas de la etapa Digitalización de Acta PREP. Capa 5: Nivel Operación.

Digitalización de Acta PREP
1. El digitalizador tiene acceso a las Actas PREP 2. El digitalizador toma de la bandeja de entrada el Acta PREP 2.1. No se encuentra en la bandeja de entrada algún acta PREP 3. El Acta PREP cuenta con un código QR correspondiente 3.1. El código QR correspondiente no está disponible 3.2. El código QR correspondiente está ilegible o de una calidad muy pobre 4. El digitalizador coloca la etiqueta con el código QR correspondiente en el recuadro superior izquierdo (pendiente de verificar) 4.1. La etiqueta del código QR se coloca de manera errónea

5. El digitalizador cuenta con algún equipo multifunción o escáner a su disposición 6. El equipo multifunción o escáner se encuentra en las condiciones necesarias para la digitalización 7. El digitalizador realiza la captura digital de la imagen PREP, por medio de un equipo multifunción o escáner 8. Se realiza el envío de la captura digital al MCAD 8.1. Es imposible realizar el envío de la captura digital al MCAD 8.2. El equipo de soporte técnico no se encuentra disponible 8.3. El equipo de soporte técnico es incapaz de solucionar la situación 9. El digitalizador tiene acceso al MCAD 9.1. El MCAD se encuentra bloqueado o con una falla en su servicio 10. El digitalizador cuenta con un manual de usuario para el sistema 10.1. El manual de usuario no está disponible 10.1.1. El equipo de soporte técnico no está disponible 10.1.2. El equipo de soporte técnico no encuentra una solución al problema 11. El digitalizador revisa en el MCAD la calidad de la imagen del Acta PREP digitalizada 11.1. El digitalizador no procesa la imagen correctamente 11.1.1. El equipo de soporte técnico no está disponible 11.1.2. El equipo de soporte técnico no encuentra una solución al problema 11.2. El digitalizador da una respuesta errónea 12. El MCAD genera de manera única y automática el hash 12.1. El MCAD no funciona correctamente 12.1.1. El equipo de soporte técnico no está disponible 12.1.2. El equipo de soporte técnico no encuentra una solución al problema 12.2. El hash no cumple con los requisitos 13. El MCAD transmite el Acta PREP al CRID 13.1. El Acta PREP no se envía satisfactoriamente 13.2. El CRID no recibe satisfactoriamente el Acta PREP 14. El CRID identifica con la imagen recibida de PREP Casilla, si el Acta PREP fue procesada anteriormente 14.1. El CRID no logra identificar la imagen 15. El digitalizador coloca el Acta PREP en la bandeja de salida 16. Se realizó el registro del proceso en la bitácora de actividades (pendiente)

Tabla 5.A.5. Actividades detalladas de la etapa Captura y Verificación de datos de Acta PREP. Capa 5: Nivel Operación.

Captura y verificación de datos de Acta PREP
1. El capturista se encuentra en el TCA correspondiente

1.1 No hay algún capturista disponible
1.2 No hay TCA disponibles
1.3 Hay error en la asignación de los capturistas
1.4 Hay dos capturistas en un sólo TCA

2. El capturista tiene acceso al sistema
2.1 El sistema no está disponible
2.2 El capturista no cuenta con las credenciales necesarias
2.3 El capturista tiene las credenciales equivocadas.

3. El capturista cuenta con un manual de usuario para el sistema
3.1 El manual de usuario no está disponible
3.2 El manual de usuario está protegido
3.2.1 Soporte no está disponible
3.2.2 Soporte no encuentra alguna solución al problema

4. El capturista tiene acceso al TCA
4.1 El sistema de TCA está restringido
4.2 El capturista no tiene las credenciales para acceder al TCA
4.3 El capturista tiene las credenciales erróneas.

5. El capturista realizó la solicitud del Acta PREP
5.1 El capturista no cuenta con la solicitud del Acta PREP
5.2 El capturista tiene una solicitud errónea.

6. Se realizó el envío del Acta PREP a un TCA disponible
6.1 El ACTA PREP no logra enviarse satisfactoriamente.
6.2 El TCA no logra recibir el Acta PREP satisfactoriamente.

7. El capturista tiene acceso al Acta PREP

8. El capturista tiene acceso al registro de datos
8.1. El sistema prohíbe el acceso al registro de datos

9. El capturista realiza el registro en el TCA de los datos asentados en el Acta PREP

10. El capturista concluyó la primera captura del Acta PREP

11. El capturista ingresa a la opción de realizar la segunda captura
11.1. No se encuentra habilitada la opción de realizar un segundo registro

12. El capturista realiza el segundo registro en el TCA de los datos asentados en el Acta PREP

13. El sistema realiza una verificación comparando que los datos capturados por los dos capturistas coincidan.

14. Se envían los datos automáticamente al CRID

15. Se realizó el registro del proceso en la bitácora de actividades

Tabla 5.A.6. Actividades detalladas de la etapa Verificación de datos de Actas PREP. Capa 5: Nivel Operación.

Verificación de datos de Actas PREP
1. Las actas son transmitidas de manera automática por el CRID al CCV 1.1 Las actas no pueden enviarse satisfactoriamente 1.2 Las actas no pueden recibirse satisfactoriamente 2. El verificador se encuentra en el CCV asignado 2.1 No hay algún verificador disponible 3. El verificador tiene acceso al sistema 3.1 El sistema no está disponible 3.2 El verificador no cuenta con las credenciales necesarias 3.3 El verificador tiene las credenciales equivocadas. 3.4 Falla la conexión de datos para conectarse al sistema 4. El verificador cuenta con un manual de usuario del sistema 4.1 El manual de usuario no está disponible 5. El primer verificador corrobora que los datos capturados en los CATD, coincidan con los datos de la imagen del Acta PREP de la casilla correspondiente digitalizada en el CATD 5.1 Hay datos faltantes en el CATD 5.2 Hay datos faltantes en la imagen de la Acta PREP 5.3 Los datos de la imagen de la Acta PREP son ilegibles. 5.4 Hay un error en el registro de la imagen y los datos en el CATD (No corresponden una con otra) 6. El primer verificador registra el acta como correcta 6.1. El primer verificador registra el acta como incorrecta 6.1.1 El segundo verificador corrobora que los datos capturados en los CATD, coincidan con los datos de la imagen del Acta PREP de la casilla correspondiente digitalizada en el CATD 6.1.2 El segundo verificador realiza las modificaciones de ser necesarias 6.1.3 El segundo verificador registra el acta como incorrecta 7. Se realizó el registro del proceso en la bitácora de actividades

Tabla 5.A.7. Actividades detalladas de la etapa Publicación de resultados. Capa 5: Nivel Operación.

Publicación de resultados
1. Se realiza la validación de que las bases de datos estén en ceros 2. Se realiza la captura de datos necesarios para la publicación

3. Se realizan los cálculos necesarios para la publicación

4. No se pueden capturar los datos necesarios para la publicación

5. Se realizan los cálculos necesarios para la publicación

6. Hay alguna falla en el sistema al realizar los cálculos

7. Se realiza la publicación de los datos

8. No se realiza correctamente la publicación de los resultados

9. Fallan los datos de conexión al realizar la publicación

10. Se realiza la publicación tardada

5.1.6 Flujo de información y actividades

En base a una serie de Casos de Uso definidos por el Ente Auditor, se identificó el flujo de información y actividades que a continuación se presenta mediante diagramas. Estos diagramas corresponden a cada una de las etapas del proceso PREP:

1. Toma fotográfica del Acta PREP en casilla (Fig. 5.A.1)
2. Acopio de Acta PREP (Fig. 5.A.2)
3. Digitalización de Acta PREP (Fig. 5.A.3)
4. Captura y verificación de datos de Acta PREP (Fig. 5.A.4)
5. Verificación de datos de Actas PREP (Fig. 5.A.5)
6. Publicación de resultados (Fig. 5.A.6)

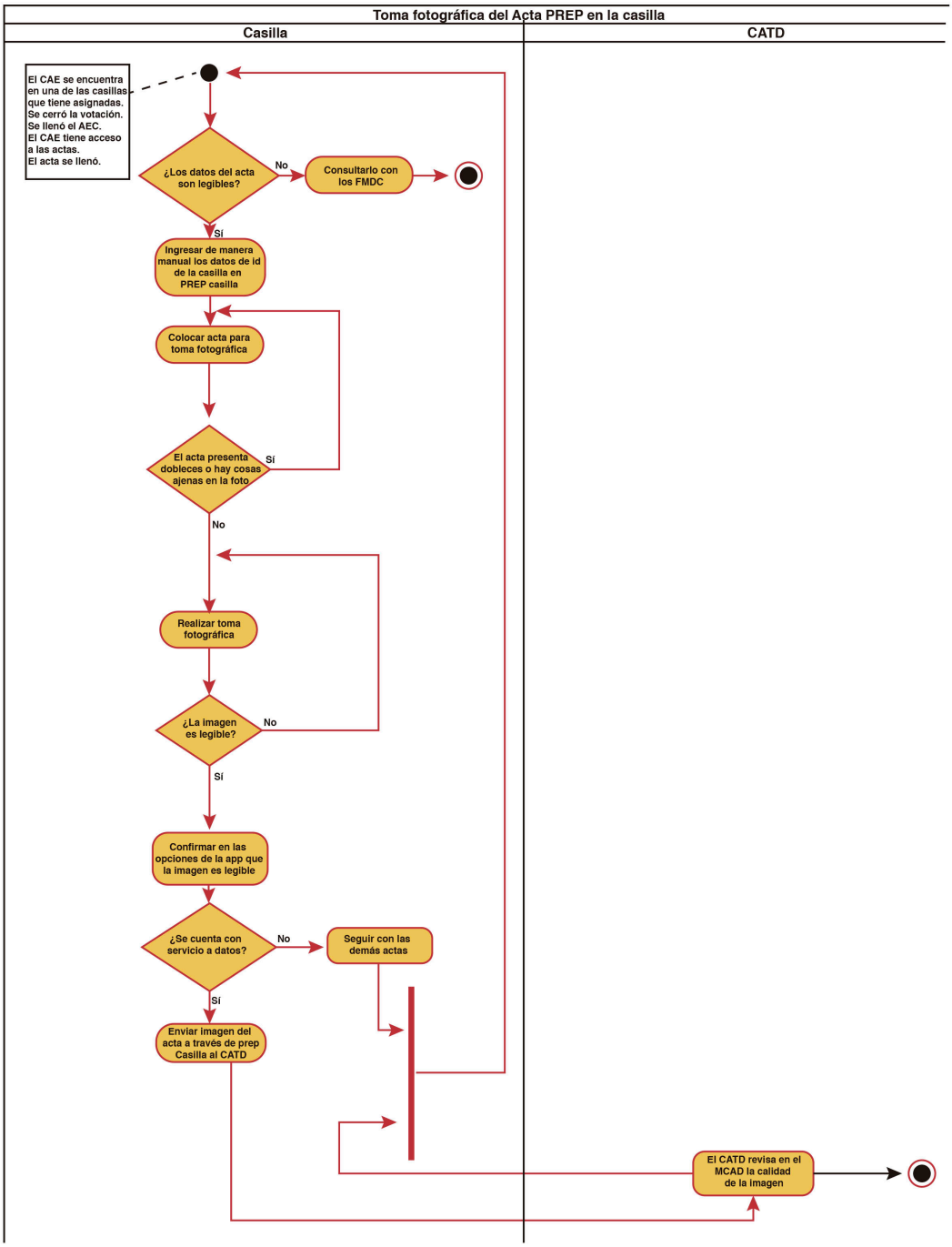


Figura 5.A.1. Toma fotográfica del Acta PREP en casilla.

Figura 5.A.1. Flujo de información y actividades de la etapa Toma Fotográfica del Acta PREP en casilla. Capa 5: Nivel Operación.

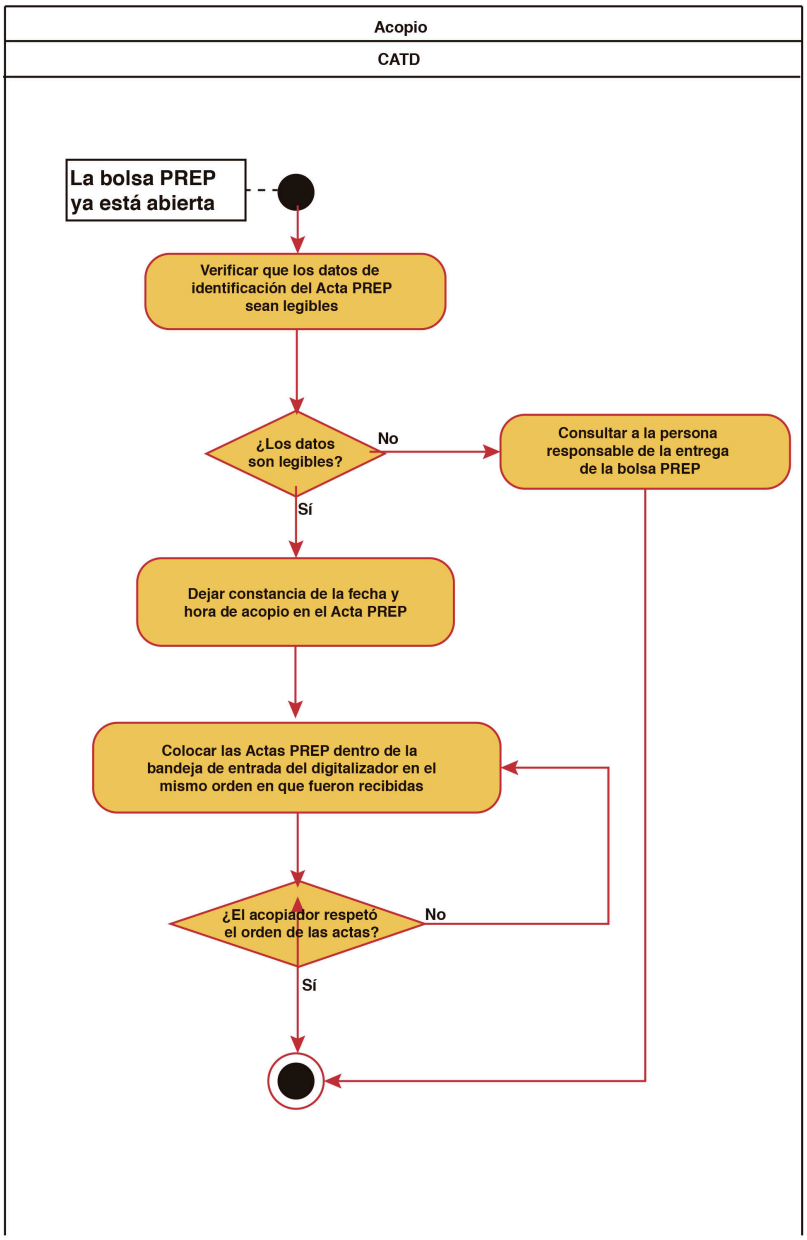


Figura 5.A.2. Acopio de Acta PREP

Figura 5.A.2. Flujo de información y actividades de la etapa Acopio de Acta PREP. Capa 5: Nivel Operación.

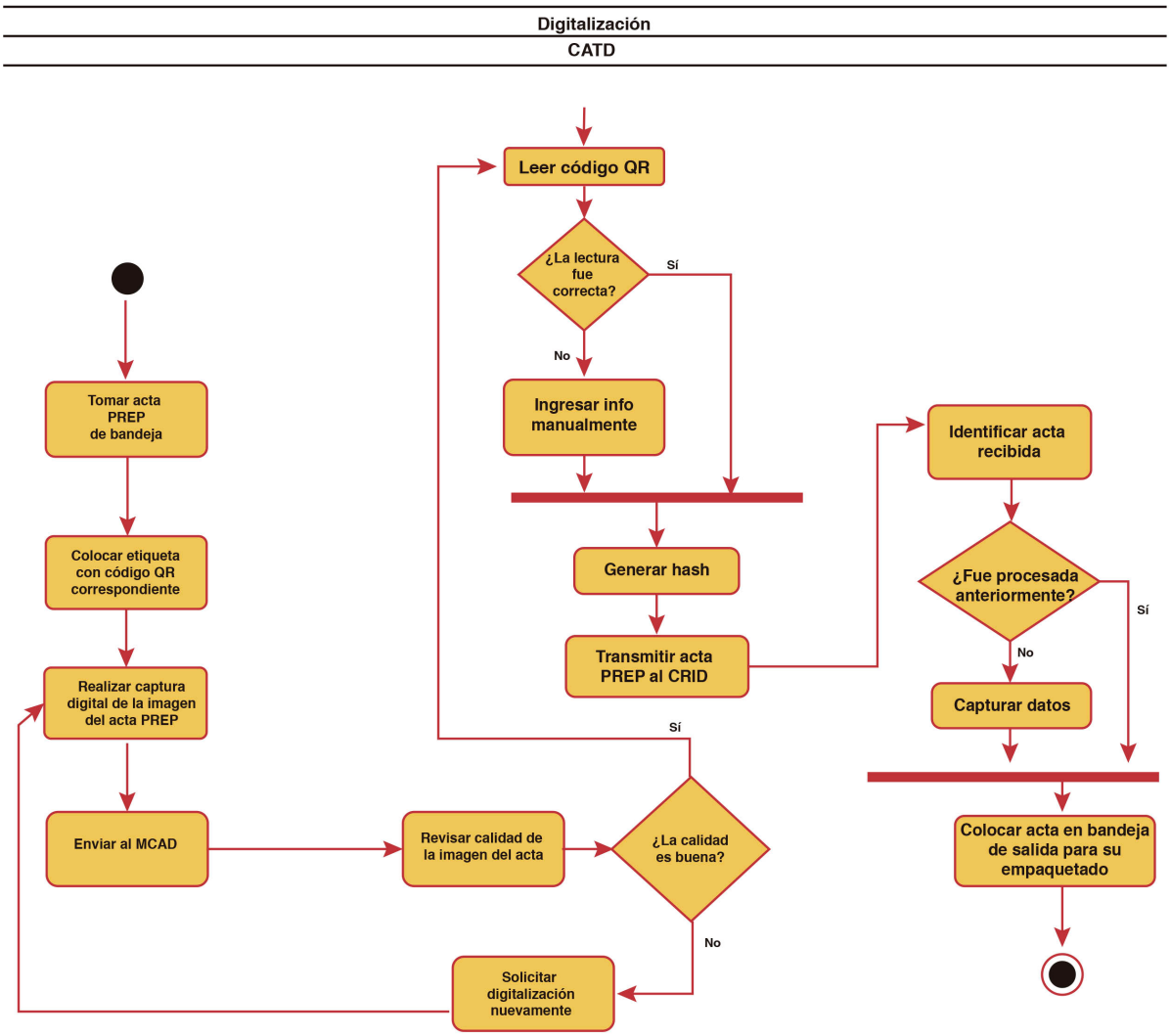


Figura 5.A.3 Digitalización de Acta PREP

Figura 5.A.3. Flujo de información y actividades de la etapa Digitalización de Acta PREP. Capa 5: Nivel Operación.

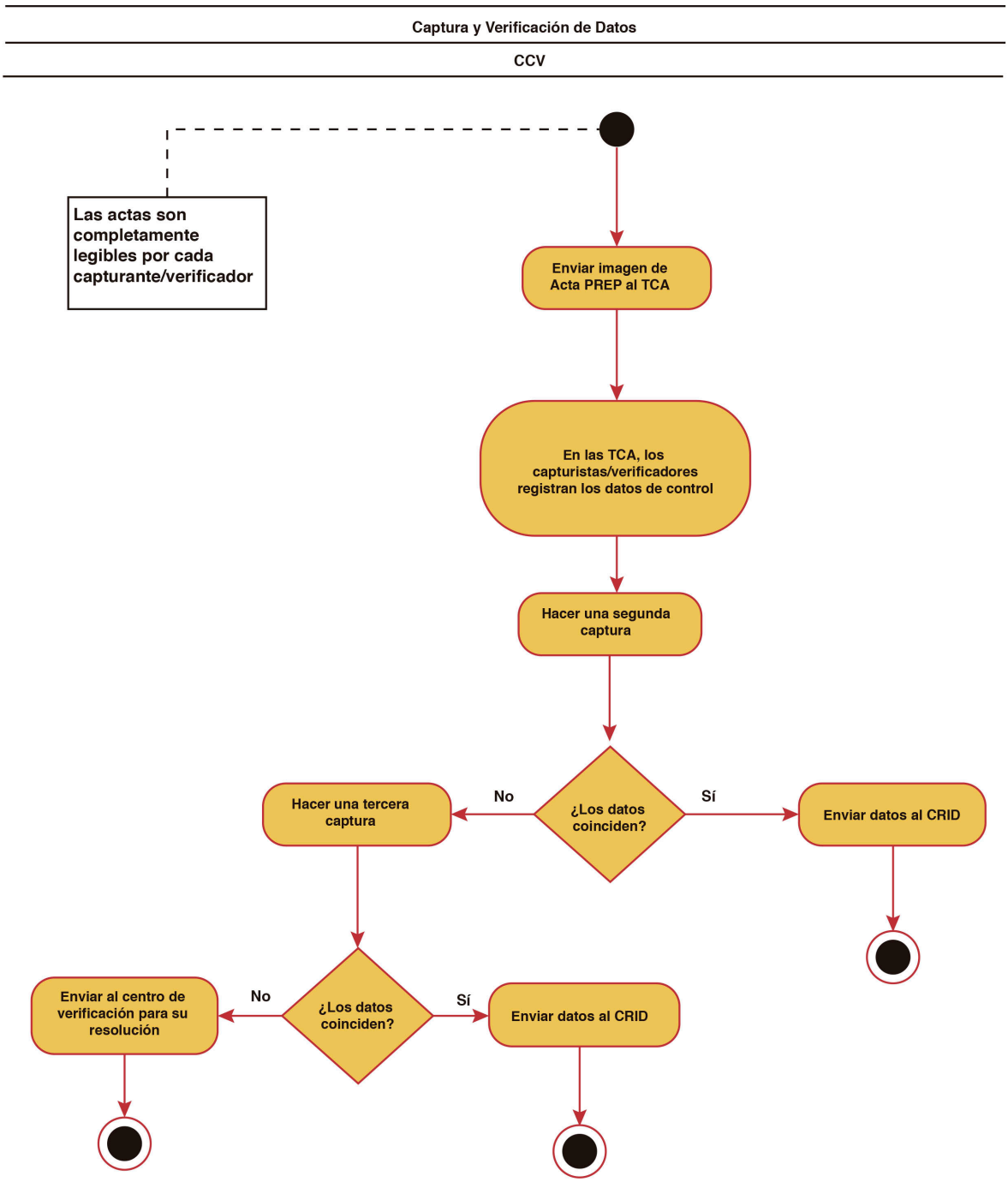


Figura 5.A.4 Captura y verificación de datos de Acta PREP

Figura 5.A.4. Flujo de información y actividades de la etapa Captura y verificación de datos de Acta PREP. Capa 5: Nivel Operación.

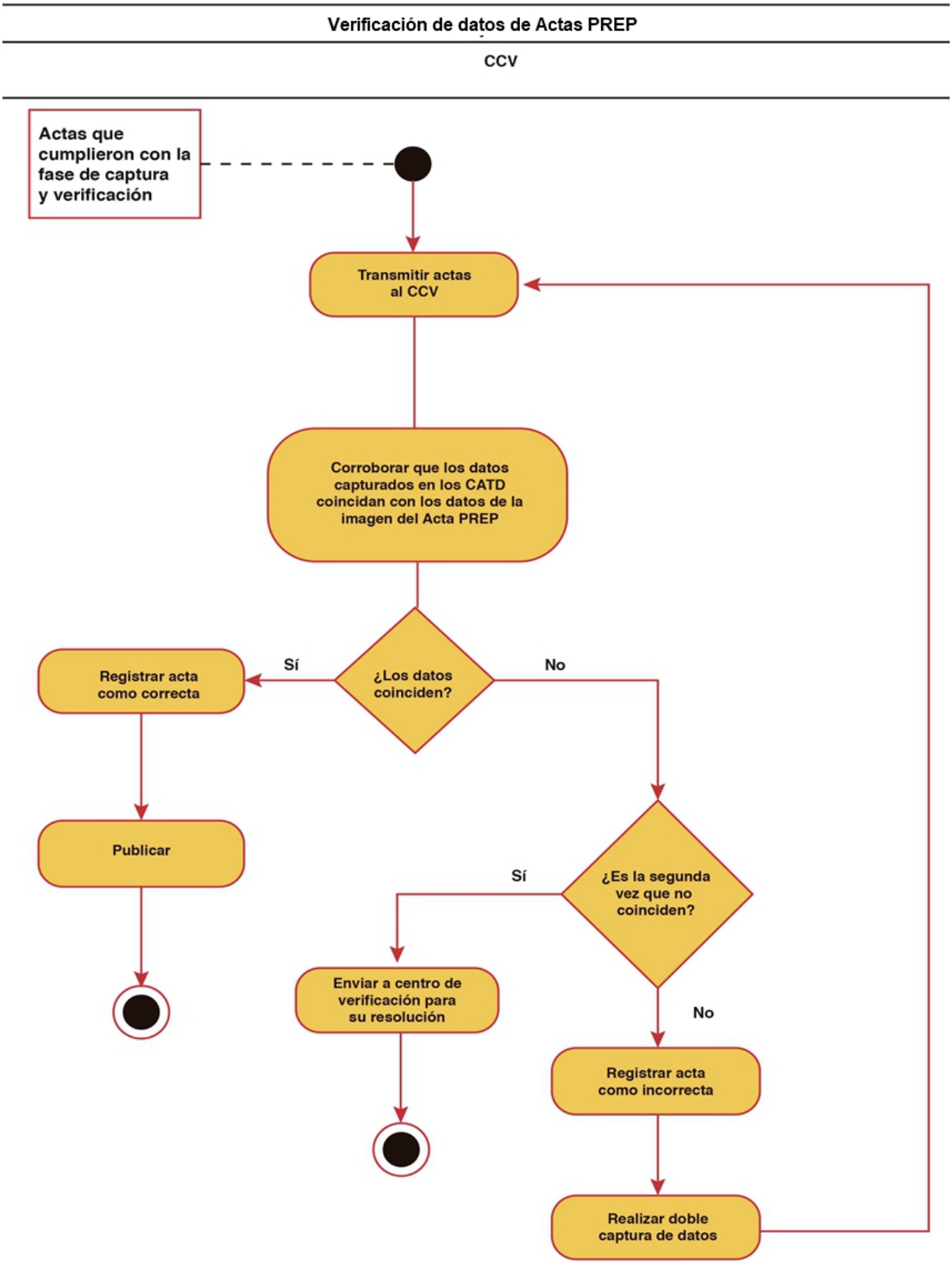


Figura 5.A.5. Verificación de datos de Actas PREP

Figura 5.A.5. Flujo de información y actividades de la etapa Verificación de datos de Actas PREP. Capa 5: Nivel Operación.

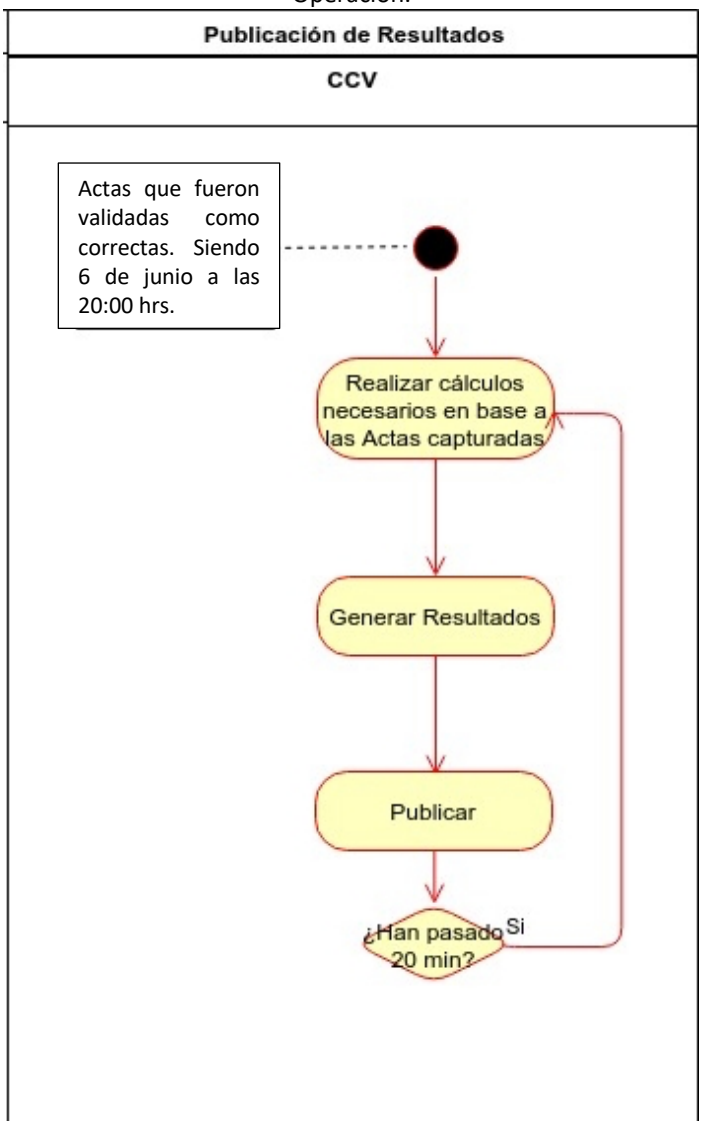


Figura 5.A.6. Flujo de información y actividades de la etapa Publicación de Resultados. Capa 5: Nivel Operación.

5.2 Requerimientos no Funcionales

Como parte del proceso operativo del PREP se han identificado roles de usuarios, los cuales están relacionados con las tareas que realizan dentro del proceso PREP.

Las operaciones que pueden realizar los usuarios de acuerdo con su rol se listan en la *Tabla 5.B.1*

Tabla 5.B.1. Operaciones de los usuarios de acuerdo con su rol para Capa 5: Nivel Operación.

Usuario	Rol	Operación
Usuario 1	CAEL	Ingresar datos casilla Tomar fotografía Enviar imagen Llenar acta Solicitar Acta
Usuario 2	Acopiador	Escribir fecha y hora en acta Colocar acta en bandeja de entrada Verificar datos legibles
Usuario 3	Digitalizador	Colocar código QR Digitalizar el acta Capturar el acta Enviar acta al MCAD Revisar calidad imagen Colocar acta PREP en bandeja de salida
Usuario 4	Capturista	Solicitar acta Registrar datos Clasificar el acta como ilegible
Usuario 5	Verificador	Corroborar datos CATD vs imagen acta PREP Registrar acta como correcta Registrar acta como incorrecta Enviar a centro de verificación para su resolución
Usuario 6	Coordinador	Realizar informe de avances
Usuario 7	Administrador	Administrar roles de usuarios Administrar usuarios

5.2.1 Revisión de procesos realizados en las etapas del PREP

Con base en los casos de uso, flujo de información y actividades y diagrama tecnológico se analizaron las diversas etapas del PREP para identificar las actividades que involucran requerimientos no

funcionales. De acuerdo con la etapa del proceso PREP, éstas se listan a continuación. La numeración refleja el orden de ejecución de las actividades en el proceso completo.

Tabla 5.B.2. Actividades que involucran Requerimientos No Funcionales de la etapa Toma Fotográfica de Acta PREP en Capa 5: Nivel Operación.

Toma Fotográfica
1. El CAEL se encuentra en la casilla asignada 1.1. El CAEL no ha llegado a la casilla asignada 1.2. El CAEL se encuentra en una casilla incorrecta 2. Se ha llenado el AEC 2.1. El AEC tiene datos faltantes 2.1.1. El CAEL no tiene acceso a los datos faltantes 2.2. La AEC se llenó incorrectamente 3. El CAEL tiene acceso al Actas PREP 3.1. El CAEL no tiene acceso a las Actas PREP 3.1.1. El equipo de soporte no está disponible 3.1.2. El equipo de soporte no encuentra alguna solución para esta situación 18. La calidad de la imagen se revisa en el MCAD del CATD correspondiente 18.1. El MCAD correspondiente a la revisión de su respectiva imagen no se encuentra disponible 18.2. La imagen no llegó al MCAD correspondiente 18.2.1. El equipo de soporte no se encuentra disponible 19. Se realizó el registro del proceso en la bitácora de actividades 20. El CAEL visita todas las casillas asignadas 20.1. El CAEL no logró visitar todas las casillas asignadas 20.2. El CAEL visitó alguna casilla errónea

Tabla 5.B.3. Actividades que involucran Requerimientos No Funcionales de la etapa Digitalización de Acta PREP en Capa 5: Nivel Operación.

Digitalización de Acta PREP
8. Se realiza el envío de la captura digital al MCAD 8.1. Es imposible realizar el envío de la captura digital al MCAD 8.2. El equipo de soporte técnico no se encuentra disponible 8.3. El equipo de soporte técnico es incapaz de solucionar la situación 9. El digitalizador tiene acceso al MCAD 9.1. El MCAD se encuentra bloqueado o con una falla en su servicio 16. Se realizó el registro del proceso en la bitácora de actividades (pendiente)

Tabla 5.B.4. Actividades que involucran Requerimientos No Funcionales de la etapa Captura y verificación de datos de Acta PREP en Capa 5: Nivel Operación.

Captura y verificación de datos de Acta PREP
1. El capturista se encuentra en el TCA correspondiente 1.1 No hay algún capturista disponible 1.2 No hay TCA disponibles 1.3 Hay error en la asignación de los capturistas 1.4 Hay dos capturistas en un sólo TCA 6. Se realizó el envío del Acta PREP a un TCA disponible 6.1 El ACTA PREP no logra enviarse satisfactoriamente. 6.2 El TCA no logra recibir el Acta PREP satisfactoriamente. 14. Se envían los datos automáticamente al CRID 15. Se realizó el registro del proceso en la bitácora de actividades

Tabla 5.B.5 Actividades que involucran Requerimientos No Funcionales de la etapa Verificación de datos de Acta PREP en Capa 5: Nivel Operación.

Verificación de datos de Actas PREP
7. Se realizó el registro del proceso en la bitácora de actividades

5.3 Aspectos de seguridad informática

REVISIÓN DE PROCESOS REALIZADOS EN LAS ETAPAS DEL PREP

Con base en los casos de uso, flujo de información y actividades y diagrama tecnológico se analizaron las diversas etapas del PREP para identificar de manera más detallada las actividades en donde se involucran aspectos de seguridad informática, las cuales se describen a continuación. La numeración refleja el orden de ejecución de las actividades en el proceso completo.

Tabla 5.C.1. Actividades que involucran Aspectos de Seguridad Informática de la etapa Toma Fotográfica de Acta PREP en Capa 5: Nivel Operación.

Toma Fotográfica
5. El CAEL tiene acceso al PREP Casilla 5.1. El CAEL no tiene acceso a la aplicación PREP Casilla 11. El CAEL tiene acceso a la toma fotográfica en el PREP Casilla

Tabla 5.C.2. Actividades que involucran Aspectos de Seguridad Informática de la etapa Digitalización de Acta PREP en Capa 5: Nivel Operación.

Digitalización de Acta PREP
9. El digitalizador tiene acceso al MCAD 9.1. El MCAD se encuentra bloqueado o con una falla en su servicio 12. El MCAD genera de manera única y automática el hash 12.1. El MCAD no funciona correctamente 12.1.1. El equipo de soporte técnico no está disponible 12.1.2. El equipo de soporte técnico no encuentra una solución al problema 12.2. El hash no cumple con los requisitos 13. El MCAD transmite el Acta PREP al CRID 13.1. El Acta PREP no se envía satisfactoriamente 13.2. El CRID no recibe satisfactoriamente el Acta PREP

Tabla 5.C.3. Actividades que involucran Aspectos de Seguridad Informática de la etapa Captura y verificación de datos de Acta PREP en Capa 5: Nivel Operación.

Captura y verificación de datos de Acta PREP
2. El capturista tiene acceso al sistema 2.1 El sistema no está disponible 2.2 El capturista no cuenta con las credenciales necesarias 2.3 El capturista tiene las credenciales equivocadas. 4. El capturista tiene acceso al TCA 4.1 El sistema de TCA está restringido 4.2 El capturista no tiene las credenciales para acceder al TCA 4.3 El capturista tiene las credenciales erróneas. 8. El capturista tiene acceso al registro de datos 8.1. El sistema prohíbe el acceso al registro de datos 9. El capturista realiza el registro en el TCA de los datos asentados en el Acta PREP

Tabla 5.C.4. Actividades que involucran Aspectos de Seguridad Informática de la etapa Verificación de datos de Acta PREP en Capa 5: Nivel Operación.

Verificación de datos de Actas PREP
1. Las actas son transmitidas de manera automática por el CRID al CCV 1.1 Las actas no pueden enviarse satisfactoriamente 1.2 Las actas no pueden recibirse satisfactoriamente 3. El verificador tiene acceso al sistema 3.1 El sistema no está disponible 3.2 El verificador no cuenta con las credenciales necesarias 3.3 El verificador tiene las credenciales equivocadas. 3.4 Falla la conexión de datos para conectarse al sistema

Tabla 5.C.5. Actividades que involucran Aspectos de Seguridad Informática de la etapa Publicación de resultados en Capa 5: Nivel Operación.

Publicación de resultados
9. Fallan los datos de conexión al realizar la publicación

5.4 Buenas prácticas de seguridad física y lógica

Los usuarios tienen requerimientos operativos para la realización de sus actividades, de acuerdo son su rol, los cuales se listan en la *Tabla 5.D.1.*

Tabla 5.D.1. Requerimientos operativos de los usuarios de acuerdo con su rol para Capa 5: Nivel Operación.

Usuario	**Rol**	**Requerimientos de Operación**
Usuario 1	CAEL	Acceder al sistema Encontrarse en la casilla asignada Contar con el dispositivo móvil asignado
Usuario 2	Acopiador	Verificar datos legibles
Usuario 3	Digitalizador	Tomar el acta de la bandeja de entrada Acceder al sistema Contar con un dispositivo escáner o multifunción
Usuario 4	Capturista	Solicitar un acta Acceder al sistema
Usuario 5	Verificador	Acceder al sistema

		Recibir imagen PREP Casilla y datos capturados en el CATD
Usuario 6	Coordinador	
Usuario 7	Administrador	Acceder al sistema

5.4.1 Revisión de procesos realizados en las etapas del PREP

Con base en los casos de uso, flujo de información y actividades y diagrama tecnológico se analizaron las diversas etapas del PREP para identificar de manera más detallada las actividades en donde se involucran aspectos de buenas prácticas de seguridad física y lógica, las cuales se describen a continuación. La numeración refleja el orden de ejecución de las actividades en el proceso completo.

Tabla 5.D.2. Actividades que involucran Aspectos de Buenas Prácticas de Seguridad Física y Lógica de la etapa Acopio de Acta PREP en Capa 5: Nivel Operación.

Acopio de Acta PREP
3. El acopiador verifica que los datos de identificación del Acta PREP sean legibles 3.1. El acopiador detecta algún error en el Acta PREP 3.1.1. El encargado del sobre no está disponible

Tabla 5.D.3. Actividades que involucran Aspectos de Buenas Prácticas de Seguridad Física y Lógica de la etapa Digitalización de Acta PREP en Capa 5: Nivel Operación.

Digitalización de Acta PREP
3. El Acta PREP cuenta con un código QR correspondiente 3.1. El código QR correspondiente no está disponible 3.2. El código QR correspondiente está ilegible o de una calidad muy pobre 10. El digitalizador cuenta con un manual de usuario para el sistema 10.1. El manual de usuario no está disponible 10.1.1. El equipo de soporte técnico no está disponible 10.1.2. El equipo de soporte técnico no encuentra una solución al problema

Tabla 5.D.4. Actividades que involucran Aspectos de Buenas Prácticas de Seguridad Física y Lógica de la etapa Captura y Verificación de datos de Acta PREP en Capa 5: Nivel Operación.

Captura y verificación de datos de Acta PREP
3. El capturista cuenta con un manual de usuario para el sistema 3.1 El manual de usuario no está disponible 3.2 El manual de usuario está protegido 3.2.1 Soporte no está disponible 3.2.2 Soporte no encuentra alguna solución al problema

Tabla 5.D.5. Actividades que involucran Aspectos de Buenas Prácticas de Seguridad Física y Lógica de la etapa Verificación de datos de Acta PREP en Capa 5: Nivel Operación.

Verificación de datos de Acta PREP
4. El verificador cuenta con un manual de usuario del sistema 4.1 El manual de usuario no está disponible

5.5 Análisis de vulnerabilidades

Con base en los roles identificados anteriormente, se han identificado los privilegios de los usuarios, los cuales se listan en la *Tabla 5.E.1.*

Tabla 5.E.1. Privilegios de los usuarios de acuerdo a su rol para Capa 5: Nivel Operación.

Usuario	**Rol**	**Privilegios en el Sistema**
Usuario 1	CAEL	Acceso a la aplicación PREP Casilla Acceso a la toma fotográfica Acceso al llenado del Acta
Usuario 2	Acopiador	Acceso a las actas PREP
Usuario 3	Digitalizador	Acceso al sistema Acceso a la aplicación Acceso a digitalizar el acta Acceso a los códigos QR asignados Acceso al MCAD
Usuario 4	Capturista	Acceso al Sistema Acceso al TCA Acceso al registro de datos Acceso a la clasificación del acta en el TCA
Usuario 5	Verificador	Acceso al sistema Acceso los datos capturados en el CATD Acceso a la imagen Acta PREP Acceso a registrar el acta como correcta o incorrecta

Usuario 6	Coordinador	Acceso a la información en tiempo real del avance
Usuario 7	Administrador	Acceso al sistema Acceso a administrar los roles de usuarios Acceso a la creación de un usuario

5.5.1 Revisión de procesos realizados en las etapas del PREP

Con base en los casos de uso, flujo de información y actividades y diagrama tecnológico se analizaron las diversas etapas del PREP para identificar de manera más detallada las actividades en donde se involucran aspectos de vulnerabilidades, las cuales se describen a continuación. La numeración refleja el orden de ejecución de las actividades en el proceso completo.

Tabla 5.E.2. Actividades que involucran Aspectos de Vulnerabilidades de la etapa Toma Fotográfica de Acta PREP en Capa 5: Nivel Operación.

Toma Fotográfica
4. El CAEL verifica que todos los datos de identificación del acta sean legibles 4.1. No se encuentran los datos de identificación del acta 4.1.1. El equipo de soporte no está disponible 4.1.2. El equipo de soporte no encuentra alguna solución para esta situación 4.2. Los datos de identificación del acta no son legibles 4.2.1. No se puede tener acceso a los datos de identificación del acta. 4.2.2. El equipo de soporte no está disponible 4.2.3. El equipo de soporte no encuentra alguna solución para esta situación

Tabla 5.E.3. Actividades que involucran Aspectos de Vulnerabilidades de la etapa Digitalización de Acta PREP en Capa 5: Nivel Operación.

Digitalización de Acta PREP
5. El digitalizador cuenta con algún equipo multifunción o escáner a su disposición 14. El CRID identifica con la imagen recibida de PREP Casilla, si el Acta PREP fue procesada anteriormente 14.1. El CRID no logra identificar la imagen

Tabla 5.E.4. Actividades que involucran Aspectos de Vulnerabilidades de la etapa Captura y verificación de datos de Acta PREP en Capa 5: Nivel Operación.

Captura y verificación de datos de Acta PREP
7. El capturista tiene acceso al Acta PREP

Tabla 5.E.5. Actividades que involucran Aspectos de Vulnerabilidades de la etapa Verificación de datos de Acta PREP en Capa 5: Nivel Operación.

Verificación de datos de Acta PREP
5. El primer verificador corrobora que los datos capturados en los CATD, coincidan con los datos de la imagen del Acta PREP de la casilla correspondiente digitalizada en el CATD 5.1 Hay datos faltantes en el CATD 5.2 Hay datos faltantes en la imagen de la Acta PREP 5.3 Los datos de la imagen de la Acta PREP son ilegibles. 5.4 Hay un error en el registro de la imagen y los datos en el CATD (No corresponden una con otra)

Tabla 5.E.6. Actividades que involucran Aspectos de Vulnerabilidades de la etapa Publicación de resultados en Capa 5: Nivel Operación.

Publicación de resultados
4. No se pueden capturar los datos necesarios para la publicación 6. Hay alguna falla en el sistema al realizar los cálculos 8. No se realiza correctamente la publicación de los resultados

5.6 Hallazgos sobre el cumplimiento del Proceso Técnico Operativo

A continuación, se describen las observaciones de las operaciones realizadas en el Simulacro 1, Simulacro 2 y Simulacro 3.

Primeramente, se presentan las observaciones de las operaciones realizadas en el Simulacro 1 en los CATD Tampico, CATD Reynosa, CCV Madero y CCV Reynosa.

5.6.1. De la toma fotográfica del Acta PREP en la casilla en Simulacro 1

Comentario general:
No se pudo observar la fase de toma fotográfica debido a que no se realiza ni en el CATD ni en el CCV.

1. La toma fotográfica de las Actas PREP en la casilla se privilegiará, siempre y cuando no obstaculice las actividades que se llevarán a cabo en la Mesa Directiva de Casilla.
   Esta actividad se ejecutará cuando:
   a) El CAEL se encuentra en una de las casillas que tiene asignadas.
   b) Se haya cerrado la votación.
   c) Se haya llenado el AEC.
   d) El CAEL tenga acceso a las Actas PREP, que no hayan sido guardadas en la Bolsa-PREP correspondiente..

2. El CAE deberá verificar que todos los datos de identificación del Acta PREP sean legibles.
   Para efectos del presente, se considera que los datos de identificación del
   Acta PREP son:
   a) Tipo de acta.
   b) Entidad federativa.
   c) Distrito electoral local.

d) Sección.
e) Tipo y número de casilla
f) Municipio.

En los casos en que el AEC no cuente con un código QR, el CAEL seleccionará el código QR con los datos correspondientes a la casilla, posteriormente procederá a pegarlo en el recuadro superior izquierdo destinado para ello.

Si se cumplen las condiciones anteriores, el CAEL deberá hacer uso de PREP Casilla.

3. El CAEL deberá verificar que los datos de identificación del ACTA PREP coincidan con los del código QR impreso en el acta, en caso contrario deberá consultarlo con los FMDC para su correcta identificación.

4. La aplicación realizará la identificación automática de la casilla mediante la lectura del código QR. Si por cualquier razón el Acta PREP no contara con el código QR, o los datos del código QR no coincidieran con los estipulados por los FMDC, el CAEL deberá capturar de manera manual los datos de identificación de la casilla en la aplicación PREP Casilla.

5. El CAEL colocará el Acta PREP de tal forma que no presente dobleces y evitando en todo momento que en la toma fotográfica se incluyan elementos ajenos al Acta PREP.

6. El CAEL realizará la toma fotográfica del Acta PREP y verificará que la imagen sea legible.

7. El CAEL confirmará en las opciones de la aplicación que la imagen es legible. En caso de que no sea así, cancelará la toma fotográfica y llevará a cabo una nueva toma fotográfica del Acta PREP.

8. Concluidos los pasos anteriores, el CAE realizará el envío de la imagen a través de PREP Casilla. La calidad de la imagen se revisará en el CCV correspondiente.
   Si no se cuenta con servicio de datos para el envío de la imagen del Acta PREP, el CAEL podrá continuar con la toma fotográfica del Acta PREP de la siguiente casilla y en cuanto se tenga conexión al servicio de datos, la aplicación PREP Casilla de manera automática intentará nuevamente su envío. .

9. Para los casos en los que el CAEL no alcance a visitar todas las casillas que le hayan sido asignadas antes de que el FMDC inicie el traslado del paquete electoral al Consejo Distrital correspondiente, el Acta PREP de esas casillas se procesará conforme a las demás fases del presente proceso técnico operativo.

5.6.2. Del Acopio en Simulacro 1

Comentario general:
El acopiador deberá de contar con un gafete de identificación. Si el acopiador tarda más de lo necesario en realizar alguna actividad de la fase, el coordinador le brindará apoyo. El acopiador es el encargado del flujo de actas en el CATD, teniendo una lista en la cual registra las actas ya capturadas y siguiendo un orden determinado a la hora de asignar las actas a cada digitalizador. Si llega a tener acceso al CATD una persona ajena al proceso, el acopiador pide apoyo al oficial encargado. El acopiador es el encargado

de retirar los dispositivos ajenos al proceso. En el caso del CATD Reynosa no contaba con un acopiador, por lo que no se pudo observar esta fase. El medio de verificación (MV) de esta etapa son los formularios F5-A-2_1, F5-A-2_2.

1. Esta fase iniciará cuando el acopiador reciba la Bolsa-PREP y la abra para obtener el Acta PREP.

   Comentarios: El oficial encargado será quien tome el Acta PREP y la copia del Acta PREP de la Bolsa PREP, y será quien entregue la copia del Acta PREP al acopiador. Debido a que fue un simulacro no se pudo observar esta acción. MV F5-A-2_1-1, F5-A-2_1-2.

2. El acopiador verificará que los datos de identificación del Acta PREP sean legibles. En caso de detectar que alguno sea ilegible, lo consultará con la persona responsable de la entrega de la Bolsa-PREP.

   Comentarios: El acopiador se encarga de verificar los datos, si llega a detectar algún error o inconsistencia, o que los datos sean ilegibles en el Acta PREP, deberá de comunicárselo al presidente de casilla. MV F5-A-2_1-3.

3. El acopiador dejará constancia de la fecha y hora de acopio en el Acta PREP. Para ello, escribirá la fecha y hora en formato de 24 horas en el recuadro que para tal efecto se encuentra en la parte superior del Acta PREP.
   Comentarios: El acopiador deja constancia de la fecha y hora de acopio en el Acta PREP. MV F5-A-2_1-4.

4. El acopiador colocará las Actas PREP dentro de la bandeja de entrada del digitalizador en el mismo orden en que fueron recibidas, de tal manera que se digitalicen primero aquellas Actas PREP que se acopiaron primero.

   Comentarios: El acopiador no coloca las actas en la bandeja de entrada, el se encarga de entregarlas una por una personalmente a los digitalizadores. MV F5-A-2_1-5, F5-A-2_1-6.

5.6.3. De la Digitalización en Simulacro 1

Comentario general:
El digitalizador deberá de contar con un gafete de identificación. El digitalizador recibirá el Acta PREP de manera personal mediante el acopiador. En el caso del CATD Reynosa, los digitalizadores ya tenías todas la Actas PREP que les tocaban, debido a que no había acopiador. El digitalizador deberá de contar con las credenciales necesarias para el sistema, las cuales se le fueron otorgadas mediante un papel impreso. El digitalizador deberá de revisar el buen funcionamiento del equipo, y que el sistema este actualizado a su versión más reciente. En caso de detectar un error en el equipo o el sistema, deberá de comunicarlo con el coordinador. Si el digitalizador tiene alguna duda acerca del proceso a realizar, deberá de pedir ayuda a su coordinador, o revisar el manual de usuario que se le fue otorgado. El digitalizador obtuvo la capacitación necesaria para realizar el proceso. El medio de verificación (MV) de esta etapa son los formularios F5-A-3_1, F5-A-3_2.

1. El digitalizador capturara los datos de identificación de la casilla mediante PREP CATD utilizando el código QR. En caso de que los datos del código QR no coincidan con los estipulados por el FMDC, o

el Acta no cuente con código QR, el capturista deberá ingresar de manera manual los datos de identificación de la casilla siendo estos: Entidad federativa, distrito electoral local, sección, tipo y número de casilla y municipio.

2. Una vez que fue identificada el AEC, el digitalizador ejecuta la captura digital de la imagen del Acta PREP, por medio de la aplicación PREP CATD, para su envío al CRID.

   Comentarios: El digitalizador realiza la digitalización del Acta PREP mediante el PREP CATD, haciendo uso del código QR. MV F5-A-3_1-5.

3. El digitalizador revisará en la aplicación PREP CATD la calidad de la imagen del Acta PREP digitalizada. En caso de requerirse, la digitalizará nuevamente.

   Comentarios: El digitalizador revisa la calidad de la imagen en el PREP CATD, de ser necesario la digitaliza nuevamente. Debido a la caja implementada para la digitalización, la mayoría de los casos no era necesario realizar una segunda digitalización. MV F5-A-3_1-7.

4. A partir de la versión digital del Acta PREP, la aplicación PREP CATD generará de manera única y automática el código hash.
   El CRID, de manera automática, identificará, si con la imagen recibida de PREP Casilla, el Acta PREP digitalizada fue procesada anteriormente, si es el caso, no se procesará para la captura de datos.

5. Concluida la digitalización, la imagen y código Hash del AEC se enviarán automáticamente al CRID y deberá colocarse el Acta PREP en la bandeja de salida.

   Comentarios: En el CATD de Tampico al inicio del simulacro hubo un retraso de aproximadamente 20 a 30 minutos para el envío de las Actas PREP ya digitalizadas. Como quiera los digitalizadores continuaban con las demás Actas PREP, en cuanto se tuvo un mejor servicio de datos se realizó automáticamente el envío de las Actas PREP faltantes.

5.6.4. De la Captura de Datos en Simulacro 1

1. La captura de la información contenida en las Actas PREP se realizará en los CCV, y podrá realizarse en los CATD, como se establece en cada caso según los procedimientos siguientes:

Del proceso de captura en los CCV

Comentario general:
El capturista cuenta con un gafete de identificación. El capturista cuenta con las credenciales para ingresar al sistema, las cuales se le brindaron mediante un papel impreso. El capturista cuenta con un manual de usuario. El capturista obtuvo una capacitación antes de realizar el simulacro. Los capturistas también pueden ser verificadores. En el CATD Reynosa al inicio del simulacro hubo un problema al tratar de iniciar sesión. El problema persistió por aproximadamente 20 minutos. Una vez resuelto el problema, los operadores pudieron trabajar con normalidad. En el simulacro ambas capturas solo se realizaron en el CCV. El medio de verificación (MV) de esta etapa son los formularios F5-A-4_1, F5-A-4_2, F5-A-5_1, F5-A-5_2.

2. La captura de la información en los CCV se realizará mediante las imágenes enviadas mediante PREP Casilla o PREP CATD.

   Comentarios: La mayoría de las Actas PREP provenientes de PREP Casilla tenían una mala calidad de la imagen, a diferencia de las Actas PREP provenientes de PREP CATD. MV F5-A-4_1-3, F5-A-5_1-3.

3. La fecha y hora de acopio para las actas recibidas por PREP CATD, será ingresada en las TCA por el capturista tomando la fecha y hora especificada en el Acta PREP de manera manual por el acopiador. Para las Actas recibidas por PREP Casilla, la fecha y hora de acopio se registrará de manera automática y será la misma que la de la toma fotográfica realizada a través de PREP Casilla.

   Comentarios: Los capturistas ingresaban la fecha que venía en el Acta PREP ya digitalizada, en el caso de tener duda sobre que fecha ingresar lo consultaban con su supervisor. MV F5-A-4_1-5, F5-A-5_1-5.

4. En las TCA, un capturista capturará conforme lo establecido en la fracción II del numeral 28 del Anexo 13 del Reglamento de Elecciones, los siguientes datos:
   a) Los datos de identificación del AEC, los cuales considerando que en los CCV se realiza la captura utilizando las imágenes de las AEC provenientes de PREP Casilla o PREP CATD, y tomando en cuenta que para estas imágenes ya fueron capturados los datos de identificación de la casilla a la que pertenecen, el capturista deberá corroborar que los datos registrados en el sistema coinciden con los de la imagen del AEC. De coincidir, procederá con la captura de la información que se establece en los incisos del b) al e) del presente numeral; de lo contrario, lo turnará al Centro de Verificación para la correcta captura de los datos de identificación del Acta PREP: entidad federativa, distrito electoral local, sección, tipo y número de casilla y municipio.
   b) La fecha y hora de acopio para las imágenes de las AEC que provienen de PREP CATD.
   c) El total de boletas sobrantes, total de personas que votaron, total de representantes de los partidos políticos y de candidaturas independientes acreditados ante casilla que votaron, y total de votos sacados de la urna.
   d) Los votos obtenidos por los partidos políticos y las candidaturas, sean estas independientes, por partido político, por candidatura común o por coalición en cualquiera de sus combinaciones, según sea el caso;
   e) El total de votos, total de votos nulos y total de votos para candidaturas no registradas.

   Concluida la primera captura, el sistema solicitará que el mismo o, un segundo capturista realice una segunda captura volviendo a registrar los datos asentados en el Acta PREP. El sistema hará una verificación comparando que los datos capturados en ambas ocasiones coincidan. Si los datos son iguales, la fase de captura y verificación de esa Acta PREP concluye.

   Comentarios: Las dos capturas en la mayoría de las veces las realizan dos diferentes operadores. MV F5-A-4_1-5, F5-A-4_1-6, F5-A-4_1-7, F5-A-4_1-8, F5-A-4_1-9, F5-A-5_1-5, F5-A-5_1-6, F5-A-5_1-7, F5-A-5_1-8, F5-A-5_1-9.

5. En los casos en los que los datos de las primeras dos capturas no sean consistentes, el sistema solicitara de manera automática se realice una nueva captura. El sistema comparará la última captura con las anteriores y en caso de ser coincidente con alguna de ellas, continuaría el proceso.

El sistema verificará el número máximo de intentos erróneos que se pueden realizar para una misma acta y, en caso de alcanzar el máximo de intentos sin que la captura sea correcta, se turnara al Centro de Verificación para su resolución definitiva. El número máximo de intentos será de un mínimo de tres y un máximo de cuatro, siendo esto una variable que se establecerá en la configuración del sistema, según se estime conveniente.

Comentarios: No se podía saber si el operador estaba realizando la segunda o de ser necesario tercer captura del Acta, ya que el sistema no muestra el número de captura en el que se encuentra. MV F5-A-4_1-7, F5-A-5_1-7.

6. En los casos en que los datos contenidos en la imagen enviada por la aplicación PREP CATD o PREP Casilla del Acta PREP, imposibiliten la captura de la información, el capturista deberá clasificarla en la TCA como “ilegible”. El sistema la deberá dejar disponible para que un segundo capturista en el CCV pueda intentar su captura. En caso de que haya sido clasificada nuevamente como ilegible y que en la verificación se defina que es posible obtener los datos necesarios para capturar, se remite al Centro de Verificación para su resolución definitiva.

   Comentarios: La mayoría de las Actas PREP provenientes de PREP Casilla tenían una muy mala calidad de la imagen. Para poder rechazar la imagen, el capturista tiene que pedir a su supervisor que ingrese sus credenciales. MV F5-A-4_1-4, F5-A-5_1-4.

7. Todas las imágenes de las Actas PREP que se hayan digitalizado mediante la aplicación PREP CATD o PREP Casilla serán enviadas al CRID, y serán a su vez enviadas para su captura en los CCV siempre y cuando no hayan sido previamente capturadas mediante PREP CATD, conforme a la solicitud de los capturistas siguiendo el procedimiento de captura descrito en el numeral 29.

5.6.5. Del proceso de captura en los CATD en Simulacro 1

Comentario general:
No se realiza ninguna captura en los CATD, solamente se realiza la fase de digitalización. Por lo que la captura de todas las actas se realiza en los CCV. El medio de verificación (MV) de esta etapa son los formularios F5-A-4_1, F5-A-4_2, F5-A-5_1, F5-A-5_2.

1. La captura de la información en los CATD se realizará directamente de las Actas PREP que fueron acopiadas. Una vez capturados los datos de identificación del AEC, PREP CATD verificará de manera automática si existe una captura previa y en caso de ser así, enviará un mensaje y no permitirá nuevamente su captura.

2. La modalidad de captura en PREP CATD se podrá habilitar en los siguientes casos:
   1. Se hayan digitalizado la totalidad de Actas PREP que corresponda acopiar al CATD conforme al Distrito o Municipio de que se trate, o se hayan agotado los medios para la recuperación de las actas.
   2. No existan actas por acopiar, aun y cuando no se haya alcanzado la totalidad de la digitalización de estas, atribuido lo anterior al retraso en la entrega de paquetes electorales.

3. La fecha y hora de acopio será ingresada en PREP CATD por el capturista, tomando la fecha y hora especificada en el Acta PREP de manera manual por el acopiador.

4. En PREP CATD, un capturista registrará los siguientes datos:
    1. Los datos de identificación del Acta PREP los cuales podrá ingresar mediante la lectura del código QR. En caso de que los datos del código QR no coincidan con los estipulados por el FMDC, o el Acta no cuente con código QR, el capturista deberá ingresar de manera manual los datos de identificación de la casilla siendo estos: Entidad federativa, distrito electoral local, sección, tipo y número de casilla y municipio.
    2. La fecha y hora de acopio.
    3. El total de boletas sobrantes, total de personas que votaron, total de representantes de los partidos políticos y de candidaturas independientes acreditados ante casilla que votaron, y total de votos sacados de la urna.
    4. Los votos obtenidos por los partidos políticos y las candidaturas, sean estas independientes, por partido político, por candidatura común o por coalición en cualquiera de sus combinaciones, según sea el caso;
    5. El total de votos, total de votos nulos y total de votos para candidaturas no registradas.

5. Concluida la primera captura, el PREP CATD solicitará que el mismo capturista realice una segunda captura volviendo a registrar los datos asentados en el Acta PREP. PREP CATD hará una validación comparando que los datos capturados en ambas ocasiones coincidan. Si los datos son iguales, la fase de captura de esa AEC concluye.

6. En caso de que los datos capturados en dos ocasiones no coincidan, PREP CATD solicitará se realice una tercera captura, en caso de ser coincidente con alguna de las dos primeras la fase de captura de esa AEC concluye. Si ninguna de las 3 capturas coincide, PREP CATD de manera automática turnará el AEC al Centro de Verificación para su resolución, con lo que concluiría su etapa de captura y verificación.

7. En los casos en que los datos contenidos en el Acta PREP imposibiliten la captura de la información, el capturista deberá clasificarla en PREP CATD como “ilegible”. El sistema la deberá dejar disponible para que un segundo capturista en algún CCV pueda intentar su captura. En caso de que haya sido clasificada nuevamente como ilegible y que en la verificación se defina que es posible obtener los datos necesarios para capturar, se remite al Centro de Verificación para su resolución, con lo que concluiría su etapa de captura y verificación.

8. Se deberá realizar la captura de todas las Actas PREP acopiadas y digitalizadas en el CATD conforme a la solicitud de los capturistas, siguiendo el procedimiento de captura descrito en el numeral 38. Lo anterior, siempre y cuando no haya sido previamente capturada en algún CCV.

5.6.6. Del Proceso de Verificación de Datos en Simulacro 1

Comentario general:
El verificador deberá de contar con un gafete de identificación. El verificador cuenta con las credenciales para tener acceso al sistema, las cuales se le fueron otorgadas en un papel impreso. El verificador cuenta con un manual de usuario para el uso del sistema, pero los supervisores son los encargados de auxiliar en caso de haber un problema. El capturista cuenta con un casillero asignado para dejar sus

pertenencias. Todos los operadores fueron capacitados para los roles de capturista 1, capturista 2, verificador 1 y verificador 2. El medio de verificación (MV) de esta etapa son los formularios F5-A-6_1_1, F5-A-6_1_2, , F5-A-6_2_1, F5-A-6_2_2 .

1. Las actas que cumplieron con la fase de captura y verificación serán transmitidas de manera automática por el CRID al CCV donde personal asignado a este realizará la verificación de la información de todas las Actas PREP.

   Comentarios:_Las actas son transmitidas de manera automática al CCV. En la mayoría de las ocasiones las actas llegaban con retraso al CCV, principalmente las actas provenientes del CATD. MV F5-A-6_1_1-1.

2. El personal asignado a la verificación de información tendrá como objetivo corroborar que los datos previamente capturados, coincidan con los datos de la imagen del Acta PREP de la casilla correspondiente digitalizada mediante PREP CATD o PREP Casilla. Si los datos coinciden se registrará el Acta como correcta y se publicará; si se detecta algún error, se registrará el Acta como incorrecta en el sistema informático.
   El sistema informático, al recibir un acta como incorrecta, la enviará al Centro de Verificación para su resolución definitiva.

   Comentarios: El verificador deberá de estar en el CCV que se le haya asignado. El verificador confirma su acceso al sistema, y que no exista una falla en la conexión. El primer verificador corrobora que los datos capturados coincidan con los datos asentados del acta. El segundo verificador corrobora que los datos capturados coincidan con los datos asentados del acta. Si el acta se clasifica como "ilegible", es necesario que el supervisor ingrese sus credenciales. Posteriormente se remitirá al Centro de Verificación para su resolución definitiva, de lo contrario se manda para la publicación, más no se contabiliza. MV F5-A-6_1_1-2, F5-A-6_1_1-3, F5-A-6_1_2-1, F5-A-6_1_2-2, F5-A-6_1_2-3, F5-A-6_1_2-4, F5-A-6_1_2-5.

3. El sistema informático deberá mantener un registro de la actividad de todas las Actas PREP, con el propósito de garantizar la confianza, transparencia y certeza respecto al presente proceso técnico operativo.

   Comentarios: Existe un módulo el cual solo tiene acceso el coordinador del CCV, en donde se puede observar el total de Actas capturadas, Actas verificadas, desglosarse por operador, o cambiar roles a los operadores.

5.6.7. De la Publicación de Resultados en Simulacro 1

Comentario general:

La publicación se realiza de manera correcta, obteniendo los datos necesarios. Se publica por cada nivel de agregación de acuerdo con lo establecido. Se encuentran disponibles las actas para su descarga. El medio de verificación (MV) de esta etapa es el formulario F5-A-7.

1. La publicación de resultados de todas las Actas PREP que cumplieron con la fase de verificación, deberá iniciar a las 20:00 horas (tiempo del centro del país) del 6 de junio de 2021, posterior a la validación del tercero con fe pública de que las bases de datos se encuentran en ceros. Para el procedimiento de validación mencionado, se deberán tomar las previsiones necesarias para que éste concluya previo al inicio de publicación de resultados.

2. Cada hora se generarán, por lo menos, tres actualizaciones tanto de los datos e imágenes, así como de las bases de datos que contengan los resultados electorales preliminares con la finalidad de publicarlos en el portal oficial del IETAM y en su caso, a través de los difusores oficiales.

3. En virtud de que la fase de publicación implicará la trasmisión de datos e imágenes, es posible que cuando los datos estén publicados en el portal del PREP, las imágenes de las Actas PREP se encuentren aún en proceso de publicación.

4. Los datos a publicar del Acta PREP, serán los establecidos en el numeral 30 del Anexo 13 del Reglamento de Elecciones.

5.6.8. Del Empaquetado de Actas en Simulacro 1

Comentario general:
La fase de empaquetado de actas no se auditó en el Simulacro 1.

1. Concluidas las fases de acopio, digitalización, captura y verificación, publicación y cotejo, se llevará a cabo el empaquetado de actas ordenándolas por tipo de elección, sección, tipo de casilla y número de casilla (cuando aplique).

   Concluido el empaquetado, se hará entrega de las Actas PREP al Presidente del Consejo Distrital para su guarda y custodia.

5.6.9. De la Publicación de Resultados en Simulacro 2

Comentarios generales:
- La publicación se realiza en automático y de manera correcta, obteniendo los datos necesarios.
- Se publica por cada nivel de agregación de acuerdo con el INE.
- Se encuentran disponibles las actas para su descarga, ya sean actas que contaron en el total de los votos, o que no contaron y fueron rechazadas.

5.6.10. Sobre la Captura de Datos provenientes de toma fotográfica (PREP Casilla) y digitalización (PREP CATD) en Simulacro 2.

Comentarios generales:
- El capturista cuenta con un gafete de identificación.
- El capturista cuenta con las credenciales necesarias para el sistema. Para el simulacro 2 el supervisor ingresó las credenciales al sistema para cada capturista.
- El capturista deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el supervisor a cargo.

- El capturista realiza la solicitud del Acta PREP. Hubo ocasiones en donde al solicitar el Acta PREP el sistema se queda congelado por aproximadamente 3 segundos.
- El capturista tiene acceso al Acta PREP y al registro de datos.
- El capturista realiza el registro de los datos asentados en el Acta PREP.
- El capturista clasifica el Acta PREP como “ilegible”. Hubo ocasiones en donde se marcó como “ilegible” el Acta PREP y se pasaba al Centro de Verificación para su solución. Para realizar esta acción es necesaria la autorización del supervisor.
- El capturista cuenta con un manual de usuario digital para el uso del sistema. Se tiene un manual de usuario físico para todos los capturistas.
- El capturista obtuvo la capacitación necesaria para realizar el proceso.
- Cada que el capturista necesita abandonar su área de trabajo cierra sesión en el sistema. Por lo que al volver el supervisor tiene que a ingresar nuevamente las credenciales para iniciar sesión.
- Hubo actas recibidas que fueron rechazadas debido a que la imagen era ilegible o estaba borrosa, como consecuencia de error del CAEL que manipula el PREP Casilla.

5.6.11. Verificación de Datos de Actas PREP en Simulacro 2

Comentarios generales:

- El verificador cuenta con gafete de identificación.
- El verificador cuenta con las credenciales necesarias para el sistema. Para el simulacro 2 el supervisor ingresó las credenciales al sistema para cada capturista.
- El verificador deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el supervisor a cargo.
- El verificador corrobora que los datos capturados coincidan con los datos de la imagen del Acta PREP digitalizada.
- El verificador clasifica el Acta PREP como “ilegible”. Hubo ocasiones en donde se marcó como “ilegible” el Acta PREP y se pasaba al Centro de Verificación para su solución. Para realizar esta acción es necesaria la autorización del supervisor.
- Hay error en el registro de los datos y los datos asentados en el Acta PREP. Hubo ocasiones en que si sucedió, por lo que se pasa al Centro de Verificación.
- El verificador cuenta con un manual de usuario digital para el uso del sistema. Se tiene un manual de usuario físico para todos los capturistas.
- El verificador obtuvo la capacitación necesaria para realizar el proceso.
- Cada que el verificador necesita abandonar su área de trabajo cierra sesión en el sistema. Por lo que al volver el supervisor tiene que a ingresar nuevamente las credenciales para iniciar sesión.

5.6.12. Centro de Verificación en Simulacro 2

Comentarios generales:

- El operador del CV cuenta con un gafete de identificación.
- El operador del CV cuenta con las credenciales necesarias para el sistema. Para el simulacro 2 el supervisor ingresó las credenciales al sistema para cada capturista.
- El operador del CV deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el supervisor a cargo.

- El operador del CV realiza la solicitud del Acta PREP y verifica el tipo de inconsistencia en el Acta PREP.
- El operador del CV realiza la primera captura del Acta PREP.
- El operador del CV realiza la segunda captura del Acta PREP.
- El operador del CV marca como “ilegible” el Acta PREP. Hay ocasiones donde los operadores del CV no pueden resolver la inconsistencia, por lo que solicitan ayuda a su supervisor antes de marcar el Acta PREP como “ilegible” y que no se contabilice.

5.6.13. Del Acopio en Simulacro 2

- El acopiador cuenta con un gafete de identificación.
- El acopiador verifica que los datos de identificación del Acta PREP sean legibles, de no ser así, deberá de acudir con el encargado del Acta PREP.
- El acopiador deja constancia de la fecha y hora (formato 24 hrs.) de acopio en el Acta PREP. Juntaba varias Actas PREP y les escribía la misma fecha y hora.
- Si el acopiador tarda más de lo necesario en realizar alguna actividad de la fase, el coordinador le brindará apoyo.
- El acopiador es el encargado del flujo de actas. En el simulacro 2 no se llevó un seguimiento de a quien le asignaba cada Acta PREP.
- El acopiador entregaba varias Actas PREP a la vez a los digitalizadores.

5.6.14. De la Digitalización en Simulacro 2

- El digitalizador cuenta con gafete de identificación.
- El digitalizador cuenta con las credenciales necesarias para el sistema. Las credenciales se les otorgaron en un papel impreso.
- El digitalizador deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el coordinador.
- El digitalizador realiza la captura digital de la imagen mediante PREP CATD utilizando el código QR. En algunas ocasiones el PREP CATD no encontraba el Acta PREP utilizando el código QR.
- El digitalizador revisa la calidad de la imagen del Acta PREP en el PREP CATD. La calidad de la imagen siempre era buena, esto debido a las cajas que se implementaron para la digitalización.
- El digitalizador ingresa la información del Acta PREP de manera manual. En algunas ocasiones el PREP CATD no encontraba el Acta PREP utilizando el código QR, por lo que el digitalizador ingresaba la información de manera manual.
- Se transmite el Acta PREP al CRID. Había un retraso al enviar las imágenes de las Actas PREP, parece ser que era por una falla de la conexión a Internet.
- Al finalizar de digitalizar todas las Actas PREP (aproximadamente 422 Actas en total) quedaban 20 Actas pendientes de envío, esto debido al retraso. El coordinador comentó que si el PREP CATD se actualizaba iba a ser necesario realizar nuevamente la digitalización de todas las Actas PREP, debido a que en la aplicación ya no aparece cuales son las Actas PREP que quedaron pendientes de enviar. Se sugiere que se escriba en disco (puede ser un archivo .txt) aquellas Actas PREP que están pendientes de enviar para que de esta manera el acopiador las detecte y solo sea necesario digitalizar esas y no todas nuevamente.

5.6.15. Sobre Captura de Datos provenientes de toma fotográfica (PREP Casilla) y digitalización (PREP CATD) en Simulacro 3

- El capturista cuenta con un gafete de identificación.
- El capturista no cuenta con las credenciales necesarias para el sistema. El supervisor tiene las credenciales de todos los operadores y es el encargado de ingresar al sistema.
- El capturista deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el supervisor a cargo.
- El capturista realiza la solicitud del Acta PREP. Hubo ocasiones en donde al solicitar el Acta PREP el sistema se queda congelado por aproximadamente 3 segundos.
- El capturista obtuvo la capacitación necesaria para realizar el proceso.
- El capturista tiene acceso al Acta PREP y al registro de datos.
- El capturista clasifica el Acta PREP como “ilegible” (rechaza el Acta PREP). Hubo ocasiones en donde se marcó como “ilegible” el Acta PREP y se pasaba al Centro de Verificación para su solución. Para realizar esta acción es necesaria la autorización del supervisor.
- El capturista cuenta con un manual de usuario digital para el uso del sistema. Se tiene un manual de usuario físico para todos los capturistas.
- Cada que el capturista necesita abandonar su área de trabajo no se cierra sesión en el sistema, solo cuando va a comer.

5.6.16. Verificación de Datos de Actas PREP en Simulacro 3

- El verificador cuenta con gafete de identificación.
- El verificador no cuenta con las credenciales necesarias para el sistema. El supervisor tiene las credenciales de todos los operadores y es el encargado de ingresar al sistema.
- El verificador deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el supervisor a cargo.
- El verificador corrobora que los datos capturados coincidan con los datos de la imagen del Acta PREP digitalizada.
- El verificador clasifica el Acta PREP como “ilegible”. Hubo ocasiones en donde se marc como “ilegible” el Acta PREP y se pasaba al Centro de Verificación para su solución. Para realizar esta acción es necesaria la autorización del supervisor.
- Hay error en el registro de los datos y los datos asentados en el Acta PREP. Hubo ocasiones que si sucedió, por lo que se pasa al Centro de Verificación.
- El verificador cuenta con un manual de usuario digital para el uso del sistema. Se tiene un manual de usuario físico para todos los capturistas.
- El verificador obtuvo la capacitación necesaria para realizar el proceso.
- Cada que el capturista necesita abandonar su área de trabajo no se cierra sesión en el sistema, solo cuando va a comer.
- En una ocasión un verificador realizó la solicitud de un Acta PREP y el sistema quedó congelado por aproximadamente 5 minutos, el supervisor brindó apoyo. Se tuvo que forzar el cierre del sistema desde el administrador de tareas, para así ingresar nuevamente.

5.6.17. Centro de Verificación en Simulacro 3

- El operador del CV cuenta con un gafete de identificación.
- El operador del CV no cuenta con las credenciales necesarias para el sistema. El supervisor tiene las credenciales de todos los operadores y es el encargado de ingresar al sistema.

- El operador del CV deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el supervisor a cargo.
- El operador del CV realiza la solicitud del Acta PREP y verifica el tipo de inconsistencia en el Acta PREP.
- El operador del CV realiza la primera captura del Acta PREP.
- El operador del CV realiza la segunda captura del Acta PREP.
- El operador del CV marca como "ilegible" el Acta PREP. Hay ocasiones donde los operadores del CV no pueden resolver la inconsistencia, por lo que solicitan ayuda a su supervisor antes de marcar el Acta PREP como "ilegible" y que no se contabilice. Para estos casos no se cuenta con un módulo que permita especificar el por qué se decidió rechazar el Acta PREP, para esto lo escriben en una nota. Se sugiere agregar un módulo que permita llevar el control de las Actas PREP rechazadas que no se contabilizan.

5.6.18. Del Acopio en Simulacro 3

- El acopiador cuenta con un gafete de identificación.
- Si el acopiador tarda más de lo necesario en realizar alguna actividad de la fase, el coórdinador le brinda apoyo.
- El acopiador es el encargado del flujo de actas. No se lleva un seguimiento de a quien se le entrega cada Acta PREP, solo se sigue un orden de entrega.
- El acopiador entregaba varias Actas PREP a la vez a los digitalizadores. Al ser simulacro no afecta.
- El acopiador verifica que los datos de identificación del Acta PREP sean legibles, de no ser así, deberá de acudir con el encargado del Acta PREP.
- El acopiador deja constancia de la fecha y hora (formato 24 hrs) de acopio en el Acta PREP. Juntaba varias Actas PREP y les escribía la misma fecha y hora.

5.6.19. De la Digitalización en Simulacro 3

- El digitalizador cuenta con gafete de identificación.
- El digitalizador cuenta con las credenciales necesarias para el sistema. Las credenciales se les otorgaron en un papel.
- El digitalizador deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el coordinador.
- El digitalizador obtuvo la capacitación necesaria para realizar el proceso.
- El digitalizador realiza la captura digital de la imagen mediante PREP CATD utilizando el código QR. En algunas ocasiones el PREP CATD no encontraba el Acta PREP utilizando el código QR, por lo que se realizaba el registro de los datos de forma manual.
- El digitalizador revisa la calidad de la imagen del Acta PREP en el PREP CATD. La calidad de la imagen siempre era buena, esto debido a las cajas que se implementaron para la digitalización.
- Se transmite el Acta PREP al CRID. Había un retraso en un solo dispositivo al enviar las imágenes de las Actas PREP. Quedaron 11 actas pendientes de enviarse por aproximadamente 1 hora, el coordinador le indico que cambiara de dispositivo por uno que tenían de respaldo. Al cambiar de dispositivo se digitalizaron nuevamente aquellas actas pendientes.

5.6.20. Captura y Verificación de Datos provenientes de Digitalización en Simulacro 3

- El capturista cuenta con un gafete de identificación.
- El capturista cuenta con las credenciales necesarias para el sistema, las cuales se le fueron

asignadas mediante un papel impreso, cada día son credenciales diferentes.
- El capturista cuenta con un manual de usuario para el uso del sistema.
- La mayoría de las actas que se digitalizaron habían sido ya capturadas por PREP Casilla, por lo que muchas veces no se realizó el proceso de captura en el CATD.
- Durante el simulacro no se encontraba un acta en el sistema para capturar, se tenía de manera física pero el sistema no mostraba la opción para capturarla.

5.6.21. De la toma fotográfica del Acta PREP en la casilla en Simulacro 3

- El CAEL cuenta con un chaleco de identificación otorgado por el INE.
- El CAEL obtuvo una capacitación antes de realizar el simulacro por parte de su supervisor del INE.
- El CAEL cuenta con las credenciales necesarias para ingresar al sistema.
- El CAEL no cuenta con un manual de usuario.
- Al CAEL se le asignó un dispositivo móvil en el cual tenía instalado el PREP Casilla.
- El CAEL al tener una duda se dirige con su coordinador.
- El CAEL verifica que todos los datos de identificación del Acta PREP sean legibles y estén completos.
- El CAEL coloca el Acta PREP de tal forma que no presente dobleces.
- El CAEL verifica que no se incluyan elementos ajenos al Acta PREP en la toma fotográfica. El CAEL indicó que a veces es necesario colocar algún objeto sobre el Acta PREP para que esta se quede en su lugar mientras realiza la toma fotográfica.
- El CAEL verifica que la imagen tomada sea legible.
- El CAEL no cuenta con un lugar asignado para la toma fotográfica.

5.7 Resumen de resultados

Con base en lo identificado y observado con la aplicación de los cuestionarios generados, se hizo un análisis para determinar el cumplimiento de las indicaciones del PTO. Esto involucró observar el funcionamiento del sistema informático, las tareas que realizaron los operadores y tomar en cuenta las opiniones a partir de las entrevistas realizadas a los empleados del proveedor del sistema informático.

De manera descriptiva, los resultados de la auditoría de la operatividad del sistema informático PREP pueden sintetizarse en los siguientes puntos:

1- Si bien los operadores del sistema informático tienen una mejor capacitación respecto a las elecciones pasadas, aún se observan algunos puntos del PTO objeto de mejora. Se puede observar que en la medida en que los operadores han tenido mejor capacitación, han adquirido también mayor pericia. Se observó que la capacidad de los operadores ha ido incrementalmente mejorando durante el desarrollo de los simulacros 1, 2 y 3.

2- Si bien los operadores tienen las facultades para operar el sistema, el control para saber si lo están haciendo bien o no aún es muy mejorable. Mediante el sistema informático, resulta muy difícil para los supervisores y los coordinadores, tener una manera explícita de conocer lo que ha realizado cada operador. Esta situación ha sido solventada mediante los coordinadores de grupo y el equipo de coordinación en el CCV. Es deseable contar con módulos del sistema que faciliten la gestión de las actividades por parte de los supervisores y coordinadores.

3- Si bien el sistema informático cumple la mayoría de los lineamientos del PTO, algunos aspectos del diseño y funcionamiento del sistema informático son mejorables. Algunos de estos aspectos suceden a nivel interno del sistema y resulta muy difícil apreciarlos mediante su operación. No obstante, la versión final del sistema informático cumple en su totalidad los aspectos funcionales requeridos en el PTO.

4- Un aspecto mejorable para el sistema, es la deseable capacidad de contar con módulos adicionales que faciliten aspectos altamente necesarios como la visualización de conteos internos, módulos para supervisores, coordinadores de CATDs y coordinadores de CAEL. Esta observación ha quedado como recomendación para versiones futuras del PREP.

Parte III

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

Esta sección describe los resultados de las pruebas realizadas al sistema, a nivel aplicación y base de datos. En primer lugar, se presentan algunos elementos preliminares (propósito, objetivos, alcance, estrategia), subsecuentemente se muestra la metodología para la obtención de datos y evidencias. Finalmente se presentan los hallazgos encontrados, vulnerabilidades y posibles amenazas.

6.1 Objetivo

Analizar el sistema informático del PREP, mediante la realización de pruebas funcionales de caja negra, para evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares.

6.2 Alcance

Las pruebas de caja negra se realizaron con base en la funcionalidad del sistema informático del PREP, y consideraron al menos los siguientes aspectos:

- Se analizó el funcionamiento de la aplicación en relación con las fases del proceso técnico operativo, considerando todas las fases del Proceso Técnico Operativo que incluyen, **toma fotográfica, acopio, digitalización, captura, validación y publicación de resultados,** mediante flujos completos e interacción entre los diversos módulos.
- Se verificó el cumplimiento de las especificaciones funcionales y requerimientos contenidos en la documentación técnica y normatividad aplicable que fue proporcionada por el IETAM.
- Se verificó la correspondencia de la captura de los datos plasmados en las Actas PREP con los presentados en la publicación, mediante reportes desplegados por el PREP que consideraron datos, imágenes y bases de datos.

Las pruebas funcionales de caja negra se realizarán sobre los siguientes módulos del sistema informático del PREP:

I. Módulo PREP Casilla
   - Obtención de toma fotográfica.
   - Envío de la imagen al módulo de captura.
   - Captura de la información contenida en las Actas PREP.

II. Módulo de Digitalización, Captura y Validación
   - Obtención de la imagen digital del acta.
   - Captura de la información contenida en las Actas PREP.
   - Validación de la información capturada.

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

El informe de las pruebas realizadas a nivel aplicación está acotado por los escenarios de prueba y atributos de calidad definidos en el plan de pruebas.

6.3 Metodología

La metodología fue divida en dos partes: 1) Nivel Aplicación y 2) Nivel Base de Datos, las cuales se presentan en las siguientes subsecciones.

6.3.1 Nivel Aplicación

A partir del documento de plan de pruebas, se procedió a ejecutar los casos de prueba de los módulos principales del sistema. Para esto, el equipo de pruebas del ente auditor se desplazó a diferentes ubicaciones en el estado de Tamaulipas donde se encuentran desplegados los módulos **CCV y CATD.**
De estas visitas y de la aplicación de los casos de prueba definidos, se realizaron varias observaciones. El plan de pruebas también definió una serie de atributos de calidad del sistema que fueron verificados a través de un conjunto de listas de verificación (checklist).

6.3.2 Nivel Datos

Para la validación de requerimientos funcionales se definió el plan de pruebas funcionales a nivel de base de datos (LA2-E1). Esta validación requirió de los siguientes recursos:

- Esquema de Base de datos (Script, modelo entidad relación, queries, credenciales).
- Esquema de almacén de datos (Script para guardar, enviar la imagen, consultar la imagen y credenciales).
- Acceso a los logs de MySQL (Error Log, The General Query Log, Slow Query).

Dados estos insumos se realizó un conjunto pruebas funcionales, pruebas que validan las operaciones CRUD (Crear, Leer, Actualiza y Borrar) para base de datos y del sistema de archivos.
Para cada prueba se propuso un conjunto valores o parámetros de entrada, así como también la salida esperada, mismo que se coteja con el resultado obtenido, después de que la prueba es aplicada. Este proceso se ilustra en la Figura 6.1, algunas de las actividades de dicho proceso se describen a continuación.

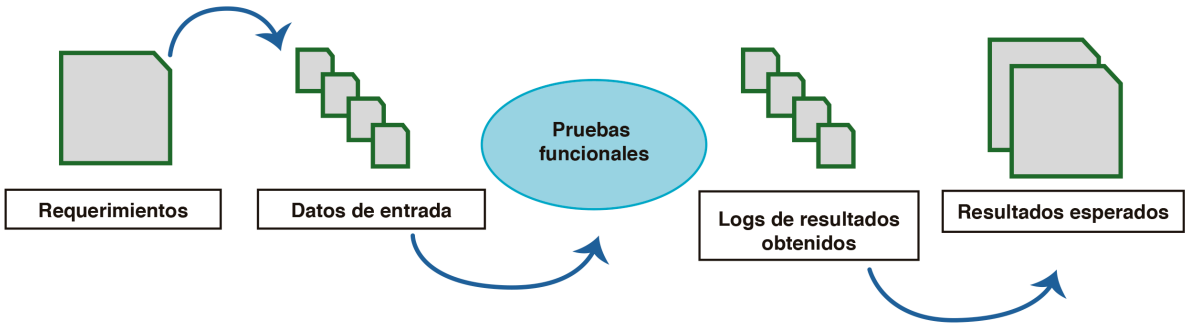


Figura 6.1 Flujo general para la validación de los requerimientos funcionales, nivel base de datos.

- Requerimientos funcionales: En esta actividad se identifican los requerimientos funcionales del sistema informático PREP para la capa de Datos.

- Datos de entrada: Para cada requerimiento funcional se crea un conjunto de datos de entrada que se describe en el LA2-E1.

- Pruebas funcionales: Hace referencia a las pruebas que harán para validar cada requerimiento funcional, se describen en el LA2-E1.

- Logs de resultados: Para cada prueba se debe de tener un registro donde se visualice si tuvieron éxito la entrada de datos o si surgió algún error, usando la información del registro se compara si la salida de cada prueba es igual a la salida esperada con el fin de validar que cada requerimiento funcional funcione correctamente y que exista una correspondencia de la información insertada a nivel de aplicación en la base de datos.

Las pruebas de caja negra fueron realizadas por personal del IETAM en conjunto con el Ente Auditor. Para estas pruebas se ejecutaron los casos de uso definidos LA1-E1 y se utilizaron como evidencias las trazas generadas por la base de datos del sistema PREP, capturas de pantalla y la bitácora del sistema PREP. Estas evidencias pueden encontrarse en los anexos N1/Evidencias de este documento. Con esta información y conforme a las observaciones realizadas en los simulacros 1 y 2, se obtuvieron resultados para cada una de las pruebas funcionales. Adicionalmente, se optó por aplicar la siguiente metodología basada en los siguientes recursos e insumos:

- Personal capacitado por parte del PROVEEDOR, que tenga conocimientos sobre la implementación de los requerimientos funcionales relativos a la base de datos y sistema de archivos.

- Acceso al web service de auditoria donde se registran todas las actividades realizadas a cada acta, de las pruebas operativas por parte de la capa de Aplicación y Operativo.

- Acceso al web service de auditoría de las pruebas operativas antes y durante los simulacros 1, 2, 3 y jornada electoral.

Obtenidos estos insumos se procedió de la siguiente forma:

- Se recopilaron evidencias a través de un checkList.

- Se recopilaron evidencias a través de la información generada por los web services mencionados. Esta recopilación tuvo lugar en los CCVs y CATD ubicados en Ciudad Victoria, Tamaulipas durante las fechas programadas para la aplicación de pruebas por parte del ente auditor y los simulacros 1,2, 3.

- El ente auditor desarrolló un script para consumir y resguardar la información que genera el web service de auditoría. Posteriormente se realizaron actividades de análisis enfocadas a validar y verificar la consistencia de la información según los requerimientos funcionales (insertar, actualizar, borrar y consulta de la información de base de datos y del sistema de archivos). El flujo para este análisis se muestra de forma general en la Figura 6.2.

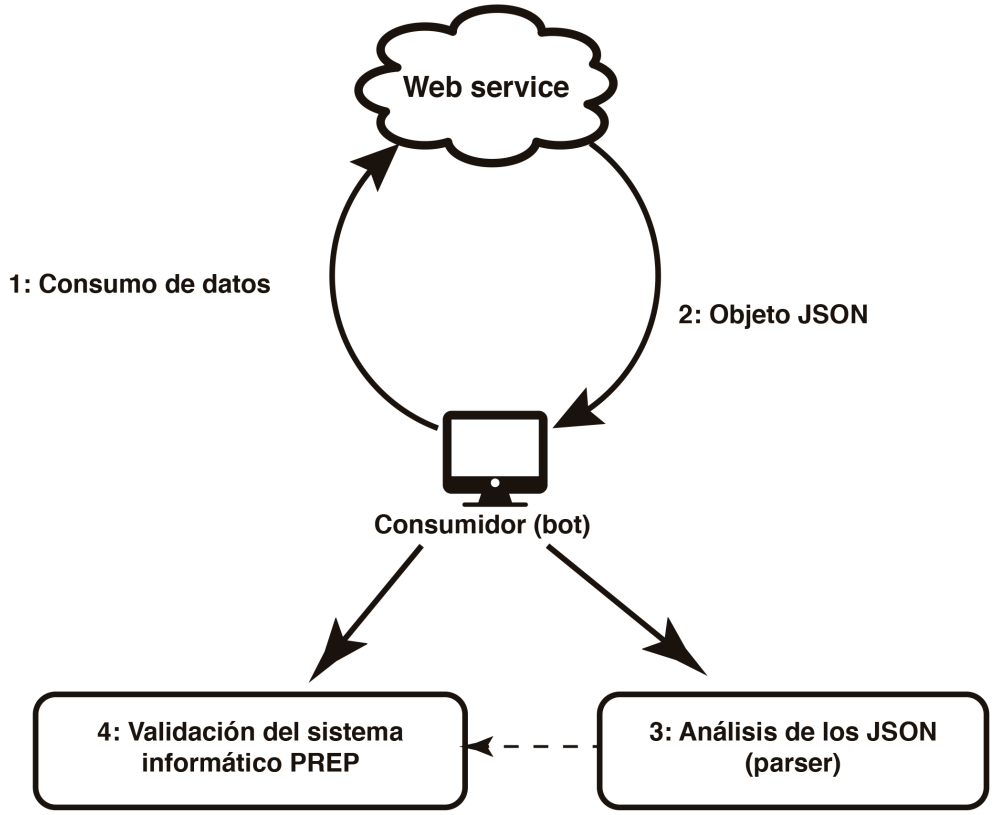


Figura 6.2 Flujo general para la validación de los requerimientos funcionales a través de la información del log del web service, nivel base de datos.

El consumidor establecerá una comunicación y realizará peticiones al web service de auditoría. El web service recibirá todas las peticiones del consumidor y responde con un objeto JSON con la información solicitada. Una vez obtenido un objeto JSON se hará una actividad de análisis de la información. Una vez identificada la información del documento JSON, se analizará la información con el fin de verificar los requerimientos funcionales y la correspondencia de la información de las pruebas operativas.

6.4 Criterios utilizados para la auditoria

A continuación, se enuncian los criterios utilizados:

- El sistema ofrece los mecanismos necesarios para dar cumplimiento a los procesos de captura, validación, cómputo y publicación señalados por el IETAM.
- Cada mecanismo deberá ser desplegado según corresponda en los CATDs y CCV de acuerdo con los lineamientos del IETAM

- El sistema deberá garantizar la integridad y consistencia de los datos a través de estrategias que integren personas, tecnología, procesos y buenas prácticas.
- Se debe garantizar la imparcialidad en el procesamiento de datos generados por el sistema respecto a afinidades políticas o intereses personales.
- Los datos publicados deberán ser consistentes y presentados de acuerdo con lo establecido por los lineamientos del IETAM.

6.5 Resultados.

A continuación, se presentan los resultados de las pruebas funcionales a nivel aplicación y a nivel de base de datos.

6.5.1 Nivel de Aplicación

Tabla 6.1 Pruebas funcionales de caja negra a nivel sistema.

ID PRUEBA	DESCRIPCION	DATOS ENTRADA	ACCIONES EJECUTADAS	RESULTADOS ESPERADOS	RESULTADOS OBTENIDOS	OBSERVACIONES
PF-01	Nombre: -Toma Fotográfica **Precondiciones**: -Acta Física -Dispositivo Móvil con aplicación PREP Casilla. -Usuario Autenticado -Contraseña **Módulo**: PREP Casilla	Acta Física	1. Seleccionar la casilla. 2. Tomar la fotografía del acta de la casilla seleccionada. 3. Envía la fotografía	1. Muestra un mensaje notificando el envío de la fotografía.	Se realiza la toma fotográfica y se envía correctamente al servidor.	La aplicación no verifica la orientación de la imagen, por lo que existen tomas de actas con orientación vertical.
PF-02	Nombre: -Escanear Acta **Precondiciones**: -Acta Física -Selección de escáner -Aplicación Controlador disponible -Sesión de usuario iniciada **Módulo**: Controlador Tamaulipas	Acta Física	1. Buscar acta a escanear (Código QR o datos de identificación) 2. Cargar datos de acta requerida. 3. Invocar la funcionalidad de escaneo de actas 4. Enviar imagen escaneada al servidor	Imagen del acta	Imagen del acta	En esta versión se incluye la denominada "Caja Digitalizadora" que resuelve los problemas de tomas Con orientaciones que dificulten la lectura u omitan partes del acta.
PF-03	Nombre: -Captura o digitalización de acta **Precondiciones**: Paquete de actas asignadas al capturista **Módulo**: Controlador Tamaulipas	Acta Física	**1.** Capturar fecha y hora de captura de votos 1. Capturar primer conteo de votos de acuerdo al acta física 2. Capturar segundo conteo de votos de acuerdo al acta física. 3. Enviar datos de captura.	1. Mensaje de que los datos capturados fueron enviados correctamente	1. Mensaje que confirma que los datos capturados fueron enviados correctamente.	1. La fechas se generan automáticamente por el sistema, esto evita errores inducidos por el usuario

ID PRUEBA	DESCRIPCION	DATOS ENTRADA	ACCIONES EJECUTADAS	RESULTADOS ESPERADOS	RESULTADOS OBTENIDOS	OBSERVACIONES
	Acciones Excepcionales	Acta Física	1. Realizar intencionalmente conteos diferentes. 2. Ingresar votos que superen la lista nominal. 3. Desconectar intencionalmente el Internet durante el proceso de envió de datos.	1. Error por diferencia entre conteos. 2. Error por exceder lista nominal 3.El sistema deberá permitir el reenvío del acta capturada	1. Error por diferencia entre conteos. 2. No se presenta error o notificación cuando se excede la lista nominal. 3. El acta capturada se pierde o queda en un estado inválido el cual no es notificado al capturista.	1. Cada que se ingresen los conteos de manera diferente además de salir el error de cantidades diferentes siempre arroja el error "fecha de acopio no ingresada". 2. Se desconoce el tratamiento de aquellas actas que exceden la lista nominal. 3. No existe un mecanismo que informe al capturista el estado del acta que no se envío adecuadamente.
PF-04	**Nombre**: -Validación de Acta **Precondiciones**: Asignación de acta previamente capturada **Módulo**: Validación	1.Acta digitalizada (imagen y datos capturados)	1. Revisar los datos digitalizados con la imagen enviada. 2. En caso de ser correctos se deben enviar. 3. En caso contrario, se envía a validador	1. Notificación del sistema de que los datos fueron enviados. 2. Notificación de inconsistencias	1. Notificación del sistema de que los datos fueron enviados.	1. En esta versión se incluyó un mecanismo para la recuperación del sistema ante eventos inesperados (cierres de sesión, terminación de aplicación). Se recupera el último estado válido del acta
PF-05	Nombre: -Validación de acta 2 **Precondiciones**: Acta denegada previamente en el proceso de verificación	Cargar acta denegada asignada (asignación automática)	1. Realizar la primera validación corroborando que los datos capturados son realmente incorrectos. 2. Si la inconsistencia es real se envía al validador 2. 3. De lo contrario el validador envía como acta válida.	1. Notificación del sistema indicando el envío del acta, ya sea como acta válida o acta que requiere un proceso adicional de validación	1. Si bien no se presenta un error, el sistema no muestra un mensaje adecuado informando el estado de la ejecución	Como prueba adicional se ingreso un número de votos mayor al número de votante y no se notificó ningún error. Al momento de guardar un acta, si ciertos campos no han sido llenados, el sistema no lo permite. Sin embargo el sistema debería notificar cuales son los

ID PRUEBA	DESCRIPCION	DATOS ENTRADA	ACCIONES EJECUTADAS	RESULTADOS ESPERADOS	RESULTADOS OBTENIDOS	OBSERVACIONES
						campos faltantes o con error.
PF-06	Nombre: Cómputo de votos	Datos capturados a través de los procesos de captura y validación de actas	Verificar el cómputo de acuerdo con el proceso técnico operativo PTO.	No deberán existir cálculos porcentuales superiores al 100%	En la publicación de actas por distrito se presentan cálculos porcentuales superiores al 100%	Se argumenta que este error es debido a las casillas especiales. Sien embargo esto podría darse a malas interpretaciones de las personas que visualizan los resultados.
PF-07	Nombre: -Publicación de resultados preliminares **Precondiciones**: -Base de datos en ceros	Datos capturados a través de los procesos de captura y validación de actas.	1. La publicación de porcentajes, los decimales deberán ser expresados a cuatro posiciones. El decimal de la cuarta posición deberá truncarse y no redondearse. 2. Actualización periódica de datos.	Estos deberán estas acordes al PTO. Actualizaciones mínimo cada 20 minutos	Los resultados preliminares satisfacen los requerimientos del PTO. Actualizaciones cada 15 minutos.	3. Podría ser útil la notificación automática al usuario que una nueva actualización está disponible.

6.5.2 Nivel de base de datos.

La validación de los requerimientos funcionales relativos al nivel de datos, fueron realizados por medio de un checklist de lo observado en la documentación y las pruebas operativas realizadas por el ente auditor durante los tres simulacros. Como resultado para cada simulacro, se generó una lista de observaciones por cada una de las aplicaciones del sistema informático PREP, estas observaciones están enfocadas en la correspondencia de la información generada en las pruebas operativas y la información registrada en el log del web service de auditoría.

A continuación, se describen los análisis que realizaron al Simulacro 1, Simulacro 2 y Simulacro 3.

Pruebas funcionales de base de datos del PREP y sugerencias en Simulacro 1 y Simulacro 2

Tabla 6.2. Pruebas funcionales para la validación del PREP con resultados en Simulacro 1 y Simulacro 2

ID	Aplicación donde se realiza	Caso de uso	Tipo de query[1] o comando que se deben de ejecutar	Prueba	Donde lo solicita el IETAM o el INE	Observaciones
PF .1	N/A	Administrar roles de usuarios	El administrador de roles puede insertar, actualizar y borrar roles de usuario.	Crear, actualizar y borrar una serie de roles con los diferentes permisos.	Anexo técnico de Contrato de Servicios de Auditoría para el PREP 2021 [2] – "Pruebas funcionales de caja negra al sistema informático del PREP" y "Validación del sistema informático del PREP y de sus bases de datos".	El proveedor (IETAM) cuenta con un sistema desde el cual el administrador gestiona los roles de cada uno de los usuarios (Anexo Evidencias/SistemaAdminUsuarios.jpg), en las pruebas se detectó lo siguiente: • El administrador puede cambiar los roles de los distintos usuarios. • El administrador no puede crear ni borrar usuarios, en cambio, puede bloquearlos. • El administrador **no puede borrar ni crear roles**. Únicamente puede utilizar aquellos que **se han definido: Capturistas, verificadores y usuarios del centro de verificación**.
PF .2	N/A	Administrar usuarios	El administrador de usuarios puede insertar, actualizar y borrar usuarios.	Crear, actualizar y borrar por lo menos un usuario de cada rol existente.	Anexo técnico de Contrato de Servicios de Auditoría para el PREP 2021 [2] – "Pruebas funcionales de caja negra al sistema informático del PREP" y "Validación del sistema informático del PREP y de sus bases de datos".	Tanto la cantidad de usuarios como la cantidad de roles fueron definidos al diseñar el sistema, siendo un total de 140 (80 para CCV Victoria, 30 para CCV Madero y 30 para CCV Reynosa). Por tal motivo, el administrador no puede crear ni borrar usuarios. El administrador puede bloquear a los usuarios. Se realizó la prueba de bloqueo de usuarios a lo cual la traza obtenida por la base de datos muestra que se ejecutó correctamente.

PF .3	En todas las aplicaciones del sistema informá-tico PREP.	Autenticación de usuarios.	Queries y comando de conexión a las diferentes bases de datos y almacén de datos.	**Datos estructurados.** Realizar una serie de conexiones a las diferentes bases de datos locales, remotas, maestras y de solo lectura. **Datos no estructurados.** Realizar una serie de conexiones a los diferentes almacenes de datos, locales, remotos y del sistema de publicación.	Anexo técnico de Contrato de Servicios de Auditoría para el PREP 2021 [2] – "Pruebas funcionales de caja negra al sistema informático del PREP" y "Validación del sistema informático del PREP y de sus bases de datos".	Las aplicaciones presentan una interfaz la cual permite a el administrador y a las y los CAE locales iniciar una sesión en la aplicación móvil. La base de datos, esta no puede ser accedida a través de internet dado que se encuentra en una red privada. Al momento de transmisión se emplea un protocolo de reconocimiento entre los nodos emisor y receptor, a partir del cual, éste último, deberá identificar al emisor y su pertinencia y procede a su autenticación, permitiendo el registro de la información en la Base de Datos, o en su defecto, interrumpiendo la comunicación.
PF .4	Aplicación móvil PREP casilla.	**Datos estructurados.** En el caso de uso de la aplicación móvil, se identifica que el usuario puede guardar información en la base de datos local (del teléfono) y remota del CRID y al CATD.	**Datos estructurados.** Se prevé que el usuario realice la operación de insertar información en la base de datos local (en el móvil) y remota (CCV).	**Datos estructurados.** Ejecutar el query insert en la base de datos local (móvil) y la base de datos remota (CCV).	En el documento de "Proceso Técnico Operativo" en el apartado De la toma fotográfica del Acta PREP en la casilla.	Para la aplicación PREP Casilla en caso de que el teléfono celular pierda conexión a internet, la aplicación guardará las imágenes de las actas de la casilla y contienda correspondiente en la base de datos local del teléfono, marcando la casilla con color amarillo, que significa "pendiente por enviar" y una vez que detecte conectividad con la central, realizará el envío de manera automática.
PF .5	Aplicación móvil PREP casilla.	**Datos no estructurados.** Se identifica	**Datos no estructurados.** Se prevé que usuarios realice la operación de	**Datos no estructurados.** Escritura de imágenes en	En el documento de "Proceso Técnico Operativo" en	Para la aplicación PREP Casilla, en caso de que el teléfono celular pierda conexión a internet, la aplicación guardará las

		que la aplicación móvil puede guardar la imagen locamente (en el teléfono) y remotamente en el almacén de datos remoto en el CCV.	escritura al almacén de dato remoto (CCV) y local (móvil).	el almacén de datos remoto (CCV) y en dispositivo móvil.	el apartado De la toma fotográfica del Acta PREP en la casilla.	imágenes de las actas de la casilla. En la bitácora se pueden encontrar registros que corroboran esta acción, tales como el mostrado a continuación: “ El Acta 1145 Extraordinaria 02 ha sido guardada con éxito en ImagenActa por PREP Casilla. ”
PF .6	MCAD	**Datos no estructurados.** Se identifica que el MCAD realizará él envió de la clave HASH al CRID.	**Datos no estructurados.** Se prevé que la aplicación MCAD pueda ejecutar comandos de escritura al sistema de archivos del CRID.	**Datos no estructurados.** Realizar una serie de digitalizaciones y el envió de las claves Hash al sistema de archivos del CRID.	En el documento de “Proceso Técnico Operativo” en el apartado De la Digitalización.	**PREP CATD:** Esta aplicación móvil permite realizar la toma fotográfica del Acta PREP desde el CATD, revisar las imágenes de las actas digitalizadas para asegurar su calidad, para el posterior envío al CRID tanto de la imagen como la información de identificación del acta y su ***hash***, para su posterior captura. **PREP Casilla:** Esta aplicación móvil permite realizar la toma fotográfica del Acta PREP desde la casilla, revisar las imágenes de las actas digitalizadas para asegurar su calidad, para el posterior envío al CRID tanto la imagen como la información de identificación del acta y su ***hash***, para su posterior captura.
PF .7	MCAD	**Datos no estructurados.** Se identifica que el MCAD generará la clave HASH y se enviará al almacén	**Datos no estructurados.** Se prevé que el MCAD pueda ejecutar comandos de escritura en el almacén de datos en el CRID.	**Datos no estructurados.** Realizar una serie de digitalizaciones y su posterior escritura de la imagen al almacén de	En el documento de “Proceso Técnico Operativo” en el apartado De la Digitalización.	El MCAD generara de manera única y automática el hash mediante el algoritmo criptográfico denominado como funciones hash (sha256 y md5). Posteriormente, el MCAD transmite el Acta PREP al CRID para iniciar el proceso de captura de datos.

		de datos del CRID.		datos del CRID.		
PF .8	Aplicación móvil PREP CATD.	**Datos estructurados.** En el caso de uso del capturista en el CATD, se identifica que el capturista guarde la información del acta capturada en la base de datos local (CATD) y remota (CCV).	**Datos estructurados.** Se prevé que el usuario capturista pueda realizar la operación de insertar en la base de datos local (CATD) y remota (CCV).	**Datos estructurados.** Ejecutar queries de inserción a la base de datos local (CATD) y remota (CCV).	En el documento de "Proceso Técnico Operativo" en el apartado De la Captura y Verificación en el CATD.	Para la aplicación PREP CATD en caso de que el teléfono celular pierda conexión a internet, la aplicación guardará las imágenes de las actas de la casilla y contienda correspondiente en la base de datos local del teléfono, marcando la casilla con color amarillo, que significa "pendiente por enviar" y una vez que detecte conectividad con la central, realizará el envío de manera automática.
PF .9	Aplicación móvil PREP CATD.	**Datos no estructurados.** Se identifica que el capturista realice la escritura de la imagen en el almacén de datos local (CATD) y remoto (CCV).	**Datos no estructurados.** Se prevé que el usuario capturista pueda realizar las operaciones de escritura de imágenes a los almacenes de datos local (CATD) y remoto (CCV).	**Datos estructurados.** Realizar comandos de escritura de imágenes al almacén de datos local (CATD) y remoto (CCV).	En el documento de "Proceso Técnico Operativo" en el apartado De la Captura y Verificación en el CATD.	Para la aplicación PREP CATD, en caso de que el teléfono celular pierda conexión a internet, la aplicación guardará las imágenes de las actas de la casilla. En la bitácora se pueden encontrar registros que corroboran esta acción, tales como el mostrado a continuación: " El Acta 0760 Básica ha sido guardada con éxito en ImagenActa por PREP CATD. "
PF . 10	Sistema CCV.	**Datos estructurados.** En el caso de uso del capturista en CCV, se identifica que el capturista guarde la informació	**Datos estructurados.** Se prevé que el usuario capturista pueda realizar la operación de insertar en la base de datos del (CCV).	**Datos estructurados.** Ejecutar queries de inserción en la base de datos del (CCV).	En el documento de "Proceso Técnico Operativo" en el apartado De la Captura y Verificación en el CATD.	Los capturistas tienen la capacidad de registrar y corroborar los datos de control de cada acta. Así mismo, realizan la captura de los votos contenidas en cada una de las actas. Las actas son registradas en la base de datos del CCV.

		n del acta capturada en la base de datos del (CCV).				En la bitácora se pueden encontrar registros que corroboran esta acción, tales como el mostrado a continuación: " El detalle del Acta 0038 Básica ha sido capturado en DetalleActa. "
PF. 11	Sistema CCV.	**Datos no estructurados.** Se identifica que el capturista realice la escritura de la imagen en el almacén de datos del (CCV).	**Datos no estructurados.** Se prevé que usuario capturista pueda realizar las operaciones de escritura de imágenes a al almacén de datos en el (CCV).	**Datos estructurados.** Realizar comandos de escritura de las actas digitalizadas al almacén de datos (CCV).	En el documento de "Proceso Técnico Operativo" en el apartado De la Captura y Verificación en el CATD.	El sistema CCV no realiza la escritura de la imagen en el almacén de datos, únicamente la consulta para la captura. La trazas evidencian la carga de la imagen y su registro en la base de datos por parte de las app PREP Casilla y PREP CATD. Esto se puede corroborar en el ANEXO Evidencias/Reporte_CapturaDeActas.docx. El sistema de archivo se encuentra ubicado en nodos de S3 de Amazon y se pudo corroborar la inserción de las imágenes con el comando *dir.*
PF. 12	Sistema CCV. Validador 1	**Datos estructurados.** En el caso de uso del validador 1, se identifica que el usuario validador 1 puede seleccionar información de la base de datos del acta que está en revisión.	**Datos estructurados.** Selección de la información de la base de datos del (CCV) de las actas que están en revisión.	**Datos no estructurados.** Realizar la selección de la información de varias actas que están revisión.	En el documento de "Proceso Técnico Operativo" en el apartado De la Captura y Verificación en el CATD.	Los usuarios validadores del sistema CCV pueden acceder adecuadamente a la información de las actas en las bases de datos. La bitácora muestra registros como el siguiente: {"id":22,"idBitacora":3568810,"Procedencia":CCV Madero,"Usuario":CCV03_009,"Descripcion":"El Acta 0579 Básica ha sido formada como en proceso de primera captura en FilaCaptura1.", "fechaHoraMovimiento": "16/05/2021 08:48:34.290"}
PF .13	Sistema CCV Validador 1	**Datos no estructurados.**	**Datos no estructurados.** Visualización de las imágenes de	**Datos no estructurados.**	En el documento de "Proceso Técnico Operativo" en	No se registran en el log las visualizaciones de las imágenes, sin embargo, se registran las capturas de información y el paso de las

		En el caso de uso del validador 1, se identifica que el usuario validador 1 puede visualizar la imagen del acta que está en revisión.	las actas del almacén de datos (CCV) que están en revisión.	Realizar varias visualizaciones de las imágenes de las actas.	el apartado De la Captura y Verificación en el CATD.	actas al centro de verificación. Se pueden encontrar registros en la bitácora como el siguiente: {"id":636,"idBitacora":3569427,"Procedencia":CCV Reynosa,"Usuario":CCV02_026,"El Acta 1337 Básica ha sido formada en FilaCV para su revisión en el Centro de Verificación.", "fechaHoraMovimiento": "16/05/2021 08:49:26.570"}
PF.14	Sistema CCV. Validador 2	**Datos estructurados.** En el caso de uso del validador 2, se identifica que el usuario validador 2 puede seleccionar información de la base de datos del (CCV).	**Datos estructurados** Query de selección de información del acta que está siendo validad.	**Datos estructurados.** Ejecutar queries de selección en la base de datos de la información de las actas que están siendo válidas.	En el documento de "Proceso Técnico Operativo" en el apartado De la Captura y Verificación en el CATD.	No se registran en el log las visualizaciones de las imágenes, sin embargo, se registran las capturas de información y el paso de las actas al centro de verificación. Se pueden encontrar registros en la bitácora como el siguiente: {"id":636,"idBitacora":3569427,"Procedencia":CCV Reynosa,"Usuario":CCV02_026,"El Acta 1337 Básica ha sido formada en FilaCV para su revisión en el Centro de Verificación.", "fechaHoraMovimiento": "16/05/2021 08:49:26.570"}
PF.15	Sistema CCV. Validador 2	**Datos estructurados.** En el caso de uso del validador 2, se identifica que el usuario validador 2 puede Actualizar datos de la base de datos del (CCV).	Query de actualización en la base de datos.	Ejecutar queries de actualización en la base de datos de la información de las actas que están siendo validadas.	En el documento de "Proceso Técnico Operativo" en el apartado De la Captura y Verificación en el CATD.	El verificador realiza la captura de los actos en el acta actualizando aquellos que sean erróneos. Una vez terminado el proceso de verificación, la bitácora muestra un registro como el siguiente: {"id":105616,"idBitacora":3676602 ,"Procedencia":CCV Victoria,"Usuario":CCV01_072,"Ha finalizado la verificación de los datos capturados del Acta 0332 Básica.", "fechaHoraMovimiento": "16/05/2021 10:30:36.387"}

PF .16	Sistema CCV. Validador 2	**Datos estructurados.** En el caso de uso del validador 2, se identifica que el usuario validador 2 puede borrar datos de la base de datos del (CCV).	Query de borrado en la base de datos.	Ejecutar queries de borrado de la información en la base de datos de las actas que está haciendo validadas.	En el documento de "Proceso Técnico Operativo" en el apartado De la Captura y Verificación en el CATD.	Los validadores pueden realizar el borrado de actas correctamente. La bitácora registra estos eventos de la siguiente manera: {"id":106989,"idBitacora":3678007,"Procedencia":CCV Victoria,"Usuario":CCV01_033,"La imagen del Acta 0749 Extraordinaria 01 Contigua 06 ha sido eliminada debido a datos erróneos en la identificación de la casilla y ésta se encuentra en espera de una nueva imagen.", "fechaHoraMovimiento": "16/05/2021 10:31:08.490"}
PF .17	Sistema CCV. Validador 2	**Datos no estructurados.** En el caso de uso del validador 2, se identifica que el usuario validador 2 puede visualizar y borrar las imágenes del almacén de datos del CCV.	**Datos no estructurados.** Ejecutar comando de visualización de imágenes de las actas. Comando de borrado de imágenes de las acatas.	**Datos no estructurados.** Ejecutar comandos de visualización de imágenes de las actas que están siendo validadas. Ejecutar comando de borrado de imágenes.	En el documento de "Proceso Técnico Operativo" en el apartado De la Captura y Verificación en el CATD.	El usuario validador puede realizar la búsqueda de actas mediante un botón denominado "Consultar Actas". En este apartado, el usuario puede buscar y elegir un acta y realizar las siguientes acciones: reiniciar acta, borrar acta o cancelar. Si el acta es borrada, la bitácora registra este evento de la siguiente manera: {"id":106989,"idBitacora":3678007,"Procedencia":CCV Victoria,"Usuario":CCV01_033,"La imagen del Acta 0749 Extraordinaria 01 Contigua 06 ha sido eliminada debido a datos erróneos en la identificación de la casilla y ésta se encuentra en espera de una nueva imagen.", "fechaHoraMovimiento": "16/05/2021 10:31:08.490"} En caso de ser reiniciada, la bitácora registra este evento de la siguiente manera:

						{"id":820825 ,"idBitacora":4393 621,"Procedencia":CCV Victoria,"Usuario":Adan,"El Acta 0102 Básica ha sido reiniciada en FilaCaptura1 debido a que los datos de identificación de la casilla eran incorrectos.", "fechaHoraMovimiento": "16/05/2021 17:48:45.510"}
PF .1 8	Sistema CCV. Validador 2	**Datos no estructura dos.** En el caso de uso del validador 2, se identifica que el usuario validador 2 puede borrar las imágenes del almacén de datos del CCV.	**Datos no estructurados.** Comando de borrado de imágenes de las actas.	**Datos no estructurado s.** Ejecutar comando de borrado de imágenes.	En el documento de "Proceso Técnico Operativo" en el apartado De la Captura y Verificación en el CATD.	Los validadores pueden realizar el borrado de actas correctamente. La bitácora registra estos eventos de la siguiente manera: {"id":106989,"idBitacora":3 678007,"Procedencia":CCV Victoria,"Usuario":CCV01_0 33,"La imagen del Acta 0749 Extraordinaria 01 Contigua 06 ha sido eliminada debido a datos erróneos en la identificación de la casilla y ésta se encuentra en espera de una nueva imagen.", "fechaHoraMovimiento": "16/05/2021 10:31:08.490"}
PF .1 9	Sistema de publicació n.	**Datos estructura dos.** En caso de uso del sistema publicador se prevé que el usuario pueda leer la informació n de las actas validadas para el cálculo de las estadística s	**Datos estructurados.** Se prevé que usuario responsable puede realizar query de selección a la base de datos del sistema de cómputo.	**Datos estructurado s.** Ejecutar queries de selección a la base de datos del sistema cómputo.	En el documento de "Proceso Técnico Operativo" en el apartado De la Publicación de Resultados.	El generador de contenido es el módulo a cargo de realizar los cortes de información y publicación de las actas. Los cortes de información son realizados cada 15 minutos y son registrados en la bitácora de la siguiente forma: {"id":221587 ,"idBitacora":3793 362,"Procedencia":Generad or de Contenido,"Usuario":Adan, "Inicio de generación de contenido para el corte número 11 con fecha-hora de publicación 16/05/2021 11:30:00 a. m",

		solicitadas por el INE, de la base de datos replicada en sistema de cómputo.				"fechaHoraMovimiento": "16/05/2021 11:21:42.170"}
PF .20	Sistema de publicación.	**Datos estructurados.** En caso de uso del sistema publicador se prevé que el usuario pueda escribir la información calculada a partir del sistema de cómputo en los diferentes sistemas de archivos replicados.	**Datos no estructurados.** Se prevé que usuario responsable de replicar la información a los sistemas de ficheros tenga permisos de solo escritura.	**Datos no estructurados.** Ejecutar comandos para la escritura de la información en los sistemas de archivos replicados.	En el documento de "Proceso Técnico Operativo" en el apartado De la Publicación de Resultados.	El sistema de publicación realiza cortes cada 15 minutos poniendo a disposición la información recopilada en el sitio de publicación. Cuando se realiza un corte, el movimiento puede ser observado en la traza al monitorear la base de datos y además en la bitácora del sistema PREP.
PF .21	Sistema informático PREP.	Realizar bitácora de las actas. El sistema informático automáticamente realiza un registro de actividad de todas las actas PREP para garantizar la confianza, transparencia y certeza	**N/A**	Ejecutar los comandos o queries para realizar la bitácora.	En el documento de "Proceso Técnico Operativo" en el apartado Del Cotejo de Actas.	La bitácora se encuentra disponible mediante un servicio web proporcionado por el IETAM. Esta bitácora es actualizada en tiempo real y puede ser consultada mediante una URL.

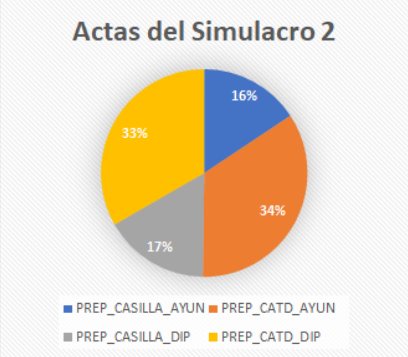
		del proceso operativo.				

Pruebas funcionales para validación de información

Tabla 6.3. Pruebas funcionales para validación de información generada antes y durante cada simulacro y la información registrada en el log del web service de auditoría y la base de datos de publicación

ID PRUEBA	OBSERVACIONES	CRITERIOS DE ACEPTACIÓN	SUGERENCIA
PFV1. Bases de datos en ceros y huella criptográfica	Previo al simulacro se entregó al proveedor un software para la captura de huellas criptográfico desarrollado por el ente auditor, el cual incluía cifrado basado en llave pública. En el protocolo de generación de llaves se establece que el proveedor generará su llave privada, la cual nunca viajará y permanecerá resguardada por el proveedor. Con esta llave como parámetro de entrada del software que producirá las huellas criptográficas. Este procedimiento resulta en que las huellas criptográficas del código fuente, serán firmadas por el proveedor para prevenir eventos de repudio. En este procedimiento el proveedor también creará una llave pública, la cual enviará al ente auditor. Es con esta llave que las huellas se descifrarán y se compararán para determinar la integridad del código fuente del software utilizado en el PREP. Durante el simulacro 2, el proveedor creó un inventario del código fuente con los archivos que a continuación se enlistan: 1. PREP_Casilla.apk: Aplicación móvil para la digitalización de actas desde las casillas. 2. PREP_CATD.apk: Aplicación móvil para digitalización de actas desde los centros de acopio y transmisión de datos (CATD). 3. Sistema_CCV.exe: Sistema para la captura, verificación y administración el PREP. 4. Sitio_Publicacion_PREP: Sitio de publicación del PREP. 5. Generador_Contenido.exe: Sistema para la generación de cortes de información.	Los datos publicados deberán ser consistentes y presentados de acuerdo con lo establecido por los lineamientos del IETAM	No se detectó ninguna inconsistencia en los archivos del inventario del IETAM. Esto indica que la integridad de las aplicaciones utilizadas se mantuvo durante el simulacro 2. Durante la generación de huellas criptográficas iniciales, el IETAM realizó el proceso de generación de huellas sin contar con la presencia del ente auditor. Es importante que el ente auditor se encuentre presente en todo momento durante la generación de huellas del inventario. Debido a lo anterior, estas huellas criptográficas fueron desechadas y se generaron nuevamente con el ente auditor presente.

	6. Base_de_datos.sql: Script de la base de datos central del PREP. 7. Sistema_Archivos: Catálogos utilizados en el sitio de publicación del PREP. 8. Base_datos.txt: Lista de bases de datos utilizadas en el PREP. 9. El proveedor procedió a utilizar el software de captura de huellas criptográficas se obtuvieron dos archivos (Original y simulacro 2) los cuales fueron enviados al responsable del ente auditor, el cual ejecutó el software de validación que a su vez generó en forma automática la constancia de hechos correspondiente. Este procedimiento de validación se realizó antes, durante y después del simulacro 2.		
PFV2. Validación de la información publicada.	En el simulacro 2 realizado el día domingo 23 de mayo del 2021, el corte del sistema PREP en su fase de publicación reportó la captura de 4,798 actas de las 4,807 actas esperadas para diputaciones, y 4,741 de las 4,775 para ayuntamientos. A cada una de las actas esperadas en el Simulacro 2 le corresponde una imagen. Se esperaba que la URL compartida por el IETAM se encuentren 9539 imágenes.	Los datos publicados deberán ser consistentes y presentados de acuerdo con lo establecido por los lineamientos del IETAM	El porcentaje de efectividad del PREP es del 99.8% para diputaciones y un 99.2% para ayuntamientos. Es necesario mantener una consistencia en el formato de nombres utilizado para las actas. Por ejemplo, el formato de nombres proporcionado por el IETAM fue el siguiente: Origen_Tipo_Eleccion_Casilla.jpg (e.g. 2_H_D_0783 Básica.jpg.), no obstante, durante el simulacro se pudieron detectar imágenes con un agregado (e.g. 2_A_A_1223 Básica_V2.jpg). Este formato no fue proporcionado al ente auditor.
PFV3. Validación de la información publicada. inconsistencias	El ente auditor desarrolló un software que consume los contenidos que el sistema PREP en su fase de publicación reportó para el simulacro 2 realizado el día domingo 23 de mayo del 2021. El software en mención reportó que: De las 4775 imágenes esperadas para ayuntamientos fueron capturadas por el PREP un total de 4741 actas de las cuales un total de 4741 fotografías (100%) fueron	Los datos publicados deberán ser consistentes y presentados de acuerdo con lo establecido por los lineamientos del IETAM	EL sistema PREP presentó fallas en los cortes de información: se observó que no se realizaron cortes desde las 10:45 a las 11:48 y de las 11:48 a la 1:21. En el sitio de publicación existen imágenes de actas que no siguen el formato de nombre que el IETAM le proporcionó al ente

	descargadas con éxito. Las 34 actas restantes no fueron capturadas por lo cual no fue posible descargarlas. De las 4807 imágenes esperadas para diputaciones fueron capturadas por el PREP un total de 4798 actas, de las cuales un total de 4798 (100%)fueron descargadas con éxito. Las 59 actas restantes no fueron capturadas por lo cual no fue posible descargarlas. Se observa que la BD del IETAM reporta un total de 9582 registros de actas, lo cual resulta en 997 actas sin procesar. A continuación, se muestra una gráfica con el resumen del conteo de las actas: 		auditor. Ciertas imágenes, presentan el agregado "_V2" al final del nombre. Se encontraron actas con nombres que NO CORRESPONDEN a la casilla correspondiente, en otras palabras, el nombre de casilla que se utiliza para nombrar a la fotografía no es el mismo al nombre que se encuentra en el acta. Publicar actas con un nombre distinto no es aceptable y se recomienda tomar acción de manera inmediata. A continuación, se listan las URL de las actas: 1. https://simulacro2.prep2021tamps.mx/assets/data/actas/ayuntamientos/1_A_A_0292%20Contigua%2001.jpg 2. https://simulacro2.prep2021tamps.mx/assets/data/actas/ayuntamientos/1_A_A_0966%20Contigua%2004.jpg 3. https://simulacro2.prep2021tamps.mx/assets/data/actas/diputaciones/1_H_D_0966%20Contigua%2005.jpg 4. https://simulacro2.prep2021tamps.mx/assets/data/actas/ayuntamientos/2_A_A_0809%20Contigua%2001.jpg 5. https://simulacro2.prep2021tamps.mx/assets/data/actas/diputaciones/1_D_D_1469%20Especial%2001.jpg Se encontraron actas que cuentan con 2 fotografías, una por parte de PREP CASILLA y otra por parte de PREP CATD, sin embargo, las fotografías no coinciden y solo una corresponde al acta en mención, se recomienda tomar acción inmediata. A continuación, se listan los partes de URLS de las actas con 2 fotografías:

			1. https://simulacro2.prep2021tamps.mx/assets/data/actas/diputaciones/1_H_D_0966%20Contigua%2005.jpg y https://simulacro2.prep2021tamps.mx/assets/data/actas/diputaciones/2_H_D_0966%20Contigua%2005.jpg 2. https://simulacro2.prep2021tamps.mx/assets/data/actas/ayuntamientos/1_A_A_0809%20Contigua%2001.jpg y https://simulacro2.prep2021tamps.mx/assets/data/actas/ayuntamientos/2_A_A_0809%20Contigua%2001.jpg Se encontraron 2 actas extra las cuales no aparecen registradas ni en el sitio de publicación ni en la base de datos del IETAM, sin embargo, es posible descargarlas utilizando la URL correspondiente. Las actas en cuestión son las siguientes: • https://simulacro2.prep2021tamps.mx/assets/data/actas/diputaciones/2_H_D_0516%20Contigua%2001.jpg • https://simulacro2.prep2021tamps.mx/assets/data/actas/diputaciones/2_H_D_0516%20B%C3%A1sica.jpg
PFV4. Validación de huella criptográfica.	El software en mención reportó que: Fue posible descargar el total de actas procesadas (9539) por el sistema PREP. No obstante, la discrepancia en el formato de nombres de algunas imágenes y las inconsistencias mencionadas en el apartado anterior, dificultan la adquisición de actas. Las actas en cuestión se listan en el anexo S2_ActasDescargadas.pdf	El sistema deberá garantizar la integridad y consistencia de los datos a través de estrategias que integren personas, tecnología, procesos y	No es aceptable que el sistema no permita descargar Actas procesadas. Se deberían eliminar estos eventos o documentar la razón por la cual dichos eventos suceden en el software del PREP. Se recomienda revisar el formato de asignación de nombres de las actas para que este sea homogéneo y de esta forma el sistema permita ser monitorizado por procesos de

		buenas prácticas.	seguimiento en tiempo real. Se recomienda corregir las inconsistencias descritas en el apartado PF.3.
PF5. Validación de huella criptográfica.	El software del auditor, mencionado en el apartado anterior, resumió que: En el simulacro, la base de datos del PREP registró 9582 actas. Del total de esas 9582 actas se logró realizar la validación de integridad de un total de 9453 de las cuales el software del auditor no encontró inconstancias de integridad. Sin embargo, no fue posible realizar la validación de integridad de 129 actas, las cuales no fue posible descargar, aunque figuraban en los registros de la base de datos.	Se debe garantizar la imparcialidad en el procesamiento de datos generados por el sistema respecto a afinidades políticas o intereses personales.	Fue posible realizar la validación del total de actas procesadas por el PREP sin encontrar inconsistencias. Es altamente recomendable corregir las inconsistencias descritas en el apartado PF.3 con el fin de mantener la integridad de las imágenes procesadas.
PFV6. Consistencia e integridad de la información registrada en el log de web service de auditoría	El PREP pone a disposición del auditor una bitácora de los eventos realizados por los compontes de dicho software. No obstante, la bitácora comenzó a presentar fallos a mitad del simulacro2. Debido a lo anterior, no le fue posible al ente auditor mantener el seguimiento de los movimientos realizados por los componentes del sistema PREP.	El sistema deberá garantizar la integridad y consistencia de los datos a través de estrategias que integren personas, tecnología, procesos y buenas prácticas.	La bitácora del sistema debería ser proporcionado para su consumo en tiempo real y de esta forma poder dar seguimiento a las acciones realizadas por los componentes del sistema PREP.
PFV7. Actualización de la base de datos de publicación.	Se realizó un análisis de las bases de datos de publicación generadas cada 15 minutos. Teniendo como resultado que la huella criptográfica de cada archivo es distinta. Esto significa que la base de datos de publicación se actualiza cada 15 minutos. Se llegaron a detectar retrasos de casi una hora minutos entre algunos cortes, lo cual dio como resultado que ciertos cortes programados se saltaran.	Los datos publicados deberán ser consistentes y presentados de acuerdo con lo establecido por los lineamientos del IETAM	Se recomienda que se repita esta buena práctica para el siguiente simulacro. Se recomienda solucionar aquellos problemas que generan los retrasos en los cortes de información.
PFV8. Análisis de comportamiento.	La bitácora que registra los eventos realizados por los componentes del sistema PREP se entregó a posteriori en formato CSV. Por lo tanto, no fue posible lleva a cabo un análisis de tiempos y movimientos de las actas en tiempo real (durante el simulacro) y el reporte del análisis de la bitácora del simulacro 1 será reportado en un informe adendum.		Se recomienda proporcionar acceso a la bitácora durante el siguiente simulacro. Se solicita que la bitácora sea adecuada para ser consumida por sistemas informáticos de auditoría

Sugerencias generales sobre el módulo de publicación de resultados: Capa Datos

- Durante el proceso de generación de huellas criptográficas del simulacro 3, no se detectó ninguna inconsistencia en los archivos del inventario del IETAM. Esto indica que la integridad de las aplicaciones utilizadas se mantuvo durante todo el proceso.
- Se encontraron inconsistencias en algunas imágenes de las actas publicadas en el sitio de publicación. Por ejemplo, al realizar la búsqueda del acta **0638 Contigua 01** esta mostraba la fotografía del acta **0638 Básica**, y viceversa (ver anexo en N1/Actas/).
- Se siguen encontrando inconsistencias en el formato de nombre utilizado por el IETAM durante el evento y el proporcionado al ente auditor previo al evento. Algunas fotografías cuentan con el agregado "_V2" o "_V3" al final del nombre de la casilla (por ejemplo, **1_H_D_0638 Contigua 01_V3.jpg**).
- Se esperaba que el número total de actas registradas en la base de datos fuera igual a la suma del total de actas de ayuntamientos (4776) y de diputaciones (4808), siendo esta la cantidad de 9584. No obstante, el total de registros en el *backup* de la base de datos disponible en el sitio de publicación tiene un total de 9585 registros. Se observa que existe un registro adicional para diputaciones, siendo el registro de un acta fuera de la lista nominal.
- No fue posible realizar la descarga de todas las imágenes correspondientes al total de actas esperadas durante el simulacro. En total no se pudieron descargar 37 actas, de las cuales, 32 actas no pudieron ser accedidas a través del sitio de publicación aún y cuando sus datos fueron ingresados en la base de datos. Se recomienda que todas las actas registradas en la base de datos sean almacenadas en el sitio de publicación, se añada una justificación para las actas que no fueron almacenadas en el sitio de publicación y se utilice el formato de nombres compartidos con el ente auditor para poder descargar el 100% de las actas registradas. A continuación se listan las actas que no pudieron ser descargadas: *E_D_0817 Especial 01, E_D_0891 Especial 01, E_D_0725 Especial 01, E_D_0898 Especial 01, E_D_0997 Especial 01, E_D_1021 Especial 01, E_D_0956 Especial 01, E_D_1117 Especial 01, E_D_1087 Especial 01, E_D_1168 Especial 01, E_D_1525 Especial 01, E_D_0671 Especial 01, E_D_0676 Especial 01, E_D_0591 Especial 01, E_D_1232 Especial 01, E_D_1632 Especial 01, E_D_1612 Especial 01, E_D_1282 Especial 01, E_D_1500 Especial 01, E_D_1722 Especial 01, E_D_0291 Especial 01, E_D_0432 Especial 01, E_D_0443 Especial 01, E_D_0014 Especial 01, E_D_0046 Especial 01, E_D_0159 Especial 01, E_D_0213 Especial 01, E_D_0243 Especial 01, E_D_1312 Especial 01, E_D_1351 Especial 01, E_D_1401 Especial 01.*
  Por otro lado, 4 actas están marcadas en la base de datos como no procesadas por las siguientes razones: SIN ACTA POR PAQUETE NO ENTREGADO y SIN ACTA POR CASILLA NO INSTALADA. A continuación, se muestra una lista con las actas no procesadas: *0069 Básica, 0070 Básica, 0071 Extraordinaria 01 Contigua 01, 1101 Extraordinaria 09.*
  Finalmente, el acta restante corresponde al registro adicional encontrado en la base de datos, cuya acta excede el catálogo de la lista nominal.
- Se observó que los cortes de información en el sitio de publicación se realizan correctamente cada 15 minutos. Estos cortes permiten la generación de los backups de la base de datos.
- De las 9548 actas descargadas por el ente auditor durante el evento, se logró realizar la comprobación de integridad de 9548 actas (el 100%). Esta validación se realizó mediante el cálculo del resumen hash SHA-256 (que utiliza el algoritmo de hash SHA-256) a cada imagen descargada y

comparándolas con los resúmenes hash registrados en la base de datos proporcionada por del IETAM buscando una correspondencia. Las 9548 actas fueron validadas correctamente y no se encontró ninguna inconsistencia.

- Se observó un comportamiento no esperado en el servicio de descarga de bitácora y una inconsistencia en el contenido de la bitácora descargada. Durante el evento se realizó la descarga de la bitácora del sistema utilizado por el IETAM en lotes de 5000 registros por petición. Se observó que no todas las peticiones a su servicio web devolvían los registros solicitados. Por tal motivo se realizaba la descarga del mismo lote hasta comprobar que los 5000 registros solicitados fueran descargados (respetando el tiempo de espera de 20s entre petición). De esta forma se consiguió obtener los lotes con 5000 registros. Siendo las 10:38:39 horas ocurrió un error y el servicio web devolvió como respuesta un Json sin registros (es decir []). Se inicio un tiempo de espera y se hicieron otras 4 peticiones a las 10:39:31, 10:40:22, 10:41:14 y 10:42:06 horas obteniendo el mismo resultado (para más detalles ver anexo N1/Bitacora/Anotaciones.pdf). A las 10:42:47 se obtuvo una respuesta con un Json que describía un error. A continuación, se muestra el contenido del error obtenido en formato Json:

  [{"Exito":0,"Error":"Transaction (Process ID 108) was deadlocked on lock resources with another process and has been chosen as the deadlock victim. Rerun the transaction."}]

  Se le informo al IETAM sobre el error obtenido al utilizar su servicio web y se pausaron las solicitudes hacia el servicio web. Se reanudo la descarga de la bitácora en cuanto el IETAM confirmó que su servicio ya había sido revisado y se encontraba otra vez en línea. A las 11:05 horas se hizo una prueba del servicio web solicitando los registros 1 a 5000, al ver que contenía 5000 registros se reanudo la descarga de los registros desde el punto en el que se había pausado (290001). La descarga de los registros de la bitácora se realizó hasta antes del inicio del proceso de generación de huellas criptográficas finales del Simulacro 3 sin errores.

- Al las 14:01:07 horas se inició un proceso de descarga del contenido de la bitácora desde el registro 1 hasta el último para tener un respaldo de la bitácora. Esta prueba finalizo a las 15:01:04 horas. La bitácora del sistema debe ser consistente y no debe de presentar modificaciones en sus registros. Los archivos descargados antes de la falla, después de la falla hasta finalizar el simulacro (anexo *N1/Bitacora/S3antes.zip*) y los obtenidos al final del simulacro (anexo *N1/Bitacora/S3despues.zip*) deben ser iguales. Al comparar los archivos que contienen el mismo rango de registros nos encontramos que los resúmenes hash sha256 obtenidos eran diferentes en la mayoría. A continuación, se muestra un resumen de la comparación de los “hash” para cada captura de log:

Inicial	Final	Hash SHA256 antes y durante	Hash SHA256 despues del simulacro	Mismo hash
1	5000	97a936947341f49664c13c2c7ca91417c9928e8bd53fadcf8499fa7bd955495c	2982e8ddd3c6c36cdb4caf1481f4fe1dd51271442221527ab2dbac5121fad62b	FALSO
5001	10000	1a6d2ac2911bafbab082060b4b5a5f0d9212cffdefae2c6e30d39939b1fe8506	6cb0f609d5e6ed43ef17e01867b649e9147819b9adf1babb162524d0dc502a69	FALSO
10001	15000	cf0f8b57a01bc22eaf0561544db548be14065c05fe3c244f12d282e015df2edc	76866beb8057069d5d56623d075041ca30da35ee908e5b57af317edfe9b1e20e	FALSO
15001	20000	230bcb11e0f475ffdc7cbd595536efc7c6b7bb9030eb5335dcfaca695beca1ea	6354863df76a5cf2538c22a8c970d72e53c0bbe6e4c0c20e6593f03dad7bb262	FALSO
20001	25000	ca117251fbd5311c162236192a1e1e8b80bcb99c1c9953c159ef04eb95c9c7b9	541f0b5e81aa0dad195cef1581077e9e2bd307740df2b4345d41add094a99383	FALSO
25001	30000	ea0aecfb0d4e97feb456a42d8a209322a15df2960f6bfbcf6938d2621f155e41	e31e8beec8b58a3e560cdd55a261ea2b3f62102c17c302495d3c2bf1b05b5753	FALSO
30001	35000	67a06f25a90783a2e96380b59bd69208b1aead586d2c4f559bbb4ce69e047fdd	4d071f7c1207b525cfcd8d3a0fb718f398b5a0e1a07fa6ea7e232d889620580b	FALSO

35001	40000	01fef21a21a4527e3ea1bf51f48dd351ef523dee4a9b33a8af40def17083d729	49573e010e196e8f8f63ef16b303daf0802b87c3d523da29be227283c2a454ea	FALSO
40001	45000	d4c71817d12db2b1c0268086d5840d307ecbcaf67b8e56db3956b27dafe62946	922f231a5a341e38077c2416c370201d3967149bc61eec097dd65217b98d5b47	FALSO
45001	50000	fc7ce3d354eecd55e514cf021f7c539f08273ea1759df2414c69bfe77659a79d	208655719be1e042d09747a3405d62b1e89f5a89d1eb9aac882e1168276c6089	FALSO
50001	55000	14eebe46ac946e85f3d6980bab2da6442601d002ce5cc0d440b9fd1e4fe0cae2	41b43a9ef14a7b55160decadb70840e882b30ede98d98a0d0e8f34f83fcefa19	FALSO
55001	60000	53b51f73a4de425700da4f21fc950045f02e39e2a84fef5d9c539d64220fe533	6e815d572edb3514cb635ed07bfddcdc4639ba4466954f4c43d9b0660b15ea72	FALSO
60001	65000	722caffb1cfcfcf5504f11f2f1ee0986e06e76d1a2474e498f22e9cdb6439161	4b7dccc180088514356faf517e82e19131394b7c547d83b3215835b104a858bc	FALSO
65001	70000	07cd2d12fb764b50555985ced6d761bf5f01de30ecc795c32236ae4ba22f50c4	d436d6958071ca03319b59d0931433475c2fbe838f4df271691ffb83732fe297	FALSO
70001	75000	bc14b0dd0d7f6f08908d061797ef00b4e460d1aa6a4b6f1f31bec85ce241f2e4	51b90b1eecf39fa4d567b03bb3741d5236759ec0445d6cb5990e76886590c05d	FALSO
75001	80000	d250eea4675cddbfa6f992fcf493c80ec54ae9ac098d5174ba360f89869f7f81	1e41ea0b6e3164c848cf1423501380825338b4a43f5ce2cfb1ac149c22a04994	FALSO
80001	85000	ab460c9fe8e8a484e672526b3983261473ed71777ea60cf855e15ba380d6b67f	8096b61dca72cfb374a87e66b6b2633cbf0f8e1d09bbf64a2aacd1fbf1e3f05f	FALSO
85001	90000	6470c108d6713e88eeef9309df3270d104dc63214ebe75cb52c6e41f6451af70	a75ba84cb4959cbf29fc6070986cac29114ad5f84af30325433 0cd2a2197cb84	FALSO
90001	95000	6e97dd7d2c97801e2b9bb4c31024dde758c2c580742ca2eeea6fa804398f3ed3	a1b4e3bf729c48947dc1f507ff6fa0f9053cb073b885b3f71062f5289951b3b6	FALSO
95001	100000	3d70c867f72be2b0db639fef82a74f711c8e69dfefff3815ae783d34d95ff721	8986be0608b9bb926a10bc29b95b731f0a502542265835676fb87bb16f99d752	FALSO
100001	105000	844d483ac65502b4a5515ce744289d4db6da6b16228f9cbac4a179bc6d009bc1	8027775c22effa2f156e131ac4a101ff8a1215256e0f83497aae325870fa2691	FALSO
105001	110000	45ae827c598a16068d8adac88d8ec658e27049558296ebcb926f37c882f5e782	fb2f41a65182901f27391b448788e53416c46cd923a2739aa3e572fb84a6fa84	FALSO
110001	115000	c5885504a9e6791a261f8c5fa3738e8d527b6be36bdcbe5b72dd91ddd12cd4f4	a16a8967af02f92a8d22554283507b2948849dac5efafe6ddbdda5ba1dce03a6	FALSO
115001	120000	acdd6b4c6c5ff0860af0b580324ccdd07a4d033cca0feeb84614375eab2356a4	941fe52a050f060855764b584b03a97ee2dae39a74f620cd308bf658c520e5a8	FALSO
120001	125000	bb7a65378688b34e33a5c00d128f38968d5a0f6d9384d4d58650dc6632280b83	f26894b51f20c7f7b8ea0c29226710645ce79b56d25983681a1a817778871d4d	FALSO
125001	130000	21801c3baf6cce40c1c33d788d46106b3b9fa54f15a9ee2db330b1c77a66a6ee	3a1201ece56d3d06dc0017044acb75249fc052edbac100fb2902087241dd1c46	FALSO
130001	135000	51ea38b0fd1b02981af149f49bfa8c5e214a4b115269df0ddab0ddaab292173c	cdf1464da1cb71d17dd2ca036278bf9fdf27ef0f61d5b44428cbe03f7f910b16	FALSO
135001	140000	a5b9fe34cba664abfac7ba29a733394c3b3f3c42228c1f9462b284bb04ca58d3	564d60e662f29baba3b76136c9006a00164143bba56849ef00a70bd9a67faf36	FALSO
140001	145000	6aae544d9906b00ae27811883d48cb68dbe32355bc1662f8fa533b55cbc68088	bdb0f72f7c42a803d2df4a55f213a71db88885f2a0c84d2d980a4fee9120c771	FALSO
145001	150000	7e36b7782a48822f12c713d1408af647551fa99ddb29b7e651f0cb96ba585534	30c4f334d24721828878e172d4136531d088b73722f439afaeea7cdb588f14c9	FALSO
150001	155000	9a71efbb40f0b339c1563862ab8b0f341486cab06fbee419634763176bb700a6	13e80568d6b4b490fbaadaf2af9584240375f5aa24a0c116f4bb21813b2f1d19	FALSO
155001	160000	b98eff95ae107562c59e8ccea1ff091e9d44f5e3d3f75a6ae37dab0a931192c2	5535e1c4f26a33bbcd121a29dc257c32258b51f6ebad4c11c3dd07bfeecfe0c1	FALSO
160001	165000	998119e8705946065122eb79656b311cf371314949abe186aedfd0175cde2bda	eaf2be92c12b0734a1aa484dca3497ef407705693a69ff862ad7f2d739730ca1	FALSO
165001	170000	ee97cac467f63ab027da5bb0e1156a2e3f555b6a356788bc00ab98fb703dac6d	bae4fdaa1e3e55c34b1f2f0435dcb9b19447d6f1e7bfec8d4657ee292c7e7c7e	FALSO
170001	175000	f058e997311a83ac3dba48accb31306816e0a8dbf6edbff83c9ae6c40dc8a8a6	1822746467836b0fba0a9e9a7caa77f8f3d4b37439f198b599f32a217b5322c3	FALSO
175001	180000	236bfa01836338979b5ce3de175d11414b2c3c010720a8370fcdb99f00caed84	49c29e4aec205eec02dd8d450db2aab7112a2ac363c0aea826cd319d3ff1656f	FALSO
180001	185000	4eeaef515c001656eda6b3b53d293060d4985cdbd7d1a10eca44adf67e4eaba7	0aa30773c19b1a16dce5b26a6306646f6fd2fc75623423eec2d3af15a734d201	FALSO
185001	190000	b0fa6aa7610b055601da6fec3f3f51b89a90d0a00b524cb87f9793b88d9ab1cb	0d2dd64130cf85f04e26d00ec1a41fa2575a6925196ff1622fec543af09cc2fd	FALSO
190001	195000	1dbfb920a4b4070d032cc821d55561ac8eb3a1d55c90e97247d56b4809401e7a	7fd9d01da460727d05057ab61ff0875a8ae64d95e03e7ba89afb1a1781f018da	FALSO
195001	200000	76bfdade77b6decc32de203a129015e4e0ef3adf9e856ff40b629128081a80f6	6e769f0cc9428ab25cbea028b55cbc8c988f5f229c5c1157255a136b06f9c9c8	FALSO
200001	205000	20a046acd1bc3ed28320ffcd9b357f11f2e8e345f3c7cbeaeeea208d9051da3b	a5f0f95cfde960a622e3946c60db2b498d7c13e53b38eb4361ae17ac0c7a90ed	FALSO
205001	210000	2581180aa4d026564e021421aa56d740dd4f393bfcd02b69bce72a7113c3ac86	77c30ee646cbf154027ac9aaec2ac26793277b69e2c511202eb4f3fdfc16467e	FALSO
210001	215000	06b1a456661a252aa3a6168fb13581d8b3190e35fcbefed53ddc66982372b9ba	1f20fc81bc5c809eb2e9bc9d5eb6f0723a0c2712b09114e085b6a1d21c01ea0d	FALSO
215001	220000	c6cdf8e90795f3747ffdca1757dd21dc85f85e4ec8c9330e4c4fcaaae58fa241	9ef6c9d188f47604e49b55797207fa3cfb7effd0d03a8cf41578c8419f039c0a	FALSO
220001	225000	c8ba7e24c9f60cff01019acc2d82702c1c50d527b16d9c4b97bfefbbb6071d5e	59c442a1ddcc37f142e4f644624d881ab2447f981bc8a19d18fd59bbc146297d	FALSO
225001	230000	c88f3cebb22b0ff467d90e8a77e3a5a4d6e591c94b399d085f2f07b452701c1e	be2103794d443fbd7510dd1fb6cf9dc7a3bb864226373cf41d9d6473a99a9454	FALSO
230001	235000	6863f9a27a3cb06aa993ff1d4be09d69420ce2275a5bb16626193414e65f7b69	18bc451e09e4fc177ecce5fa5ee6e011b5a32d5316c645c380d766c789207047	FALSO
235001	240000	c6d4cf90ab2f2d492c27b55385a22dfc17fbae6a6ca2eb0189a0d670ae247dc3	f0b6f447db349f1689679ec0b09b712b57bf33ae1e30f4d7be0db2aa1696ace5	FALSO
240001	245000	c760726809af14ee2e105ee066611ef2976e9c203586d5733113494e4e388e60	761b7072c0d4756ff0ae1853570e957c8fb76b4cdc44147759fdb2ca18e30a86	FALSO
245001	250000	960d9865fa28385d0281ebd782cd3829ef734fb15664bfdc800b2154abbaef99	fcd8b1f8ef00e445dc707d5e47806bc2964a9e74224e9733b85b15fc8ae3fe67	FALSO
250001	255000	e2b0505648ea10d114b685bfbd899916dcc76b378e76c8677e4ad8cdc81751a4	febc1d9bfa5c5eaf28bdc0b4c2dcc4cfc794a3245ce23bffb532e53e4aee9f17	FALSO

255001	260000	888077ba088c1887b79011d81622b07c8c8b73b78068ae2dbe163d8a02c11ee2	1950a3a9ab74c27ed188830cc8c32b4159bcb08387d94d7bc1b7ec88f6586a91	FALSO
260001	265000	f397d3c319febcacc6421abb683288a0e0c3d503bcf4feda90d1fac6745e29e8	721618c9eae74300b06edf63b1d9c6015170521ccfe112a40e15557cc3aaf743	FALSO
265001	270000	6ffeae917d082a0def3952f0f25d8a4f25f72ee930b5b364322ec8cc68e09491	d2f95d3afb04ce8e8cb039691a8e4d1580d8452d531f6a1b3e07fafb4f05e819	FALSO
270001	275000	17578e827f1fc248a146ecbe6a5ad7ba4d1b168da7853e6f1c783c71d030ef1a	3e7b5579b552687848eeccbe0a1a3993570bd441bebfa610d2766257f1991a46	FALSO
275001	280000	e69ce19d08b8fdf4f85b81ba9373a45fa129f715b9d41182a00fab61c2eafd4f	21f465f9d58119ac44af7d3ec0ca9e38f8044ed3b9cbc2c5f38f1cbf258d3b46	FALSO
280001	285000	85289836fa72b2aeef48ad3041886e24d5057b63700f064c0b0759738e96fe0c	dae0a8f3fe9233bdae5a0b88132f953e445a6320ec4aa18cdc075de26840c5f2	FALSO
285001	290000	692a3623520b36a4bdd21c17ef9b47ecab0410350b5c104156e4c1973565a8d2	d8d77f35cc85db8c12672ef3c1b8da273dc0b850287639e213ac2cac9d677171	FALSO
290001	295000	8fe3907e3df8b9d622a0f72f5f71df0aae94cb2f0166ca915a141e7d93dddc1f	55f7b32f6e3e7df5d955adf484ac6b9fcf8894561ee3059b4c8a64334b509720	FALSO
295001	300000	c889409b623e2520f3f0deaca676372ee1e10bfd61dda5046f78698dfd449f6b	9dfb1e97d18c87b36b8267857be8fd6a1c28ba733fb7561ca7fbe32eea3d8e3c	FALSO
300001	305000	cde22a47b744e4762c79b79cdc3f747a032fc8d842926ea694723a64742e181b	cd89b9ed8aed709d05283a966b35cec1ccf54b856d3a08c2ee6ffc9e8ec4bc90	FALSO
305001	310000	7c1676625ce71ceabe8b3016f0d2e380128768160c0287bf7b64d8611c34fa73	a8b64c8506518e82b870693da02414db8c8fc96fa86613982779d4a6503f5ca0	FALSO
310001	315000	f1fac30bbf139ba6330acd5a0667e7e3a839137da113b75e264219edfd2d7247	a721fb2637ac95479eca44f0a3b1bb04f9ba9c42f3c26e76c3a9e073975cb842	FALSO
315001	320000	0f4ecdfd0ab597621b82d61a8220de66d9258744c546f5abec1db6c3141645c8	748a2f71b2158e22517ebece7e5bc655aa67bbb567c59a5c51bb7d7318c83e6f	FALSO
320001	325000	6718c889bfd17d5ff1b5f01404b45b33797864b832eacecf298b1e467e2aa9e8	da4ef0e6504807e3843cdee59ad42f5bb9d2c4e29c32b4a1f99b1216dde5aaed	FALSO
325001	330000	eddae6d1c33da0761576126cc2a717451148ccec087bd925ee32716f8f1810a5	6edc1343b174c1ef32a17d3c9a72f171d92a249f94eb3a79f3fe927797376e28	FALSO
330001	335000	6166cad64cea6bbc92f552ced3a0d3e6ce456cc621027fbcf8db6f23152340b6	080bde72a06d9b4f10eaeefd6fadce713072e3208f851e5e31b560e37edbd915	FALSO
335001	340000	8f4ac97e22126cfbb33562f3711a3f5ae9c958bf86b0ef33cbc7794aa15c53ec	4d7aa391b43e5554fa7e4aa0b6e46c962af93347b860694cde73a5503d7f5677	FALSO
340001	345000	3cbdd2fc12df03df4ee6d068888580923fd8d8473d5a70f3664c8df954259b7b	d4cb18f5b6c264c7deca829c45ce73fc9a0bfc720e45aeb4b9f4f8ba97efae2e	FALSO
345001	350000	8d42d1cf7cc1bb84dee6b1d9794fb8f2c1fa9e05b83787e9357b6729696c0d56	18fdac40d8ab177ad184d8fa0dd7d52898a206e12503eb75af0262ecb124fff6	FALSO
350001	355000	b341467f39c59c0c064291353cc426a045fd54647207c1b4a9b0642f550d6264	561c966acaabb340c822bbd874ca05fc46a53900ff269862f3d9ef547a6bd046	FALSO
355001	360000	e173663d10080e81ac57d151797b0649cfeac4673f41c57882c5439ba9c0a1a2	156e29174c1ca68cab06942ad6586724565d87a4f3cbde4dae490025772fe055	FALSO
360001	365000	d18d62e4eedcdf8e9333a0468fb256e4e6e890cfd80de98074b27304ff8bb481	2a07b3d464a17091c2e8cf549e3596da9a8ca57cc820212a4b6743b2914dc7b9	FALSO
365001	370000	4e06b2c600cf314b18366d44468ed2e6e16917112a57c764178cd608ac2e7252	d057b38e57b3acd9600df744c816ccb53bbdd331f2bd1e26cb38755dc584b4fa	FALSO
370001	375000	0bf31e9518ebc2cfd729135472aacffda65139ebbbe2af6b3c99904f6e3b2e34	7e2c77f7c293143237255134a52a6e3dc702693bd0407c2aca60d74a59a58b37	FALSO
375001	380000	306e54b94b51ff771713f258d51cae53999746048d885f7745c248d453cb0e07	374931e159a0cb4e5b8c927b48f7c0f9435d2e67e36cc034c30811d3a8bd2ef1	FALSO
380001	385000	ba535e1ff2d3d08ab697ca903773756622a1d72d9e9c3e0432ea2b3e0b69f5b8	0846dd9910c81e3fcde2447fbcfb8d14364a1fefe3eba27cb4d2a1550b8e50c5	FALSO
385001	390000	e95ecd1e5bffe242a09cf70fcc3e09aaa94e6353102f4d26d8c416107ee317f3	d28b7abd058dc4dbdec0089bfb6892777e66eefb6b3cfae95b2e08a9931d8c46	FALSO
390001	395000	ac169b006e7771bb7296ff215beeed36a484ec3d31e59d057b8b8aac7a278bea	10cb75e66b95031caa5beeed646411f4ca438b6361ebfe13063d86c6b0c3b784	FALSO
395001	400000	1e4df70488f3d6174bb2e16b94331fc37b96efbc37e38d45aa17c4913a8932e2	c6dd4f5881e556348c56b305aa8b48ae234c5fe954d68ea24169d6b061fd964d	FALSO
400001	405000	7bed1d0672d98154b10128378445e824a506f83281f5d68e1b7f83b1334dc3b4	1db63d4194908f348bfad748e824e5b8029d421c75a1c042b8986cff51da643f	FALSO
405001	410000	32c1ffba3221db76d50c5413071964d7576ee39dcfcda5448562aece4fc883e6	22a0da3a06e330df93ff79360fd0ba4647d9a3f04af20367003ac4d72277e6c5	FALSO
410001	415000	2493cdc9c0313221f1a35b9546e262344152957ab03207b7de3ebea51eab5b0f	59dec19fd7a086117968b1caf85fb04050649b569dc61acdf36a07ecab6be316	FALSO
415001	420000	b4de31fe021ca398292b044eff35d745fa08f457f9de6a7bd0637b6bbfb6a5cf	7d4bcfba08c97b8cb2481e9f36330240e3603adc630b6696ef2a3638f29a8b7c	FALSO
420001	425000	c5f7f65e7050e713d7e931d7b6938503edfae0f410c403848b21d0e686bf56fc	a3917d8d23cb13fabd862da95248737facb4530f548d5b7f8b1936f61ce03d38	FALSO
425001	430000	c7332e719beb282b25cf79490a18d79b09fd43ea4e55c830f88782f401a2cb0a	af143a07d06360959cd85e3b8e3ca5011b3af56e8569b6f8b088f413873fc2c1	FALSO
430001	435000	19de387fe941b5c1baa57b59fd756df6f4577fd3755d4664091fa0465e28c41f	d874845350c34fd9904774b91f1a15680d6898bc4ee29b0ac4ad018a31d12e11	FALSO
435001	440000	8b8b1d4863a8037d5fe69907eb7feab21e057d1e758f1c0f702e7261ebc557a8	e15fcab6f663e34f1fbd8dbe2d0b27fa828912bb0b80513194762b4acb54e6d2	FALSO
440001	445000	9e528f3252fcecb49fa8a9281c8a70c7be8c573771c13269ae2bbd748ba19362	754a360d5cb8f26a1a5631b346fe163665300bf3356eb858003c791f0e9fdd7a	FALSO
445001	450000	e290d0c94e154d2bd2c2c574763ddb245498ca377c50569abfec039c5fcb2b11	b85d345076b342c1b167f81e98ae17833c7c7e645bc1b7b0676e8273528efb25	FALSO
450001	455000	eb43e73ec766f7763c18469a0fa3e8fce84a5ac57749d47271c6feb89a306b9d	61ea03cd996af32d46d838f4bb5a50d04eb5bb8601cb26799eaeb23559c4fee2	FALSO
455001	460000	45256ecc06aa6d7ad98ec6d6d7a89ee5539a1a8b4cf004a8025224d8b9f6211f	c491c2096938726f41d6dea7fd5a27eadc281a15598b75210edddfb3c2f2d446	FALSO
460001	465000	9bff90345aff42e9e3d585d430da8f25b4d39cdf78889e7bee41763ee6d8198b	58c0e265a45b396cfe846f706f5d4c42e1c1ed2e6f258fdcb6fc6313940273b0	FALSO
465001	470000	e1fde1102ada4e0ead310884be819f714d4c46c8984cc1570cd2511baddf36ad	0074ae3a2ca1be7bba924a8e065dff728e642c58f8fad8869e8bdc66ee9f264b	FALSO
470001	475000	f734d3e9506b1eb21a9235b79f538ed217beb2aa670a18e88a9d91cf276b7292	3d5f85a91fbafdf68f716c51ab9d3d7b5f44c98594ee8bfc24cf13c4c9952372	FALSO

475001	480000	5c27ad948c82e4557c734385fb072f9928702a411893891e4bfed6379bd06db8	61a7b3b830baccd5a59c51047c8dd806f6a674fbff316412a1b7ba84dc496a6e	FALSO
480001	485000	0a9bafd4c7a21c67f09a8036934f9041c9caa19d0f42038e9968e393a30752de	ba06cecfc9844afc0d94fdbed42b05f875993be861a5530edd02a56144f79fb7	FALSO
485001	490000	5ce68925be8767c405c04dfa8442ac3919f28941fc6a1a6328f2e894c3ad7952	48ce64e100c6277b5c9a73585b69af45de8a8fbc1436170526fad5cc749b2dfe	FALSO
490001	495000	0fad9cf17c9dfa1d124c1550c2db98de3fa1f7fc97f82f3260eb938caf683efb	32e1d4ac224a10fff53ab0b7b74032abdee282037abf5897577448245b0771f1	FALSO
495001	500000	7bc21889c7e9b71cdeb3851d4464be375daeabf52d5e12d88fd93669be58cfd6	d37aa1eee3922cdfed865771d8c0049ddf6b3668d1e503c7c5da66bf74acb850	FALSO
500001	505000	22d3203dd710c10805e0fd6ef2c93eeff06d301d0d4c4d2bba96dc58475fe906	7f84c7851b8478ec6b79ffcecd9b28309253a62bcf4191f21531709fb6253dcf	FALSO
505001	510000	4b6a62bfc352952f961bb0b042c1f19555702cda08ac82acc9209bf7fbc01ab0	f67790fdf1d55b8a6f87637e765e3dae0b4b82c018fc85a1aacd8e09a817d230	FALSO
510001	515000	a1b6122223c3700f13b5365ac272e0b58a81beed4b1e8379c8f862f26bc359f1	0bc8a3d1f138aadc2399ef0abd90d97d1fe11da504ea50092b4d0e257807f4fa	FALSO
515001	520000	e64c0e86ede3985543c765ab692578ed06c2ed42e9eae9220274868134b78d9d	7ab6c81611a7b57b3a41bb59f0bd352ea4006abee06f8a13732a9ac583a45545	FALSO
520001	525000	73a6aff4316f44ded063602db681f4707b683b63237652cdf78ddd9f6bb5bbdf	2424fd0b3e073db8ba7a29980836e16483b177aa29301cf06ea818b649a08fdd	FALSO
525001	530000	1d58dac20bfcee54efd1b8287bcca2d3f9d73a16f0e0873c2ad9b59d3fe5533d	633532d45844472871f91f9fea67d140a91e7f169d13215d2daa89f05182243f	FALSO
530001	535000	6d63fe0336e5fcbbf50fe971461ef5fb8ccc180cc3328217b14ba1c2add3ed3c	82d8fe794a7efc2a290c02d65215ad39be111599b6f578c296babd71afde20e6	FALSO
535001	540000	1a40a4d1c373b9d57bbeccfcc153ab0565a5c6de8fb540d83f2a7016f6a619ae	cb8eb090fd72d3d94fb57165e13be7db711b4d3cd3cf895146cb1acdc7783b37	FALSO
540001	545000	afdbb2c30c781a725336a6e6bc5bb103762a3ff1c0196aa0e38ff05c0c31d314	849dfdcc0d3dd3491ee3d52d1746bea3e20935e275d9bb9abac61090849a7e77	FALSO
545001	550000	37f7326a13bf8c73964990031e7611002a383e041dc02d7cc7a9a132b6114457	478b539ee81ad19c8f77e374b930c4842b773e6b7ec9612accd5bd82ba94dca1	FALSO
550001	555000	ba59643f5dfc5403a87614bc4351041dda0f38556c32c7f4c60a26358433c476	ba59643f5dfc5403a87614bc4351041dda0f38556c32c7f4c60a26358433c476	VERDADERO
555001	560000	d47db896fac2267cc4ac02a969d2626b80e5bce57cef7216903333ab1ad1bd28	d47db896fac2267cc4ac02a969d2626b80e5bce57cef7216903333ab1ad1bd28	VERDADERO
560001	565000	9009b8fb664b79b71c3882584d0fb4c3cc1130b63b15d0c6c69c9f3d98f0f836	9009b8fb664b79b71c3882584d0fb4c3cc1130b63b15d0c6c69c9f3d98f0f836	VERDADERO
565001	570000	43c25f015457388f5d555185a020cba2f559e50827e0023c2e74a2b6e81dab25	43c25f015457388f5d555185a020cba2f559e50827e0023c2e74a2b6e81dab25	VERDADERO
570001	575000	5f05cb860f7146bb8ff20a5c6f499ab6aba3dc8fc4b5ec71706f84fdbb2bcf09	258e2e31ea90e8760f74f6cbb09164c2ce83173cd660b73f16e2f6389b8eb12b	FALSO

Debido a la detección de inconsistencias observadas en la bitácora (descritas en los puntos anteriores) no es posible realizar un análisis de la bitácora obtenida durante el simulacro tres por las siguientes razones:

- No es posible realizar el análisis de seguimiento de las actas utilizando los archivos json obtenidos por el servicio proporcionado por el IETAM. El servicio devolvió contenidos diferentes para un mismo rango de registros.
- No hay forma de identificar qué bitácora es la correspondiente al Simulacro número 3. Al analizar los archivos con los registros de 1 a 5000 se encontraron registros diferentes. Este comportamiento es persistente en la mayoría de los archivos.
- No es posible realizar un seguimiento a través del tiempo de las acciones que se realizaron durante el Simulacro número 3. Se encontraron diferencias en los atributos de los registros conservando los campos de estampa de tiempo (*fechaHoraMovimiento*) e *idBitacoraAuditor* intactos.
- No es posible dar seguimiento a las actas a través de todo el ciclo de vida del Simulacro 3, algunos registros que interactúan directamente con las actas tienen contenido diferente en la misma estampa de tiempo en los archivos analizados.

Un análisis más detallado de la bitácora se puede encontrar en el anexo *N1/Bitacora/Anotaciones.pdf.*

6.6 Conclusiones

Con base a la correspondencia de la información (imágenes, base de datos, datos) de las pruebas operativas y el análisis del log del web service proporcionado por el proveedor se puede concluir que

el sistema informático es altamente funcional, que cumple con los lineamientos requeridos por el IETAM sin embargo, a partir de las pruebas se encontraron diferentes áreas de oportunidad las cuales se listan a continuación:

Conclusiones Nivel de Aplicación

- Se implementó un mecanismo para la asignación de roles y usuarios. El proceso de asignación de contraseña involucra actividades manuales que generan algunas vulnerabilidades relativas a la seguridad del sistema.
- La eficiencia de algunos procesos puede ser mejorada, por ejemplo el proceso de validación podría implementar un mecanismo de notificaciones que informe a los validadores cuándo un acta está disponible.
- Aún no existe un módulo del sistema que permita hacer seguimiento detallado de las variables de control del proceso, como por ejemplo actas en estados inconsistentes, acceso de usuarios, métricas de desempeño de los operadores, demanda del sistema.
- Se desconoce si existe un mecanismo de liberación y versionamiento del sistema que asegure al 100% que las versiones auditadas no pueden ser cambiadas durante el simulacro de una jornada electoral.
- Se desconoce si el desrrollo de la aplicación sigue un modelo de proceso que guie el desarrollo del sistema (SCRUM, RUP, TSP, etc)
- De acuerdo con el pérfil de calidad obtenido existen algunas áreas de oportunidad del sistema que pueden considerarse para los eventos subsiguientes antes de la jornada electoral. Por ejemplo en lo relacionado con las buenas prácticas.

Conclusiones Nivel Base de Datos

- Aunque el proveedor del PREP cuenta con un log general que pone a disposición del Ente Auditor, existe una gran área de oportunidad para que de manera sistemática sea posible garantizar al 100% la correspondencia entre los datos generados por el proceso operativo y los datos publicados pues existen inconsistencias en la publicación de resultados que impiden corroborar el total de las actas en tiempo real, aunque se cuentan con medios para hacerlo de manera semi-automática.
- Se observaron algunos puntos de mejora en el diseño de algunas tablas, más específicamente en aquellas donde se registran los votos contabilizados para candidatos independientes.
- Existen áreas de oportunidad en el diseño del modelo de los datos (tipo de dato de los campos y nombre de campos). Si bien el proveedor del PREP ofreció un mecanismo (web service) para auditar algunos elementos del proceso, la información obtenida de dicho mecanismo es limitada. No es recomendable que el proveedor defina qué tipo de información es susceptible de ser auditada.
- Se observaron áreas de oportunidad para mejorar el rendimiento en el webservice proporcionado por el IETAM.
- Las actas registradas en la base de datos de publicación han mostrado una correspondencia directa con las imágenes publicadas en el sitio de publicación, no obstante, aún existen inconsistencias en el sitio que deben ser corregidas, como los son los errores en los nombres de las actas.
- Hasta el momento de la realización del Simulacro 3 no se han encontrado en la base de datos de publicación registros de imágenes de actas sin huellas criptográficas.
- En el repositorio de imágenes del sistema de publicación se han llegado a encontrar más imágenes de las procesadas.
- Se ha observado retrasos en los cortes de información realizados en el sitio de publicación.

En general el proceso de auditoría ha sido ejecutado satisfactoriamente aunque se han presentado algunos eventos que han retrasado ligeramente la planeación prevista por el ente auditor. Entre estos eventos cabe destacar:

- El proveedor entregó parcialmente y con algunos retrasos la documentación solicitada por el ente auditor.
- La documentación entregada no contiene un diseño detallado de la solución.
- No fue posible verificar detalladamente las buenas prácticas de diseño e implementación de los componentes del sistema tanto a nivel aplicación como de base de datos.

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

7.1 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. La validación respecto a la correspondencia del software auditado y el utilizado en la operación del PREP, se tendrá que realizar al inicio, durante y al final de la operación del sistema informático del PREP.

7.2 Alcance

Especialistas del ente auditor deberán llevar a cabo un procedimiento técnico para verificar que los programas auditados se encuentren operando desde el inicio y hasta el cierre de operación del sistema informático del PREP, así como que la base de datos se encuentre debidamente inicializada. Dicho procedimiento deberá ser validado por el personal que el OPL designe para tal efecto, contemplando los siguientes aspectos como mínimo:

1. El procedimiento deberá contar con un diagrama de flujo.
2. El procedimiento deberá incluir los roles y responsabilidades de los involucrados.
3. El procedimiento deberá documentar como mínimo, las siguientes etapas:
    - Generación, obtención y validación de huellas criptográficas en SHA3-256 del software PREP auditado.
    - Generación, obtención y validación de huellas criptográficas en SHA3-256 del software PREP instalado en el ambiente productivo que operará el día de la Jornada Electoral.
    - Validación de la información inicial y final de la base de datos del PREP.
    - Constancia de hechos.

7.3 Procedimiento técnico para la validación del PREP

7.3.1 Flujo de trabajo general

La validación de la inicialización de las bases de datos y aplicaciones se realizará mediante huellas criptográficas para cada evento considerado por el IETAM (simulacros y jornada electoral). El proceso de validación, mostrado en Figura 7.1, se realizará en 4 etapas. En la primera de ellas llamada GHC Inicial, un software, desarrollado por el ente auditor, automáticamente creará las huellas criptográficas de las bases de datos y las aplicaciones inicializadas por el PROVEEDOR (mediante el algoritmo SHA3-256) y son firmados digitalmente utilizando el algoritmo RSA para la creación de llaves pública/privada). Este modelo garantiza que solo se validarán las huellas criptográficas creadas por el PROVEEDOR.

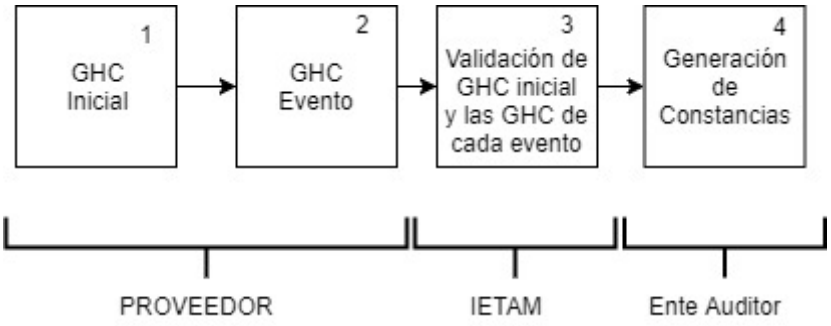


Figura 7.1. Diagrama de Flujo 1 Flujo general de trabajo para la validación de la información inicial y final de la base de datos y del software instalado en el ambiente productivo que operará en día de la jornada electoral.

En la segunda etapa llamada GHC Evento, el proceso se repetirá por cada evento considerado por el IETAM (3 simulacros y 1 jornada electoral). En la tercera etapa (Validación de GHC inicial y las GHC de cada evento), el IETAM ejecutará el software de validación que comparará cada huella criptográfica generada en cada evento y que las firmas de cada huella correspondan a la firma del PROVEEDOR (este proceso es automático). En la última etapa (Generación de Constancias), el ente auditor descargará el reporte detallando la coincidencia o no de cada criptográfica y su correspondiente firma digital. Este reporte es generado por el servicio de validación invocado por el IETAM. Esta etapa finaliza cuando el ente auditor presenta el reporte (sin incidencias) al notario y se procederá a la firma de la constancia correspondiente. Los detalles de cada etapa de este proceso son descritas y detalladas a continuación.

7.3.2 Etapa 1: Generación de huellas criptográficas iniciales (GHC inicial).

Esta llamada GHC Inicial se describe el diagrama de flujo diseñado por el ente auditor para la generación de huellas criptográficas iniciales.

Generación de llaves para firma digital

En la actividad 1, mostrada en el Diagrama de Flujo 2 de la Figura 7.2, el PROVEEDOR invocará el software ***generarLlaves*** para crear dos llaves (una privada conocida como SK y otra pública conocida como PK).

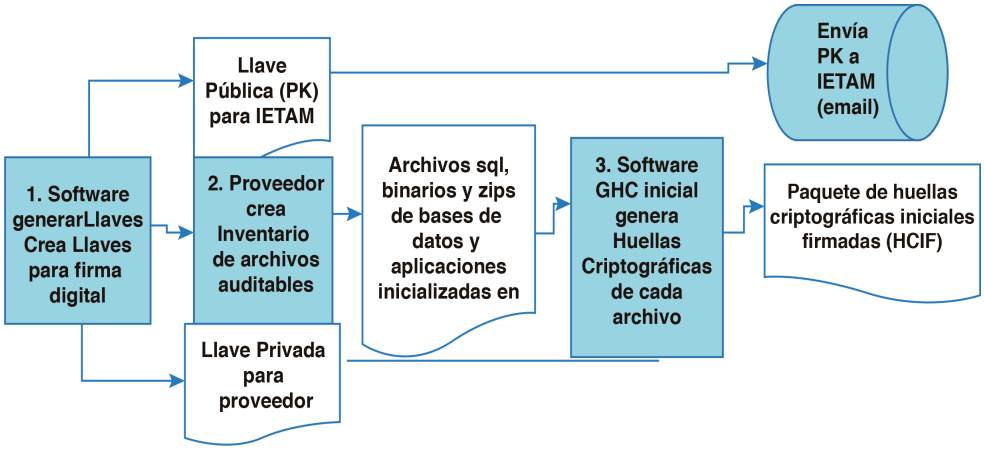


Figura 7.2 Diagrama de Flujo 2 Flujo de trabajo para la generación de huellas criptográficas iniciales de archivos del inventario firmadas por el proveedor.

El software generar llaves depositará la llave SK en el lugar donde el proveedor invocó dicho software.
El PROVEEDOR deberá enviar la llave pública a el Ente Auditor y el IETAM por correo electrónico.
El flujo de trabajo para la generación de la llave pública (PK) y privada (SK) es el siguiente:

1. El personal del PROVEEDOR ejecutará la aplicación ***generarLlaves*** para generar las llaves PK y SK.
2. La llave SK se quedará almacenada de manera local en la carpeta indicada en la ejecución de la aplicación, esta llave quedará al resguardo del personal del PROVEEDOR, el sistema no la enviará a ninguno entidad involucrada, el proveedor es responsable de resguardarla ser usada en los siguientes eventos tales como los 3 simulacros o la jornada elector (se recomienda al proveedor conservar la llave y por ningún motivo compartirla con terceros).

Para detalles técnicos sobre los algoritmos utilizados por ***generarLlaves*** dirigirse al Diagrama de Flujo 3.
Para ejecutar el software ***generarLlaves***, la única operación que debe realizar el PROVEEDOR es abrir una terminal de línea de comandos y copias y pegar en esa terminal el siguiente comando:

java -jar 2103Proveedor.jar generarLlaves Llavero/ Original.

Donde ***java -jar 2103Proveedor.jar*** es el ejecutable creado para el proveedor, ***generarLlaves*** indica la acción que el software debe realizar, ***Llavero/*** es la ruta donde se guardarán las dos llaves de forma local (para no comprometer la seguridad del proveedor se sugiere crear esta carpeta) y **Original** es el nombre de la actividad que se está realizando.
Nota: El software ***generarLlaves*** detecta si en la ruta ***Llavero*** ya existen las llaves. Si es el caso muestra un mensaje que ya existen las llaves y no se generan. Esto ocurre porque las llaves se deben de generar una sola vez.

Inventario de archivos

En la actividad 2, el Proveedor deberá organizar los archivos de los cuales se obtendrá la huella digital y procederá a organizarlos en una carpeta llamada ***Inventario***, la cual deberá incluir los archivos que se listan a continuación:

Base de datos y sistema de archivos.

- El proveedor deberá proporcionar una lista con todas sus bases de datos.
- El proveedor deberá proporcionar un dump de cada una de sus bases de datos vacía e inicializadas, para realizar este paso es necesario ingresar a la terminal de mysql con un usuario y password con privilegios para realizar un respaldo y ejecutar el comando (mysqldump nombre_de_Base_de_Datos > nombre_de_la_base_de_datos.sql). El nombre del sql producido debe ser el mismo que el de la base de datos lista y no deberá contener espacios.
- El proveedor deberá proporcionar información del sistema de archivos para publicación vacío e inicializado. El PROVEEDOR realizará un dir (widows) y guardará la información en un archivo llamado “SISTEMADEARCHIVOS.txt” como se muestra el siguiente ejemplo “dir > SISTEMADEARCHIVOS.txt” o su caso para Linux realizará un ls, estos comandos deben de ser ejecutados en la carpeta donde se almacena la información (json) para su publicación y se colará el archivo resultante en la carpeta de inventario.

Al realizar el dump de base de datos el PROVEEDOR deberá de omitir la estampa de tiempo que se genera en el archivo .sql de forma automática por el gestor de base de datos. Esto es importante para no generar conflictos a la hora de mantener la integridad de los archivos.
Una vez obtenidos estos dumps el proveedor deberá depositarlos en la carpeta de inventario.

Aplicación.
La siguiente lista enumera las aplicaciones que conforman el sistema informático PREP y que por ende es requerido verificar que sus versiones liberadas en producción correspondan a la última versión liberada por el proveedor.

1. Aplicación PREP Casilla.
2. Aplicación PREP CATD
3. Sistema para verificación y administración del PREP
4. Sitio de publicaciones del PREP
5. Sistema de generación de cortes de información.

Para esto, se requiere que el proveedor realice un inventario de todos los elementos que componen cada una de las dichas aplicaciones y especifique la ubicación física de cada uno de ellos con el fin de ejecutar un proceso de generación de firmas que se describe en las siguientes secciones.

Generación de huellas criptográficas iniciales (GHC inicial).

El PROVEEDOR ejecutará de nueva cuenta la aplicación ***2103Proveedor.jar***, pero en esta ocasión indicará como la acción a realizar ***firmarArchivos*** y proporcionará la ruta de la llave privada (SK) (***Llavero/LlavePrivada)***.
A continuación, se describe el flujo de trabajo para la Aplicación de firmas.

1. El PROVEEDOR ejecuta la aplicación ***2103Proveedor.jar*** dando como entrada la ruta donde se encuentra el inventario de archivos y la ruta de la llave privada SK.
2. La aplicación en forma automática realizará las siguientes acciones:
    a. Se obtendrán las huellas criptográficas de cada documento que se encuentre en el inventario de archivos usando el algoritmo SHA3-256. Si el archivo es superior a 1Mb, se realiza una división del archivo en 4 partes iguales (*chunks*). Cada *chunk* es procesado en paralelo obteniendo su hash (H) y finalmente se realiza un hash de la concatenación de estos 4. Este proceso se puede expresar con la siguiente formula:

$$\mathrm{H}(H(\mathrm{Chunk}_1) + H(\mathrm{Chunk}_2) + H(\mathrm{Chunk}_3) + H(\mathrm{Chunk}_4))$$

    Nota: Si los datos no pueden ser divididos en 4 partes iguales, el *chunk* numero 4 se queda con el sobrante.
    b. Cada huella criptográfica será firma digitalmente utilizando la llave privada SK mediante el algoritmo RSA.

Para más detalles técnicos dirigirse al Diagrama de Flujo 4.

Procedimiento para ejecutar la aplicación.
Para ejecutar la aplicación detallada anteriormente, el PROVEEDOR debe abrir una terminal y ejecutar el siguiente comando:
java -jar 1904Proveedor.jar firmarArchivos Inventario/ Llavero/LlavePrivada Original Ciudad
Donde ***java -jar 1904Proveedor.jar*** es la aplicación de generación de huellas criptográficas y firmas digitales, ***Inventario/*** es la ruta donde se encuentran los archivos de las bases de datos y aplicaciones vacías e inicializadas, ***Llavero/LlavePrivada*** es la ruta donde se encuentra la llave privada del PROVEEDOR (SK) y ***Original*** es el nombre que se le da al lote de firmas iniciales y **Ciudad** es el nombre de la ciudad en la que fue realizada la generación de firmas.

7.3.3 Etapa 2. Generación de firmas criptográficas por eventos (GHC eventos).

Esta actividad es similar que la Generación de firmas criptográficas iniciales (GHC inicial). La única diferencia es que el PROVEEDOR ejecutará la aplicación de firmas antes de cada uno de los 3 simulacros y antes de la jornada electoral. Por cada simulacro y jornada electoral se generará un lote de huellas criptográficas y sus correspondientes firmas.
Procedimiento para ejecutar la aplicación.
Para ejecutar la aplicación, el PROVEEDOR debe ejecutar el siguiente comando en una terminal:
java -jar 2103Proveedor.jar firmarArchivos Inventario/ Llavero/LlavePrivada S1 CiudadVictoria.
Donde ***java -jar 2103Proveedor.jar*** es la aplicación, ***Inventario/*** es la ruta donde se encuentra el inventario de archivos, ***Llavero/LlavePrivada*** es la ruta donde se encuentra la llave privada SK y ***S1*** indica al sistema que se está generando un lote de huellas criptográficas y firmas del evento llamado Simulacro 1 y **CiudadVictoria** indica que se está realizando en Ciudad Victoria. Para los siguientes eventos el único parámetro que se debe cambiar es el nombre del evento: por ejemplo: S2 para Simulacro 2, S3 para Simulacro 3 y JE para la Jornada Electoral.

7.3.4 Etapa 3. Validación de las firmas criptográficas (GHC inicial) contra las firmas generadas en la generación de firmas por eventos (GHC eventos).

Para la validación de las firmas generadas durante los simulacros y la jornada electoral. El IETAM contará con un software para la validación de que las huellas criptográficas generados en GHC Eventos para cada archivo sean iguales a los generados en GHC iniciales.
El flujo de trabajo para la validación es el siguiente:

1. El personal Auditor ejecutará la Aplicación de validación dando como entradas la llave pública (PK) y el evento que quiere validar (simulacro 1 [S1], simulacro 2 [S2], simulacro 3 [S3], jornada electoral [JE] o todos [ALL]).
2. La aplicación de validación en forma automática realizará las siguientes acciones:
    a. Descargará el paquete de firmas generados en GHC Inicial.
    b. Descargará el paquete o paquetes de firmas generados en GHC Eventos.
    c. Para cada paquete desencriptará la firma de cada archivo.
    d. Se comparará si la firma criptografía (HASH) desencriptada del paquete generado en GHC Eventos es igual a las firmas criptográficas (HASH) del paquete generado en GHC Inicial.
        i. Si son iguales la validación es correcta, lo que significa que no se presentó ninguna incidencia
        ii. Caso contrario la validación es incorrecta, lo que significa que los archivos firmados por el PROVEEDOR en la etapa inicial no son iguales a los firmados durante los simulacros o jornada electoral.
    e. Se generará un reporte describiendo la validación de cada huella criptográfica y su correspondiente firma digital para cada evento contra las huellas criptográficas generados en GHC Inicial.

Para más detalles dirigirse al Diagrama de Flujo 5.
Procedimiento para ejecutar la aplicación.
Para ejecutar la aplicación detallada anteriormente, el IETAM debe de abrir la línea de comando y ejecutar el siguiente comando:

java -jar 2103IETAM.jar validar Llavero/LlavePublica Original Evento.

Donde ***java -jar 2103IETAM.jar*** es la aplicación, ***validar*** es el nombre de la actividad que se está realizando, ***Llavero/LlavePublica*** es la ruta donde se encuentran la llave pública (n/a, si desea descargar la llave del servicio de almacenamiento), **Original** es el nombre del lote de firmas generadas inicialmente y ***Evento*** es el nombre del paquete de firmas que se quiere validar: Simulacro 1 (S1), Simulacro 2 (S2), Simulacro 3 (S3), Jornada Electoral (JE) o todos (ALL).

7.3.5 Etapa 4. Generación de constancias.

En esta etapa el ente auditor realizará las siguientes actividades:

1. Generar constancia que incluye el reporte de validación.
2. Imprimir la constancia que incluye el reporte de validación que deberá ser firmada por parte del IETAM y Ente Auditor.
3. Genera reporte de validación de integridad de archivos.
4. Imprimir el reporte de validación de integridad de los archivos del inventario inicial y los archivos de los inventarios usados tanto en los simulacros como en la jornada electoral.
5. Firmar la constancia de hechos de la generación de huellas criptográficas.
6. Entregar la constancia de hechos firmada por Ente Auditor al Notario público que dará fe de la validación de los documentos firmados.

7.3.6 Diagramas de flujo

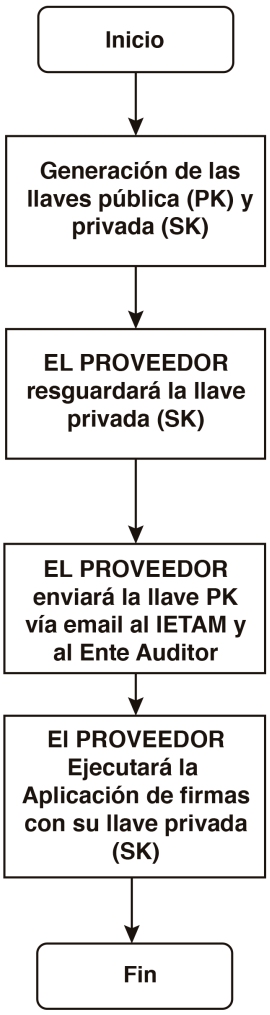


Figura 7.3 Diagrama de Flujo 3 Flujo de trabajo para la generación de las llaves pública y privada por parte del personal del PROVEEDOR.

Flujo de trabajo para la generación de las firmas de los documentos del inventario.

1. El PROVEEDOR ejecuta la aplicación de firmas y dará como entrada su llave SK y la ruta donde se encuentra el inventario de archivos.
2. Cada documento que se encuentra en el inventario de archivos se le aplicará una función SHA3-256, pero con la posibilidad de cambiar el tamaño del hash a SHA3-224, SHA3-384 y SHA3-512 para obtener su clave HASH (H) y se respalda en el paquete packH.
3. Una vez teniendo los HASH's (H_i) de cada archivo del inventario, se realiza una firma de cada HASH (H_i) usando el método RSA que tiene como entrada H_i y la llave SK y su salida es un HASH firmado FH_i. FH_i y H_i se guardan en un paquete llamado PackFH como un par de valores. Al final de este proceso se tendrá por cada archivo un HAHS H_i y su correspondiente HASH firmado (FH_i).
4. El último paso es el envío del paquete packFH y vía email al IETAM y al Ente Auditor.

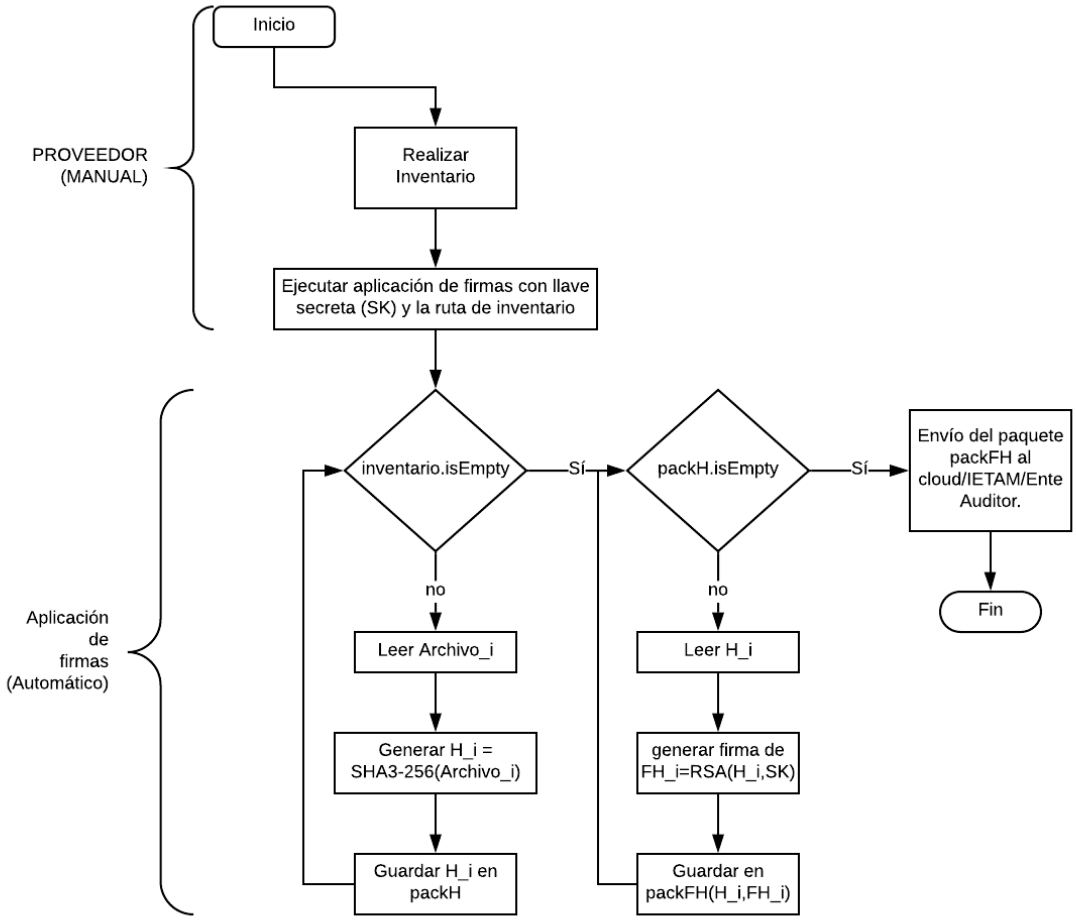


Figura 7.4 Diagrama de Flujo 4 Flujo de trabajo para la generación de las firmas de los documentos del inventario.

Flujo de trabajo para la generación de las firmas de los documentos del inventario

1. El Auditor ejecutará la Aplicación de validación dando como entradas la llave pública (PK) y el paquete que quiere validar (Prueba 1, Paquete simulacro 1, paquete simulacro 2, paquete simulacro 3 o paquete jornada electoral).
2. La aplicación de validación descargará el paquete inicial (packini)
3. La aplicación de validación descargará el paquete o paquetes de las firmas seleccionadas (Paquetes). Donde por cada archivo firmado estará su HASH (H_i) y su firma FH_i.
4. Para cada paquete.
    a. La aplicación de validación para el paquete_j desencriptará la firma FH_i de cada archivo y se respalda en HD.
    b. La aplicación de validación comparará si HD es igual al HASH (H-ini) del paquete inicial (packini).
    c. Si HD y H-ini son iguales la validación es correcta
    d. Si HD y H-ini no son iguales validación es incorrecta lo que significa que los archivos firmados por el PROVEEDOR en la etapa inicial no son iguales a los firmados durante los simulacros o jornada electoral.

5. La aplicación arrojará un reporte donde se mostrarán los HASH's (H) del paquete inicial y sus firmas (FH) en la primera columna, en las siguientes columnas se mostrarán los HASH' (H) y sus firmas de los paquetes del simulacro 1, 2 y 3 y la jornada electoral. En la última columna se mostrará el resultado de comparar los HASH's del paquete inicial con los HASH's de los paquetes de los simulacros y jornada electoral. En el Diagrama de Flujo 4 se muestra el flujo de trabajo de validación.

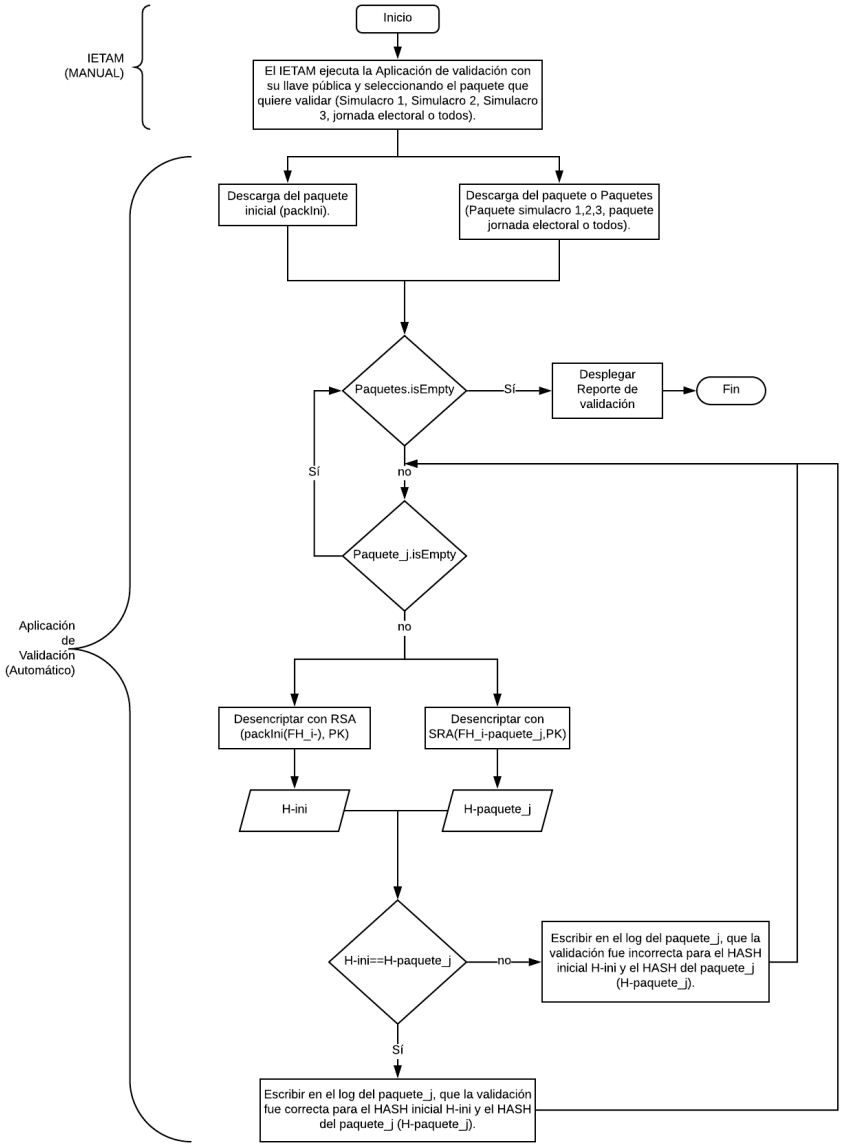


Figura 7.5 Diagrama de Flujo 5 Flujo de trabajo para la validación de las firmas iniciales con las firmas generadas durante los simulacros y la jornada electoral.

7.3.7 Resultados

El procedimiento definido se ha puesto a prueba con éxito durante los simulacros 1, 2 y 3 llevados a cabo el 16, 23 y 30 de mayo de 2021, respectivamente. El procedimiento se realizará el domingo 6 de junio de 2021 en las instalaciones del IETAM, concluyendo el 7 de junio y será atestiguado por un tercero con fe pública designado por el IETAM.

En la Figura 7.6 se presenta la constancia de la generación de huellas criptográficas realizada al final del Simulacro 3.

Ciudad Victoria, Tamaulipas, 30 de Mayo de 2021

Constancia de hechos de la validación de los programas y de la base de datos del sistema informático PREP.

Siendo las 14 horas con 11 minutos del día 30 del mes de Mayo del año 2021 y, en cumplimiento al numeral 14, del Anexo 13 "LINEAMIENTOS DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES (PREP)", el cual menciona que se deberá establecer un procedimiento que garantice y deje evidencia que los programas auditados sean los utilizados durante la operación del PREP, así como un procedimiento que garantice que las bases de datos no cuenten con información antes de su puesta en operación el día de la Jornada Electoral; se procedió a realizar la validación de los módulos funcionales y bases de datos del sistema PREP del estado de Tamaulipas.

Dicha validación consistió en comparar las huellas criptográficas obtenidas a partir de la versión auditada del sistema respecto a las huellas criptográficas del mismo, minutos antes de iniciar la Jornada Electoral.

Para esta validación se contó con la presencia del Lic. José Guadalupe G. Ramos Charre en su calidad de Consejero Presidente del Instituto Electoral de Tamaulipas, del Dr. Javier Rubio Loyola por parte del Cinvestav Tamaulipas en su calidad de Ente Auditor, de la Mtra. Nohemí Argüello Sosa en su calidad de Presidenta de la Comisión Especial de Seguimiento a la Implementación y Operación del Programa de Resultados Electorales, y el Lic. José de los Santos González Picazo en su calidad de Titular de la Instancia Interna Responsable del PREP.

A continuación, se muestran los componentes sujetos a este procedimiento, acompañados del nombre del archivo, la huella criptográfica original (SHA3-256 inicial), la huella criptográfica minutos antes de iniciar la jornada electoral (SHA3-256 inicial) y el resultado de la comparación.

Nombre del Archivo: Base_datos.txt	**Evento: Proceso Electoral Tamaulipas 2021 Fecha validación 2021-05-30 14:10:45**
SHA3-256 Inicial	fd22e5fe04dd0ea2513811575747e559bcea7f2624d7f2dddb036395aa60dc01
SHA3-256 del evento	fd22e5fe04dd0ea2513811575747e559bcea7f2624d7f2dddb036395aa60dc01
Estado	Correcto
Observaciones	Se considera correcto porque las huellas criptográficas evaluadas para este archivo son iguales. Las aplicaciones no deben modificarse, por lo tanto se espera que las huellas criptográficas sean iguales.
Nombre del Archivo: Base_de_datos.sql	**Evento: Proceso Electoral Tamaulipas 2021 Fecha validación 2021-05-30 14:10:45**

Figura 7.6 Constancia de Generación de Huellas Criptográficas del PREP: Página 1.

SHA3-256 Inicial	34f1a1ad83945236af4bc0ad2b251ffd3a25fd0b67dcde5014f474fb4822a849
SHA3-256 del evento	34f1a1ad83945236af4bc0ad2b251ffd3a25fd0b67dcde5014f474fb4822a849
Estado	Correcto
Observaciones	Se considera correcto porque las huellas criptográficas evaluadas para este archivo son iguales. Las aplicaciones no deben modificarse, por lo tanto se espera que las huellas criptográficas sean iguales.
Nombre del Archivo: Generador_Contenido.exe	**Evento: Proceso Electoral Tamaulipas 2021 Fecha validación 2021-05-30 14:10:45**
SHA3-256 Inicial	aaa1ba4df0b7a80e89133c8acbc8e246de07e8432ffc3b2434c609697e808895
SHA3-256 del evento	aaa1ba4df0b7a80e89133c8acbc8e246de07e8432ffc3b2434c609697e808895
Estado	Correcto
Observaciones	Se considera correcto porque las huellas criptográficas evaluadas para este archivo son iguales. Las aplicaciones no deben modificarse, por lo tanto se espera que las huellas criptográficas sean iguales.
Nombre del Archivo: PREP_Casilla.apk	**Evento: Proceso Electoral Tamaulipas 2021 Fecha validación 2021-05-30 14:10:45**
SHA3-256 Inicial	b1c4278d4d5128431725965363979 9b5c033a5ec82da695e3c1c929f253b9839
SHA3-256 del evento	b1c4278d4d5128431725965363979 9b5c033a5ec82da695e3c1c929f253b9839
Estado	Correcto
Observaciones	Se considera correcto porque las huellas criptográficas evaluadas para este archivo son iguales. Las aplicaciones no deben modificarse, por lo tanto se espera que las huellas criptográficas sean iguales.
Nombre del Archivo: PREP_CATD.apk	**Evento: Proceso Electoral Tamaulipas 2021 Fecha validación 2021-05-30 14:10:45**
SHA3-256 Inicial	3b4acd48e3efcc5b4e654062947528d7bfe145a6d0709410d59cd2b2cfb32cbd
SHA3-256 del evento	3b4acd48e3efcc5b4e654062947528d7bfe145a6d0709410d59cd2b2cfb32cbd
Estado	Correcto
Observaciones	Se considera correcto porque las huellas criptográficas evaluadas para este archivo son iguales. Las aplicaciones no deben modificarse, por lo tanto se espera que las huellas criptográficas sean iguales.
Nombre del Archivo: Sistema_Archivos	**Evento: Proceso Electoral Tamaulipas 2021 Fecha validación 2021-05-30 14:10:45**
SHA3-256 Inicial	edbbe13351cea570b831a4693494156fe086d7fd49d57217765bb70b7e21b936
SHA3-256 del evento	edbbe13351cea570b831a4693494156fe086d7fd49d57217765bb70b7e21b936
Estado	Correcto
Observaciones	Se considera correcto porque las huellas criptográficas evaluadas para este archivo son iguales. Las aplicaciones no deben modificarse, por lo tanto se espera que las huellas criptográficas sean iguales.
Nombre del Archivo: Sistema_CCV.exe	**Evento: Proceso Electoral Tamaulipas 2021 Fecha validación 2021-05-30 14:10:45**
SHA3-256 Inicial	c23d9539b597198cba1f75bed595bf826bd5e39f03b3931818a7867780bbe285
SHA3-256 del evento	c23d9539b597198cba1f75bed595bf826bd5e39f03b3931818a7867780bbe285
Estado	Correcto
Observaciones	Se considera correcto porque las huellas criptográficas evaluadas para este archivo son iguales. Las aplicaciones no deben modificarse, por lo tanto se espera que las huellas criptográficas sean iguales.
Nombre del Archivo: Sitio_Publicacion_PREP	**Evento: Proceso Electoral Tamaulipas 2021 Fecha validación 2021-05-30 14:10:45**

Figura 7.6 Constancia de Generación de Huellas Criptográficas del PREP: Página 2.

SHA3-256 Inicial	a3887e2b55f95bd7819c5cea97a55f65e11edf2359535a5067523fd656121fb6
SHA3-256 del evento	a3887e2b55f95bd7819c5cea97a55f65e11edf2359535a5067523fd656121fb6
Estado	Correcto
Observaciones	Se considera correcto porque las huellas criptográficas evaluadas para este archivo son iguales. Las aplicaciones no deben modificarse, por lo tanto se espera que las huellas criptográficas sean iguales.

A continuación, se describe brevemente cada uno de los archivos validados.

Nombre	Descripción
Base_datos.txt	Lista de bases de datos utilizadas en el PREP.
Sistema_Archivos	Catálogos utilizados en el sitio de publicación PREP.
PREP_Casilla.apk	Aplicación móvil para digitalización de actas desde las casillas.
PREP_CATD.apk	Aplicación móvil para digitalización de actas desde los Centros de Acopio y Transmisión de Datos (CATD).
Sistema_CCV.exe	Sistema para la captura, verificación y administración del PREP.
Sitio_Publicacion_PREP	Sitio de publicación del PREP
Generador_Contenido.exe	Sistema para la generación de cortes de información.
Base_de_datos.sql	Script de la base de datos central del PREP.

Firman la presente constancia los representantes de las entidades que intervienen, el Lic. José Guadalupe G. Ramos Charre en su calidad de Consejero Presidente del Instituto Electoral de Tamaulipas, el Dr. Javier Rubio Loyola por parte del Cinvestav Tamaulipas en su calidad de Ente Auditor, la Mtra. Nohemí Argüello Sosa en su calidad de Presidenta de la Comisión Especial de Seguimiento a la Implementación y Operación del Programa de Resultados Electorales, y el Lic. José de los Santos González Picazo en su calidad de Titular de la Instancia Interna Responsable del PREP.

Lic. José Guadalupe G. Ramos Charre
Consejero Presidente del Instituto Electoral de Tamaulipas

Mtra. Nohemí Argüello Sosa
Presidenta de la Comisión Especial de Seguimiento a la Implementación y Operación del Programa de Resultados Electorales

Dr. Javier Rubio Loyola
Ente Auditor

Lic. José de los Santos González Picazo
Titular de la Instancia Interna Responsable del PREP

Figura 7.6 Constancia de Generación de Huellas Criptográficas del PREP: Página 3.

8. Análisis de vulnerabilidades a la infraestructura tecnológica

8.1 Objetivos de análisis de vulnerabilidades

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

- Clasificar el impacto y documentar las vulnerabilidades identificadas con el propósito de recomendar al IETAM las posibles medidas para la mitigación de las vulnerabilidades que previamente fueron identificadas y documentadas.

- Verificar que las medidas implementadas por el IETAM hayan atendido adecuadamente las vulnerabilidades reportadas.

8.2 Alcance de análisis de vulnerabilidades

El análisis de vulnerabilidades de la infraestructura tecnológica se realizó como se describe a continuación:

I. Se convocó al personal desarrollador del PREP del IETAM con el objetivo de agendar una serie de visitas y reuniones consideradas como parte de la auditoría, definir los roles y responsabilidades de las partes, establecer las metodologías y estándares con las que se realizará la auditoría, así como los tiempos generales de ejecución.

   - El Ente Auditor solicitó la información referente a la infraestructura tecnológica y de comunicaciones empleada por el IETAM y el proveedor del servicio para la operación del PREP.
   - Se realizaron visitas a los espacios de trabajo del CCV1, CCV2, CATD-Victoria y CATD Tampico en donde se realizó el análisis de vulnerabilidades a la infraestructura tecnológica del sistema.
   - Se agendaron las ventanas de tiempo solicitadas para la ejecución de la auditoría.

II. **Plan de trabajo detallado.** El ente auditor elaboró un plan de trabajo con los detalles del proyecto de auditoría de seguridad a la infraestructura tecnológica del PREP. En el plan de trabajo se incluyeron dos tipos de pruebas de auditoría:

   - Revisión de configuraciones de seguridad
   - Pruebas de penetración (*pentest*)

8.3 Revisión de configuraciones

8.3.1 Resumen

El presente documento tiene la finalidad de presentar los resultados obtenidos durante la revisión de las configuraciones de la infraestructura tecnológica que será utilizada en los CCV y CATD para el funcionamiento del sistema PREP 2021. Adicionalmente se presentan las recomendaciones identificadas con la finalidad de fortalecer el desempeño de la infraestructura con base en las mejores prácticas desde la perspectiva de seguridad informática.

8.3.2 Objetivo General de revisión de configuraciones

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

8.3.3 Objetivos específicos de revisión de configuraciones

- Identificar debilidades de seguridad en la infraestructura tecnológica.
- Clasificar el impacto y documentar las vulnerabilidades identificadas con el propósito de recomendar al OPL las posibles medidas para la mitigación de las vulnerabilidades que previamente fueron identificadas y documentadas.
- Verificar que las medidas implementadas por el OPL hayan atendido adecuadamente las vulnerabilidades reportadas.

8.3.4 Alcance de revisión de configuraciones

La revisión de las configuraciones de la infraestructura se realizó de acuerdo con el **"Plan de revisión de configuraciones a la infraestructura"** entregado previamente y el cual fue elaborado de acuerdo con la propuesta técnica presentada al IETAM. Las actividades incluidas en el plan son las siguientes:

1. Verificación del control de acceso físico a los equipos
2. Verificación de control de acceso lógico a los equipos de cómputo
3. Revisión de la configuración de los equipos de comunicaciones
4. Revisión de la configuración del sistema operativo
5. Revisión de la configuración de aplicaciones
6. Funcionamiento de la planta eléctrica de emergencia
7. Funcionamiento de los sistemas de alimentación ininterrumpida (SAI)

La realización de las actividades del plan de revisión de configuraciones de la infraestructura fue dividida en dos partes:

A. Documentación de las configuraciones implementadas mediante entrevistas con el personal técnico del proveedor de la implementación del sistema PREP y mediante documentos de trabajo.
B. Validación de las configuraciones implementadas a través de herramientas de software especializado para seguridad informática en las actividades que así lo requieran.

El desarrollo de las actividades mencionadas fue realizado de acuerdo con el siguiente calendario:

Tabla 8.1 Calendario. Nivel Plataforma Tecnológica.

Ubicación	Fecha
CCV y CATD Reynosa	10 de Mayo 2021
CCV y CATD Victoria	11 de Mayo 2021
CCV y CATD Madero	12 de Mayo 2021

8.3.5 Hallazgos y recomendaciones

A continuación, se presentan los resultados obtenidos durante la realización de las actividades en las ubicaciones definidas por el IETAM.

8.3.5.1 Verificación del control de acceso físico a los equipos.

En esta actividad se realizó la verificación del aseguramiento del acceso físico a las instalaciones que deben estar bajo acceso restringido.

Procedimiento de la revisión

- Visita de inspección a los CCV y CATD
- Entrevista con el personal técnico asignado por el proveedor del sistema PREP

Información recopilada

- El aseguramiento del acceso físico a las instalaciones de los CCV y CATD en lo general será provisto por personal de la secretaría de Seguridad Pública del Gobierno del Estado.
- El sistema de video-vigilancia en los CCV's está implementado y en funcionamiento.
- La credencialización del personal que participará en la jornada electoral es realizada mediante gafetes impresos por el proveedor.
- El registro de control de acceso y asistencia del personal operativo que participará en la jornada electoral es realizado vía telefónica.

Observaciones

O3-C-1 Los espacios físicos donde están ubicados los CCV y los CATD no cuentan con sistema de alarmas ni con sistema de control de acceso físico automatizado.

O3-C-2 El proveedor no cuenta con personal dedicado para el monitoreo del sistema de videovigilancia.

Recomendaciones

R3-C-1 Es recomendable que al menos la instalación de los equipos de comunicaciones y de seguridad perimetral de los Centros de Captura y Verificación (CCV) este implementada si al interior del mismo edificio, pero en un espacio físico distinto a donde estará trabajando el personal operativo de la jornada electoral y con acceso restringido al menos por una puerta con acceso controlado o por un sistema de control de acceso físico automatizado.

R3-C-2 Es altamente recomendable que se defina personal dedicado para el monitoreo de la operación del sistema de videovigilancia.

R3-C-3 Es recomendable que al menos en los CCV se implemente un sistema de control de acceso físico automatizado tipo biométrico para todo el personal operativo que participará en la jornada electoral, mediante el cual sería posible tener un mayor control de los accesos a los espacios y evidencia ante posibles incidencias de parte de personas ajenas al OPL y/o instituciones acreditadas participantes de la jornada electoral.

8.3.5.1 Verificación de control de acceso lógico a los equipos de cómputo.

En esta actividad se realizó la revisión general de la configuración de los equipos y aplicaciones utilizadas para la protección del acceso lógico a los equipos.

Procedimiento de la revisión

- Visita de inspección a los CCV y CATD
- Entrevista con el personal técnico asignado por el proveedor del sistema PREP

Información recopilada

- Todos los servidores que serán utilizados en el proceso electoral están implementados en un servicio en la nube con el proveedor Amazon y configurados dentro de una red privada dentro del mismo servicio.
- Todos los equipos de cómputo de los CCV y CATD cuentan con software antivirus y actualizaciones del sistema operativo.

Observaciones

O3-C-3 La cuenta de usuario por de los equipos de cómputo esta debidamente delimitada para sus actividades y no cuenta con privilegios de administrador

Recomendaciones

R3-C-4 Es altamente recomendable que para procesos futuros si la infraestructura referente a los servidores donde serán implementadas las aplicaciones para el sistema PREP será provista mediante servicios en la nube, el proveedor brinde al ente auditor más información técnica y a tiempo sobre la arquitectura desplegada con la finalidad de realizar la revisión de las configuraciones en tiempo y forma

8.3.5.3 Revisión de la configuración de los equipos de comunicaciones

En esta actividad se realizó la revisión de la configuración de los parámetros de conectividad en la red local de los CCV y CATD que serán utilizados por la infraestructura.

Procedimiento de la revisión

- Visita de inspección a los CCV y CATD
- Entrevista con el personal técnico asignado por el proveedor del sistema PREP
- Revisión de la configuración del equipo de seguridad perimetral mediante el acceso a la consola de administración del equipo
- Ejecución de análisis de detección de vulnerabilidades mediante software de reconocimiento y escaneo de puertos.

Información recopilada

- Los equipos de comunicaciones en los CCV están configurados con direccionamiento IP estático privado
- Los equipos de comunicaciones en los CATD están configurados con direccionamiento IP dinámico privado
- Los CCV cuentan con un equipo de seguridad perimetral con políticas de filtrado.
- Los servicios de acceso remoto al equipo de seguridad perimetral del CCV están activos.
- Los equipos de conmutación y direccionamiento en los CATD son los módems VDSL y sus puertos de administración están activos.

Observaciones

O3-C-4 El servicio de Internet en los equipos de cómputo de los CATD estaba abierto durante la revisión, aunque para el simulacro 1 ya fue restringido con acceso solamente a las aplicaciones del sistema PREP.

Recomendaciones

R3-C-5 Es recomendable que la configuración del direccionamiento IP sea estática en todos los CATD y CCV o dinámica, pero con un control de autenticación habilitado por ejemplo mediante MAC ADDRESS o por 802.1X para ambos esquemas, así como deshabilitar los puertos físicos en los switches o módems que no estén utilizados.

R3-C-6 Es altamente recomendable mantener las restricciones en el acceso a Internet en la red de los CATD durante la jornada electoral.

8.3.5.4 Revisión de la configuración del sistema operativo

En esta actividad se realizó la revisión de los parámetros del sistema operativo de los equipos de cómputo.

Procedimiento de la revisión

- Visita de inspección a los CCV y CATD
- Entrevista con el personal técnico asignado por el proveedor del sistema PREP
- Ejecución de análisis de detección de vulnerabilidades mediante el software reconocimiento y escaneo de puertos.

Información recopilada

- Las estaciones de trabajo de los CATD y CCV están configuradas con el sistema operativo Microsoft Windows 10 Pro de 64 bits versión 20H2
- Las estaciones de trabajo de los CATD y CCV no requieren proveer servicios activos.

Observaciones

O3-C-9 La imagen del sistema operativo es la misma en todas las estaciones de trabajo
O3-C-10 Los puertos USB en los equipos de cómputo de los CCV están activos

Recomendaciones

R3-C-7 Es altamente recomendable hacer disponible la evidencia de los esquemas de licenciamiento con los cuales cuenta el proveedor para el software propietario utilizado en todas las estaciones de trabajo para la jornada electoral
R3-C-8 Es altamente recomendable ejecutar una actualización general mediante Windows Update en todas las estaciones de trabajo para la jornada electoral con la finalidad de que se encuentren protegidas contra vulnerabilidades de reciente descubrimiento

8.3.5.5 Revisión de la configuración de aplicaciones

En esta actividad se realizó la revisión de la configuración de las aplicaciones instaladas en los equipos que serán utilizados en el proceso.

Procedimiento de la revisión

- Visita de inspección a los CCV y CATD
- Entrevista con el personal técnico asignado por el proveedor del sistema PREP

Información recopilada

- Todos los servidores que serán utilizados en el proceso electoral están implementados en un servicio en la nube contratado con el proveedor Amazon y configurados dentro de una red privada dentro del mismo servicio, a los cuales no se pudo tener acceso para su revisión.
- Las estaciones de trabajo tienen instaladas solamente las aplicaciones requeridas para el sistema PREP.

Observaciones

Ninguna

Recomendaciones

Ninguna

8.3.5.6 Funcionamiento de la planta eléctrica de emergencia

En esta actividad se realizó la revisión general del funcionamiento de la integración de la planta eléctrica de emergencia a la instalación eléctrica provista para los equipos de la plataforma tecnológica, la cual protege a los equipos que serán utilizados en el proceso ante posibles fallas en el suministro de energía eléctrica.

Procedimiento de la revisión

- Visita de inspección a los CCV y CATD
- Entrevista con el personal técnico asignado por el proveedor del sistema PREP

Información recopilada

- En el CCV Victoria se validó la instalación y puesta a punto de la planta de emergencia.
- En el CCV de Reynosa y Madero, así como en sus CATD no se pudieron realizar pruebas dado que los equipos (plantas de emergencia) no estuvieron disponibles durante las visitas.

Observaciones

O3-D-1 La planta de emergencia en el CCV Victoria funcionó de manera correcta.

Recomendaciones

R3-D-1 Es altamente recomendable realizar las actividades de revisión del funcionamiento de las plantas de emergencia al menos de forma semanal previamente al desarrollo de la jornada electoral.

8.3.5.7 Funcionamiento de los sistemas de alimentación ininterrumpida (SAI)

En esta actividad se realizó la revisión del funcionamiento de los equipos de alimentación ininterrumpida (SAI o UPS por sus siglas inglés) que protegerán a los equipos que serán utilizados en el proceso ante perturbaciones transitorias, interrupciones, bajada de tensión / subtensión, aumento de tensión / sobretensión que se presentan durante el suministro de energía eléctrica.

Procedimiento de la revisión

- Visita de inspección a los CCV y CATD
- Entrevista con el personal técnico asignado por el proveedor del sistema PREP

Información recopilada

- Cada estación de trabajo y escáner en los CCV y CATD tiene instalado un SAI individual con las capacidades adecuadas para la protección hasta de 5 a 10 minutos en promedio ante los problemas más comunes presentados en el suministro de energía eléctrica.

Observaciones

O3-D-2 Algunos equipos en los CATD no estaban debidamente conectados a los contactos protegidos por las baterías, situación que fue corregida al ser reportada durante la revisión.

Recomendaciones

R3-D-2 Es altamente recomendable realizar las actividades de revisión del funcionamiento de los equipos SAI al menos de forma semanal previamente al desarrollo de la jornada electoral.

8.4 Pruebas de penetración (pentest).

8.4.1 Introducción

Las pruebas de penetración también llamadas “pentesting” forman parte de una técnica utilizada en el contexto de seguridad informática para poner a prueba un sistema informático con la finalidad de encontrar vulnerabilidades que un atacante mal intencionado podría utilizar (explotar) con determinados propósitos. A través de técnicas y herramientas de Hackeo Ético se busca explotar activamente las vulnerabilidades de seguridad para obtener información relevante, tal como lo intentaría un intruso.

Las pruebas de penetración también pueden ser utilizadas para validar el cumplimiento de las políticas de seguridad de una organización, así como su capacidad para identificar y hacer frente a incidentes de seguridad informática y crear conciencia entre las personas que hacen uso de los dispositivos informáticos.

Un ataque de penetración puede realizarse de manera remota (desde el exterior por ejemplo desde Internet) o localmente (desde a red interna de la organización). En el siguiente reporte se presentan los resultados de las pruebas de penetración realizadas a la infraestructura tecnológica provista por el OPL , incluyendo los diferentes dispositivos presentes en la infraestructura que son clave para llevar a cabo el Proceso Técnico Operativo del sistema PREP para el estado de Tamaulipas.

Las pruebas se realizaron y ejecutaron en dos fases, la primera se desarrolló del 10 al 12 de mayo y la segunda el 16 de mayo de 2021. En la primera fase se analizó la infraestructura local de los Centros de Captura y Verificación (CCV) Victoria, Reynosa y Madero y los Centros de Acopio y Transmisión de Datos (CATD) ubicados en los mismos municipios. En la segunda fase se analizó la plataforma externa (nube) desplegada a través de los servicios del proveedor Amazon.

El alcance de las pruebas realizadas se centró en la identificación de riesgos a la plataforma tecnológica que pudieran afectar el proceso técnico operativo. Para ello, mediante herramientas especializadas se recabó información relevante de los dispositivos, misma que pudiera ser utilizada para la identificación de posibles vulnerabilidades, así como la explotación de estas. Las pruebas se centraron en vulnerabilidades que pudieran ser usadas para comprometer la funcionalidad del sistema PREP durante la jornada electoral 2021.

La planeación de las pruebas de penetración sobre la infraestructura tecnológica provista para los servicios del sistema PREP Tamaulipas está elaborada con base en las siguientes metodologías:

- *Open Source Security Testing Methodology (OSSTMM) v3”* creado por el *“Institute for Security and Open Methodologies (ISECOM)”*, capítulos 7, 8, 9,10 y 11
- Penetration Testing Execution Standard (PTES), secciones: Intelligence Gathering, Threat Modeling, Vulnerability Analysis y Exploitation.
- Information Security Testing and Assessment of the National Institute of Standards and Technology (NIST), capítulos 2, 3, 4, 5, 6 y 7.
- Open Web Application Security Project Testing Guide v.4.0, capítulo 4.

Adicionalmente se utilizó la base de conocimiento mundial de tácticas y técnicas MITRE ATT&CK para la planificación de las pruebas a realizar, en específico de las técnicas utilizadas por el grupo APT28 el cual está directamente relacionado con los servicios producto de la presente auditoria.

8.4.2 Alcance

Para el análisis y detección de posibles vulnerabilidades en los equipos de la plataforma tecnológica, es necesario utilizar herramientas que permitan realizar las actividades descritas a continuación:

- Pruebas de seguridad en el contexto del personal operativo del sistema
- Pruebas de seguridad en el contexto del acceso físico a la infraestructura tecnológica
- Pruebas de seguridad mediante extracción y recolección de información de la plataforma tecnológica alámbrica e inalámbrica
- Escaneo de puertos e identificación de servicios
- Búsqueda y explotación de vulnerabilidades

8.4.7 Hallazgos de las pruebas de penetración

8.4.7.1 CCV Reynosa

Tabla 8.2 Resultado de pruebas en CCV Reynosa

Actividad	Resultados
Filtrado MAC	No se tiene configurado el filtrado por MAC Address como se menciona en los insumos, ya que fue posible utilizar uno de los puertos físicos con solamente detectar el direccionamiento IP privado de la red.
Identificación de segmentos de red	Los segmentos de red identificados fueron los siguientes: • Red 1 (Equipos administrativos): 192.168.1.0/24. • Puerta de enlace: 192.168.1.254 • Servicio DHCP habilitado • Red no administrada por el equipo de seguridad perimetral • Red 2 (Equipos de captura): 192.168.89.0/24. • Puerta de enlace: 192.168.89.1 • Red administrada por el equipo de seguridad perimetral • Servicio DHCP deshabilitado • 30 equipos de cómputo identificados • Se identificaron los puertos 80 y 443 abiertos en la puerta de enlace
Análisis de redes inalámbricas	• El SSID se encuentra visible, con el nombre y contraseña por default provista por el proveedor. • - 115 -Acceso libre a internet • Las redes WIFI detectadas son vulnerables a un ataque de

	denegación de servicio (DoS).
Análisis de vulnerabilidades	• No se encontraron vulnerabilidades que se pudieran explotar en los equipos de captura
Análisis de puertos físicos activos	• Los puertos físicos están deshabilitados de forma correcta
Entrevista de personal técnico	• La transmisión de datos entre los equipos del CCV y los servicios en la nube se dice en los insumos que se lleva a cabo mediante un protocolo de reconocimiento. Al preguntar al personal sobre cuál es ese protocolo y en qué consiste su respuesta fue que utilizan un protocolo TCP y no facilitaron más información.

8.4.7.2 CCV Victoria

Tabla 8.3 Resultado de pruebas en CCV Victoria

Actividad	Resultados
Filtrado MAC	No se tiene configurado el filtrado por MAC Address como se menciona en los insumos, ya que fue posible utilizar uno de los puertos físicos con solamente detectar el direccionamiento IP privado de la red.
Identificación de segmentos de red	Los segmentos de red identificados fueron los siguientes: • Red 1 (Equipos administrativos): 192.168.0.0/24. • Puerta de enlace: 192.168.0.1 • Servicio DHCP habilitado • Red administrada por el equipo de seguridad perimetral • En esta red se identificaron 20 equipos • Red 2 (Equipos de captura): 192.168.89.0/24. • Puerta de enlace: 192.168.89.1 • Red administrada por el equipo de seguridad perimetral • Servicio DHCP deshabilitado • 48 equipos de cómputo identificados • Red 3 (Equipos de captura): 192.168.90.0/24. • Puerta de enlace: 192.168.90.1 • Red administrada por el equipo de seguridad perimetral • Servicio DHCP deshabilitado • 35 equipos de cómputo identificados
Análisis de redes inalámbricas	• El SSID se encuentra visible, con el nombre y contraseña provista por el personal del OPL. • Acceso libre a internet • Las redes WIFI detectadas son vulnerables a un ataque de denegación de servicio (DoS).
Análisis de vulnerabilidades	No se encontraron vulnerabilidades que se pudieran explotar en los equipos de captura, pero se identificaron abiertos los siguientes servicios: • Red 1: 80,443,515,631,5061,5357,7070, 8080, 9100 y 62078 TCP

	• Puerta de enlace equipos en Red 1: 22, 80 y 1900 TCP • Puerta de enlace equipos en Red 2: 21, 22, 23,53,80,2000 y 8291 • Puerta de enlace equipos en Red 3: : 21, 22, 23,53,80,2000 y 8291 • Laptop de administrador de red: 80,135,139,445,515,1801,1947,2103,2105,2107,3389,5357
Análisis de puertos físicos activos	• Los puertos físicos están deshabilitados de forma correcta
Entrevista de personal técnico	• La transmisión de datos entre los equipos del CCV y los servicios en la nube se dice en los insumos que se lleva a cabo mediante un protocolo de reconocimiento. Al preguntar al personal sobre cuál es ese protocolo y en qué consiste su respuesta fue que utilizan un protocolo TCP y no facilitaron más información.

8.4.7.3 CCV Madero

Tabla 8.4 Resultado de pruebas en CCV Madero

Actividad	Resultados
Filtrado MAC	No se tiene configurado el filtrado por MAC Address como se menciona en los insumos, ya que fue posible utilizar uno de los puertos físicos con solamente detectar el direccionamiento IP privado de la red.
Identificación de segmentos de red	Los segmentos de red identificados fueron los siguientes: • Red 1 (Equipos administrativos): 192.168.1.0/24. • Puerta de enlace: 192.168.1.254 • Servicio DHCP habilitado • Red no administrada por el equipo de seguridad perimetral • 9 equipos de cómputo identificados • Red 2 (Equipos de captura): 192.168.89.0/24. • Puerta de enlace: 192.168.89.1 • Red administrada por el equipo de seguridad perimetral • Servicio DHCP deshabilitado • 32 equipos de cómputo identificados
Análisis de redes inalámbricas	• El SSID se encuentra visible, con el nombre y contraseña por default provista por el proveedor. • Acceso libre a internet • Las redes WIFI detectadas son vulnerables a un ataque de denegación de servicio (DoS).
Análisis de vulnerabilidades	No se encontraron vulnerabilidades que se pudieran explotar en los equipos de captura, pero se identificaron abiertos los siguientes servicios: • Red 1: 80,135,139,443,445,515,554,631,2869,5357,7070, 8080, 9100 y 10243 TCP • Puerta de enlace equipos en Red 1: 22, 53, 80, 443 y 5001 TCP

	• Puerta de enlace equipos en Red 2: 21, 22, 23,53,80,2000 y 8291
Análisis de puertos físicos activos	• Los puertos físicos están deshabilitados de forma correcta
Entrevista de personal técnico	• La transmisión de datos entre los equipos del CCV y los servicios en la nube se dice en los insumos que se lleva a cabo mediante un protocolo de reconocimiento. Al preguntar al personal sobre cuál es ese protocolo y en qué consiste su respuesta fue que utilizan un protocolo TCP y no facilitaron más información.

8.4.7.4 CATD Reynosa

Tabla 8.5 Resultado de pruebas en CATD Reynosa

Actividad	Resultados
Acceso a Internet	Acceso restringido en dispositivos móviles a través del S.O., sin embargo, el servicio de Internet contratado está accesible sin restricciones.
Identificación de segmentos de red	Los segmentos de red identificados fueron los siguientes: • Red: 192.168.1.0/24. • Puerta de enlace: 192.168.1.254 • Servicio DHCP habilitado • Red administrada por el módem del servicio contratado • Se detectó solo un equipo de cómputo móvil y cuatro equipos smartphone
Análisis de redes inalámbricas	• El SSID se encuentra visible, con el nombre y contraseña por default provista por el proveedor. • Acceso libre a internet • Las redes WIFI detectadas son vulnerables a un ataque de denegación de servicio (DoS).
Análisis de vulnerabilidades	• No se encontraron vulnerabilidades que se pudieran explotar en los equipos de captura

8.4.7.5 CATD Victoria

Tabla 8.6 Resultado de pruebas en CATD Victoria

Actividad	Resultados
Acceso a Internet	Acceso restringido en dispositivos móviles a través del S.O., sin embargo, el servicio de Internet contratado está accesible sin restricciones.
Identificación de segmentos de red	Los segmentos de red identificados fueron los siguientes: • Red: 192.168.1.0/24. • Puerta de enlace: 192.168.1.254 • Servicio DHCP habilitado • Red administrada por el módem del servicio contratado • Se detectó solo un equipo de cómputo móvil y cinco equipos smartphone • Se detectaron los puertos 80 y 443 abiertos en el módem de servicio • Se detectó abierto el puerto 7070 en laptop asignada al CATD
Análisis de redes inalámbricas	• El SSID se encuentra visible, con el nombre y contraseña por default provista por el proveedor. • Acceso libre a internet • Las redes WIFI detectadas son vulnerables a un ataque de denegación de servicio (DoS).
Análisis de vulnerabilidades	• No se encontraron vulnerabilidades que se pudieran explotar en los equipos de captura

8.4.7.6 CATD Madero

Tabla 8.7 Resultado de pruebas en CATD Madero

Actividad	Resultados
Acceso a Internet	Acceso restringido en dispositivos móviles a través del S.O., sin embargo, el servicio de Internet contratado está accesible sin restricciones.
Identificación de segmentos de red	Los segmentos de red identificados fueron los siguientes: • Red: 192.168.1.0/24. • Puerta de enlace: 192.168.1.254 • Servicio DHCP habilitado • Red administrada por el módem del servicio contratado • Se detectaron 16 equipos de cómputo de los cuales algunos no forman parte del PREP y cuatro equipos smartphone
Análisis de redes inalámbricas	• El SSID se encuentra visible, con el nombre y contraseña por default provista por el proveedor. • - 119 -Acceso libre a internet • Las redes WIFI detectadas son vulnerables a un ataque de

	denegación de servicio (DoS).
Análisis de vulnerabilidades	No se encontraron vulnerabilidades que se pudieran explotar en los equipos de captura, sin embargo se detectaron abiertos en el modem de servicio los siguientes servicios: • 22,53,80, 443 y 5001 TCP

8.4.7.7 Infraestructura en la nube

Tabla 8.8 Resultado de pruebas en infraestructura en la nube

Actividad	Resultados
Acceso desde Internet	Acceso restringido. No fue posible ingresar a los servicios desde algún equipo no identificado por el firewall de aplicación de la plataforma en la nube (WAF).
Identificación de segmentos de red	Acceso restringido. No fue posible ingresar a los servicios desde algún equipo no identificado por el firewall de aplicación de la plataforma en la nube (WAF).
Análisis de vulnerabilidades	Acceso restringido. No fue posible ingresar a los servicios desde algún equipo no identificado por el firewall de aplicación de la plataforma en la nube (WAF).

8.4.7.8 Sitio web de publicación

Tabla 8.9 Resultado de pruebas en sitio web de publicación

Actividad	Resultados
Acceso desde Internet	**Prueba1:** Acceso al sitio estuvo activo por HTTP y no por HTTPS. **Simulacro1:** Acceso al sitio por HTTPS redireccionando automáticamente las peticiones por HTTP. Se detectó una caída del servicio alrededor de las 10:00 hrs., durante la ejecución del simulacro.
Identificación de segmentos de red	**Prueba1:** Site: http://prueba.prep2021tamps.mx Netblock Owner: Amazon Technologies Inc. Hosting company: Amazon - US East (Northern Virginia) datacenter Hosting country: us IPv4 address: 54.161.238.254 IPv4 autonomous systems: AS14618 IPv6 address: Not Present IPv6 autonomous systems: Not Present Reverse DNS: ec2-54-161-238-254.compute-1.amazonaws.com Domain: prep2021tamps.mx Nameserver: ns1.akkyservicios.mx

	Nameserver organization: whois.mx DNS admin: hostmaster@akkyservicios.mx.prep2021tamps.mx Top Level Domain: Mexico (.mx) DNS Security Extensions: Enabled **Simulacro1:** Site: https://simulacro1.prep2021tamps.mx Netblock Owner: Amazon Technologies Inc. Hosting company: Amazon - US East (Northern Virginia) datacenter Hosting country: us IPv4 autonomous systems: AS16509 IPv6 address: Not Present IPv6 autonomous systems: Not Present Reverse DNS: ec2-54-161-238-254.compute-1.amazonaws.com Domain: prep2021tamps.mx Nameserver: ns1.akkyservicios.mx Nameserver organization: whois.mx DNS admin: hostmaster@akkyservicios.mx.prep2021tamps.mx Top Level Domain: Mexico (.mx) DNS Security Extensions: Enabled • Address 1: 13.249.64.41 server-13-249-64-41.dfw53.r.cloudfront.net • Address 2: 13.249.64.106 server-13-249-64-106.dfw53.r.cloudfront.net • Address 3: 13.249.64.82 server-13-249-64-82.dfw53.r.cloudfront.net • Address 4: 13.249.64.30 server-13-249-64-30.dfw53.r.cloudfront.net
Análisis de vulnerabilidades	**Prueba 1:** • Se detecta que el sitio ES VULNERABLE a un ataque del tipo Slowloris (CVE-2007-6750), aunque esto será validado con precisión durante las pruebas de penetración subsecuentes. • Se detecta que el sitio NO tiene vulnerabilidades del tipo CSRF. • Se detecta que el sitio NO tiene vulnerabilidades del tipo DOM XSS. • Se detecta que el sitio NO tiene vulnerabilidades del tipo stored XSS. • Se detecta que el sitio esta desplegado en tecnología Amazon Web Services - EC2 • Se detecta que el sitio esta desarrollado con tecnología Javascript

	Simulacro 1: • A partir de la revisión de las versiones utilizadas de Bootstrap y JQuery, se detectó que pueden ser vulnerables a las siguientes amenazas de riesgo medio: o CVE-2016-10735 Bootstrap - Cross Site Scripting (XSS) o CVE-2018-14041 Bootstrap - Cross Site Scripting (XSS) o CVE-2018-14040 Bootstrap - Cross Site Scripting (XSS) o CVE-2019-11358 JQuery - Cross Site Scripting (XSS) Es importante mencionar que estás amenazas no son de gran impacto y pueden ser mitigadas con solamente utilizar versiones más recientes. • A partir de la revisión del sitio de publicación a través de un equipo proxy, se detectaron las siguientes alertas de impacto medio- bajo o Encabezado X-Frame-Options no incluido en las respuestas de HTTP el cual brinda protección ante ataques del tipo ClickJacking. *Riesgo medio*. o Encabezado Cache-Control no incluido o no configurado propiamente, lo cual permite que el navegador o proxies almacenen contenido en caché . *Riesgo bajo.* o El encabezado Anti-MIME-Sniffing X-Content-Type-Options no está configurado como “nosniff”, esto permite que versiones anteriores de Internet Explorer y Chrome realicen MIME-sniffing. *Riesgo bajo.* o Information Disclosure.- A través de los encabezados es posible saber la versión de sistema operativo y servidor web utilizados. *Riesgo bajo.* Es importante mencionar que estás amenazas no son de gran impacto y pueden ser mitigadas utilizando headers seguros.
Certificados SSL	**Simulacro1:** Scan report for simulacro1.prep2021tamps.mx (13.226.201.102) Host is up (0.00052s latency). Other addresses for simulacro1.prep2021tamps.mx (not scanned): 13.226.201.20 13.226.201.54 13.226.201.95 rDNS record for 13.226.201.102: server-13-226-201-102.dfw55.r.cloudfront.net PORT STATE SERVICE 443/tcp open https | ssl-cert: Subject: commonName=*.prep2021tamps.mx

	| Subject Alternative Name: DNS:*.prep2021tamps.mx | Issuer: commonName=Amazon/organizationName=Amazon/countryName=US | Public Key type: rsa | Public Key bits: 2048 | Signature Algorithm: sha256WithRSAEncryption | Not valid before: 2021-04-30T00:00:00 | Not valid after: 2022-05-29T23:59:59 | MD5: f742 d4c6 8b73 3450 f8b6 06da 30c5 7230 |_SHA-1: 7356 6354 4201 d6b2 3d5f 5593 0a26 7501 16cb 4d85 | ssl-enum-ciphers: | TLSv1.2: | ciphers: | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (ecdh_x25519) - A | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A | compressors: | NULL | cipher preference: server |_ least strength: A

8.4.7.9 Sitio web del OPL

Tabla 8.10 Resultado de pruebas en sitio web del OPL

Actividad	Resultados
Acceso desde Internet	Acceso al sitio por HTTPS redireccionando automáticamente las peticiones por HTTP.
Identificación de segmentos de red	Name: www.ietam.org.mx Address 1: 104.209.178.154 Site: http://www.ietam.org.mx Netblock Owner: Microsoft Corporation Hosting company: Microsoft - US East 2 (Virginia) datacenter Hosting country: us IPv4 address: 104.209.178.154 IPv4 autonomous systems: AS8075 IPv6 address: Not Present IPv6 autonomous systems: Not Present Reverse DNS: unknown Domain: ietam.org.mx Nameserver: ns1.akkyservicios.mx Domain register: whois.mx

	Nameserver organization: whois.mx Organisation: Ciudad Victoria, Mexico DNS admin: hostmaster@akkyservicios.mx.ietam.org.mx Top Level Domain: Mexico (.org.mx) DNS Security Extensions: Enabled
Análisis de vulnerabilidades	• Se detecta que el sitio ES VULNERABLE a un ataque del tipo Slowloris (CVE-2007-6750), aunque esto será validado con precisión durante las pruebas de penetración subsecuentes. • Se detecta que el sitio ES VULNERABLE a un ataque de Man in the middle mediante SSL POODLE CVE:CVE-2014-3566 • Se detecta que el sitio NO tiene vulnerabilidades del tipo CSRF. • Se detecta que el sitio NO tiene vulnerabilidades del tipo DOM XSS. • Se detecta que el sitio NO tiene vulnerabilidades del tipo stored XSS. • Se detecta que el sitio esta desplegado en un servidor con Microsoft Windows Server 2016 • Se detecta que el sitio utiliza Microsoft-IIS/10.0 • Se detecta que el sitio utiliza Microsoft SQL Server 2008 R2 10.50.1600; RTM como manejador de base de datos • Se detecta que el sitio tiene abierto el protocolo FTP (21) • Se detecta que el sitio tiene abierto el protocolo para escritorio remoto (3389)
Certificados SSL	PORT STATE SERVICE 443/tcp open https | ssl-cert: Subject: commonName=www.ietam.org.mx/organizationName=INSTITUTO ELECTORAL DE TAMAULIPAS/stateOrProvinceName=Tamaulipas/countryName=MX | Subject Alternative Name: DNS:www.ietam.org.mx, DNS:ietam.org.mx | Issuer: commonName=DigiCert TLS RSA SHA256 2020 CA1/organizationName=DigiCert Inc/countryName=US | Public Key type: rsa | Public Key bits: 2048 | Signature Algorithm: sha256WithRSAEncryption | Not valid before: 2021-01-27T00:00:00 | Not valid after: 2022-01-31T23:59:59 | MD5: a117 1a09 5bdd 806c 5a1f fc2a 80e3 3608 |_SHA-1: 4574 fc1b e74e 57cb 0c20 d6af 7d8d 1911 567c 710d | ssl-enum-ciphers: | TLSv1.2: | ciphers: | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A

	| TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (ecdh_x25519) - A | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A | TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A | TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A | TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A | TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A | TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A | TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A | TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A | TLS_RSA_WITH_AES_128_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 |_ least strength: C

9. Pruebas de denegación de servicio a sitios del PREP y al principal del OPL

9.1 Objetivo

Realizar pruebas de ataques de denegación de servicio para identificar, evaluar y aplicar las medidas necesarias para asegurar la correcta y continua disponibilidad del servicio Web de los sitios de publicación de resultados del PREP y del sitio principal del IETAM, durante el periodo de operación del PREP. Documentar los hallazgos detectados durante la realización de las pruebas.

9.2 Alcance

Generar tráfico de red desde la infraestructura del ente auditor hacia los servicios web que se publican dentro del dominio del IETAM.

Las pruebas de negación de servicio consideraron los siguientes tipos:

- Tráfico no malintencionado que consiste en transacciones sintéticas que simulen el tráfico legítimo que se espera el día de la jornada.
- Tráfico de red malintencionado, consistente en paquetes de red malformados.

Los ataques de negación de servicio contemplaron tráfico de red malintencionado con las siguientes características:

- Ataques volumétricos por protocolo TCP
  - SYN FLOOD
- Ataques volumétricos por protocolo UDP
  - DNS AMPLIFICATION
- Ataques volumétricos por protocolo ICMP
  - ICMP FLOOD
- Ataques en la capa de aplicación (HTTP)
  - SLOWRIS ATACK

Las pruebas mencionadas anteriormente generaron tráfico malintencionado (SYN FLOOD, ICMP FLOOD, SLOWRIS ATACK) en un volumen que representa las condiciones de un ataque.

Durante las pruebas, cada simulación de ataque se apegó a las condiciones de un ataque para hacer que el sitio web que se esté probando quedara no disponible (si fuera el caso) por al menos 2 minutos.

A continuación, se describe el procedimiento para realizar las pruebas de denegación de servicios y los resultados que se obtuvieron. Los resultados se presentan por ataque realizado, tal como lo indican los requerimientos del INE, a los sitios de publicación del proveedor y al sitio principal del IETAM. Se describen primero los términos generales de los ataques contemplados. Posteriormente, se describe con mayor detalle cada uno de los ataques realizados y los resultados obtenidos. Finalmente, se presenta un resumen de los hallazgos encontrados como resultado de la ejecución de las pruebas.

9.3 Descripción general de la metodología

Los ataques que se consideraron se describen en la Tabla 9.1.

Tabla 9.1. Ataques recomendados por el INE y realizados a los sitios de publicación de resultados del PREP y sitio principal del IETAM.

Ataque	Descripción
Volumétricos	
TCP SYN Flood	El atacante envía repetidamente paquetes SYN (sincronización) a cada puerto en el servidor víctima, usando direcciones IP falsas. En una comunicación de tres vías, el cliente respondería con un ACK para notificar al servidor la recepción del mensaje SYN. Sin embargo, este mensaje nunca es devuelto, dejando la conexión en pausa y abierta.
ICMP Flood	El atacante envía de forma continua un número elevado de paquetes ICMP Echo request (ping) de tamaño considerable a la víctima, de tal forma que la respuesta con paquetes ICMP Echo reply (ping) produce una sobrecarga tanto en la red como en el sistema de la víctima. Dependiendo de la relación entre capacidad de procesamiento de la víctima y el atacante, el grado de sobrecarga varía, es decir, si un atacante tiene una capacidad mucho mayor, la víctima no puede manejar el tráfico generado.
DNS Amplification	El atacante usa la capacidad de cómputo y ancho de banda de servidores DNS para que sean éstos los que manden tráfico excesivo a la víctima.
En capa de aplicación	
Slowloris	A diferencia de los ataques por saturación, éste es un ataque que no inunda las redes. Todos los servicios de la víctima permanecen intactos pero el servidor web por sí mismo es inaccesible completamente. La idea principal es manejar tantas conexiones abiertas como sea posible enviando únicamente peticiones HTTP parciales.
HTTPS-GET	Mediante este tipo de ataque se envía una gran cantidad de solicitudes GET a un servicio HTTPS hasta colapsar la infraestructura donde esta desplegado el servicio dejando este inhabilitado.

Para la realización de los ataques se uso la infraestructura descrita en las siguientes tablas.

Tabla 9.2 Infraestructura utilizada para ataques TCP Syn Flood, ICMP Flood, Slowloris y HTTPS GET

Plataforma	Loddos
Empresa	Barikat GTH
Bots utilizados	50
Operador de los ataques	Barikat GTH / CINVESTAV Unidad Tamaulipas
Ancho de banda contratado	3000 Mbps
Total de ataques realizados	8

Tabla 9.3 Infraestructura utilizada para ataque DNS Amplification

Plataforma	Infraestructura del ente auditor
Institución	CINVESTAV Unidad Tamaulipas
Bots utilizados	30
Servidores utilizados	11
Operador de los ataques	CINVESTAV Unidad Tamaulipas
Ancho de banda contratado	500 Mbps
Total de ataques realizados	2

Tabla 9.4 Calendarización de ataques a los sitios de publicación de resultados del PREP y sitio principal del IETAM.

Sitio	Puerto	Ataque	25-may	26-may
simulacro2.prep2021tamps.mx	443	DNS Amplification	✓	
		TCP SYN Flood		✓
		ICMP Flood		✓
		HTTPS GET		✓
		Slowloris		✓
www.ietam.org.mx	443	DNS Amplification	✓	
		TCP SYN Flood		✓
		ICMP Flood		✓
		HTTPS GET		✓
		Slowloris		✓

9.4 Resumen de resultados y hallazgos

En la Tabla 9.5 se resumen los hallazgos realizados en la ejecución de las pruebas de negación de servicios realizadas como parte de los requerimientos del IETAM.

Tabla 9.5. Resumen de los hallazgos de la pruebas de negación de servicios.

Sitio	TCP SYN Flood	ICMP Flood	Slowloris	HTTPS GET	DNS Amplification
simulacro2.prep2021tamps.mx					
www.ietam.org.mx					

	No vulnerable y/o protegido
	Vulnerable por segundos
	No revisado
	Vulnerable

9.5 Conclusiones sobre ataques

1. Para el sitio de publicación no se tienen recomendaciones ya que durante la ejecución de las pruebas de denegación de servicio se pudo validar que esta protegido y bien dimensionado para soportar carga y/o ataques hasta por un ancho de banda de 3000 Mbps.
2. Al respecto de las vulnerabilidades detectadas en el sitio del OPL (www.ietam.org.mx) se recomienda que al menos durante el desarrollo de la jornada electoral este sitio sea protegido y/o desplegado con la misma infraestructura y servicios utilizados para el sitio de publicación con la finalidad de que las vulnerabilidades detectadas puedan ser mitigadas. Otra alternativa para este sitio dado que las vulnerabilidades detectadas están relacionadas con la carga de usuarios que puede soportar sería escalar el servicio a través de más instancias de este e integrando y un proxy o balanceador de carga o alguna solución equivalente.

10. Pruebas de Usabilidad y Experiencia de Usuario

10.1 Introducción

Las pruebas usabilidad y experiencia de usuario definidas en este documento, están enfocadas a evaluar la interacción del usuario y su percepción en la ejecución de las funcionalidades del sistema PREP. Estas pruebas fueron aplicadas a cada uno de los módulos del sistema los cuales se definen en la sección de metodología. Además de los módulos a ser evaluados, se definió un **grupo de participantes** o involucrados en la ejecución de las pruebas los casos de prueba que van a ser aplicados. Para la ejecución de las pruebas se han elaborado un conjunto de instrumentos (checklist y cuestionarios) que permitirán recabar las opiniones de los participantes y los resultados de la interacción con el sistema. Finalmente, se incluyen las observaciones y resultados obtenidos.

10.2 Metodología

En esta sección se presenta la metodología usada para la ejecución del plan. Dicha metodología está conformada por una serie de etapas las cuales se ilustran en la Figura 10.1 y se describen en las secciones subsiguientes.

Figura 10.1. Etapas de la metodología para las pruebas de usabilidad y experiencia

10.2.1 Determinación de los módulos del sistema a ser evaluados

De acuerdo con el análisis de información presentado por el IETAM, el sistema PREP 2021 está conformado por un conjunto de elementos funcionales o módulos, los cuales se presentan a continuación. Adicionalmente se especifican las tareas o propósito principal de cada uno de éstos desde la perspectiva del usuario.

Aplicación PREP Casilla

- Obtención de la imagen digital del acta desde la casilla.
- Transmisión de los datos al CCV

Aplicación PREP CATD

- Obtención de la imagen digital del acta PREP en el Centro de Acopio y Transmisión de Datos.
- Captura en su caso de la información contenida en las Actas PREP.
- Validación de la información capturada.
- Transmisión de los datos al CCV.

Módulo de CCV

- Captura de la información contenida en las imágenes de las Actas PREP
- Verificación de los datos capturados.
- 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.

Módulo de Resultados Preliminares

- Publicación y seguimiento de resultados

10.2.2. Definición de roles y participantes

De acuerdo con la especificación funcional del sistema (ver ANEXO 3), existen diferentes roles que son asignados a diferentes usuarios. Para efectos de este documento es necesaria la participación de por lo menos tres usuarios por cada uno de los siguientes roles:

- **Usuario de Resultados Preliminares.** Observar e interactuar con el sitio que muestra el conteo de las votaciones en tiempo real.
- **Usuario del PREP Casilla.** Interactuar con la aplicación móvil PREP Casilla con el objetivo de transmitir las actas capturadas desde la misma.
- **Usuario del PREP CATD.** Interactuar con el módulo de CATD del sistema con el objetivo de capturar y transmitir las actas recibidas.
- **Usuario del PREP CCV.** Interactuar con el módulo de CCV del sistema con el objetivo de capturar y verificar los resultados de las actas recibidas.

10.2.3. Perfiles de Evaluación

Para cada uno de los módulos indicados en la sección 3.1, se evaluarán diferentes aspectos que han sido agrupados en lo que en adelante se denominará *Perfiles de Evaluación*.

1. **Interfaz principal.** Perfil que evalúa los aspectos principales que debe tener una interfaz inicial en cualquier sistema o aplicación (existencia de ciertos elementos, legibilidad, comprensión de los módulos que muestra, entre otros).
2. **Diseño.** Perfil que evalúa la apariencia y consistencia general de la aplicación o sistema.

3. **Accesibilidad.** Perfil que evalúa el acceso general a todos los módulos que comprende la aplicación o sistema, así como también la experiencia de uso del usuario.
4. **Navegación.** Perfil que evalúa el flujo de las acciones y/o actividades que se llevan a cabo dentro de la aplicación o sistema.
5. **Enlaces.** Perfil que evalúa el acceso y presencia explícita a todos los enlaces y/o botones que contiene la aplicación o sistema.
6. **Formularios.** Perfil que evalúa la estructura de los formularios dentro de la aplicación o sistema.
7. **Contenido.** Perfil que evalúa la calidad en texto, color y posicionamiento de elementos dentro de la aplicación o sistema.

10.2.4. Instrumentos y materiales

1. Checklist
2. Cuestionario web para la evaluación del perfil de Interfaz Principal
3. Cuestionario web para la evaluación del perfil de Diseño
4. Cuestionario web para la evaluación del perfil de Accesibilidad
5. Cuestionario web para la evaluación del perfil de Navegación
6. Cuestionario web para la evaluación del perfil de Enlaces
7. Cuestionario web para la evaluación del perfil de Formularios
8. Cuestionario web para la evaluación del perfil de Formularios
9. Cuestionario web para la evaluación del perfil de Contenido

10.2.5. Configuración del entorno

La configuración del entorno de pruebas deberá contemplar los siguientes elementos:

1. Despliegue y configuración de componentes de software en los dispositivos móviles y TCAs.
2. Creación de **usuarios de aplicación** para la ejecución de los diferentes componentes del sistema con fines de auditoría. Estos deberán estar asociados a los roles definidos en la matriz de roles y funcionalidades.
3. Las TCAs y los dispositivos móviles deberán tener un usuario de acceso a los mismos (preferiblemente no administrador) con las credenciales adecuadas para el ingreso a la aplicación.
4. Para los componentes de backend es necesario desplegarlos en una instancia del servidor creada y configurada específicamente para pruebas y auditoría.
5. De igual forma es necesario que el sistema de base de datos se ejecute en dicha instancia o en una instancia específicamente creada para propósitos de prueba auditoría.

10.2.6. Casos de prueba

Los casos de prueba están definidos en función del número de módulos del sistema que serán objeto de la prueba y los diferentes perfiles de evaluación mencionados con anterioridad.

10.3 Criterios usados para la auditoría

En esta sección se presenta la metodología usada para la ejecución del plan. Dicha metodología está conformada por una serie de etapas las cuales se ilustran en la Figura 10.1 y se describen en las secciones subsiguientes.

10.3.1 Selección de usuarios participantes

Los usuarios participantes en las pruebas fueron seleccionados por el IETAM a petición del ente auditor. Específicamente se solicitó el correo electrónico de los usuarios con la única condición de que estos deben desempeñar los diferentes roles definidos en la aplicación (Capturista, Validador, PREP Casilla). Dichos usuarios recibieron a través de correo un enlace de un cuestionario cuyo propósito fue evaluar la percepción del usuario relativa a la usabilidad y experiencia de interacción con el sistema.

10.3.2. Instrumento de percepción del usuario

Se elaboró un cuestionario que evalúa características de usabilidad e interacción desde la perspectiva de los usuarios del sistema. Dichas características fueron agrupadas en los siguientes aspectos:

- **Interfaz principal.** En este aspecto se evalúan diferentes características básicas que debiera tener la pantalla principal de la aplicación para que el usuario se sienta en control de lo que sucede al ver dicha pantalla. El objetivo principal es detectar si el usuario comprende la razón de ser de la aplicación en cuestión y no tiene problema en empezar a moverse dentro de ella a partir de lo que observa en la pantalla inicial. (6 preguntas)

- **Diseño.** En este aspecto se evalúa si existe una percepción positiva del usuario hacia el diseño gráfico de la aplicación y los elementos dinámicos que esta contiene. Su principal objetivo es detectar la simpleza, organización e intuitividad de la aplicación a través del criterio personal de quien lo usa. (11 preguntas)

- **Accesibilidad.** En este aspecto se evalúa la comodidad del usuario con respecto a la facilidad con la que se puede mover dentro de la aplicación, El objetivo principal es detectar si existe cierto descontento en general por parte del usuario al desempeñar la funcionalidad de la aplicación. (4 preguntas)

- **Navegación.** En este aspecto se evalúa la facilidad con la que el usuario avanza en sus actividades dentro del sistema y cómo los elementos que lo incluyen lo ayudan a cumplir con dichas actividades. El principal objetivo es detectar si el usuario puede llegar a confundirse al navegar en la aplicación y no llegar al último estado de funcionalidad de la aplicación. (6 preguntas)

- **Enlaces.** En este aspecto se evalúa que el usuario no tenga ningún problema de direccionamiento en enlaces que puedan existir dentro del sistema y/o aplicación. (3 preguntas)

- **Formularios.** Este aspecto evalúa la percepción del usuario respecto al ingreso de información a través de formularios y componentes de entrada como cajas de texto, combos de selección, etc. El

objetivo principal es conocer si el usuario se siente cómodo respondiendo dichos formularios en función de el contenido que se le solicita en ellos y la apariencia en general. (8 preguntas)

- **Contenido.** En este aspecto se evalúa que todo el contenido dentro del sistema y/o aplicación sea necesario y suficiente para que el usuario complete sus actividades dentro del mismo y que no existan elementos que obstruyan la legibilidad de dicho contenido. (3 preguntas).

10.3.3. Niveles de Satisfacción

Las preguntas que se han integrado en el cuestionario tienen 5 posibles respuestas con una escala del 1 al 5, en donde 1 es la puntuación más baja y 5 la más alta. Y se clasifican de la siguiente manera:

- Muy bajo
- Bajo
- Medio
- Alto
- Muy alto

10.3.4. Mecanismo de ponderación

Como se mencionó cada pregunta tiene una valoración cualitativa de Muy Bajo (MB), Bajo (B), Medio (M), Alto (A), Muy alto (MA). Para dar una valoración cuantitativa a las respuestas dadas por los usuarios se procedió a realizar un resumen por cada pregunta como el que se muestra en la siguiente tabla (con datos de ejemplo para fines ilustrativos).

Tabla 10.1. Valoración cuantitativa de las respuestas de los usuarios

Niveles de Respuesta	Valores	Usuarios	Proporción de usuarios	Impacto de la respuesta
Muy Alto (MA)	5.00	1.00	0.10	0.50
Alto (A)	4.00	0.00	0.00	0.00
Medio (M)	3.00	9.00	0.90	2.70
Bajo (B)	2.00	0.00	0.00	0.00
Muy Bajo (MB)	1.00	0.00	0.00	0.00
	Total Usuarios	10	Impacto Final	3.2

El impacto general o valoración final de las respuestas de los usuarios a una pregunta, es calculado como la suma de los productos de la valoración i-ésima de la pregunta por la proporción de usuarios que respondieron con dicha valoración. Esto se expresa matemáticamente como:

$$\text{Impacto} = \sum_{i=1}^{5} \text{Valoracion}_i \text{Proporcion}_i$$

Ecuación 1

Para el ejemplo de la Tabla X, el impacto expresado en la Ecuación 1 es 3.2. Definido el impacto o valoración final de las respuestas para cada pregunta del cuestionario, es posible valorar numéricamente cada uno de los siete aspectos evaluados (interfaz, contenido, etc.). Dicha valoración esta definida como el promedio del impacto de cada una de las preguntas que pertenecen a un determinado aspecto. Por lo tanto, dado un *aspecto* $_i$ su valoración numérica se expresa matemáticamente como:

$$aspecto_j = \frac{1}{K}\sum_{i=1}^{K} impacto_i$$

Ecuación 2

Donde *K* es el número de preguntas que pertenecen al aspecto evaluado.

Lo anterior es aplicado después de recopilar todas las respuestas obtenidas de los usuarios selección para obtener los que se denomina el perfil de usabilidad.

10.4 Perfil de Usabilidad

Aplicando el mecanismo de ponderación se determinó el impacto de las respuestas de los usuarios a cada pregunta y se determinó una valoración numérica de los aspectos del sistema evaluados, la cual se presenta en la siguiente gráfica.

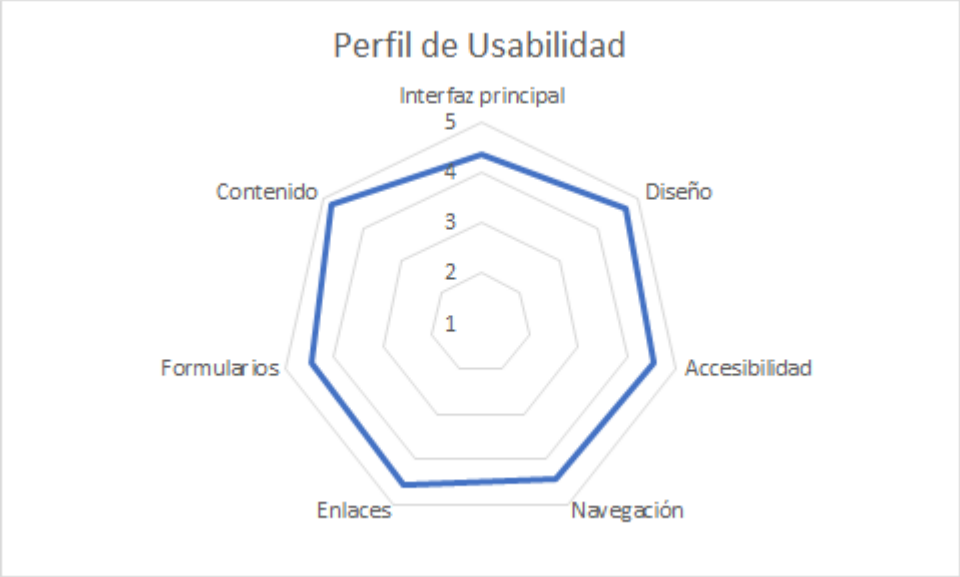


Figura 10.2 Perfil de usabilidad del sistema PREP

NOTA: los resultados presentados fueron obtenidos al finalizar la ejecución del tercer simulacro.

10.5 Conclusiones

Del perfil de usabilidad obtenido, se puede observar que en términos generales el sistema PREP tiene una valoración positiva por parte de los usuarios, sin embargo, existen áreas de oportunidad para mejorar dicha valoración en lo relacionado con la interfaz y la navegación. No obstante, puede decirse que el sistema es lo suficientemente intuitivo y presenta buena usabilidad, además de que los simulacros han sido útiles para que los usuarios se familiaricen con el sistema y sus interfaces de forma que en el siguiente evento no se espera que ocurran inconvenientes causados por la aplicación o por confusión en los usuarios debido a la interfaz.

Parte IV

11. Simulacros

Se realizaron 3 simulacros los días 16, 23 y 30 de mayo de 2021. El Ente Auditor tuvo presencia durante los tres simulacros. A continuación, se presentan las observaciones realizadas por el Ente Auditor a la operación del PREP durante los tres simulacros.

11.1 Comentarios y observaciones resultantes de Simulacro 1

11.1.1 Módulo de publicación de resultados

CAPA DE DATOS

- Se detectó una inconsistencia en el archivo nombrado como “Sistema_Archivos” el cual corresponde a una carpeta con los catálogos utilizados por el sitio de publicación. La inconsistencia se presentó durante la toma de huellas intermedias por lo que el origen del cambio en las huellas puede deberse a una estampa de tiempo interna dentro de los catálogos.
- El porcentaje de efectividad del PREP es del 89.09% para diputaciones y un 94% para ayuntamientos. Es necesario mantener una consistencia en el formato de nombres utilizado para las actas. Por ejemplo, el formato de nombres proporcionado por el IETAM fue el siguiente: Origen_Tipo_Eleccion_Casilla.jpg (e.g. 2_H_D_0783 Básica.jpg.), no obstante, durante el simulacro se pudieron detectar imágenes con un agregado (e.g. 2_A_A_1223 Básica_V536.jpg). Este formato no fue proporcionado al ente auditor por lo cual no fue posible descargar estas actas.
- EL sistema PREP reportó, en el ultimo corte de información realizado a las 18:31H, el 98% de las actas registradas en la base de datos. Al no realizar un corte adicional no se pudieron descargar el 2% restante. Por lado, e observó que el cirterio de asignación de nombres de las actas cambia durante el simulacro, lo cual no es recomendable si se desea tener un proceso de manejo de datos uniforme
- No es aceptable que el sistema no permita descargar Actas procesadas. Se deberían eliminar estos eventos o documentar la razón por la cual dichos eventos suceden en el software del PREP. Se recomienda revisar el formato de asignación de nombres de las actas para que este sea homogéneo y de esta forma el sistema permita ser monitorizado por procesos de seguimiento en tiempo real.
- No es aceptable que el sistema no permita descargar actas procesadas. Se deberían eliminar estos eventos o documentar la razón por la cual dichos eventos suceden en el software del PREP
- La bitácora del sistema debería ser proporcionado para su consumo en tiempo real y de esta forma poder dar seguimiento a las acciones realizadas por los componentes del sistema PREP. La sobreescritura de los registros de esta bitácora no permite que se realice un siguiente en tiempo real.
- Se recomienda que se repita esta buena práctica para el siguiente simulacro.
- Se recomienda proporcionar acceso a la bitácora durante el siguiente simulacro. Se solicita que la bitácora sea adecuada para ser consumida por sistemas informáticos de auditoría

CAPA DE APLICACIONES

- En la actualización periódica de resultados, podría ser útil la notificación automática al usuario que le informe que una nueva actualización está disponible.
- Algunos usuarios reportaron que las actualizaciones de resultados no se realizaron dentro del intervalo definido para tal fin (15 minutos)
- Ausencia de geolocalización de casillas dentro del mapa interactivo en el sitio de publicación de resultados, dicha característica podría mostrar un proceso más detallado dentro de la jornada. Según el testimonio de algunos usuarios esta funcionalidad la ofrecía el proveedor anterior, sin embargo, el IETAM asegura que dicha funcionalidad no hace parte de los requerimientos funcionales determinados por el INE.

CAPA DE PLATAFORMA TECNOLÓGICA

- De 10:00 a 10:30 hrs. el sitio de publicación de resultados estuvo inaccesible (https://simulacro1.prep2021tamps.mx), el acceso a este fue probado desde la red institucional del ente auditor y desde un servicio público del proveedor Totalplay.
- Al analizar los encabezados del sitio se pudo obtener que el sitio está desplegado utilizando las siguientes tecnologías:

o Amazon Web Services
o Amazon Cloudfront
o Amazon S3
o Bootstrap
o JQuery
o 5 IPS en 2 países y a través de 5 dominios con 14 transacciones HTTP

- A partir de la revisión de las versiones utilizadas de Bootstrap y JQuery, se detectó que pueden ser vulnerables a las siguientes amenazas de riesgo medio:

o CVE-2016-10735 Bootstrap - Cross Site Scripting (XSS)
o CVE-2018-14041 Bootstrap - Cross Site Scripting (XSS)
o CVE-2018-14040 Bootstrap - Cross Site Scripting (XSS)
o CVE-2019-11358 JQuery - Cross Site Scripting (XSS)

Es importante mencionar que estás amenazas no son de gran impacto y pueden ser mitigadas con solamente utilizar versiones más recientes.

- A partir de la revisión del sitio de publicación a través de un equipo proxy, se detectaron las siguientes alertas de impacto medio- bajo

o Encabezado X-Frame-Options no incluido en las respuestas de HTTP el cual brinda protección ante ataques del tipo ClickJacking. Riesgo medio.
o Encabezado Cache-Control no incluido o no configurado propiamente, lo cual permite que el navegador o proxies almacenen contenido en caché . Riesgo bajo.
o El encabezado Anti-MIME-Sniffing X-Content-Type-Options no está configurado como “nosniff”, esto permite que versiones anteriores de Internet Explorer y Chrome realicen MIME-sniffing. Riesgo bajo.
o Information Disclosure.- A través de los encabezados es posible saber la versión de sistema operativo y servidor web utilizados. Riesgo bajo.

- Es importante mencionar que estás amenazas no son de gran impacto y pueden ser mitigadas utilizando headers seguros.
- Es importante mencionar que estás amenazas no son de gran impacto y pueden ser mitigadas con solamente utilizar versiones más recientes.

11.1.2 CCV Principal

CAPA DE APLICACIONES

- El sistema valida adecuadamente el doble inicio de sesión del mismo usuario.
- Las credenciales de acceso son proporcionadas a los usuarios en papel, lo cual podría representar un riesgo de seguridad.
- El sistema implementa mecanismos que permiten la recuperación del último estado válido del acta.
- Se observó que el sistema es seguro ante un posible acuerdo entre un capturista y un verificador (con propósitos de fraude) ya que la asignación de actas a un verificador se realiza de manera aleatoria.

CAPA DE PLATAFORMA TECNOLÓGICA

- A las 9:30 de la mañana se realizó la simulación de una falla de equipo, dicho equipo fue seleccionado al azar de los equipos disponibles en las salas de captura. Durante este proceso personal de soporte realizó varias pruebas como: verificar conectividad y reinicio del equipo, posteriormente se reemplazó el CPU del equipo por otro. Sin embargo, el nuevo equipo presentó fallas de conectividad debido a que no se había registrado la dirección MAC para poder acceder a la red, el personal de soporte y el administrador de la red tardaron 45 minutos en darse cuenta de esto por lo cual el capturista pudo ingresar a la aplicación de captura a las 10:15 de la mañana. Una observación importante aquí es que el personal de soporte le solicitó al personal de captura su usuario y contraseña los cuales se los proporcionó mediante un papel. Se considera que es importante que los equipos de respaldo se encuentren debidamente probados y configurados para que puedan ser utilizados oportunamente en caso de la presencia de una falla.
- A las 10:30 de la mañana se simuló el corte de energía en las salas de captura bajando las pastillas en las tres salas las cuales funcionaron mediante los UPS durante 5 minutos sin ningún problema.
- A las 11:00 de la mañana se simuló el corte de energía en todo el edificio entrando en funcionamiento la planta de energía la cual funcionó sin ningún problema.

CAPA DE INFRAESTRUCTURA DE COMUNICACIONES

- Se verificó que el sitio web del PREP utiliza "https" y no "http".
- A las 11:15 de la mañana se realizó la prueba de desconexión del enlace (Failover). Para esto se desconectó la fibra óptica del proveedor Telmex de manera física, lo cual no afectó el proceso de captura ya que todos los equipos tenían de manera predeterminada como salida el enlace del proveedor Totalplay. Por lo cual solicitamos modificar esto y reiniciar la prueba; como resultado se observó que los equipos de captura vieron interrumpida su conexión con el servidor principal, es decir, no se redirigió el tráfico por el enlace redundante. Se recomienda configurar de forma

adecuada el equipo de seguridad perimetral de forma que al detectar que uno de los servicios de acceso a Internet contratados presente falla el servicio de respaldo de forma automatizada provea de continuidad a los equipos del CCV.

11.1.3 CCV Madero

CAPA DE APLICACIONES

- Existen ciertos errores desconocidos que se reflejaban en ocasiones al seleccionar la opción de "descargar acta", los cuáles son: error 07, error C14, error C26 y error C23.
- Las credenciales de acceso son proporcionadas a los usuarios en papel, lo cual podría representar un riesgo de seguridad.
- Se observó que en ciertas ocasiones para cambiar de rol (e ingresar nuevamente sus credenciales ya que es necesario cerrar sesión para ver los cambios de rol aplicados), se les ha permitido a los usuarios utilizar sus celulares personales para obtener la información de inicio de sesión.
- Se observó que el sistema es seguro ante un posible acuerdo entre un capturista y un verificador (para efectos de posible fraude) ya que la asignación de actas a un verificador se realiza de manera aleatoria.
- Los usuarios y contraseñas permanecen iguales durante los simulacros pero el día de la jornada se crean nuevos en caso de que haya personas que no asistan y cuenten con esa información.
- Se implementó un esquema de usuarios y roles que permite una mejor administración del acceso al sistema
- La primera vez que se captura un acta, el usuario tiene la opción de "rechazar" dicha acta por algún tipo de incidencia que encuentre. Para completar el proceso de rechazo es necesario que el supervisor autorice dicho rechazo a través de su contraseña.

11.1.4 CCV Reynosa

CAPA DE APLICACIONES

- Al inicio del simulacro el sistema expulsó a todos los usuarios impidiendoles iniciar sesión nuevamente mostrando el mensaje: "Hay una sesión iniciada con el mismo usuario".
- Los usuarios reiniciaron la aplicación para intentar iniciar sesión nuevamente y la aplicación se congeló mostrando el mensaje: "PREP2021_CCV.exe no responde)
- La aplicación de captura de actas se congela repentinamente en algunas máquinas.
- La aplicación de captura de actas presenta retardos significativos al recibir una nueva acta.
- La aplicación se congela por unos segundos al enviar un acta.
- A las 10 a.m. se detuvo la recepción de actas. Después empezaron a llegar actas de PREP CATD para las cuales los usuarios no tenían claro qué hora indicar para la captura de las actas. Se desconoce la razón por la cual los usuarios (capturistas) deben indicar manualmente la hora de captura pudiéndose realizar de forma automática.
- Al parecer las actas no se distribuyen equitativamente entre los capturistas del CCV. Se observaron tiempos muertos para algunos capturistas mientras otros tenían excesiva carga de trabajo.

11.1.5 CATD Victoria

CAPA APLICACIONES

- Se implementó un mecanismo eficiente para la recuperación del sistema ante eventos inesperados (cierres de sesión, terminación de aplicación). Si el acta queda en un estado inválido las actas se recuperan de forma automática.
- Al momento de guardar un acta, si ciertos campos no han sido llenados, el sistema no lo permite, pero el sistema no notifica cuales son los campos faltantes o con error.
- Las credenciales de acceso son proporcionadas a los usuarios en papel, lo cual podría representar un riesgo de seguridad.
- El sistema permite ingresar cualquier fecha en el sistema, así sea una fecha demasiado antigua o una fecha que aún no ha llegado.
- En esta versión del PREP, el sistema implementa mecanismos que permiten la recuperación del último estado válido del acta.
- Se observó que el sistema es seguro ante un posible acuerdo entre un capturista y un verificador (para efectos de posible fraude) ya que la asignación de actas a un verificador se realiza de manera aleatoria.

11.1.6 CATD Madero

CAPA APLICACIONES

- Al inicio del simulacro la aplicación PREP CATD no estaba enviando las actas lo que provocaba que todas estuvieran en un estado de “no enviado” por un largo tiempo. Se desconoce la razón.
- Para efectos de captura, la aplicación PREP CATD requiere que el dispositivo tenga una orientación horizontal. Sin embargo, cuando dicho dispositivo se usa para otras funcionalidades como la visualización del historial y estado de actas, la interfaz cambia a una orientación vertical alterando el despliegue de esta información.
- Se observó que el sistema es seguro ante un posible acuerdo entre un capturista y un verificador (para efectos de posible fraude) ya que la asignación de actas a un verificador se realiza de manera aleatoria

11.1.7 CATD Reynosa

CAPA APLICACIONES

- La caja de digitalización presenta fallos (las actas se deslizan, aparecen sombras en la fotografía).
- Los dispositivos móviles utilizados para la toma fotográfica, no cuentan con suministro continuo de corriente eléctrica.
- No se pudo comprobar si existen dispositivos móviles de reemplazo o emergencia.
- Las cajas de digitalización son manipuladas por los capturistas, algunas piezas de la caja fueron removidas por los usuarios.
- No se pudo comprobar si existe un mecanismo que informe al capturista el estado del acta que no se envió adecuadamente.
- La aplicación no detecta el doble inicio de sesión del mismo usuario.
- Las credenciales de acceso son proporcionadas a los usuarios en papel, lo cual podría representar un riesgo de seguridad.

11.1.8 Observaciones y Comentarios de la Capa Operativa en Simulacro 1

- No se pudo observar la fase de toma fotográfica debido a que no se realiza ni en el CATD ni en el CCV.
- El acopiador deberá de contar con un gafete de identificación. Si el acopiador tarda más de lo necesario en realizar alguna actividad de la fase, el coordinador le brindará apoyo. El acopiador es el encargado del flujo de actas en el CATD, teniendo una lista en la cual registra las actas ya capturadas y siguiendo un orden determinado a la hora de asignar las actas a cada digitalizador. Si llega a tener acceso al CATD una persona ajena al proceso, el acopiador pide apoyo al oficial encargado. El acopiador es el encargado de retirar los dispositivos ajenos al proceso. En el caso del CATD Reynosa no contaba con un acopiador, por lo que no se pudo observar esta fase. El medio de verificación (MV) de esta etapa son los formularios F5-A-2_1, F5-A-2_2.
- El digitalizador deberá de contar con un gafete de identificación. El digitalizador recibirá el Acta PREP de manera personal mediante el acopiador. En el caso del CATD Reynosa, los digitalizadores ya tenías todas la Actas PREP que les tocaban, debido a que no había acopiador. El digitalizador deberá de contar con las credenciales necesarias para el sistema, las cuales se le fueron otorgadas mediante un papel impreso. El digitalizador deberá de revisar el buen funcionamiento del equipo, y que el sistema este actualizado a su versión más reciente. En caso de detectar un error en el equipo o el sistema, deberá de comunicarlo con el coordinador. Si el digitalizador tiene alguna duda acerca del proceso a realizar, deberá de pedir ayuda a su coordinador, o revisar el manual de usuario que se le fue otorgado. El digitalizador obtuvo la capacitación necesaria para realizar el proceso. El medio de verificación (MV) de esta etapa son los formularios F5-A-3_1, F5-A-3_2.
- El capturista cuenta con un gafete de identificación. El capturista cuenta con las credenciales para ingresar al sistema, las cuales se le brindaron mediante un papel impreso. El capturista cuenta con un manual de usuario. El capturista obtuvo una capacitación antes de realizar el simulacro. Los capturistas también pueden ser verificadores. En el CATD Reynosa al inicio del simulacro hubo un

problema al tratar de iniciar sesión. El problema persistió por aproximadamente 20 minutos. Una vez resuelto el problema, los operadores pudieron trabajar con normalidad. En el simulacro ambas capturas solo se realizaron en el CCV. El medio de verificación (MV) de esta etapa son los formularios F5-A-4_1, F5-A-4_2, F5-A-5_1, F5-A-5_2.

- No se realiza ninguna captura en los CATD, solamente se realiza la fase de digitalización. Por lo que la captura de todas las actas se realiza en los CCV. El medio de verificación (MV) de esta etapa son los formularios F5-A-4_1, F5-A-4_2, F5-A-5_1, F5-A-5_2.
- El verificador deberá de contar con un gafete de identificación. El verificador cuenta con las credenciales para tener acceso al sistema, las cuales se le fueron otorgadas en un papel impreso. El verificador cuenta con un manual de usuario para el uso del sistema, pero los supervisores son los encargados de auxiliar en caso de haber un problema. El capturista cuenta con un casillero asignado para dejar sus pertenencias. Todos los operadores fueron capacitados para los roles de capturista 1, capturista 2, verificador 1 y verificador 2. El medio de verificación (MV) de esta etapa son los formularios F5-A-6_1_1, F5-A-6_1_2, , F5-A-6_2_1, F5-A-6_2_2 .
- La publicación se realiza de manera correcta, obteniendo los datos necesarios. Se publica por cada nivel de agregación de acuerdo con lo establecido. Se encuentran disponibles las actas para su descarga. El medio de verificación (MV) de esta etapa es el formulario F5-A-7.
- La fase de empaquetado de actas no se auditó en el Simulacro 1.

11.2 Comentarios y observaciones resultantes de Simulacro 2

11.2.1 Módulo de publicación de resultados

CAPA DE DATOS

- No se detectó ninguna inconsistencia en los archivos del inventario del IETAM. Esto indica que la integridad de las aplicaciones utilizadas se mantuvo durante el simulacro 2.
- Durante la generación de huellas criptográficas iniciales, el IETAM realizó el proceso de generación de huellas sin contar con la presencia del ente auditor. Es importante que el ente auditor se encuentre presente en todo momento durante la generación de huellas del inventario. Debido a lo anterior, estas huellas criptográficas fueron desechadas y se generaron nuevamente con el ente auditor presente.
- El porcentaje de efectividad del PREP es del 99.8% para diputaciones y un 99.2% para ayuntamientos.
- Es necesario mantener una consistencia en el formato de nombres utilizado para las actas. Por ejemplo, el formato de nombres proporcionado por el IETAM fue el siguiente: Origen_Tipo_Eleccion_Casilla.jpg (e.g. 2_H_D_0783 Básica.jpg.), no obstante, durante el simulacro se pudieron detectar imágenes con un agregado (e.g. 2_A_A_1223 Básica_V2.jpg). Este formato no fue proporcionado al ente auditor.
- EL sistema PREP presentó fallas en los cortes de información: se observó que no se realizaron cortes desde las 10:45 a las 11:48 y de las 11:48 a la 1:21.
- En el sitio de publicación existen imágenes de actas que no siguen el formato de nombre que el IETAM le proporcionó al ente auditor. Ciertas imágenes, presentan el agregado “_V2” al final del nombre.
- Se encontraron actas con nombres que NO CORRESPONDEN a la casilla correspondiente, en otras palabras, el nombre de casilla que se utiliza para nombrar a la fotografía no es el mismo al nombre

que se encuentra en el acta. Publicar actas con un nombre distinto no es aceptable y se recomienda tomar acción de manera inmediata.

- Se encontraron actas que cuentan con 2 fotografías, una por parte de PREP CASILLA y otra por parte de PREP CATD, sin embargo, las fotografías no coinciden y solo una corresponde al acta en mención, se recomienda tomar acción inmediata.
- Se encontraron 2 actas extra las cuales no aparecen registradas ni en el sitio de publicación ni en la base de datos del IETAM, sin embargo, es posible descargarlas utilizando la URL correspondiente.
- No es aceptable que el sistema no permita descargar Actas procesadas. Se deberían eliminar estos eventos o documentar la razón por la cual dichos eventos suceden en el software del PREP. Se recomienda revisar el formato de asignación de nombres de las actas para que este sea homogéneo y de esta forma el sistema permita ser monitorizado por procesos de seguimiento en tiempo real. Se recomienda corregir las inconsistencias descritas en el apartado PF.3.
- Fue posible realizar la validación del total de actas procesadas por el PREP sin encontrar inconsistencias.
- Es altamente recomendable corregir las inconsistencias descritas en el apartado PF.3 con el fin de mantener la integridad de las imágenes procesadas.
- La bitácora del sistema debería ser proporcionado para su consumo en tiempo real y de esta forma poder dar seguimiento a las acciones realizadas por los componentes del sistema PREP.
- Se recomienda que se repita esta buena práctica para el siguiente simulacro.
- Se recomienda solucionar aquellos problemas que generan los retrasos en los cortes de información.
- Se recomienda proporcionar acceso a la bitácora durante el siguiente simulacro. Se solicita que la bitacora sea adecuada para ser consumida por sistemas informáticos de auditoría

CAPA DE APLICACIÓN

- En la actualización periódica de resultados, podría ser útil la notificación automática al usuario que le informe que una nueva actualización está disponible.
- Algunos usuarios reportaron que las actualizaciones de resultados no se realizaron dentro del intervalo definido para tal fin (15 minutos)
- Ausencia de geolocalización de casillas dentro del mapa interactivo en el sitio de publicación de resultados, dicha característica podría mostrar un proceso más detallado dentro de la jornada. Según el testimonio de algunos usuarios esta funcionalidad la ofrecía el proveedor anterior, sin embargo, el IETAM asegura que dicha funcionalidad no hace parte de los requerimientos funcionales determinados por el INE.

11.2.2 CCV Principal

CAPA DE APLICACIONES

- El sistema valida adecuadamente el doble inicio de sesión del mismo usuario.
- Las credenciales de acceso son proporcionadas a los usuarios en papel, lo cual podría representar un riesgo de seguridad.
- El sistema implementa mecanismos que permiten la recuperación del último estado válido del acta.
- Se observó que el sistema es seguro ante un posible acuerdo entre un capturista y un verificador (con propósitos de fraude) ya que la asignación de actas a un verificador se realiza de manera

aleatoria.

CAPA DE PLATAFORMA TECNOLÓGICA

- A las 9:30 de la mañana se realizó la simulación de una falla de equipo, dicho equipo fue seleccionado al azar de los equipos disponibles en las salas de captura. Durante este proceso personal de soporte realizó varias pruebas como: verificar conectividad y reinicio del equipo, posteriormente se reemplazó el CPU del equipo por otro. Sin embargo, el nuevo equipo presentó fallas de conectividad debido a que no se había registrado la dirección MAC para poder acceder a la red, el personal de soporte y el administrador de la red tardaron 15 minutos Buenas prácticas: solo una persona tenía acceso a todos los usuarios y contraseñas de los equipos y él introducía los datos requeridos; además, los equipos en stock ya cuentan con su registro MAC con la finalidad de reducir el tiempo en el cambio del equipo.
- A las 10:30 de la mañana se simuló el corte de energía en las salas de captura bajando las pastillas en las tres salas las cuales funcionaron mediante los UPS durante 5 minutos sin ningún problema. Únicamente un monitor se apagó debido a la interrupción eléctrica, dado que no se encontraba conectado a una toma de batería.
- A las 11:00 de la mañana se simuló el corte de energía en todo el edificio entrando en funcionamiento la planta de energía la cual funcionó sin ningún problema. El monitor de la sala de captura se volvió apagar y las pantallas en la sala de información también por lo que procedieron a conectarlos a UPS.

CAPA OPERATIVA

Captura y Verificación de Datos provenientes de PREP Casilla y digitilización

- El capturista cuenta con un gafete de identificación.
- El capturista cuenta con las credenciales necesarias para el sistema. Para el simulacro 2 el supervisor ingresó las credenciales al sistema para cada capturista.
- El capturista deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el supervisor a cargo.
- El capturista realiza la solicitud del Acta PREP. Hubo ocasiones en donde al solicitar el Acta PREP el sistema se queda congelado por aproximadamente 3 segundos.
- El capturista tiene acceso al Acta PREP y al registro de datos.
- El capturista realiza el registro de los datos asentados en el Acta PREP.
- El capturista clasifica el Acta PREP como “ilegible”. Hubo ocasiones en donde se marcó como “ilegible” el Acta PREP y se pasaba al Centro de Verificación para su solución. Para realizar esta acción es necesaria la autorización del supervisor.
- El capturista cuenta con un manual de usuario digital para el uso del sistema. Se tiene un manual de usuario físico para todos los capturistas.
- El capturista obtuvo la capacitación necesaria para realizar el proceso.
- Cada que el capturista necesita abandonar su área de trabajo cierra sesión en el sistema. Por lo que al volver el supervisor tiene que a ingresar nuevamente las credenciales para iniciar sesión.
- Hubo actas recibidas que fueron rechazadas debido a que la imagen era ilegible o estaba borrosa, como consecuencia de error del CAEL que manipula el PREP Casilla.
- El verificador cuenta con gafete de identificación.
- El verificador cuenta con las credenciales necesarias para el sistema. Para el simulacro 2 el

supervisor ingresó las credenciales al sistema para cada capturista.

- El verificador deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el supervisor a cargo.
- El verificador corrobora que los datos capturados coincidan con los datos de la imagen del Acta PREP digitalizada.
- El verificador clasifica el Acta PREP como “ilegible”. Hubo ocasiones en donde se marcó como “ilegible” el Acta PREP y se pasaba al Centro de Verificación para su solución. Para realizar esta acción es necesaria la autorización del supervisor.
- Hay error en el registro de los datos y los datos asentados en el Acta PREP. Hubo ocasiones en que si sucedió, por lo que se pasa al Centro de Verificación.
- El verificador cuenta con un manual de usuario digital para el uso del sistema. Se tiene un manual de usuario físico para todos los capturistas.
- El verificador obtuvo la capacitación necesaria para realizar el proceso.
- Cada que el verificador necesita abandonar su área de trabajo cierra sesión en el sistema. Por lo que al volver el supervisor tiene que a ingresar nuevamente las credenciales para iniciar sesión.

Del Centro de Verificación

- El operador del CV cuenta con un gafete de identificación.
- El operador del CV cuenta con las credenciales necesarias para el sistema. Para el simulacro 2 el supervisor ingresó las credenciales al sistema para cada capturista.
- El operador del CV deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el supervisor a cargo.
- El operador del CV realiza la solicitud del Acta PREP y verifica el tipo de inconsistencia en el Acta PREP.
- El operador del CV realiza la primera captura del Acta PREP.
- El operador del CV realiza la segunda captura del Acta PREP.
- El operador del CV marca como “ilegible” el Acta PREP. Hay ocasiones donde los operadores del CV no pueden resolver la inconsistencia, por lo que solicitan ayuda a su supervisor antes de marcar el Acta PREP como “ilegible” y que no se contabilice.

11.2.3 CATD Victoria

CAPA DE APLICACIONES

- Se ha observado que los usuarios tienen acceso a su celular personal.
- Existe una discrepancia en la aplicación PREP CATD, en donde al tener actas pendientes de envíos (por fallas del internet) si se selecciona la opción de “actualizar”, los estados de todas las actas (hayan sido enviadas o no) se reflejan como no enviadas y deben de capturarlas todas de nuevo. Esto genera trabajo extra y una falta de comunicación para conocer lo que se ha recibido en los CCV y lo que no. Se recomienda tener un control de las actas recibidas y reflejar dicho control en las aplicaciones de captura.
- Se observó que no existen reemplazos de dispositivos móviles en caso de que lleguen a fallar, se recomienda conservar al menos uno para agilizar el trabajo en caso de que esto suceda.
- La aplicación es capaz de detectar si un QR no es correcto para el acta que se desea digitalizar y ofrece la opción de hacerlo manualmente, lo cual es una alternativa apropiada para situaciones en

que existan actas con QR erróneos.

- Se implementó un mecanismo eficiente para la recuperación del sistema ante eventos inesperados (cierres de sesión, terminación de aplicación). Si el acta queda en un estado inválido las actas se recuperan de forma automática.
- Las credenciales de acceso son proporcionadas a los usuarios en papel, lo cual podría representar un riesgo de seguridad.
- El sistema permite ingresar cualquier fecha en el sistema, así sea una fecha demasiado antigua o una fecha que aún no ha llegado.
- En esta versión del PREP, el sistema implementa mecanismos que permiten la recuperación del último estado válido del acta.
- Se observó que el sistema es seguro ante un posible acuerdo entre un capturista y un verificador (para efectos de posible fraude) ya que la asignación de actas a un verificador se realiza de manera aleatoria.
- Existe el riesgo de que ocurra un fallo con la aplicación PREP CATD para el cual, la solución sea reiniciar por completo la aplicación borrando la caché del dispositivo. El coordinador menciona que al hacer esto, el historial de actas capturadas se elimina, con lo cual hace imposible determinar cuáles actas habían sido enviadas con éxito y cuáles quedaron en un estado pendiente de envío. Esto obliga a los usuarios a capturar de nuevo **todas** las actas.
- En ocasiones las actas tardan en ser enviadas o incluso no se envían. Se asume que el problema es causado por la reducida capacidad de carga de datos proporcionada por el proveedor de internet.
- Existen dos instalaciones para proveer acceso a internet en el CATD. El coordinador decidió conectar los dispositivos móviles a una red secundaria y no a la red especialmente dedicada para el proceso de envío de actas digitalizadas.

CAPA OPERATIVA

Del Acopio

- El acopiador cuenta con un gafete de identificación.
- El acopiador verifica que los datos de identificación del Acta PREP sean legibles, de no ser así, deberá de acudir con el encargado del Acta PREP.
- El acopiador deja constancia de la fecha y hora (formato 24 hrs.) de acopio en el Acta PREP. Juntaba varias Actas PREP y les escribía la misma fecha y hora.
- Si el acopiador tarda más de lo necesario en realizar alguna actividad de la fase, el coordinador le brindará apoyo.
- El acopiador es el encargado del flujo de actas. En el simulacro 2 no se llevó un seguimiento de a quien le asignaba cada Acta PREP.
- El acopiador entregaba varias Actas PREP a la vez a los digitalizadores.

De la Digitalización

- El digitalizador cuenta con gafete de identificación.
- El digitalizador cuenta con las credenciales necesarias para el sistema. Las credenciales se les otorgaron en un papel impreso.
- El digitalizador deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el coordinador.
- El digitalizador realiza la captura digital de la imagen mediante PREP CATD utilizando el código QR.

En algunas ocasiones el PREP CATD no encontraba el Acta PREP utilizando el código QR.

- El digitalizador revisa la calidad de la imagen del Acta PREP en el PREP CATD. La calidad de la imagen siempre era buena, esto debido a las cajas que se implementaron para la digitalización.
- El digitalizador ingresa la información del Acta PREP de manera manual. En algunas ocasiones el PREP CATD no encontraba el Acta PREP utilizando el código QR, por lo que el digitalizador ingresaba la información de manera manual.
- Se transmite el Acta PREP al CRID. Había un retraso al enviar las imágenes de las Actas PREP, parece ser que era por una falla de la conexión a Internet.
- Al finalizar de digitalizar todas las Actas PREP (aproximadamente 422 Actas en total) quedaban 20 Actas pendientes de envío, esto debido al retraso. El coordinador comentó que si el PREP CATD se actualizaba iba a ser necesario realizar nuevamente la digitalización de todas las Actas PREP, debido a que en la aplicación ya no aparece cuales son las Actas PREP que quedaron pendientes de enviar. Se sugiere que se escriba en disco (puede ser un archivo .txt) aquellas Actas PREP que están pendientes de enviar para que de esta manera el acopiador las detecte y solo sea necesario digitalizar esas y no todas nuevamente.

11.3 Comentarios y observaciones resultantes de Simulacro 3

11.3.1 Módulo de publicación de resultados

CAPA DE DATOS

- Durante el proceso de generación de huellas criptográficas del simulacro 3, no se detectó ninguna inconsistencia en los archivos del inventario del IETAM. Esto indica que la integridad de las aplicaciones utilizadas se mantuvo durante todo el proceso.
- Se encontraron inconsistencias en algunas imágenes de las actas publicadas en el sitio de publicación. Por ejemplo, al realizar la búsqueda del acta **0638 Contigua 01** esta mostraba la fotografía del acta **0638 Básica**, y viceversa (ver anexo en N1/Actas/).
- Se siguen encontrando inconsistencias en el formato de nombre utilizado por el IETAM durante el evento y el proporcionado al ente auditor previo al evento. Algunas fotografías cuentan con el agregado "_V2" o "_V3" al final del nombre de la casilla (por ejemplo, **1_H_D_0638 Contigua 01_V3.jpg**).
- Se esperaba que el número total de actas registradas en la base de datos fuera igual a la suma del total de actas de ayuntamientos (4776) y de diputaciones (4808), siendo esta la cantidad de 9584. No obstante, el total de registros en el *backup* de la base de datos disponible en el sitio de publicación tiene un total de 9585 registros. Se observa que existe un registro adicional para diputaciones, siendo el registro de un acta fuera de la lista nominal.
- No fue posible realizar la descarga de todas las imágenes correspondientes al total de actas esperadas durante el simulacro. En total no se pudieron descargar 37 actas, de las cuales, 32 actas no pudieron ser accedidas a través del sitio de publicación aún y cuando sus datos fueron ingresados en la base de datos. Se recomienda que todas las actas registradas en la base de datos sean almacenadas en el sitio de publicación, se añada una justificación para las actas que no fueron almacenadas en el sitio de publicación y se utilice el formato de nombres compartidos con el ente auditor para poder descargar el 100% de las actas registradas.
- Se observó que los cortes de información en el sitio de publicación se realizan correctamente cada 15 minutos. Estos cortes permiten la generación de los backups de la base de datos.

- De las 9548 actas descargadas por el ente auditor durante el evento, se logró realizar la comprobación de integridad de 9548 actas (el 100%). Esta validación se realizó mediante el cálculo del resumen hash SHA-256 (que utiliza el algoritmo de hash SHA-256) a cada imagen descargada y comparándolas con los resúmenes hash registrados en la base de datos proporcionada por del IETAM buscando una correspondencia. Las 9548 actas fueron validadas correctamente y no se encontró ninguna inconsistencia.
- Se observó un comportamiento no esperado en el servicio de descarga de bitácora y una inconsistencia en el contenido de la bitácora descargada. Durante el evento se realizó la descarga de la bitácora del sistema utilizado por el IETAM en lotes de 5000 registros por petición. Se observó que no todas las peticiones a su servicio web devolvían los registros solicitados. Por tal motivo se realizaba la descarga del mismo lote hasta comprobar que los 5000 registros solicitados fueran descargados (respetando el tiempo de espera de 20s entre petición). De esta forma se consiguió obtener los lotes con 5000 registros. Siendo las 10:38:39 horas ocurrió un error y el servicio web devolvió como respuesta un Json sin registros (es decir []). Se inicio un tiempo de espera y se hicieron otras 4 peticiones a las 10:39:31, 10:40:22, 10:41:14 y 10:42:06 horas obteniendo el mismo resultado (para más detalles ver anexo N1/Bitacora/Anotaciones.pdf). A las 10:42:47 se obtuvo una respuesta con un Json que describía un error. A continuación, se muestra el contenido del error obtenido en formato Json:
- [{"Exito":0,"Error":"Transaction (Process ID 108) was deadlocked on lock resources with another process and has been chosen as the deadlock victim. Rerun the transaction."}]. Se le informo al IETAM sobre el error obtenido al utilizar su servicio web y se pausaron las solicitudes hacia el servicio web. Se reanudo la descarga de la bitácora en cuanto el IETAM confirmó que su servicio ya había sido revisado y se encontraba otra vez en línea. A las 11:05 horas se hizo una prueba del servicio web solicitando los registros 1 a 5000, al ver que contenía 5000 registros se reanudo la descarga de los registros desde el punto en el que se había pausado (290001). La descarga de los registros de la bitácora se realizó hasta antes del inicio del proceso de generación de huellas criptográficas finales del Simulacro 3 sin errores.
- Al las 14:01:07 horas se inició un proceso de descarga del contenido de la bitácora desde el registro 1 hasta el último para tener un respaldo de la bitácora. Esta prueba finalizo a las 15:01:04 horas. La bitácora del sistema debe ser consistente y no debe de presentar modificaciones en sus registros. Los archivos descargados antes de la falla, después de la falla hasta finalizar el simulacro (anexo *N1/Bitacora/S3antes.zip*) y los obtenidos al final del simulacro (anexo *N1/Bitacora/S3despues.zip*) deben ser iguales. Al comparar los archivos que contienen el mismo rango de registros nos encontramos que los resúmenes hash sha256 obtenidos eran diferentes en la mayoría.
- Debido a la detección de inconsistencias observadas en la bitácora (descritas en los puntos anteriores) no es posible realizar un análisis de la bitácora obtenida durante el simulacro tres por las siguientes razones:
    - No es posible realizar el análisis de seguimiento de las actas utilizando los archivos json obtenidos por el servicio proporcionado por el IETAM. El servicio devolvió contenidos diferentes para un mismo rango de registros.
    - No hay forma de identificar qué bitácora es la correspondiente al Simulacro número 3. Al analizar los archivos con los registros de 1 a 5000 se encontraron registros diferentes. Este comportamiento es persistente en la mayoría de los archivos.
    - No es posible realizar un seguimiento a través del tiempo de las acciones que se realizaron durante el Simulacro número 3. Se encontraron diferencias en los atributos

de los registros conservando los campos de estampa de tiempo (*fechaHoraMovimiento*) e *idBitacoraAuditor* intactos.

- No es posible dar seguimiento a las actas a través de todo el ciclo de vida del Simulacro 3, algunos registros que interactúan directamente con las actas tienen contenido diferente en la misma estampa de tiempo en los archivos analizados.

Un análisis más detallado de la bitácora se puede encontrar en el anexo *N1/Bitacora/Anotaciones.pdf.*

CAPA DE APLICACIONES

- En la actualización periódica de resultados, podría ser útil la notificación automática al usuario que le informe que una nueva actualización está disponible.
- Algunos usuarios reportaron que las actualizaciones de resultados no se realizaron dentro del intervalo definido para tal fin (15 minutos).
- Ausencia de geolocalización de casillas dentro del mapa interactivo en el sitio de publicación de resultados, dicha característica podría mostrar un proceso más detallado dentro de la jornada. Según el testimonio de algunos usuarios esta funcionalidad la ofrecía el proveedor anterior, sin embargo, el IETAM asegura que dicha funcionalidad no hace parte de los requerimientos funcionales determinados por el INE.
- En este simulacro no hubo reporte de retraso en las actualizaciones del sistema.
- A la mitad de la jornada se descargó la base de datos y se cotejó que la información general (número de actas, votos, etc.) correspondiera a lo reportado en el sitio web en ese momento tanto para ayuntamientos como diputaciones.

CAPA OPERATIVA

- La publicación se realiza en automático y de manera correcta, obteniendo los datos necesarios.
- Se publica por cada nivel de agregación de acuerdo con el INE.
- Se encuentran disponibles las actas para su descarga, ya sea actas que contaron en el total de los votos, o que no contaron y fueron rechazadas.

11.3.2 CCV Principal

CAPA DE APLICACIONES

- El sistema valida adecuadamente el doble inicio de sesión del mismo usuario.
- En simulacros anteriores, las credenciales de acceso eran proporcionadas al usuario en papel y a partir del simulacro que se está reportando, son utilizadas por personas autorizadas que ingresan antes a la aplicación para que el usuario empiece a utilizarla. El usuario no sabe cuáles son las credenciales de acceso.
- El sistema implementa mecanismos que permiten la recuperación del último estado válido del acta.
- Se observó que el sistema es seguro ante un posible acuerdo entre un capturista y un verificador (con propósitos de fraude) ya que la asignación de actas a un verificador se realiza de manera aleatoria.
- El centro de verificación cuenta con una opción de buscar información sobre las actas para corroborar que estén correctas.

- Los usuarios del centro de verificación capturan dos veces la misma acta por lo que se asegura con seguridad las correcciones que se están ejecutando.
- Al recibir un acta en el centro de verificación, se cuenta con una descripción del porqué ha llegado hasta ese punto del flujo del proceso.
- Los verificadores están mezclados con los capturistas del CCV. No existe un área designada especialmente al centro de verificación.
- En la interfaz de captura de actas en el módulo de verificación existe una opción para seleccionar el origen del acta (acta fila CV y acta fuera de catálogo). Los usuarios no utilizan la segunda opción para comprobar si existen actas fuera de catálogo.

CAPA DE PLATAFORMA TECNOLÓGICA

- A las 9:30 de la mañana se realizó la simulación de una falla de equipo, dicho equipo fue seleccionado al azar de los equipos disponibles en las salas de captura. Durante este proceso personal de soporte realizó varias pruebas como: verificar conectividad y reinicio del equipo, posteriormente se reemplazó el CPU del equipo por otro. El personal de soporte no tuvo ningún problema en el conocimiento de la IP y la puerta de enlace. El tiempo total para cambiar el equipo fue de 13 minutos y no se registró ningún problema, el capturista pudo continuar trabajando sin problema después del cambio del CPU. Buenas prácticas: solo una persona tenía acceso a todos los usuarios y contraseñas de los equipos y él introducía los datos requeridos; además, los equipos en stock ya cuentan con su registro MAC con la finalidad de reducir el tiempo en el cambio del equipo.
- A las 10:30 de la mañana se simuló el corte de energía en las salas de captura bajando las pastillas en las tres salas las cuales funcionaron mediante los UPS durante 5 minutos sin ningún problema.
- A las 11:00 de la mañana se simuló el corte de energía en todo el edificio entrando en funcionamiento la planta de energía la cual funcionó sin ningún problema.

CAPA DE INFRAESTRUCTURA DE COMUNICACIONES

- Se verificó que el sitio web del PREP utiliza "https" y no "http".
- A las 11:15 de la mañana se realizó la prueba de redundancia y tolerancia a fallos del enlace (Failover). Para esto se desconectó la fibra óptica del proveedor TotalPlay de manera física, lo cual afectó a los equipos de captura entre 15 a 20 segundos en lo que se dirigía el tráfico por el enlace redundante Telmex.

CAPA OPERATIVA

Captura de Datos provenientes de toma fotográfica (PREP Casilla) y digitalización (PREP CATD).

- El capturista cuenta con un gafete de identificación.
- El capturista no cuenta con las credenciales necesarias para el sistema. El supervisor tiene las credenciales de todos los operadores y es el encargado de ingresar al sistema.
- El capturista deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el supervisor a cargo.
- El capturista realiza la solicitud del Acta PREP. Hubo ocasiones en donde al solicitar el Acta PREP el sistema se queda congelado por aproximadamente 3 segundos.
- El capturista obtuvo la capacitación necesaria para realizar el proceso.
- El capturista tiene acceso al Acta PREP y al registro de datos.

- El capturista clasifica el Acta PREP como “ilegible” (rechaza el Acta PREP). Hubo ocasiones en donde se marcó como “ilegible” el Acta PREP y se pasaba al Centro de Verificación para su solución. Para realizar esta acción es necesaria la autorización del supervisor.
- El capturista cuenta con un manual de usuario digital para el uso del sistema. Se tiene un manual de usuario físico para todos los capturistas.
- Cada que el capturista necesita abandonar su área de trabajo no se cierra sesión en el sistema, solo cuando va a comer.

Verificación de Datos de Actas PREP

- El verificador cuenta con gafete de identificación.
- El verificador no cuenta con las credenciales necesarias para el sistema. El supervisor tiene las credenciales de todos los operadores y es el encargado de ingresar al sistema.
- El verificador deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el supervisor a cargo.
- El verificador corrobora que los datos capturados coincidan con los datos de la imagen del Acta PREP digitalizada.
- El verificador clasifica el Acta PREP como “ilegible”. Hubo ocasiones en donde se marc como “ilegible” el Acta PREP y se pasaba al Centro de Verificación para su solución. Para realizar esta acción es necesaria la autorización del supervisor.
- Hay error en el registro de los datos y los datos asentados en el Acta PREP. Hubo ocasiones que, si sucedió, por lo que se pasa al Centro de Verificación.
- El verificador cuenta con un manual de usuario digital para el uso del sistema. Se tiene un manual de usuario físico para todos los capturistas.
- El verificador obtuvo la capacitación necesaria para realizar el proceso.
- Cada que el capturista necesita abandonar su área de trabajo no se cierra sesión en el sistema, solo cuando va a comer.
- En una ocasión un verificador realizó la solicitud de un Acta PREP y el sistema quedó congelado por aproximadamente 5 minutos, el supervisor brindó apoyo. Se tuvo que forzar el cierre del sistema desde el administrador de tareas, para así ingresar nuevamente.

Centro de Verificación

- El operador del CV cuenta con un gafete de identificación.
- El operador del CV no cuenta con las credenciales necesarias para el sistema. El supervisor tiene las credenciales de todos los operadores y es el encargado de ingresar al sistema.
- El operador del CV deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el supervisor a cargo.
- El operador del CV realiza la solicitud del Acta PREP y verifica el tipo de inconsistencia en el Acta PREP.
- El operador del CV realiza la primera captura del Acta PREP.
- El operador del CV realiza la segunda captura del Acta PREP.
- El operador del CV marca como “ilegible” el Acta PREP. Hay ocasiones donde los operadores del CV no pueden resolver la inconsistencia, por lo que solicitan ayuda a su supervisor antes de marcar el Acta PREP como “ilegible” y que no se contabilice. Para estos casos no se cuenta con un módulo que permita especificar el por qué se decidió rechazar el Acta PREP, para esto lo escriben en una nota. Se sugiere agregar un módulo que permita llevar el control de las Actas PREP rechazadas que no se contabilizan.

10.3.3 CATD Victoria

CAPA DE APLICACIONES

- Se ha observado que los usuarios tienen acceso a su celular personal.
- Existe una discrepancia en la aplicación PREP CATD, en donde al tener actas pendientes de envíos (por fallas del internet) si se selecciona la opción de “actualizar”, los estados de todas las actas (hayan sido enviadas o no) se reflejan como no enviadas y deben de capturarlas todas de nuevo. Esto genera trabajo extra y una falta de comunicación para conocer lo que se ha recibido en los CCV y lo que no. Se recomienda tener un control de las actas recibidas y reflejar dicho control en las aplicaciones de captura.
- Se observó que no existen reemplazos de dispositivos móviles en caso de que lleguen a fallar, se recomienda conservar al menos uno para agilizar el trabajo en caso de que esto suceda.
- La aplicación es capaz de detectar si un QR no es correcto para el acta que se desea digitalizar y ofrece la opción de hacerlo manualmente, lo cual es una alternativa apropiada para situaciones en que existan actas con QR erróneos.
- Se implementó un mecanismo eficiente para la recuperación del sistema ante eventos inesperados (cierres de sesión, terminación de aplicación). Si el acta queda en un estado inválido las actas se recuperan de forma automática.
- Las credenciales de acceso son proporcionadas a los usuarios en papel, lo cual podría representar un riesgo de seguridad.
- El sistema permite ingresar cualquier fecha en el sistema, así sea una fecha demasiado antigua o una fecha que aún no ha llegado.
- En esta versión del PREP, el sistema implementa mecanismos que permiten la recuperación del último estado válido del acta.
- Se observó que el sistema es seguro ante un posible acuerdo entre un capturista y un verificador (para efectos de posible fraude) ya que la asignación de actas a un verificador se realiza de manera aleatoria.
- Existe el riesgo de que ocurra un fallo con la aplicación PREP CATD para el cual, la solución sea reiniciar por completo la aplicación borrando la caché del dispositivo. El coordinador menciona que al hacer esto, el historial de actas capturadas se elimina, con lo cual hace imposible determinar cuáles actas habían sido enviadas con éxito y cuáles quedaron en un estado pendiente de envío. Esto obliga a los usuarios a capturar de nuevo **todas** las actas.
- En ocasiones las actas tardan en ser enviadas o incluso no se envían. Se asume que el problema es causado por la reducida capacidad de carga de datos proporcionada por el proveedor de internet.
- Existen dos instalaciones para proveer acceso a internet en el CATD. El coordinador decidió conectar los dispositivos móviles a una red secundaria y no a la red especialmente dedicada para el proceso de envío de actas digitalizadas.
- Se realizó una prueba que simula fallas en un equipo de cómputo durante el proceso de captura de un acta, donde la aplicación se cierra de manera abrupta. En este sentido se verificó que el acta en proceso (antes de la falla) es reasignada a otro capturista de forma automática.
- En la misma simulación de falla se observó que el operador o capturista no puede iniciar sesión con su usuario hasta que el supervisor le proporcione la contraseña. Esto es una mejora de las jornadas anteriores ya que las contraseñas las conocían los operadores previamente y podrían aumentar el riesgo de malos usos de éstas.

- Al presentarse una falla, la sesión del usuario queda abierta por lo que tiene que cerrarse desde el módulo de administración del sistema para volver a iniciar. Esto puede ser una ventaja para controlar la creación de sesiones múltiples. El problema es que el sistema no informa al usuario de que está intentando iniciar una sesión ya existente y le muestra código de error poco intuitivo acerca de lo que está pasando.
- Por parte de los supervisores se sugiere en futuras versiones un módulo de supervisión (de preferencia en un dispositivo móvil) que permita realizar más eficientemente el control de incidencias.
- Al parecer la caja digitalizadora no funciona correctamente o bien los usuarios no la manipulan adecuadamente. Las imágenes de las actas que llegan al CCV presentan desplazamientos, arrugas o dobleces, lo cual dificulta su legibilidad.
- Los verificadores tienen que capturar (a petición de personal del IETAM) en un bloc de notas las actas que envían al centro de verificación, así como el motivo por el cual las envían.

CAPA DE PLATAFORMA TECNOLÓGICA

- Los equipos (smartphone) no tienen salida a Internet salvo a la aplicación del PREP.
- En el sitio se tiene al menos un equipo UPS el cual protege al modem.
- En el sitio se cuenta con planta de emergencia, sin embargo, no existe personal en el CATD que esté capacitado para operar este equipo. Estaba programada una prueba donde debería arrancar la planta por 5 minutos en el CATD, pero no se realizó debido a que no hay personal para operar el equipo. El coordinador del sitio comentó que nunca se ha realizado la prueba por falta de personal.

CAPA DE INFRAESTRUCTURA DE COMUNICACIONES

- No se está utilizando el enlace a Internet asignado para el proceso electoral. El coordinador en sitio menciona que esto es debido a que si se utiliza el enlace asignado no se envían las imágenes correctamente por el mal servicio este. Todos los dispositivos están conectados al servicio a Internet del consejo donde se encuentra instalado el CATD. El coordinador comentó que fue personal del proveedor de Internet a revisar el módem, pero no se ha solucionado el problema mencionado.
- Se detectó que varios dispositivos personales (los cuales no están relacionados con el proceso electoral) están haciendo uso también del mismo servicio a Internet que los equipos utilizados para la jornada electoral.
- Las redes inalámbricas están configuradas con las credenciales por default.

CAPA OPERATIVA

Del Acopio

- El acopiador cuenta con un gafete de identificación.
- Si el acopiador tarda más de lo necesario en realizar alguna actividad de la fase, el coórdinador le brinda apoyo.
- El acopiador es el encargado del flujo de actas. No se lleva un seguimiento de a quien se le entrega cada Acta PREP, solo se sigue un orden de entrega.
- El acopiador entregaba varias Actas PREP a la vez a los digitalizadores. Al ser simulacro no afecta.

- El acopiador verifica que los datos de identificación del Acta PREP sean legibles, de no ser así, deberá de acudir con el encargado del Acta PREP.
- El acopiador deja constancia de la fecha y hora (formato 24 hrs) de acopio en el Acta PREP. Juntaba varias Actas PREP y les escribía la misma fecha y hora.

De la Digitalización

- El digitalizador cuenta con gafete de identificación.
- El digitalizador cuenta con las credenciales necesarias para el sistema. Las credenciales se les otorgaron en un papel.
- El digitalizador deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el coordinador.
- El digitalizador obtuvo la capacitación necesaria para realizar el proceso.
- El digitalizador realiza la captura digital de la imagen mediante PREP CATD utilizando el código QR. En algunas ocasiones el PREP CATD no encontraba el Acta PREP utilizando el código QR, por lo que se realizaba el registro de los datos de forma manual.
- El digitalizador revisa la calidad de la imagen del Acta PREP en el PREP CATD. La calidad de la imagen siempre era buena, esto debido a las cajas que se implementaron para la digitalización.
- Se transmite el Acta PREP al CRID. Había un retraso en un solo dispositivo al enviar las imágenes de las Actas PREP. Quedaron 11 actas pendientes de enviarse por aproximadamente 1 hora, el coordinador le indico que cambiara de dispositivo por uno que tenían de respaldo. Al cambiar de dispositivo se digitalizaron nuevamente aquellas actas pendientes.

Captura y Verificación de Datos provenientes de Digitalización

- El capturista cuenta con un gafete de identificación.
- El capturista cuenta con las credenciales necesarias para el sistema, las cuales se le fueron asignadas mediante un papel impreso, cada día son credenciales diferentes.
- El capturista cuenta con un manual de usuario para el uso del sistema.
- La mayoría de las actas que se digitalizaron habían sido ya capturadas por PREP Casilla, por lo que muchas veces no se realizó el proceso de captura en el CATD.
- Durante el simulacro no se encontraba un acta en el sistema para capturar, se tenía de manera física pero el sistema no mostraba la opción para capturarla

11.3.4 PREP Casilla

CAPA DE APLICACIONES

- Se visitó una casilla ubicada en la Escuela Primaria Ejército Méxicano en Ciudad Victoria, con el propósito de observar el proceso de toma fotográfica y envío de actas. En este sentido los resultados obtenidos fueron satisfactorios. La única observación al respecto es que algunas actas quedan temporalmente pendientes de envío al parecer por problemas de conexión.
- Se sugiere para futuras versiones que los coordinadores tengan un módulo de chequeo que permita verificar eficientemente que todas las actas de los operadores a su cargo se envíen adecuadamente.

CAPA OPERATIVA

De la toma fotográfica del Acta PREP en la casilla

- El CAEL cuenta con un chaleco de identificación otorgado por el INE.
- El CAEL obtuvo una capacitación antes de realizar el simulacro por parte de su supervisor del INE.
- El CAEL cuenta con las credenciales necesarias para ingresar al sistema.
- El CAEL no cuenta con un manual de usuario.
- Al CAEL se le asignó un dispositivo móvil en el cual tenía instalado el PREP Casilla.
- El CAEL al tener una duda se dirige con su coordinador.
- El CAEL verifica que todos los datos de identificación del Acta PREP sean legibles y estén completos.
- El CAEL coloca el Acta PREP de tal forma que no presente dobleces.
- El CAEL verifica que no se incluyan elementos ajenos al Acta PREP en la toma fotográfica. El CAEL indicó que a veces es necesario colocar algún objeto sobre el Acta PREP para que esta se quede en su lugar mientras realiza la toma fotográfica.
- El CAEL verifica que la imagen tomada sea legible.
- El CAEL no cuenta con un lugar asignado para la toma fotográfica.

12. Análisis de Riesgos

12.1 Metodología usada para el análisis de riesgos

El análisis de riesgos se realizó con base a la metodología Mageritv3 que sigue la normativa ISO 31000, Mageritv3 responde a lo que se denomina “Proceso de gestión de los riegos”.

La metodología de Mageritv3 contempla los siguientes procesos:

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
2. Determinar a qué amenazas están expuestos los activos.
3. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
4. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

11.1.1 Valoración de amenazas.

Las amenazas encontradas han sido valoradas con base a su degradación o cuán perjudicial resultaría para cada activo y cuán probable o improbable es que se materialice la amenaza, tomando en cuenta los niveles de degradación de valor y probabilidad de ocurrencia de la metodología Megeritv3 que se muestran en las Tablas 11.1 y 11.2, respectivamente.

Tabla 11.1 Degradación del valor.

Acrónimo	Nivel	Criterio	Criterio	Valor
MA	Muy alta	Casi seguro	Fácil	5
A	Alta	Muy alto	Medio	4
M	Media	Posible	Difícil	3
B	Baja	Poco probable	Muy difícil.	2
MB	Muy baja	Muy raro	Extremadamente difícil.	1

Tabla 11.2. Probabilidad de ocurrencia

Acrónimo	Probabilidad	Criterio	Criterio	Valor
MA	100	Muy frecuente	A diario	5
A	10	Frecuente	Mensualmente	4
M	1	Normal	Una vez al año	3
B	1/10	Poco frecuente	Cada varios años.	2
MB	1/100	Muy poco frecuente.	Siglos	1

11.1.2 Determinación del riesgo potencial

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia. El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo.

Siguiendo la metodología de Megeritv3 se identificaron las siguientes zonas de riesgo y se mapearon en la Tabla 3:

1. Zona de riesgo 1. Abarca los siguientes riegos:
    a. Riesgos de muy bajo impacto y de muy baja posibilidad de que se materialice el riesgo.
    b. Riesgos de bajo impacto y de muy baja posibilidad de que se materialice el riesgo.
    c. Riegos de muy bajo impacto y de baja posibilidad de que se materialice el riesgo.
    d. Riesgos de bajo impacto y de media posibilidad de que se materialice el riesgo.
    e. Riego de muy bajo impacto y de baja posibilidad de que se materialice el riesgo.
    f. Riesgos de muy bajo impacto y de media posibilidad de que se materialice el riesgo.
2. Zona de riesgo 2. Abarca los siguientes riesgos:
    a. Riesgos de medio impacto y de muy baja posibilidad de que se materialice el riesgo.
    b. Riesgos de medio impacto y de baja posibilidad de que se materialice el riesgo.
    c. Riesgos de medio impacto y de media posibilidad de que se materialice el riesgo.
    d. Riesgos de bajo impacto y de alta posibilidad de que se materialice el riesgo.
    e. Riesgos de muy bajo impacto y de alta posibilidad de que se materialice el riesgo.
    f. Riesgos de bajo impacto y de muy alta posibilidad de que se materialice el riesgo.
    g. Riesgo de muy bajo impacto y de muy alta posibilidad de que se materialice el riesgo.

3. Zona de riesgo 3. Abarca los siguientes riesgos:
    a. Riesgos de muy alto impacto y de muy baja posibilidad de que se materialice el riesgo.
    b. Riesgo de alto impacto y de muy baja posibilidad de que se materialice el riesgo.
    c. Riesgo de muy alto impacto y de baja posibilidad de que se materialice el riesgo.
    d. Riesgos de alto impacto y de baja posibilidad de que se materialice el riesgo.
    e. Riesgos de alto impacto y de media posibilidad de que se materialice el riesgo.
    f. Riesgo de medio impacto y de alta posibilidad de que se materialice el riesgo.

4. Zona de riesgo 4. Abarca los siguientes riesgos:
    a. Riesgo de muy alto impacto y de media posibilidad de que se materialice el riesgo.
    b. Riesgo de muy alto impacto y de alta posibilidad de que se materialice el riesgo.
    c. Riesgo de alto impacto y de alta posibilidad de que se materialice el riesgo.
    d. Riesgo de muy alto impacto y de muy alta posibilidad de que se materialice el riesgo.
    e. Riesgo de alto impacto y de muy alta posibilidad de que se materialice el riesgo.
    f. Riesgo de medio impacto y de muy alta posibilidad de que se materialice el riesgo.

Tabla 11.3. Zonas de riesgos.

5	**MA**	3	3	4	4	4
4	**A**	3	3	3	4	4
3	**M**	2	2	2	3	4
2	**B**	1	1	1	2	2
1	**MB**	1	1	1	2	2
		MB	**B**	**M**	**A**	**MA**
		1	**2**	**3**	**4**	**5**

A continuación, se presentan las vulnerabilidades y amenazas identificadas para el Nivel Operativo y Nivel de Datos y Aplicación, en cada uno de sus eventos y sus valoraciones de acuerdo con la metodología MAGERIT v.3.

12.2 Análisis de Riesgo de Nivel Operativo

11.2.1 Identificación de activos/eventos de Nivel Operativo

Con el propósito de simplificar el análisis de riesgo, se identificaron los activos/eventos que son representativos de la implementación del Proceso Técnico Operativo para el PREP. A continuación, se presentan las vulnerabilidades y amenazas identificadas en el Nivel Operativo del PREP, en cada uno de los eventos y su valoración de acuerdo con la metodología MAGERIT v.3.

Tabla 11.4. Vulnerabilidades y amenazas identificadas. Nivel: Operativo.

EVENTO	TAREA /VULNERABILIDAD	AMENAZA	IMPACTO SOBRE LA OPERACIÓN DEL SISTEMA	POSIBILIDAD DE QUE SE MATERIALICE LA AMENAZA	IMPACTO PROMEDIO	MATERIALIZACIÓN PROMEDIO
Toma Fotográfica	Disponibilidad del acta	A la llegada del CAE el acta se haya enviado	4	5	4.5	4.5
	Fotos parciales o mal enfocadas	El CAE no verifica que la foto sea legible	5	4		
Acopio	Identificación errónea del acta	El acta está mal identificada desde el origen	5	2	5.0	2.0
Digitalización	Imagen errónea/parcial de acta	El digitalizador no sabe cómo orientar el	3	4	3.5	4.0

		acta para escanearla				
	Imagen errónea/parcial de acta	El digitalizador no verifica la legibilidad del acta escaneada	4	4		
Captura y Verificación PREP Tradicional	Captura errónea de datos	El capturista introduce mal los datos	3	4	3.0	4.0
Captura y Verificación PREP Casilla	Fotos parciales o mal enfocadas	Imposibilidad de capturar el acta	5	2	5.0	2.0
Cotejo	Imagen errónea/parcial del acta	Imposibilidad de corregir los datos capturados del acta	5	2	5.0	3.5
	No se registran las actividades del operador verificador 2	El operador verificador tiene la facultad de modificar todos los datos del acta sin que quede registro de ello	5	5		
Publicación	Demora en reflejar actas capturadas y contabilizadas	Retraso en la obtención de resultados	2	5	2	5

11.2.2 Concentrado de impacto y materialización promedio de los eventos detectados a Nivel Operativo

Tabla 11.5 Impacto y materialización. Nivel Operativo.

	IMPACTO PROMEDIO	MATERIALIZACIÓN PROMEDIO
Toma Fotográfica	4.5	4.5
Acopio	5.0	2.0
Digitalización	3.5	4.0
Captura y Verificación PREP Tradicional	3.0	4.0
Captura y Verificación PREP Casilla	5.0	2.0
Cotejo	5.0	3.5
Publicación	2.0	5.0

11.2.3 Mapa de calor de riesgos de Nivel Operativo

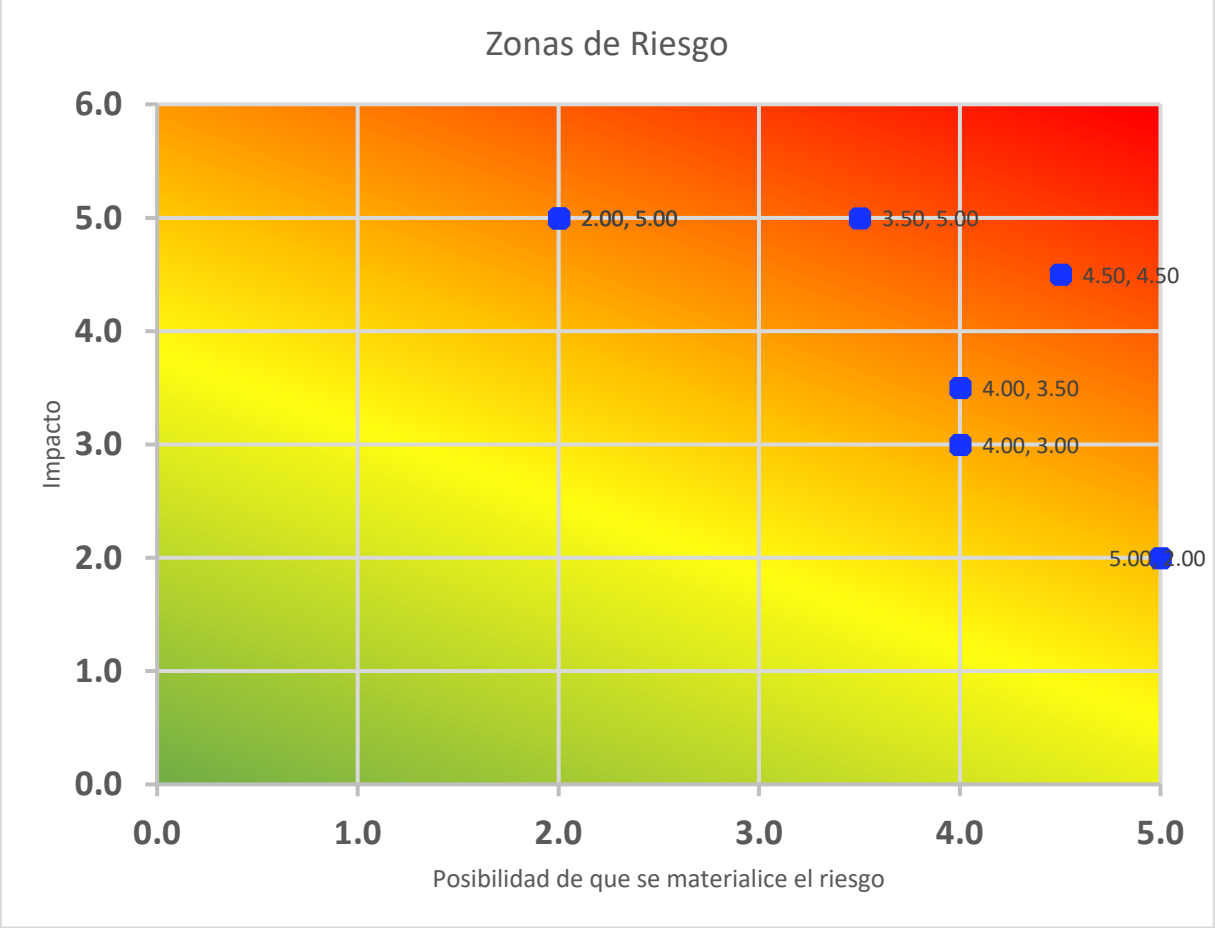


Figura 11.1 Mapa de calor. Nivel: Operativo.

12.3 Análisis de Riesgo de Nivel Datos y Aplicación

Siguiendo la metodología Mageritv3 se determinó el siguiente análisis de riesgos para en Nivel de Aplicación

11.3.1 Identificación de activos/eventos de Nivel Datos y Aplicación

A partir de las vulnerabilidades encontradas, se determinaron las posibles amenazas o riesgos que representan. Para cuantificar el nivel de riesgo se procedió a determinar el nivel de impacto y el nivel de ocurrencia con base en lo observado durante los diferentes simulacros del sistema, esto se muestra en la Tabla 11.6.

Tabla 11.6 Análisis de Riesgos de la capa 1 y 2.

EVENTO	EVENTO	TAREA/VULNERABILIDAD	AMENAZA	IMPACTO SOBRE LA OPERACIÓN DEL SISTEMA	POSIBILIDAD DE QUE SE MATERIALICE LA AMENAZA
Datos	Inicialización y manejo de la base de datos y del sistema de archivos.	No se realiza una inicialización en ceros de la base de datos en presencia del ente Auditor.	Intento de fraude o sabotaje	5	2
		No se realiza una inicialización en ceros del sistema de archivos en presencia del ente auditor.	Intento de fraude o sabotaje	5	3
		No existe un registro o log de la inicialización de la base de datos y del sistema de archivos.	Intento de fraude o sabotaje	5	2
		El sistema no cuenta con la detección de errores en las bases de datos (Checksum).	Resultados y datos inconsistentes	4	1
		No existe un monitoreo de los accesos a la base de datos y del sistema de archivos.	Acceso a información privada por parte de personas no autorizadas	3	1
		No se realizó el inventario con los archivos de las bases de datos y del sistema de archivos solicitados por el Ente Auditor para su huella criptográfica.	Intento de fraude o sabotaje	5	1

		La base de datos cumple parcialmente con las buenas prácticas.	Latencia en el proceso	1	2
		A pesar de que se ejecutó el proceso de firma de la aplicación, no hay certeza de que el código fuente no sea cambiado durante el proceso. No existe un mecanismo de versionamiento por parte del proveedor que dé garantías al 100% de la versión productiva no cambia.	Intento de fraude o sabotaje	5	4
Datos	Captura de información	No existe un registro de la actividad de captura en el log del web service de auditoría.	Resultados y datos inconsistentes	1	4
		Se pueden propagar errores en los tres niveles de validación/captura	Latencia en el proceso	1	2
		Inconsistencia de actas escaneadas	Resultados y datos inconsistentes	3	2
		Inconsistencia de fechas y hora de captura o digitalización de actas No hay evidencia de que los datos sin conexión se eliminan de la computadora	Resultados y datos inconsistentes	4	2
		Perdida de la acta que esté siendo capturada	Resultados y datos inconsistentes	4	1
		Pueden existir errores operativos que afectan los resultados	Resultados y datos inconsistentes	4	2
		Vulnerabilidad de acceso a datos privados por mal manejo y administración de usuarios	Acceso a información privada por parte de personas no autorizadas	4	1
		Estado inconsistente de acta	Resultados y datos inconsistentes	4	4
		Manejo inadecuado de datos de sesión	Resultados y datos inconsistentes	3	4
		El capturista introduce mal los datos	Latencia en el proceso/Resultados y datos inconsistentes	3	3
		El registro de la captura no logró enviarse correctamente	Latencia en el proceso/Resultados y datos inconsistentes	1	1

Datos	Validación	Existen actas que no pueden ser recuperadas siguiendo el flujo operativo.	Latencia en el proceso	1	2
		El Validador 2 realiza cambios sin ser auditado	Intento de fraude o sabotaje	5	1
		Perdidas de información que puede ocasionar inconsistencias durante el proceso	Resultados y datos inconsistentes	4	3
		Ineficiencias en el proceso	Latencia en el proceso	4	3
		Tiempos muertos en el proceso validación	Latencia en el proceso	3	4
		Posibles retrasos y latencias durante el proceso de validación	Latencia en el proceso	3	3
		Posibles inconsistencias en los datos	Resultados y datos inconsistentes	4	3
		Existe la posibilidad de acuerdo mal intencionado entre un capturista y un verificador. A través de algún medio el capturista le puede hacer saber al verificador las actas que capturará (favoreciendo a un partido), con el fin de que este las deje pasar sin problema alguno si le son asignadas	Intento de fraude o sabotaje	5	1
		Existe una probabilidad considerable del que el verificador caiga en omisiones de verificación. El sistema debería resaltar o indicar los campos y valores cuya verificación es fundamental.	Resultados y datos inconsistentes	4	2
		Los datos del acta son ilegibles.	Latencia en el proceso/Resultados y datos inconsistentes	3	3
		Se reciben imágenes parciales o mal enfocadas.	Latencia en el proceso	1	2
		El verificador 1 y 2 asigna una respuesta/percepción incorrecta sobre un acta.	Resultados y datos inconsistentes	5	1

Datos	Publicación de resultados	No se recupera toda la información de las actas capturas en la base de datos de publicación (SHA256).	Resultados y datos inconsistentes	4	2
		Existe información de más en la base de datos de publicación.	Resultados y datos inconsistentes	1	1
		El nombre de las imágenes de acta no tiene correspondencia con la clave que se encuentra en la base de datos de publicación.	Resultados y datos inconsistentes	1	5
		No se recupera todas las imágenes de las actas capturadas.	Resultados y datos inconsistentes	1	2
		La información de la base de datos de publicación discrepa con la información de log del web service de auditoria.	Resultados y datos inconsistentes	5	5
		EL tiempo que le toma a las actas desde su captura hasta su publicación es tardado.	Latencia en el proceso	1	2
		Existe la posibilidad de descargar el sitio web (a través de web crawling) con propósitos mal intencionados.	Intento de fraude o sabotaje	4	2
Datos	Auditoría a los eventos del proceso	Las operaciones realizadas a cada acta no están debidamente registradas en el log del web service de auditoría.	Resultados y datos inconsistentes	1	3
		La información del log del web service de auditoría no permite realizar una correspondencia de la información capturada en la bases de datos maestra.	Resultados y datos inconsistentes	4	3
		No se tiene un reloj único para sincronizar la hora, para poder realizar una traza en el tiempo de las actividades realizadas a las actas que se registran en el log de web service de auditoría	Resultados y datos inconsistentes	2	4

Datos	Disponibilidad / Escalabilidad	El equipo de seguridad instalado no es lo suficientemente robusto para garantizar la continuidad ante una incidencia.	Afectación a la continuidad del proceso.	1	5
		No existe suficiente información para identificar los protocolos de tolerancia a fallos, escalabilidad y redundancia.	Afectación a la operación del proceso.	4	2
		No se realizaron pruebas de usuarios concurrentes por parte del PROVEEDOR. Antes de liberar a producción (Simulacros y Jornada electoral).	Sistema fuera de servicio	4	1
Aplicación	Captura de Actas	Inconsitencia de actas escaneadas	Resultados y datos inconsistentes	3	2
Aplicación	Captura de Actas	Posibles fallas en el servicio del sistema	Sistema fuera de servicio	5	3
Aplicación	Captura de Actas	Inconsistencia de datos cargados	Resultados y datos inconsistentes	3	4
Aplicación	Captura de Actas	Estado inconsistente de acta	Resultados y datos inconsistentes	4	4
Aplicación	General	Puede transmitirse información confidencial como por ejemplo las credenciales de los usuarios	Intento de fraude o sabotaje	5	3
Aplicación	General	Acceso a la información por medio de periféricos externos desconocidos por el soporte técnico del proyecto	Acceso a información privada por parte de personas no autorizadas	4	2
Aplicación	General	Apesar de que se ejecutó el proceso de firma de la aplicación, no hay certeza de que el código fuente no sea cambiado durante el proceso. No existe un mecanismo de versionamiento por parte del proveedor que de garantias al 100% de la	Intento de fraude o sabotaje	5	4

		versión productiva no cambia.			
Aplicación	PREP Casilla	Inconsistencia de los datos	Resultados y datos inconsistentes	3	2
Aplicación	Toma Fotográfica	El proceso de envío de imagen PREP se ve interrumpido constantemente	Latencia en el proceso	5	2
Aplicación	Validación	Acceso de personas no autorizadas	Acceso a información privada por parte de personas no autorizadas	4	4
Aplicación	Validación	Tiempos muertos en el proceso validación	Latencia en el proceso	3	4
Aplicación	Validación	Posibles inconsistencias en los datos	Resultados y datos inconsistentes	4	3
Aplicación	Validación	Acceso de usuario no autorizado en un CCV	Acceso a información privada por parte de personas no autorizadas	4	4
Aplicación	Validación	Desinformación del usuarion en el proceso	Latencia en el proceso	4	2
Validación	Validación	Demora en el proceso	Latencia en el proceso	3	1

11.2.2 Concentrado de impacto y materialización promedio de los eventos detectados a Nivel de Datos y Aplicación

El impacto y materialización del riesgo obtenido del análisis anterior, se promediaron por escenario como se muestra en la Tabla 11.7.

Tabla 11.7 Ponderación del impacto y la materialización, de los riesgos identificados en la capa de datos y aplicación.

	ESCENARIO	IMPACTO PROMEDIO	MATERIALIZACIÓN PROMEDIO
ID-01	Inicialización y manejo de la base de datos y del sistema de archivos.	4.1	2
ID-02	Captura de información	2.9	2.4
ID-03	Validación	3.5	2.3
ID-04	Toma Fotográfica	2	2.3
ID-05	Publicación de resultados	2.4	2.7
ID-06	Auditoría a los eventos del proceso	2.3	3.3
ID-07	Disponibilidad / Escalabilidad	3	2.7
ID-08	Captura de Actas	3.8	2.9
ID-09	Publicación	4.5	1.5
ID-10	Toma Fotográfica	3.5	2.0
ID-11	Validación	4.0	3.2
ID-12	Prep-Casilla	3.0	2.0
ID-13	General	4.4	2.8

11.2.3 Mapa de calor de riesgos de Nivel de Datos y Aplicación

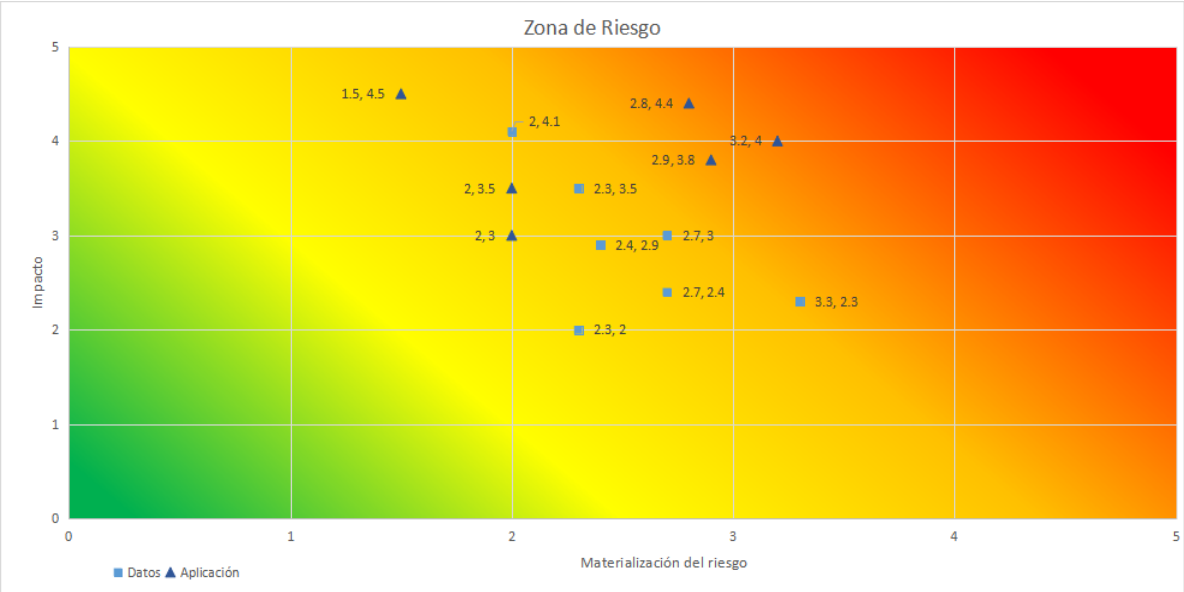


Figura 11.2 Zona de riesgos de los eventos identificados en la capa de datos y aplicación.

Del anterior diagrama se observa un nivel de riesgo considerable en los escenarios que corresponden:

- Validación.
- General de la aplicación.

Por lo anterior, se deberá poner especial atención a minimizar estos riesgos durante la Jornada Electoral.

13. Conclusiones

En el presente documento se presentaron los resultados más relevantes del proceso de Auditoría al Sistema Informático y a la Infraestructura Tecnológica del Programa de Resultados Electorales para el Proceso Electoral Ordinario Local 2020-2021 (PREP) llevado a cabo entre el 5 de marzo y el 5 de junio de 2021.

Este documento es uno de los entregables acordados para la prestación de tales servicios entre el Ente Auditor y el Instituto Electoral de Tamaulipas. La documentación complementaria explica a detalle cada una de las actividades, metodologías, resultados, hallazgos y análisis de información realizados.

Durante el proceso de auditoría se tuvo una comunicación fluida con el personal desarrollador del PREP del Instituto Electoral de Tamaulipas, quienes mostraron en todo momento disposición para proporcionar la información requerida.

Se han documentado observaciones específicas sobre algunos aspectos relacionados con el Proceso Técnico Operativo, sobre algunas funcionalidades del sistema informático del PREP, sobre la base de datos que lo compone, y en términos generales se han atendido la mayor parte de ellas. Existe una cantidad de elementos mejorables que se han reportado en la documentación complementaria, las cuales no son críticas para la operación del PREP y son consideradas como áreas de oportunidad para procesos futuros.