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 2019

Informe Final de Auditoría al PREP 2019

V0.1

Ciudad Victoria, Tamaulipas. 1 de junio de 2019

Versión	0.1
Fecha de elaboración	Junio 1, 2019

HISTORIAL DE VERSIONES	
Número de Versión	0.1
Fecha de actualización	Junio 1, 2019
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	Líder de la capa 3: Plataforma tecnológica
De la elaboración	Miguel Morales Sandoval/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.
CAE	Capacitador-Asistente Electoral.
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 2019	Programa de Resultados Electorales Preliminares para el año 2019
PREP Casilla	Aplicación móvil que permitirá realizar la toma fotográfica del acta PREP y su envío para su captura.
PROISI	Es la empresa proveedora de servicios que se encargará del programa de resultados electorales.
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 2018-2019 (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 4 de marzo y el 1 de junio de 2019. 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:

LA1. Pruebas funcionales de caja negra al sistema informático del PREP 2019.
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 OPL.

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 para completar el flujo de información de 7 pasos descrito en el párrafo anterior.

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**, comprendida entre el 4 de marzo y el 30 de abril de 2019, realizó los servicios de revisión del sistema completo y la entrega de informes parciales de acuerdo con las líneas de trabajo establecidos en los lineamientos del INE. La

fase 2 preliminar, incluye la revisión de la operación del PREP acorde con las líneas de trabajo identificadas por el INE durante los tres simulacros realizados el 12, 19 y 26 de mayo de 2019.

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. 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 146 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, al primer día del mes de junio de dos mil diecinueve.

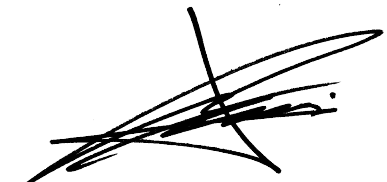
Dr. Javier Rubio Loyola
Ente Auditor
Cinvestav-IPN
Unidad Tamaulipas

Dictamen

Con base en la revisión llevada a cabo entre el 4 de marzo y el 1 de junio de 2019 de la implementación del Proceso Técnico Operativo para el Programa de Resultados Electorales Preliminares del Estado de Tamaulipas para el proceso electoral 2018-2019, 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 2 de junio de 2019.
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 2 de junio de 2019.
3. El procedimiento técnico metodológico también valida que las bases de datos a usar antes del inicio del PREP, el 2 de junio de 2019, 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 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 primer día del mes de junio de dos mil diecinueve.



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

Parte I

Informe Preliminar de Auditoría al PREP 2019

1. Introducción

El 2 de junio de 2019 se llevarán a cabo elecciones locales en el Estado de Tamaulipas como parte del Proceso Electoral Local 2018-2019 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 instrumentado un Programa de Resultados Preliminares (PREP) mismo que el día de la elección tendrá la función de difundir los resultados preliminares (no oficiales) de la elección. La instrumentación del PREP ha iniciado con seis meses de anticipación al día de la jornada electoral y durante dicho periodo se ha llevado a cabo la implementación del PREP, tres simulacros de su operación general, y su operación real en el día de la jornada electoral, la 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. De acuerdo con esta reglamentación, 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 estableció 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 2019, 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.

En este documento, la Unidad Tamaulipas del Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional presenta los resultados del desarrollo de los servicios de auditoría informática al PREP para el año 2019. Los servicios de auditoría han tomado como base a 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 2019 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 las líneas de acción mínimas requeridas por el INE:

LA1. Pruebas funcionales de caja negra al sistema informático del PREP 2019.
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.

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 realizó en dos fases. La **fase 1**, comprendida entre el 4 de marzo y el 30 de abril de 2019, incluyó los servicios de auditoría informática del sistema completo y la entrega de informes parciales de acuerdo con las líneas de trabajo establecidos en los lineamientos del INE. La **fase 2**, incluyó la revisión de la operación del PREP acorde con las líneas de trabajo identificadas por el INE durante los tres simulacros realizados el 12, 19 y 26 de mayo de 2019, el día de la jornada electoral (2 de junio de 2019) y la entrega del informe final (17 de junio de 2019).

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 2.1.

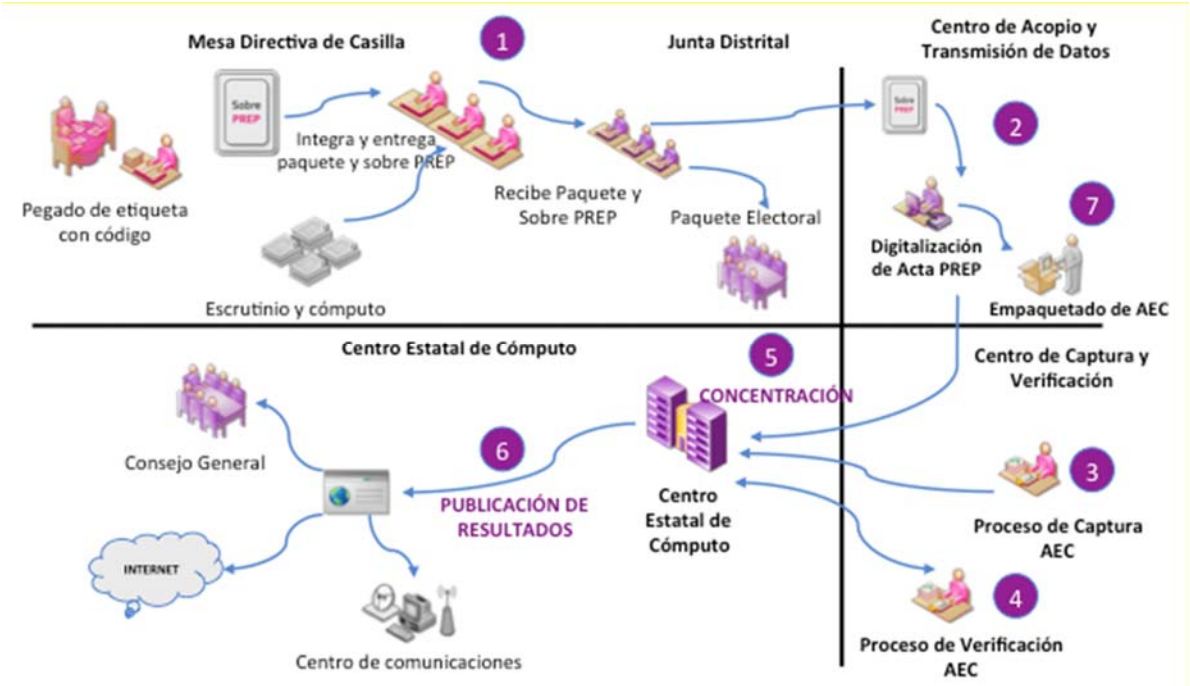


Figura 2.1. Centros de información típicos que participan en el PREP.

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 la Junta Distrital. En el Centro de Acopio y Transmisión de Datos se obtienen copias de las Actas de Escrutinio (AEC), se procede a la digitalización y envío de la información. En los centros de captura y verificación se procede a la captura de la información obtenida en la copia digitalizada del Acta y se realiza la verificación de los datos capturados. Los datos verificados del acta son transmitidos (concentrados) en el Centro Estatal de Cómputo para procesamiento, contabilización, almacenado y conservación.

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 2.2. 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 acopia 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 IETAM y hacia los difusores previamente autorizados por el IETAM. 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, ciframiento de comunicaciones, por citar algunos de los más usados.

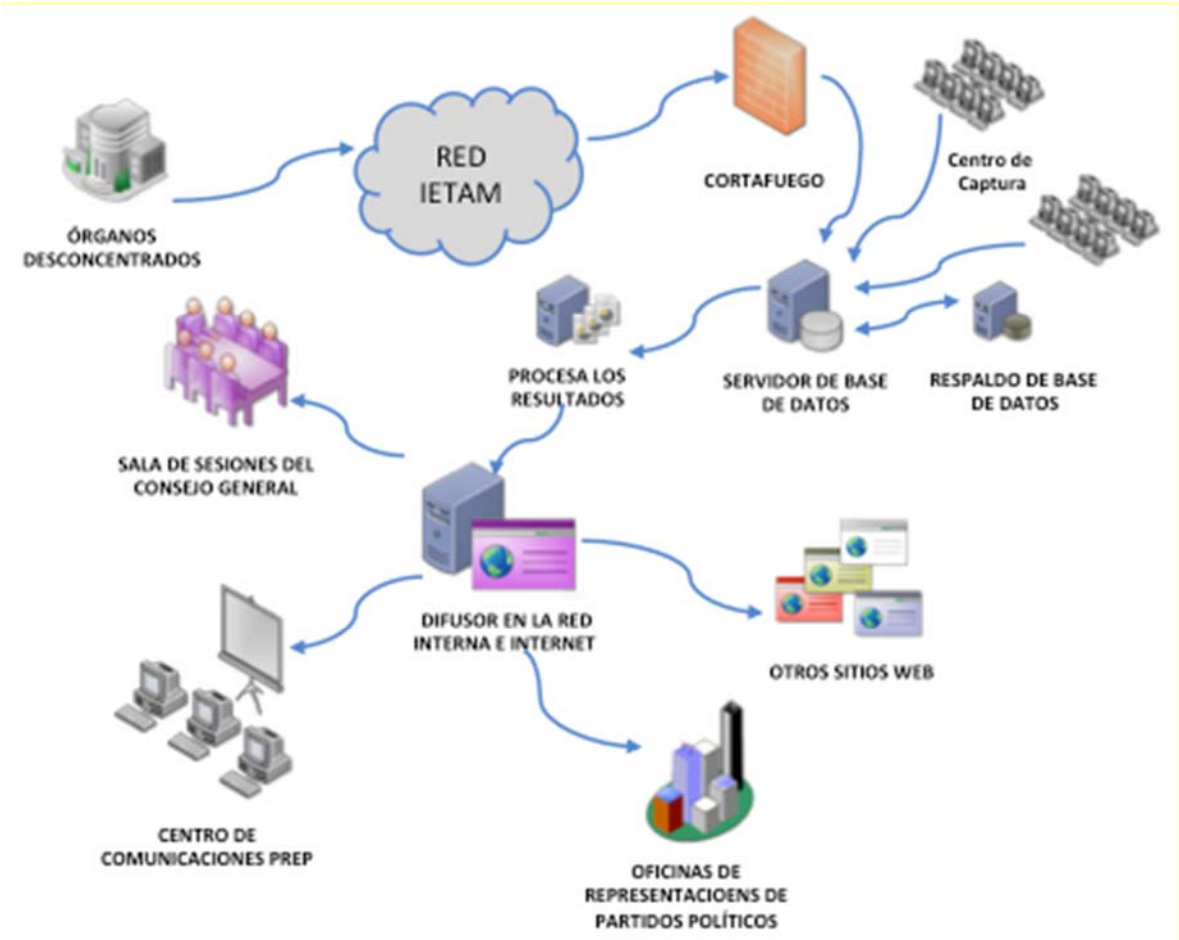


Figura 2.2. Infraestructura típica usada un Sistema PREP.

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 permita la verificación y análisis de los sistemas informáticos que se utilizan 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 que:

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:

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 al menos pruebas de penetración y revisión de configuraciones a la infraestructura tecnológica del PREP.

El personal del ente responsable de llevar a cabo la auditoría debe demostrar contar con experiencia en auditorías a sistemas informáticos, conforme a lo establecido en el párrafo anterior, así como apegarse a una metodología y conducirse con imparcialidad.

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

El Instituto Nacional Electoral en su documento "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", establece cuatro líneas de acción mínimas para llevar cabo los servicios de auditoría al PREP que se describen a continuación:

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. El ente auditor 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 tendrá que realizar al inicio, durante y al final de la operación del sistema informático del PREP.

LA3. Análisis de vulnerabilidades a la infraestructura tecnológica. El Ente Auditor identifica las debilidades de seguridad en la infraestructura tecnológica mediante la ejecución de pruebas de penetración y revisión de configuraciones de seguridad. También, 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. El ente auditor verifica que las medidas implementadas por el OPL hayan atendido adecuadamente las vulnerabilidades reportadas.

LA4. Pruebas de negación de servicio a sitios web del PREP y al sitio principal del IETAM. El ente auditor realizar ataques de negación 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.

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 a 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 al 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 a 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. Cotejo de Actas PREP.
6. Publicación de resultados.

Se identificaron los siguientes modelos conceptuales de trabajo para la implementación del PREP:

- 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 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 11/mayo/2019	Pruebas preliminares	Revisión parcial al sistema informático
12/mayo/2019	Simulacro 1	Revisión parcial al sistema informático
19/mayo/2019	Simulacro 2	Revisión parcial al sistema informático
26/mayo/2019	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
1. El CAE se encuentra en la casilla asignada 1.1. El CAE no ha llegado a la casilla asignada 1.2. El CAE se encuentra en una casilla incorrecta 2. Se ha llenado el AEC 2.1. El AEC tiene datos faltantes 2.1.1. El CAE no tiene acceso a los datos faltantes 2.2. La AEC se llenó incorrectamente 3. El CAE tiene acceso al Actas PREP 3.1. El CAE 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 CAE 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 CAE tiene acceso al PREP Casilla
5.1. El CAE no tiene acceso a la aplicación PREP Casilla

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

7. El CAE cuenta con dispositivo móvil para realizar la toma fotográfica
7.1. El CAE no cuenta con dispositivo móvil
7.2 El dispositivo móvil se encuentra descargado
7.3. El CAE 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 CAE ingresa de manera manual los datos de identificación de la casilla en PREP Casilla
9.1. El CAE 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 CAE coloca el Acta PREP de tal forma que no presente dobleces
10.1 El acta sufrió un doblez al momento de acomodarla

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

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

15. El CAE confirma en la aplicación que la imagen es legible
15.1. El CAE 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 CAE 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 CAE visita todas las casillas asignadas 20.1. El CAE no logró visitar todas las casillas asignadas 20.2. El CAE 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 Cotejo de Actas PREP. Capa 5: Nivel Operación.

Cotejo 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

De los casos de uso listados anteriormente 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. Cotejo de Actas PREP (Fig. 5.A.5)
6. Publicación de resultados (Fig. 5.A.6)

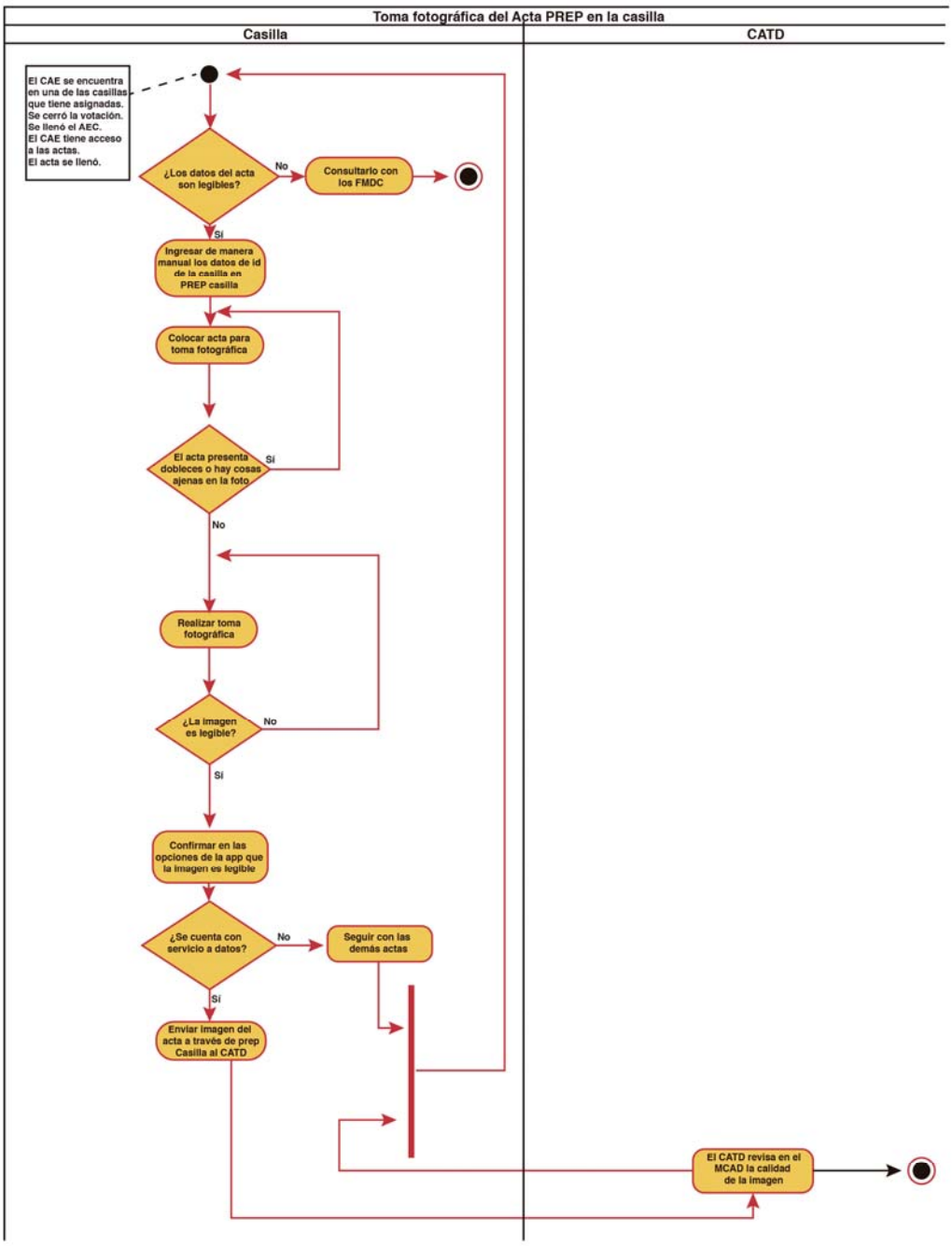


Figura 5.A.1. Toma fotográfica del Acta PREP en casilla.

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

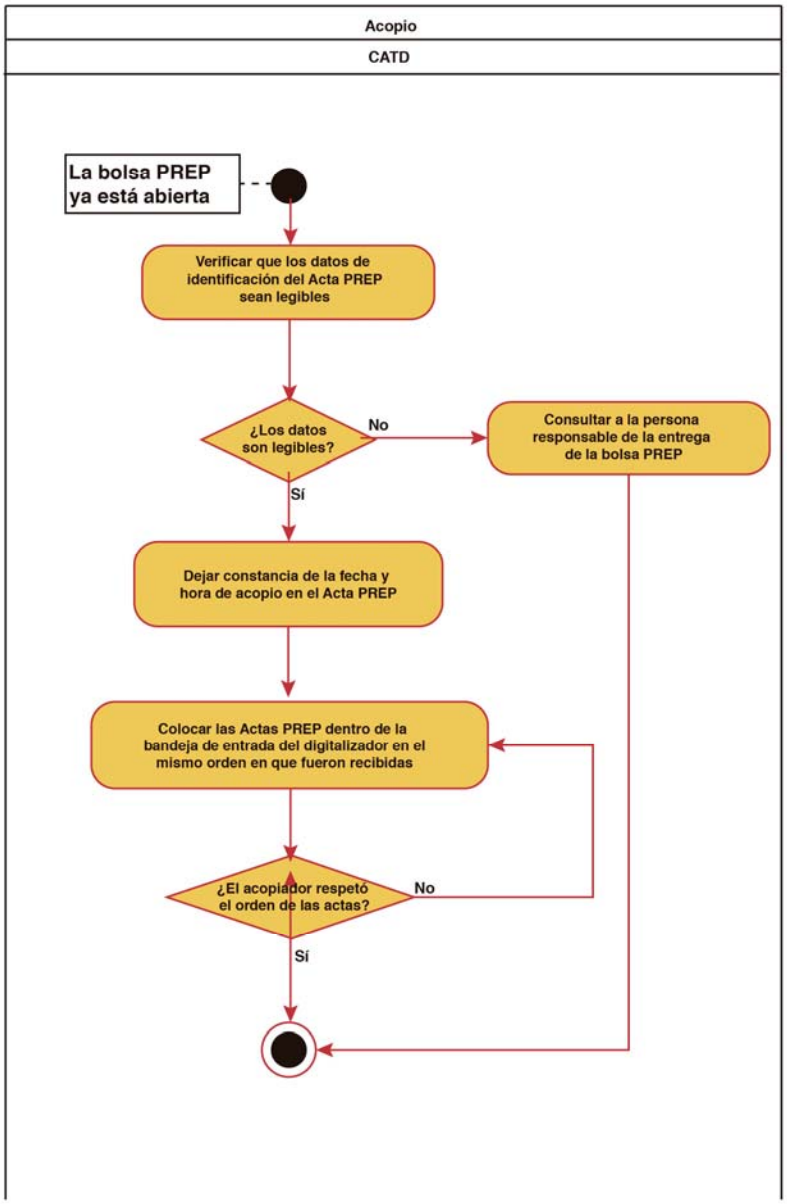


Figura 5.A.2. Acopio de Acta PREP

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

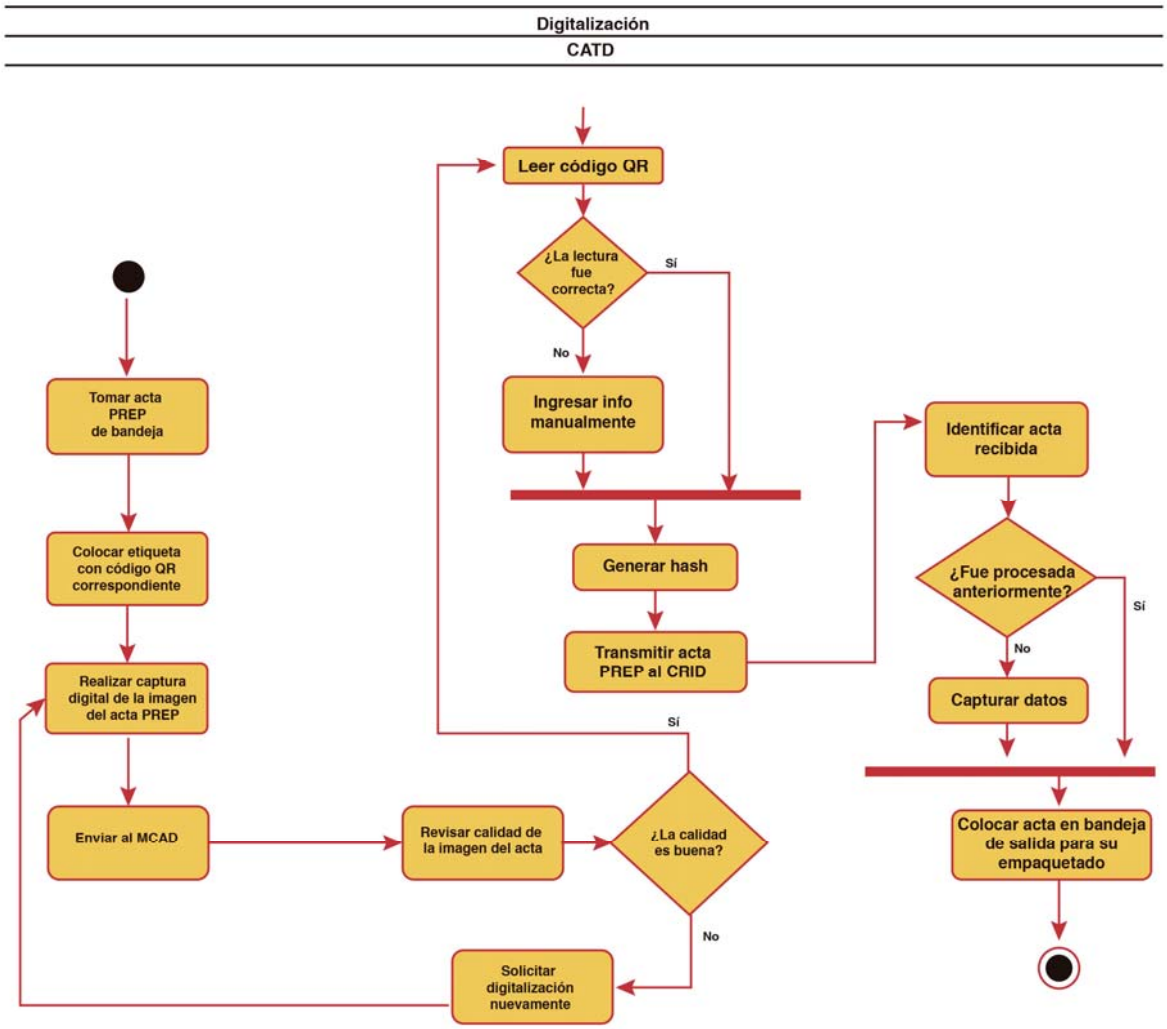


Figura 5.A.3 Digitalización de Acta PREP

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

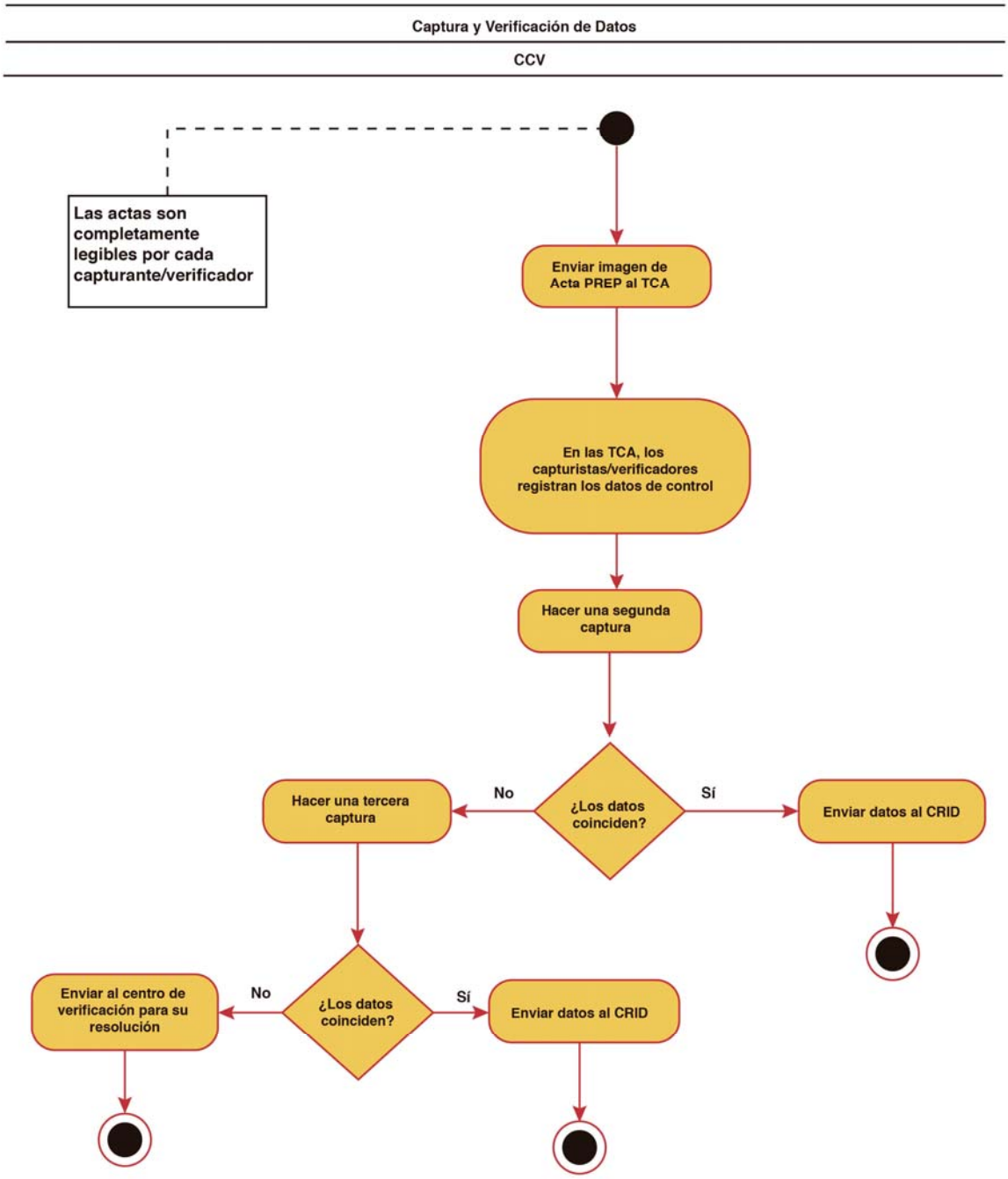


Figura 5.A.4 Captura y verificación de datos de Acta PREP

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

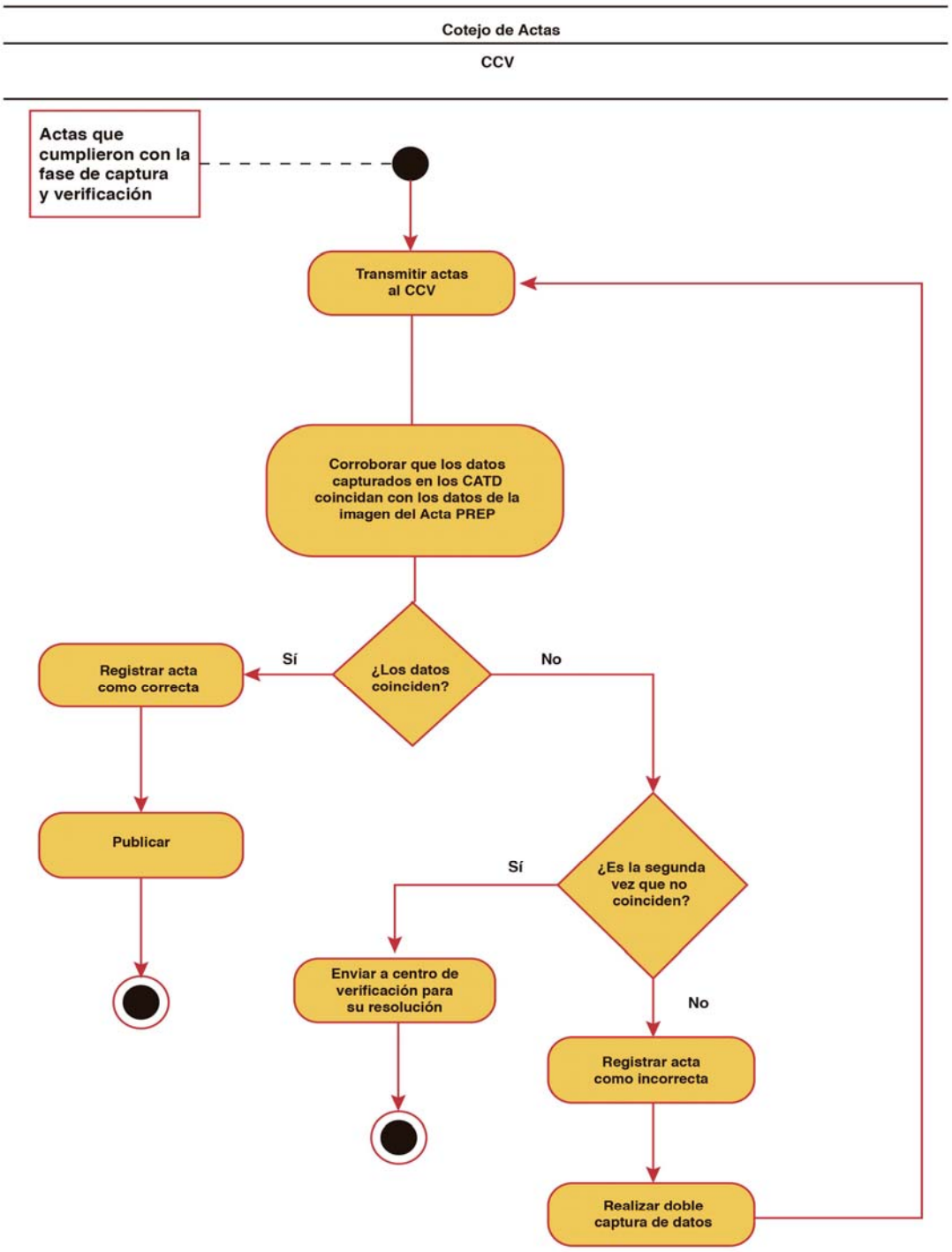


Figura 5.A.5. Cotejo de Actas PREP

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

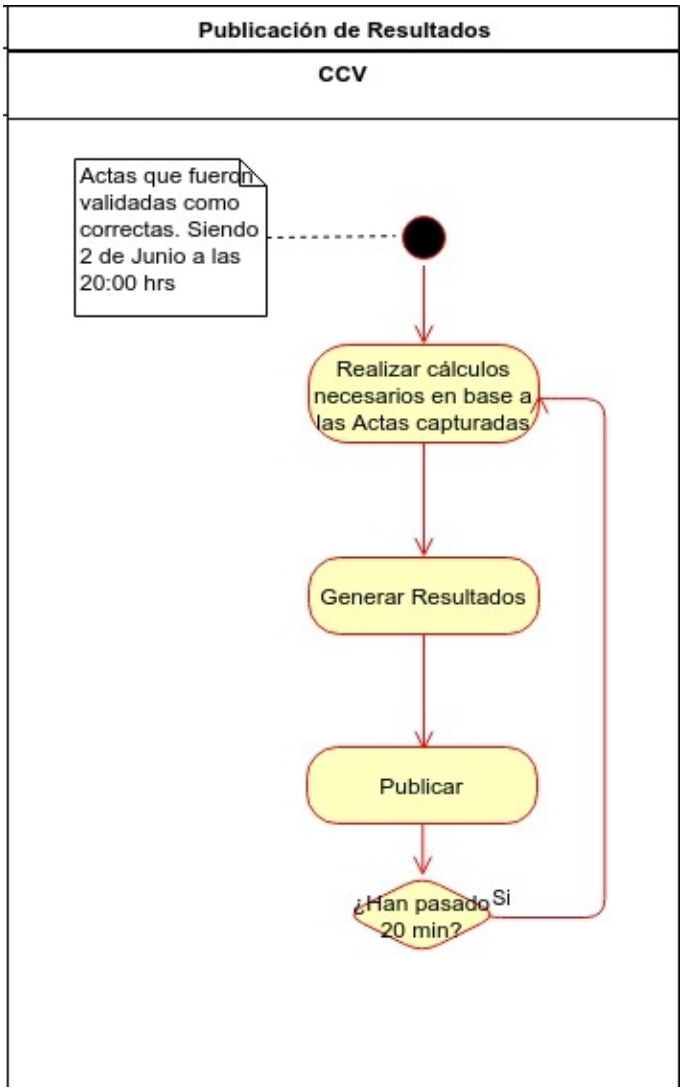


Figura 5.A.6. Flujo de información y actividades de la etapa Publicación de Resultados. Capa 5: Nivel Operación.

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 a su rol se listan en la *Tabla 5.B.1*

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

Usuario	Rol	Operación
Usuario 1	CAE	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 CAE se encuentra en la casilla asignada 1.1. El CAE no ha llegado a la casilla asignada 1.2. El CAE se encuentra en una casilla incorrecta 2. Se ha llenado el AEC 2.1. El AEC tiene datos faltantes 2.1.1. El CAE no tiene acceso a los datos faltantes 2.2. La AEC se llenó incorrectamente 3. El CAE tiene acceso al Actas PREP 3.1. El CAE 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 CAE visita todas las casillas asignadas 20.1. El CAE no logró visitar todas las casillas asignadas 20.2. El CAE 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 Cotejo de Acta PREP en Capa 5: Nivel Operación.

Cotejo 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 CAE tiene acceso al PREP Casilla 5.1. El CAE no tiene acceso a la aplicación PREP Casilla 11. El CAE 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 Cotejo de Acta PREP en Capa 5: Nivel Operación.

Cotejo 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 a su rol para Capa 5: Nivel Operación.

Usuario	**Rol**	**Requerimientos de Operación**
Usuario 1	CAE	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 Cotejo de Acta PREP en Capa 5: Nivel Operación.

Cotejo 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	CAE	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 CAE 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 Cotejo de Acta PREP en Capa 5: Nivel Operación.

Cotejo 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

5.6.1 De la toma fotográfica del Acta PREP en la casilla

Comentario general:

La fase de toma fotográfica no se auditó debido a que no se contaba con lo necesario, ya que el INE había solicitado al proveedor unos cambios en la aplicación y en el dispositivo celular. El medio de verificación (MV) de esta etapa es el formulario F5-A-1_1 y F5-A-1_2.

1. La toma fotográfica del Acta 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 CAE se encuentra en una de las casillas que tiene asignadas.
   b) Se haya cerrado la votación.
   c) Se haya llenado el AEC, conforme se establece en el Programa de Asistencia Electoral del Proceso Electoral Federal 2018-2019.
   d) El CAE tenga acceso al Acta PREP siempre que no haya sido guardada 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) Entidad federativa.
   b) Distrito electoral local.
   c) Municipio.
   d) Sección.
   e) Tipo y número de casilla.

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

3. El CAE deberá verificar que los datos de identificación del ACTA PREP sean legibles, en caso contrario deberá consultarlo con los FMDC para su correcta identificación.

4. El CAE deberá pegar la etiqueta con el código QR en el lugar destinado para ello en el Acta PREP, con lo que la aplicación realizará la identificación automática de la casilla. Si por cualquier razón el CAE no contará con la etiqueta con el código QR, este deberá ingresar de manera manual los datos de identificación de la casilla en PREP Casilla.

5. El CAE 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 CAE realizará la toma fotográfica del Acta PREP y verificará que la imagen sea legible.

7. El CAE 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 MCAD del CATD correspondiente.

   Si no se cuenta con servicio de datos para el envío de la imagen del Acta PREP, el CAE podrá continuar con la toma fotográfica del Acta PREP de la siguiente casilla y en cuanto se tenga conexión al servicio de datos intentar nuevamente su envío.

9. Para los casos en los que el CAE 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 Municipal correspondiente, el Acta PREP de esas casillas se procesará conforme a las demás fases del presente proceso técnico operativo.

5.6.2 Del Acopio

Comentario general:

El acopiador, a su vez se le asigna el rol de coordinador. 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 supervisor por parte del proveedor le brindará apoyo. El acopiador es el encargado del flujo de actas. 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. El medio de verificación (MV) de esta etapa es el formulario F5-A-2_1 y F5-A-2_2.

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

    Comentarios: El oficial encargado del CATD será quien entregue la Bolsa-PREP correspondiente al acopiador. El oficial puede ser quien saque el Acta PREP de la Bolsa-PREP y se la entregue al acopiador.

11. 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 en el Acta PREP deberá de comunicárselo al presidente de casilla.

12. El acopiador dejará constancia de la fecha y hora de acopio en el Acta PREP.

    Comentarios: El acopiador se encarga de dejar constancia de la fecha y hora. La hora y minuto en el momento en que recibe el Acta PREP.

13. El acopiador deberá para efectos de identificación digital, colocarle al Acta PREP, la etiqueta con el código QR correspondiente en el recuadro superior, destinado para ello.

Comentarios: El acopiador no realiza la tarea de colocar el código QR, debido a que el código QR ya se encuentra impreso en el Acta PREP.

14. El acopiador colocará las Actas PREP dentro de la bandeja de entrada del digitalizador en el mismo orden en que fueron recibidas.

Comentarios: El acopiador no coloca las actas en la bandeja de entrada, el se encarga de entregarlas personalmente al digitalizador.

5.6.3 De la Digitalización

Comentario general:

El digitalizador deberá de contar con un gafete de identificación. El digitalizador recibirá el Acta PREP de manera personal mediante el acopiador. El digitalizador deberá de contar con las credenciales necesarias para el sistema, 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 su supervisor encargado. En caso de ser necesario, el equipo multifunción para la digitalización puede cambiarse. Si el digitalizador tiene alguna duda acerca del proceso a realizar, deberá de pedir ayuda a su supervisor, o revisar el manual de usuario que se le fue otorgado. El digitalizador obtuvo la capacitación necesaria para realizar el proceso. El rol de digitalizador y capturista lo realiza una misma persona, a excepción del capturista de PREP Casilla. El medio de verificación (MV) de esta etapa es el formulario F5-A-3_1 y F5-A-3_2.

15. El digitalizador realizará la captura digital de la imagen del Acta PREP, por medio de equipos multifunción o escáner, para su envío al MCAD.

Comentarios: El digitalizador realizará la captura digital del Acta PREP mediante el equipo asignado, en el sistema puede cambiar la posición de la imagen del Acta PREP, con tal de tener un mejor entendimiento de esta. Si por alguna razón el equipo de escáner deja de funcionar existe en el sistema una opción para poder importar una imagen que se encuentre almacenada en el ordenador. También se tiene la opción de almacenar la imagen escaneada del Acta PREP en la computadora.

16. El digitalizador revisará en el MCAD la calidad de la imagen del Acta PREP digitalizada. En caso de requerirse, la digitalizará nuevamente.

Comentarios: El digitalizador deberá de revisar la imagen digitalizada en el MCAD del sistema, si es necesario puede digitalizarla nuevamente.

17. Cuando el MCAD no realice una lectura correcta del código QR se ingresará la información de manera manual en el MCAD. La fecha y hora de recepción para las actas acopiadas en el CATD será ingresada en el MCAD por el digitalizador tomando la hora especificada en el Acta PREP por el acopiador.

Para las imágenes recibidas por PREP Casilla la fecha y hora de acopio será la misma que la de la toma fotográfica realizada a través de PREP Casilla.

Comentarios: El acopiador pone como prioridad el ingresar la información de manera manual, por encima de la lectura del QR, por lo que este proceso siempre se tiene que realizar.

18. A partir de la versión digital del Acta PREP, el MCAD generará de manera única y automática el hash y transmitirá el Acta PREP al CRID para iniciar el proceso de captura de datos.

    El CRID, de manera automática, identificará, con la imagen recibida de PREP Casilla, si el Acta PREP digitalizada fue procesada anteriormente, si es el caso, no se procesará para la captura de datos.

    Comentarios: Queda pendiente de verificar la generación del hash.

19. Concluida la fase de digitalización, deberá colocarse el Acta PREP en la bandeja de salida para su empaquetado.

    Comentarios: El digitalizador deberá de entregar el Acta PREP al acopiador, y el será el encargado de el empaquetado del acta.

5.6.4 De la Captura y Verificación de Datos de las imágenes provenientes de PREP Casilla

Comentario general:

Este proceso no se auditó, debido a que no se contaba con lo necesario, ya que el INE había solicitado al proveedor unos cambios en la aplicación y en el dispositivo celular para el uso de PREP Casilla. El medio de verificación (MV) de esta etapa es el formulario F5-A-4_1 y F5-A-4_2.

20. Todas las imágenes que se hayan digitalizado mediante PREP Casilla serán enviadas al CRID, y serán a su vez enviadas para su captura a alguno de los CATD ubicados en el CCV principal y en el CCV de respaldo conforme a la solicitud de los capturistas/verificadores. En caso de que la imagen del Acta PREP sea de mala calidad e imposibilite la captura de datos, el capturista/verificador deberá clasificarla en la TCA como “ilegible”. El sistema enviará automáticamente la misma imagen del Acta PREP a un segundo capturista/verificador. Si en dos ocasiones la imagen se clasifica como “ilegible” se remite al Centro de Verificación para su resolución definitiva. En caso de que se defina que es posible obtener los datos necesarios para capturar, se procederá a su captura, verificación, cotejo y publicación.

5.6.5 De la Captura y Verificación de Datos en el CATD

Comentario general:

El capturista deberá de contar con un gafete de identificación. El capturista deberá de contar con las credenciales necesarias para el sistema, las cuales se le fueron asignadas mediante un papel impreso, cada día son credenciales diferentes. El capturista primeramente deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el supervisor a cargo. El capturista cuenta con un manual de usuario para el uso del sistema. El capturista obtuvo la capacitación necesaria para realizar el proceso. El medio de verificación (MV) de esta etapa es el formulario F5-A-5_1 y F5-A-5_2 .

21. Cada Acta PREP recibida en el CATD que no haya sido previamente capturada por haber sido enviada mediante PREP Casilla, se capturará en una de las TCA disponible.

    Comentarios: El capturista deberá de realizar el registro de todas las actas, si alguna de estas ya fue previamente capturada no le permitirá enviarla al CRID para su verificación.

22. En las TCA, un capturista/verificador registrará los datos correspondientes a los resultados de la votación, boletas sobrantes, total de personas que votaron, total de representantes de partidos políticos, y de candidaturas independientes acreditados ante casilla que votaron y total de votos sacados de la urna.

    Comentarios: El capturista deberá de contar con las credenciales para poder acceder al sistema. El capturista deberá de registrar los datos, tal y como se muestran en la imagen del Acta PREP.

    Concluida la primera captura, el sistema solicitará que el capturista/verificador realice una segunda captura volviendo a capturar 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.

    En caso de que los datos capturados en dos ocasiones no coincidan, el sistema de manera automática reiniciará el proceso de captura hasta que se cuente con una doble captura con datos coincidentes.

    Comentarios: El mismo capturista deberá de realizar un segundo registro de los datos, el cual el sistema lo habilita en automático. Al finalizar el segundo registro de los datos, el sistema realizará una comparación de los datos de los dos registros, si los datos no coinciden el capturista deberá de volver a realizar los dos registros.

23. Concluido el proceso de captura y verificación, los datos se enviarán automáticamente al CRID.

    Comentarios: Los datos y la imagen se envían al CRID del CCV, en el cual se verifica que los datos coincidan con la imagen del Acta PREP.

24. En caso de que los datos contenidos en el Acta PREP imposibiliten la captura de datos, el

capturista/verificador deberá clasificarla en la TCA como "ilegible". El sistema enviará automáticamente la imagen del Acta PREP al CRID, quien a su vez la turnará a alguno de los CATD ubicados en los CCV para intentar su captura y verificación y posterior cotejo. En caso de que en el cotejo se defina que es posible obtener los datos necesarios para capturar, se remite al Centro de Verificación para su resolución definitiva.

Comentarios: El capturista deberá de clasificar el acta como "ilegible" de ser necesario, y automáticamente el sistema inhabilita cualquier opción del registro, se envía al CCV, y un verificador se encarga de validar la información.

5.6.6 Del Cotejo de Actas

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. Si el verificador tiene las credenciales equivocadas deberá de pedirle ayuda al supervisor. 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. En el CCV1 todos los operadores fueron capacitados para los roles de verificador 1, verificador 2 y capturista de PREP Casilla. En el CCV2 solo se cuenta con el rol de verificador 1.El medio de verificación (MV) de esta etapa es el formulario F5-A-6_1_1, F5-A-6_1_2, F5-A-6_2_1 y F5-A-6_2_2.

25. 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 el cotejo de la información de todas las Actas PREP capturadas en los CATD.

    Comentarios: Las actas son transmitidas de manera automática al CCV. En algunas ocasiones las actas llegan con retraso al CCV.

26. El personal asignado al cotejo de información tendrá como objetivo corroborar que los datos previamente capturados en los CATD, coincidan con los datos de la imagen del Acta PREP de la casilla correspondiente digitalizada en el CATD.

    Si los datos coinciden se registrará el Acta como correcta y se publicará; si se detecta 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 deberá de confirmar su acceso al sistema, y que no exista una falla en la conexión. El primer verificador deberá de verificar que los datos capturados coincidan con los datos asentados del acta. El primer verificador solo tiene la opción de clasificar el acta, en caso de clasificarla como "incorrecta", se va a un segundo verificador. El segundo verificador tiene la opción de modificar los datos si ocurrió algún error en la captura. Si el segundo verificador clasifica el acta como "ilegible" se remitirá al Centro de Verificación para su resolución definitiva, de lo contrario se manda para la publicación.

27. 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: No se lleva una bitácora de las actividades realizadas durante esta etapa.

5.6.7 De la Publicación de Resultados

Comentario general:

En la fase de publicación de resultados se realizó una demostración de ejemplo por parte del proveedor, por lo que no se realizaron algunos pasos, pero se pretende que en la jornada se realice cada uno de ellos. Se tenía un pequeño retraso en la conexión de los datos de 4 a 5 segundos. El medio de verificación (MV) de esta etapa es el formulario F5-A-7.

28. La publicación iniciará a partir de las 20:00 horas (Tiempo del Centro) del 2 de junio de 2019 posterior a la validación del tercero con fe pública de que las bases de datos se encuentran en ceros.

29. 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.

30. 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.

31. Los datos a publicar del Acta PREP, serán aquellos que derivado de su captura y cálculo se obtengan.

32. Para la publicación de porcentajes, los decimales deberán ser expresados a cuatro posiciones. El decimal de la cuarta posición deberá truncarse y no redondearse.

33. Los datos que se capturarán serán los siguientes:
    I. La hora y fecha de acopio del Acta PREP.
    II. Como mínimo, del Acta PREP, se deberá capturar lo siguiente:
    a) Los datos de identificación del Acta PREP
    b) 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;
    c) Los votos obtenidos por los partidos políticos y las candidaturas, sea estas independientes, por partido político, por candidatura común o por coalición.
    d) Total de votos, total de votos nulos y total de votos para candidaturas no registradas, y
    e) La imagen del Acta PREP

34. Los datos a calcular, en cada nivel de agregación serán los siguientes:
    I. Total numérico de actas esperadas;
    II. Total numérico de actas capturadas y su correspondiente porcentaje respecto al total de actas esperadas;
    III. Total numérico de actas contabilizadas y su correspondiente porcentaje respecto al total de actas esperadas;
    IV. Total de actas fuera de catálogo;
    V. El porcentaje calculado de participación ciudadana;
    VI. Total de votos por AEC, y
    VII. Agregados a nivel municipal, sección y acta, según corresponda.

35. Los datos a publicar serán al menos los siguientes:
    I. Lista nominal;
    II. Lista nominal de las actas contabilizadas;
    III. Participación ciudadana;
    IV. Datos capturados, en el caso del total de votos asentado, únicamente se publicará en la base de datos descargable del portal del PREP. Este dato no deberá utilizarse para calcular los agregados publicados en el portal;
    V. Datos calculados;
    VI. Imágenes de las Actas PREP;
    VII. Identificación del Acta PREP con inconsistencias, así como el porcentaje de actas con inconsistencias con respecto al total de actas esperadas;
    VIII. Las bases de datos con los resultados electorales preliminares, en un formato de archivo CSV y de acuerdo a la estructura establecida por el Instituto Nacional Electoral, y
    IX. Hash o código de integridad obtenido a partir de cada imagen de las Actas PREP, con el estándar definido por el Instituto Nacional Electoral.

Para el cálculo del porcentaje de actas con inconsistencias, no se tomarán en cuenta las actas que presenten las inconsistencias que se refieren a la divergencia entre la cantidad asentada en letra y número, así como a las que se refieren a la cantidad de votos que solo ha sido asentada en letra pero no en número o, en número pero no en letra, descritas debido a que los criterios definidos permiten registrar una cantidad de votos en el sistema.

Tampoco se deben tomar en cuenta las Actas que presenten la inconsistencia que se refiere a las actas fuera del catálogo debido a que el universo con base en el cual se calcula este porcentaje es el de las actas esperadas y, por definición, las actas fuera de catálogo no pertenecen al conjunto de actas esperadas.

Asimismo, tampoco se tomarán en cuenta los supuestos en los que el Acta PREP no ha sido entregada junto con el paquete electoral, ni ha sido posible que el Consejo Electoral correspondiente proporcione el AEC o una copia de la misma.
En todos los sistemas informáticos, en los que se reflejen resultados electorales preliminares, deberán presentarse todos los niveles de agregación, teniendo como unidad básica el AEC correspondiente a una casilla aprobaba.

La información deberá publicarse por cada nivel de agregación, es decir por Municipio, sección y acta.

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 cuándo se cumplen 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:
La mayor parte del incumplimiento de los lineamientos del PTO se deben a la falta de capacitación o pericia de los operadores del sistema informático. Esta situación se ha solventado con el desarrollo de los simulacros 1, 2 y 3.
Si bien los operadores tienen las facultades para operar el sistema, no hay un control para saber si lo están haciendo bien o no. No hay 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.
Si bien el sistema informático cumple la mayoría de los lineamientos del PTO, algunos aspectos del diseño y funcionamiento del sistema informático hacen que algunos lineamientos no se cumplan. La versión final del sistema informático resuelve en su totalidad los aspectos funcionales requeridos en el PREP.
El sistema informático podría contar con módulos adicionales que faciliten conocer algunos aspectos que no están claros actualmente cómo se realizan o qué es lo que sucede en el funcionamiento del sistema. Esto observación ha quedado como recomendación para versiones futuras del PREP

Parte III

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

Este documento describe el informe de 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 y por el proveedor de servicios.
- 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 mencionados. En particular se visitaron los siguientes lugares:

1. **CCV -** Oficinas IETAM centro, 13 y 14 Morelos, Ciudad Victoria, Tamaulipas.
2. **CATD 1 -** Consejo Distrital 15, Calle 10 y Ceros Hidalgo No. 2721 entre 10 ceros (José Vasconcelos) y 11 ceros (Artemio del Valle), Col. Tamaulipas, Ciudad Victoria, Tamaulipas.
3. **CATD 2 -** Consejo Distrital 14, Boulevard Enrique Cárdenas González No. 1207 Fracc. Valle De Aguayo entre Juan C. Doria y Filósofos, Ciudad Victoria, Tamaulipas

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 insumos:

- 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 aplicó realizar 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.

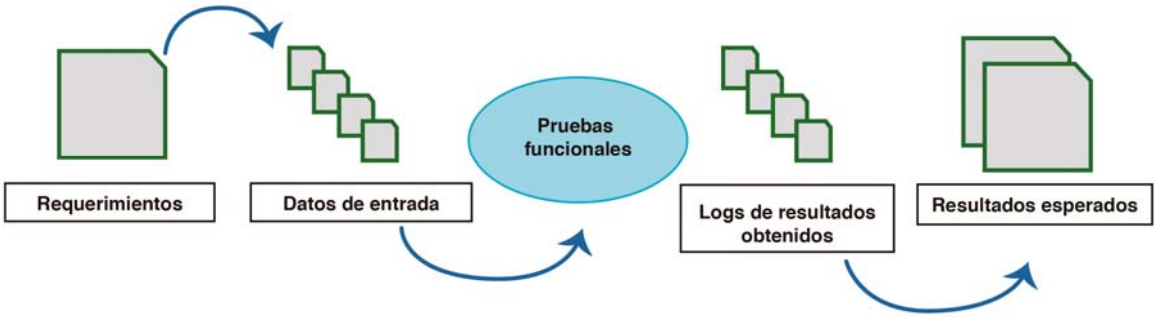


Figura 6.1 Flujo general para la validación de los requerimientos funcionales, nivel base de datos.

- 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.

Dado que el proveedor del sistema no proporcionó los insumos requeridos, se optó por aplicar alternativamente la siguiente metodología basada en los siguientes 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 servicios web 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 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.

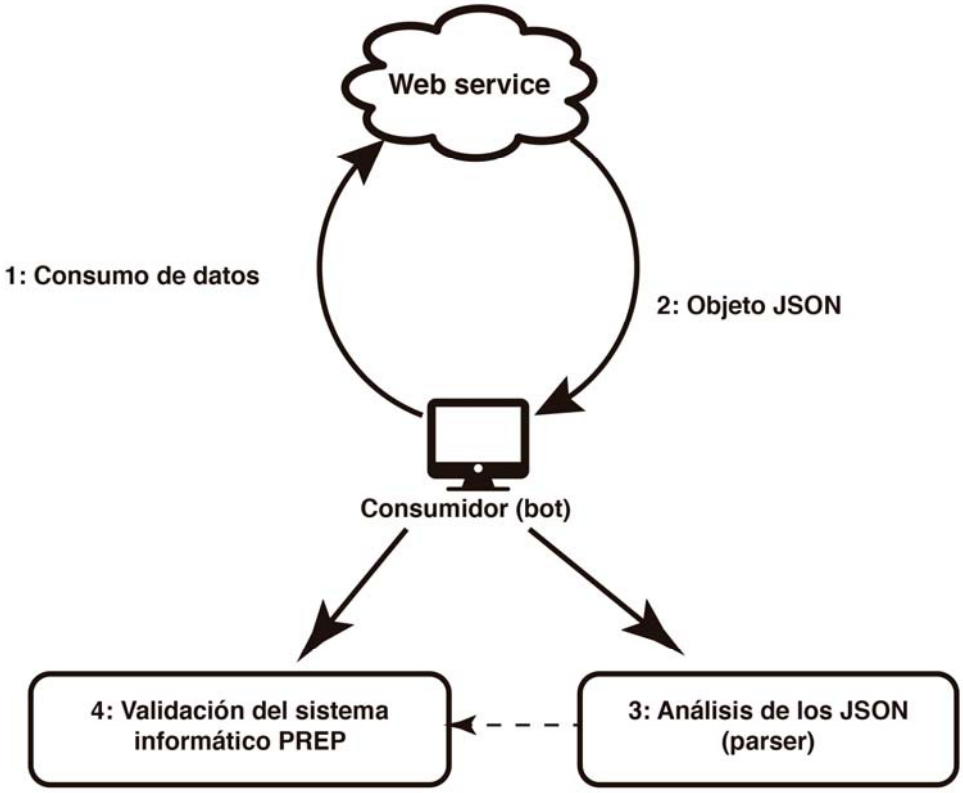


Figura 6.2 Flujo general para la validación de los requerimientos funcionales a través de la información del log del web service, nivel base de datos.

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 al parecer 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	Se observó que cuando se desea cambiar el escáner predeterminado, es necesario reiniciar y autenticarse en la aplicación.
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 de que los datos capturados fueron enviados correctamente.	1. Los rangos de fecha deberían estar acotados a los días de la jornada electoral. Es posible ingresar fecha posteriores y anteriores a la jornada electoral.

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. 2. Cuando se cierra abruptamente la aplicación (navegador) el acta en proceso se pierde.	1. No existe un mecanismo eficiente para la recuperación del sistema ante eventos inesperados (cierres de sesión, terminación de aplicación). El acta queda en un estado inválido que tiene que restaurarse a través de procesos manuales por el administrador del sistema. 2. Los datos de sesión de usuario se mantienen a pesar de cerrar la ejecución del

ID PRUEBA	DESCRIPCION	DATOS ENTRADA	ACCIONES EJECUTADAS	RESULTADOS ESPERADOS	RESULTADOS OBTENIDOS	OBSERVACIONES
						navegador o apagar la computadora.
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 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 describe los análisis que realizaron al Simulacros 1 y las observaciones que se realizaron para el Simulacro 2 y Simulacro 3.

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

Tabla 6.2. Resultados de pruebas funcionales de la base de datos del PREP en Simulacro 1

ID PRUEBA	OBSERVACIONES	CRITERIOS DE ACEPTACIÓN	SUGERENCIA
PF1. 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 1, el proveedor creó un inventario del código fuente con los archivos que a continuación se enlistan: 1. central.zip Web services de recepción de captura y archivos digitalizados 2. :Ydb-tamps-2019.sql Esquema de la base de datos central del PREP. 3. sitio.zip Archivos de publicación web de resultados preliminares 4. generador.zip Programa de generación de folios y contenidos estáticos El proveedor procedió a utilizar el software de captura de huellas criptográficas se obtuvieron dos archivos (Original y simulacro 1) 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 1.	Los datos publicados deberán ser consistentes y presentados de acuerdo con lo establecido por los lineamientos del IETAM	El proveedor debe inicializar la base de datos en ceros y la generación de las huellas criptográficas del inventario solicitado por el ente auditor. Es necesario que el proveedor coloque todos los archivos del inventario antes de iniciar la prueba ya que el proveedor omitió el archivo llamado Programa Remoto.zip.

ID PRUEBA	OBSERVACIONES	CRITERIOS DE ACEPTACIÓN	SUGERENCIA
PF2. Validación de la información publicada.	En el simulacro 1 realizado el día domingo 12 de mayo del 2019, el corte del sistema PREP en su fase de publicación reportó la captura de 4710 actas. A cada una de las 4710 actas esperadas en el Simulacro 1 le corresponden dos imágenes. El formato de nombres para para las imágenes es el siguiente: NumActa.jpg y NumActa_C.jpg. Se esperaba que en la url compartida por el proveedor se encuentren 9420 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 bueno, sin embargo, es necesario automatizar procesos manuales, por ejemplo cuando las actas entran a un estado inconsistente el proceso para regresarlas a un estado consistente es manual. El uso de dos archivos para un solo evento no parece ser la mejor opción a menos que exista un esquema de mapeo inequívoco que garantice que ambas archivos son tratados como un solo evento en la elección.
PF3. 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 1 rrealizado el día domingo 12 de mayo del 2019. El software en mención reportó que: De las 9420 imágenes esperadas, fueron descargadas con éxito 9395 imágenes. No fue posible descargar 25 imágenes, 11 corresponden al formato NumActa.jpg y las otras 14 imágenes al formato NumActa_C.jpg. El número de actas que cuenta con ambos archivos es 4685. Como resultado 25 actas no fueron publicadas y no se encuentran registros de las mismas.	Los datos publicados deberán ser consistentes y presentados de acuerdo con lo establecido por los lineamientos del IETAM	El uso de dos archivos para un solo evento no parece ser la mejor opción a menos que exista un esquema de mapeo inequívoco que garantice que ambos archivos son tratados como un solo evento en la elección.
PF4. Validación de huella criptográfica.	El software en mención reportó que: De un total de 4710 posibles imágenes con el formato NumActa.jpg, se descargaron 4699. A continuación, se listan los nombres de las 11 actas que no se pudieron ser descargadas junto con la url en la que debía ser colocada. Número de acta Url 4671 https://difusores.prep2019tamps.mx/actas/26/4671.jpg 4673 https://difusores.prep2019tamps.mx/actas/26/4673.jpg 4683 https://difusores.prep2019tamps.mx/actas/26/4683.jpg 4684 https://difusores.prep2019tamps.mx/actas/26/4684.jpg 4691 https://difusores.prep2019tamps.mx/actas/26/4691.jpg 4692 https://difusores.prep2019tamps.mx/actas/26/4692.jpg 4693 https://difusores.prep2019tamps.mx/actas/26/4693.jpg 4694 https://difusores.prep2019tamps.mx/actas/26/4694.jpg 4697 https://difusores.prep2019ta	El sistema deberá garantizar la integridad y consistencia de los datos a través de estrategias que integren personas, tecnología, procesos y buenas prácticas.	Actas faltantes no es aceptable. Se deberían eliminar estos eventos o documentar en forfehaciente la razón por la cual dichos eventos suceden en el software del PREP

ID PRUEBA	OBSERVACIONES	CRITERIOS DE ACEPTACIÓN	SUGERENCIA
	mps.mx/actas/26/4697.jpg 4698 https://difusores.prep2019tamps.mx/actas/26/4698.jpg 4703 https://difusores.prep2019tamps.mx/actas/26/4703.jpg 1.2 Imágenes con formato NumActa_C.jpg De un total de 4710 posibles imágenes con el formato NumActa_C.jpg, se descargaron 4685. A continuación, se listan las 14 imágenes que no pudieron ser descargadas junto con la url en la que debía ser colocada. Número de acta Url 4634_C https://difusores.prep2019tamps.mx/actas/26/4634_C.jpg 4635_C https://difusores.prep2019tamps.mx/actas/26/4635_C.jpg 4636_C https://difusores.prep2019tamps.mx/actas/26/4636_C.jpg 4647_C https://difusores.prep2019tamps.mx/actas/26/4647_C.jpg 4663_C https://difusores.prep2019tamps.mx/actas/26/4663_C.jpg 4664_C https://difusores.prep2019tamps.mx/actas/26/4664_C.jpg 4665_C https://difusores.prep2019tamps.mx/actas/26/4665_C.jpg 4666_C https://difusores.prep2019tamps.mx/actas/26/4666_C.jpg 4667_C https://difusores.prep2019tamps.mx/actas/26/4667_C.jpg 4668_C https://difusores.prep2019tamps.mx/actas/26/4668_C.jpg 4674_C https://difusores.prep2019tamps.mx/actas/26/4674_C.jpg 4695_C https://difusores.prep2019tamps.mx/actas/26/4695_C.jpg 4702_C https://difusores.prep2019tamps.mx/actas/26/4702_C.jpg 4710_C https://difusores.prep2019tamps.mx/actas/26/4710_C.jpg		
PF5. Validación de huella criptográfica.	El software en mención resumió que: De un total de 4710 actas pertenecientes al Simulacro 1, la base de datos contiene 4681 actas. Por lo tanto, hace falta que el Proveedor registre 29 actas en la base de datos. De los 4681 registros en la base de datos hay 1495 registros cuyo valor del campo SHA de la base de datos coincide con el SHA-256 obtenido de algunas de las imágenes descargadas, las otras 3186 no coinciden. Los motivos por los cuales no coinciden las imágenes pueden ser los siguientes: ● El proveedor utilizó diferentes algoritmos de hash para obtener los valores insertados en el campo SHA de la base de datos. ● El proveedor insertó valores incorrectos en el campo SHA de la base de datos. ● El proveedor cargó a la url compartida imágenes diferentes a que las que utilizó para generar el hash insertado en el campo SHA de la base de datos. Al hacer una revisión de los archivos físico de las actas en cuestión se llegó a la conclusión de que dichos archivos habían sido cargados al sistema de publicación con errores (el tamaño de las actas que no pudieron ser validadas por el software era inferior al tamaño promedio de las actas validadas).	Se debe garantizar la imparcialidad en el procesamiento de datos generados por el sistema respecto a afinidades políticas o intereses personales.	Se requiere el Hash de origen capturado por fuente/aplicación que ha creado el acta, así como el hash del acta que ha sido depositada en el repositorio del sistema de publicación. No se deberían presentar inconsistencias con las huellas criptográficas de las actas publicadas por lo que esto implica para el proceso electoral.

ID PRUEBA	OBSERVACIONES	CRITERIOS DE ACEPTACIÓN	SUGERENCIA
	Adicionalmente se pudo comprobar las actas que presentaban estos problemas no se podían leer usando visualizadores de imágenes correspondientes al formato utilizado por el proveedor (JPG)		
PF6. Consistencia e integridad de la información registrada en el log de web service de auditoría	Se detectó que el nombre de origen que viene acompañada cada una de las actividades del log del web services es muy general y se repite en actividades diferentes. Por ejemplo, el origen de las actividades: envió de la imagen a través de la aplicación PREP casilla y la captura de los datos de las imágenes en el TCA web tiene el mismo origen "PREP Casilla"	El sistema deberá garantizar la integridad y consistencia de los datos a través de estrategias que integren personas, tecnología, procesos y buenas prácticas.	El origen que se registra en el log del web service debe registrarse con los nombres de las actividades del proceso técnico operativo.
PF7. 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.	Los datos publicados deberán ser consistentes y presentados de acuerdo con lo establecido por los lineamientos del IETAM	N/A
PF8. Análisis de comportamiento.	Para el simulacro 1 Aunque el ente auditor desarrolló un software para realizado el análisis de líneas de tiempo de las actas publicadas por el PREP, así como las etapas por las cuales las actas transitan durante el proceso de elección, Este software no se ha corrido aún debido a que el proveedor ha cambiado el servicio Web de logs en algunas de sus características y el software aún se debe adecuar a dichos cambios.		N/A

Sugerencias en base a pruebas funcionales de base de datos del PREP en Simulacro 2

- Antes de iniciar el simulacro 2, el Proveedor mostró que el inventario de archivos a los cuales se le calculó las huellas criptográficas contiene cinco archivos. Sin embargo, el Proveedor no mostró el proceso, script o método utilizado para recolectar, comprimir sus aplicaciones y generar los archivos comprimidos. No fue posible entonces, por parte del ente auditor dar fe de que el contenido de los cinco archivos de los cuales se calcularon las huellas criptográficas y que las mismas correspondan a las aplicaciones utilizadas. Se recomienda que el proveedor muestre el contenido de los scripts utilizados para colectar los archivos del inventario y ejecute dicho script en presencia del Ente auditor antes del inicio del siguiente simulacro, así como la Jornada Electoral.
- Durante el simulacro 2, el proveedor omitió el paso de generar las huellas criptográficas "originales" e inició con la generación de las huellas iniciales. Debido a esta acción del proveedor, fue necesario realizar la validación de las huellas iniciales del simulacro 2 consigo mismas y así poder generar la constancia de hechos inicial, también fue necesario utilizar las huellas del inicio del simulacro como si fueran las huellas "originales" con la finalidad de poder generar las constancias de hechos intermedia y final. Es necesario que proveedor genere las huellas

criptográficas "originales" antes de iniciar el siguiente simulacro justo después de realizar la recolección del inventario en parecencia del Ente Auditor. Al inicio del simulacro se realizará por segunda vez las huellas del inventario, dichas huellas serán utilizadas para compararlas con las huellas originales obtenidas antes de iniciar el simulacro. Se adjuntan como anexo las constancias pertenecientes al Simulacro 2.

- Durante el análisis de los archivos correspondientes a las actas registradas durante el simulacro dos, no fue posible realizar la descarga de múltiples imágenes. Se recomienda que el proveedor realice la carga de las fotografías e imágenes de todas las actas o indicar el motivo por el cual no se encuentran disponibles.
- Durante el análisis de las actas registradas en la base de datos junto con las imágenes descargadas del servicio del proveedor (fotografías e imágenes escaneadas), no fue posible identificar la imagen de 27 actas marcadas como contabilizadas ni 1 marcadas como no contabilizadas (adicional a las 6 marcadas como sin acta en la base de datos). Se recomienda que el proveedor realice la carga de todas las imágenes correspondientes al SHA registrado en la base de datos debido a que si carga una imagen distinta no será posible realizar la validación de las mismas.

Sugerencias en base a pruebas funcionales de base de datos del PREP en Simulacro 3

- Al inicio del simulacro 3, el *proveedor* no incluyó el script utilizado para la recolección y compresión de sus aplicaciones en la carpeta creada para la concentración del inventario. En el transcurso del simulacro 3, el *proveedor* compartió dicho *script* a través de correo electrónico y el *Ente Auditor*, al revisarlo, acordó que el contenido del *script* era adecuado para llevar a cabo la recolección y compresión de las aplicaciones y servicios que hacen parte del PREP.
- El *proveedor* ejecutó el software de generación de huellas criptográficas a la carpeta de inventario llamado “original” e informó al *Ente Auditor* que había realizado un cambio en el contenido de dicho inventario. El cambio en cuestión consistía en que el archivo “logs.zip” contenía un script en lugar del contenido comprimido del archivo “log.txt”, los cuales deberían ser iguales en principio. Además, el *proveedor* indicó que la huella criptográfica del archivo “logs.zip” no debía cambiar durante la captura de las huellas criptográficas posteriores a la original. En respuesta a los cambios realizados por el *proveedor*, el *Ente Auditor a su vez,* realizó los cambios necesarios en software de obtención de huellas criptográficas para que reflejara el cambio que el *proveedor* había realizado. Se recomienda que el *proveedor* notifique con anticipación al *Ente auditor* los cambios en el inventario que desee realizar y se solicita que el *proveedor* proporcione la descripción actualizada del archivo “logs.zip”.
- Durante la generación de la constancia de hechos inicial, el software de verificación de huellas criptográficas que compara las huellas criptográficas originales con las huellas del software a utilizar en el simulacro, etiqueto **seis** archivos como “No validado” de los diez archivos almacenados en el inventario, lo que significa que las huellas criptográficas de esos seis archivos no coincidían con las huellas criptográficas originales capturadas antes de iniciar el simulacro y que hacen parte del inventario etiquetado como “Original”. Las inconsistencias detectadas fueron observadas por el software en la constancia de hechos. El *proveedor* realizó un análisis de los archivos recolectados y llegó a la conclusión de que la inconsistencia fue producida por archivos temporales que se guardaron dentro de los archivos comprimidos. Después de corregir el error, el *proveedor* volvió a realizar la recolección y generación de huellas criptográficas originales e iniciales. El software del *Ente Auditor* generó la constancia de hechos inicial nuevamente. En la nueva constancia de hechos, el software no observó inconsistencias marcando a cada uno de los archivos del inventario auditado como “Correcto”.

- En la dirección url https://difusores.prep2019tamps.mx/entregables/38/ proporcionada por el *proveedor* para la descarga de la base de datos, se encontraba un archivo llamado "20190525_2237_PREP.zip" el cual fue generado el día 25 de mayo a las 10:37 pm, por lo cual se asume que dicho archivo fue generado antes de iniciar el *Simulacro 3 (específicamente un día antes del simulacro)*. Lo anterior representa una inconsistencia ya que se espera que el dicha URL no contenga ningún archivo. Al realizar el corte inicial de la base de datos, se generó el archivo "20190526_1041_PREP.zip". Debido a que no se esperaba la existencia de más de un archivo en esta etapa inicial del Simulacro 3, fue necesario realizar un análisis por parte del *Ente Auditor* del contenido del archivo cargado antes del simulacro 20190525_2237_PREP.zip contra el respaldo de la base de datos inicial 20190526_1041_PREP.zip generado por el PREP. Lo anterior con el fin de verificar que realmente se encontrará vacía. Después del análisis del contenido de los dos archivos, el *Ente auditor* llegó a la conclusión de que la base de datos inicial 20190526_1041_PREP.zip se encontraba vacía. Se le recomienda al *proveedor* realizar una revisión del contenido de sus sistemas de archivos para evitar que se repitan este tipo de inconsistencias debido a que no deberían existir archivos en la carpeta del URL de difusores (https://difusores.prep2019tamps.mx/entregables/38/), lo anterior sería trivial tomando en cuenta que el PREP incluye botones para el "borrado y/o puesta en ceros de la base de datos".
- Durante el análisis de los archivos correspondientes a las actas registradas durante el Simulacro 3, no fue posible realizar la descarga de múltiples imágenes (adicionales a las marcadas como "Sin acta" en la base de datos). Se recomienda que el *proveedor* realice la carga de las fotografías e imágenes de todas las actas, de no ser posible debe de indicar el motivo por el cual no se encuentran disponibles. Durante el análisis de las actas registradas en la base de datos junto con las imágenes descargadas del servicio del proveedor (fotografías e imágenes escaneadas) correspondientes al Simulacro 3, no fue posible identificar las imágenes de 193 actas marcadas como "contabilizadas" ni 8 marcadas como "no contabilizadas" (adicional a las 4 actas marcadas como "sin acta" en la base de datos). Se recomienda que el *proveedor* realice la carga de todas las imágenes correspondientes al SHA registrado en la base de datos, debido a que si carga una imagen distinta, al generar el SHA de la imagen descargada se obtendrá un SHA diferente al registrado en la base de datos y no será posible realizar la validación de las actas. Para mayor información del análisis de las actas registradas en la base de datos junto con las imágenes descargadas del servicio del *proveedor*.

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

- Si bien existe una aplicación que da inicio al proceso de captura y validación, esta no notifica automáticamente a otros módulos del sistema (por ejemplo PREP-Casilla) cuando dicho proceso ha sido iniciado. La falta de dicha notificación, puede causar desinformación en los usuarios del sistema y la realización de capturas previas al inicio formal de la jornada electoral.

- Durante los procesos de captura, existen algunos eventos excepcionales que no se manejan adecuadamente ocasionando que algunas actas queden temporalmente en estados inconsistentes.
- No existe información descriptiva para los usuarios del sistema que indique la causas y las posibles acciones a ejecutar, cuando un acta se encuentra en estado inconsistente.
- Se recomienda definir un mecanismo automático para la asignación de roles y usuarios al sistema que garantice la autenticación y trazabilidad de las acciones ejecutadas por los usuarios de acuerdo a su rol. En la actualidad dicha asignación involucra actividades manuales que generan algunas vulnerabilidades relativas a la seguridad del sistema.
- A través del proceso de captura y validación sería conveniente incluir algunas verificaciones automáticas (por ejemplo rangos de fechas) que eviten posibles inconsistencias en los datos, ocasionadas ya sea por omisiones de los operadores del sistema o en menor grado algunas posibles acciones mal intencionadas.
- Algunas interfaces de usuario carecen de mecanismos de notificación automática que permitirían incrementar la eficiencia de algunos procesos.Por ejemplo, en el proceso de validación se podría implementar un mecanismo de notificaciones que informe a los validadores cuándo un acta nueva está disponible para validación.
- Existen algunas herramientas por parte del proveedor para hacer seguimiento detallado de algunas variables de control del proceso. Sin embargo seria deseable disponer de un módulo unificado para control y monitoreo (dashboard), que permita desde una sola aplicación controlar actas en estados inconsistentes, acceso de usuarios, métricas de desempeño de los operadores, demanda del sistema, etc. En este mismo sentido se recomienda hace un esfuerzo definir los indicadores o variables de control claves del proceso (KPIs por sus siglas en inglés)
- No es posible garantizar al 100% que las versiones de los componentes del sistema auditados son en efecto los utilizados durante los simulacros de la jornada electoral. Dado que el alcance de la auditoría no obliga a validar las fuentes y código de dichos componentes, seria deseable para futuras jornadas, diseñar e implementar un mecanismo de auditoría que permita dar certeza total de los componentes liberados.
- El proveedor no cuenta aún con un modelo de proceso que permita gestionar y controlar el diseño y desarrollo del sistema (SCRUM, RUP, CMMi, etc.)

Conclusiones Nivel Base de Datos

En general, se concluye lo siguiente:

- El sistema de bases de datos es funcional y permite llevar a cabo la función toral del sistema auditado.
- El sistema de publicación y difusión de resultados es funcional y permite llevar a cabo la función toral del sistema auditado.
- Aunque se han observado obstáculos técnicos para comprobar fehacientemente la generación de huellas criptográficas, estas se han podido verificar satisfactoriamente.

Observaciones:

Sobre el Sistema de bases de datos:

- Se observaron algunos puntos de mejora en el diseño del modelo de datos (normalización, nombrado de tablas y campos).
- No fue posible verificar detalladamente las buenas prácticas de diseño e implementación de los componentes tanto del sistema de bases de datos como como del sistema publicación, lo cual solo fue posible corroborar a través de cuestionarios.

- Aún no existe una separación adecuada entre la capa de aplicación y la capa de datos. El sistema auditado hace uso de procedimientos almacenados que sería conveniente reducir en lo posible para cumplir con buenas prácticas estandarizadas en la industria. En este sentido, utilizar patrones de diseño sería recomendable.
- Se observa que el control sobre las bases de datos remotas se encuentra en cierta forma desacoplado del sistema de bases de datos central.

Sobre el Sistema de publicación y difusión de datos:

- Con la información proporcionada por el proveedor aún no es posible garantizar al 100% la correspondencia entre los datos generados por el proceso operativo y los datos publicados.
- El proveedor ofreció un mecanismo (web service) para auditar algunos elementos del proceso, la información obtenida de dicho mecanismo se encuentra limitada por los usos horarios de los servidores que procesan dichos registros (presumiblemente ubicados en lugares donde los usos horarios difieren de los usos horarios de México), por lo cual no es posible dar un seguimiento riguroso a las etapas por las cuales pasa cada acta digital y los datos a través del tiempo de la jornada electoral.
- No es recomendable que el proveedor defina qué tipo de información es susceptible de ser auditada.
- Las actas registradas en la base de datos de publicación aún no tienen una correspondencia directa con las imágenes del repositorio del sistema de publicación (actas digitales) debido principalmente a los siguientes eventos observados:

  1. En la base de datos de publicación existen registros de imágenes de actas sin huellas criptográficas.
  2. En el repositorio de imágenes del sistema de publicación existen más imágenes de las procesadas.
  3. En los dos casos anteriores aún no existe explicación u observación de por qué no se registró dicha información en el sistema de bases de datos específicamente en el servicio de logs entregado por el proveedor (web service).

- El control sobre el manejo de las actas digitales no es riguroso. Lo anterior debido a que el sistema de detección criptográfica del ente auditor encontró alteraciones en las actas digitales. Las alteraciones detectadas criptográficamente en las actas digitales se deben principalmente a procesos realizados por los operadores del sistema y el proveedor justificó cabalmente dichas alteraciones. En consecuencia, se recomienda que el proveedor considere esquemas criptográficos que permitan asegurar que las actas digitales no sean alteradas y/o modificadas desde origen, a través de las etapas y en lugar final donde son preservadas. En caso de que las alteraciones sean inevitables, se recomienda generar registros inmutables de las alteraciones realizadas en cada etapa indicando cada proceso o usuario que realice cada alteración con el fin de justificar cabalmente cada alteración en forma automática.

Sobre la generación de huellas criptográficas:

- Aunque existió reticencia por parte del proveedor para realizar procesos automáticos para la generación de huellas criptográficas sobre el código del sistema auditado, el proveedor ha accedido a compartir con el ente auditor sus procesos de colección de los componentes del sistema auditado, los cuales han permitido al ente auditor tener garantías básicas para llevar a cabo la generación de huellas criptográficas, la comprobación de estas, la realización del correspondiente proceso de validación y generación las constancias de hechos.

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.

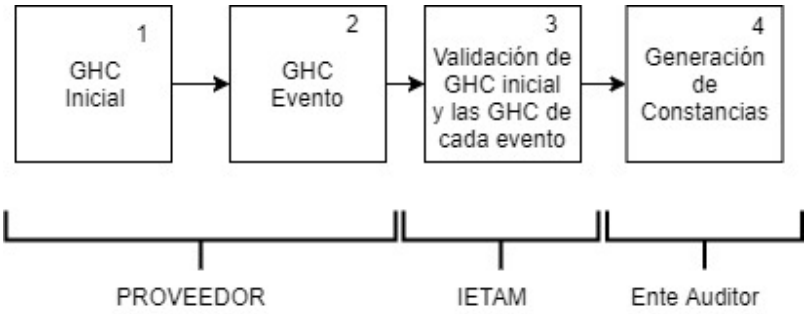


Figura 7.1. Diagrama de Flujo 1 Flujo general de trabajo para la validación de la información inicial y final de la base de datos y del software instalado en el ambiente productivo que operará en día de la jornada electoral.

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).

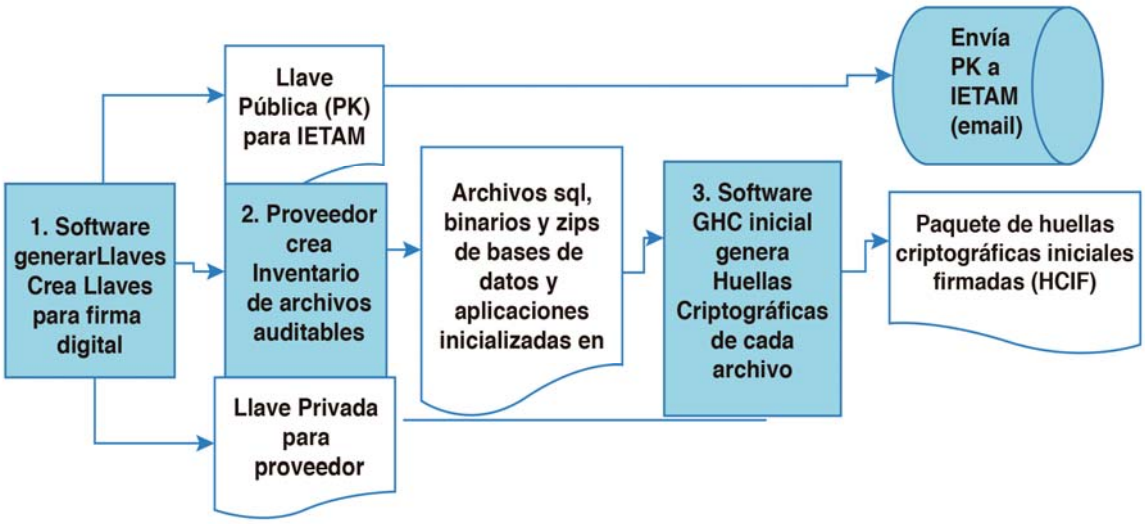


Figura 7.2 Diagrama de Flujo 2 Flujo de trabajo para la generación de huellas criptográficas iniciales de archivos del inventario firmadas por el proveedor.

El software generar llaves depositará la llave SK en el lugar donde el proveedor invocó dicho software, enviará la llave pública a el Ente Auditor y el IETM por correo electrónico y por el último la depositará en el servicio de validación creado por el Ente Auditor.
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).
3. El software ***generarLlaves*** cargará la llave pública (PK) en al servicio de verificación creado por el Ente Auditor y mandará un correo electrónico tanto al IETAM como al Ente Auditor con una liga para descargar la llave pública (PK).

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 1904Proveedor.jar generarLlaves Llavero/ Original.

El software generar llaves depositará la llave SK en el lugar donde el proveedor invocó dicho software, enviará la llave pública a el Ente Auditor y el IETM por correo electrónico y por el último la depositará en el servicio de validación creado por el Ente Auditor. Donde java -jar 1904Proveedor.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.
La siguiente lista comprende los archivos de base de datos y sistema de archivos que se solicita al PROVEEDOR para su firma.

1. Base de datos *Maestra 1* vacía e inicializada, el PROVEEDOR realizará un dump de la base de datos, 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_solictado.sql) o en su defecto se debe de realizar una exportación de la base de datos en un ambiente gráfico, el resultado será un archivo sql que el PROVEEDOR nombrará el archivo como “DB_MAESTRA1” y colocará el archivo en la carpeta del inventario.
2. Base de datos Maestra 2 vacía e inicializada, el PROVEEDOR realizará un dump de la base de datos, 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_solictado.sql) o en su defecto se debe de realizar una exportación de la base de datos en un ambiente gráfico, el resultado será un archivo sql que el PROVEEDOR nombrará el archivo como “DB_MAESTRA2” y colocará el archivo en la carpeta del inventario.
3. Base de datos de solo lectura Cómputo-Maestra1 vacía e inicializada, el PROVEEDOR realizará un dump de la base de datos, 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_solictado.sql) o en su defecto se debe de realizar una exportación de la base de datos en un ambiente gráfico, el resultado será un archivo sql que el PROVEEDOR nombrará el archivo como “DB_COMPUTO_MAESTRA1” y colocará el archivo en la carpeta del inventario
4. Base de datos de solo lectura Auditoria-Maestra1 vacía e inicializada, el PROVEEDOR realizará un dump de la base de datos, para realizar este paso es necesario ingresar a la terminal de mysql con un usuario y password con privilegios para realizar respaldos y ejecutar el comando (mysqldump nombre_de_Base_de_Datos > nombre_solictado.sql) o en su defecto se debe de realizar una exportación de la base de datos en un ambiente gráfico, el resultado será un archivo sql que el PROVEEDOR nombrará el archivo como “DB_AUDITORIA_MAESTRA1” y colocará el archivo en la carpeta del inventario
5. Base de datos de solo lectura Generador de contenidos-Maestra1 vacía e inicializada, el PROVEEDOR realizará un dump de la base de datos, 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_solictado.sql) o en su defecto se debe de realizar una exportación de la base de datos en un ambiente gráfico, el resultado será un

archivo sql que el PROVEEDOR nombrará el archivo como “DB_GENERADORDECONTENIDOS _MAESTRA1” y colocará el archivo en la carpeta del inventario

6. Base de datos de solo lectura Cómputo-Maestra2 vacía e inicializada, el PROVEEDOR realizará un dump de la base de datos, 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_solictado.sql) o en su defecto se debe de realizar una exportación de la base de datos en un ambiente gráfico, el resultado será un archivo sql que el PROVEEDOR nombrará el archivo como “DB_COMPUTO_MAESTRA2” y colocará el archivo en la carpeta del inventario
7. Base de datos de solo lectura Auditoria-Maestra2 vacía e inicializada, el PROVEEDOR realizará un dump de la base de datos, 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_solictado.sql) o en su defecto se debe de realizar una exportación de la base de datos en un ambiente gráfico, el resultado será un archivo sql que el PROVEEDOR nombrará el archivo como “DB_AUDITORIA_MAESTRA2” y colocará el archivo en la carpeta del inventario
8. Base de datos de solo lectura Generador de contenidos-Maestra2 vacía e inicializada, el PROVEEDOR realizará un dump de la base de datos, 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_solictado.sql) o en su defecto se debe de realizar una exportación de la base de datos en un ambiente gráfico, el resultado será un archivo sql que el PROVEEDOR nombrará el archivo como “DB_GENERADORDECONTENIDOS _MAESTRA2” y colocará el archivo en la carpeta del inventario
9. Base de datos del dispositivo Móvil vacía e inicializada, el PROVEEDOR realizará un dump de la base de datos o en su defecto realizará una exportación de la base de datos en un ambiente gráfico, el resultados será un archivo slq que el PROVEEDOR nombrará el archivo como “DB_MOVIL” y colará el archivo en la carpeta de inventario.
10. Base de datos Central-Desktop vacía e inicializada, el PROVEEDOR realizará un dump de la base de datos, 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_solictado.sql) o en su defecto se debe de realizar una exportación de la base de datos en un ambiente gráfico, el resultados será un archivo slq que el PROVEEDOR nombrará el archivo como “DB_CENTRAL_DESKTOP” y colará el archivo en la carpeta de inventario.
11. Sistema de archivos – 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 comando 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.
12. El PROVEEDOR una vez vaciado e inicializado las bases de datos mencionadas en los puntos anteriores colocará los logs de MySql en la carpeta de inventario, con la siguiente nomenclatura: DB_MAESTRA1_LOG, DB_MAESTRA2_LOG, DB_COMPUTO_MAESTRA1_LOG, DB_AUDITORIA_MAESTRA1_LOG, DB_GENERADORDECONTENIDOS _MAESTRA2_LOG, DB_COMPUTO_MAESTRA2_LOG, DB_AUDITORIA_MAESTRA2_LOG,

DB_GENERADORDECONTENIDOS _MAESTRA2_LOG, DB_MOVIL_LOG, DB_CENTRAL_DESKTOP. También se le solicita al PROVEEDOR incluir el log de sistema de ficheros vacío e inicializado con el siguiente nombre SISTEMADEARCHIVOS_LOG.

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.

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 Controlador
2. Aplicación de Validación y Verificación
3. Aplicación Captura PREP Casilla
4. Aplicación de Cómputo
5. Aplicación de Publicación
6. Aplicación de PREP Casilla

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 ***1904Proveedor.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 ***1904Proveedor.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.
    b. Cada huella criptográfica será firma digitalmente utilizando la llave privada SK mediante el algoritmo RSA.
    c. Se enviará el conjunto de huellas criptográficas y sus firmas digitales al servicio de verificación desarrollado por el Ente Auditor y una notificación por correo electrónico será enviada al IETAM.

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 1904Proveedor.jar firmarArchivos Inventario/ Llavero/LlavePrivada S1 CiudadVictoria.
Donde ***java -jar 1904Proveedor.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 una 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 del IETAM 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 1904IETAM.jar validar Llavero/LlavePublica Original Evento.
Donde ***java -jar 1904IETAM.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 al cloud (servidor del Ente Auditor) o/y vía email al IETAM y al Ente Auditor.

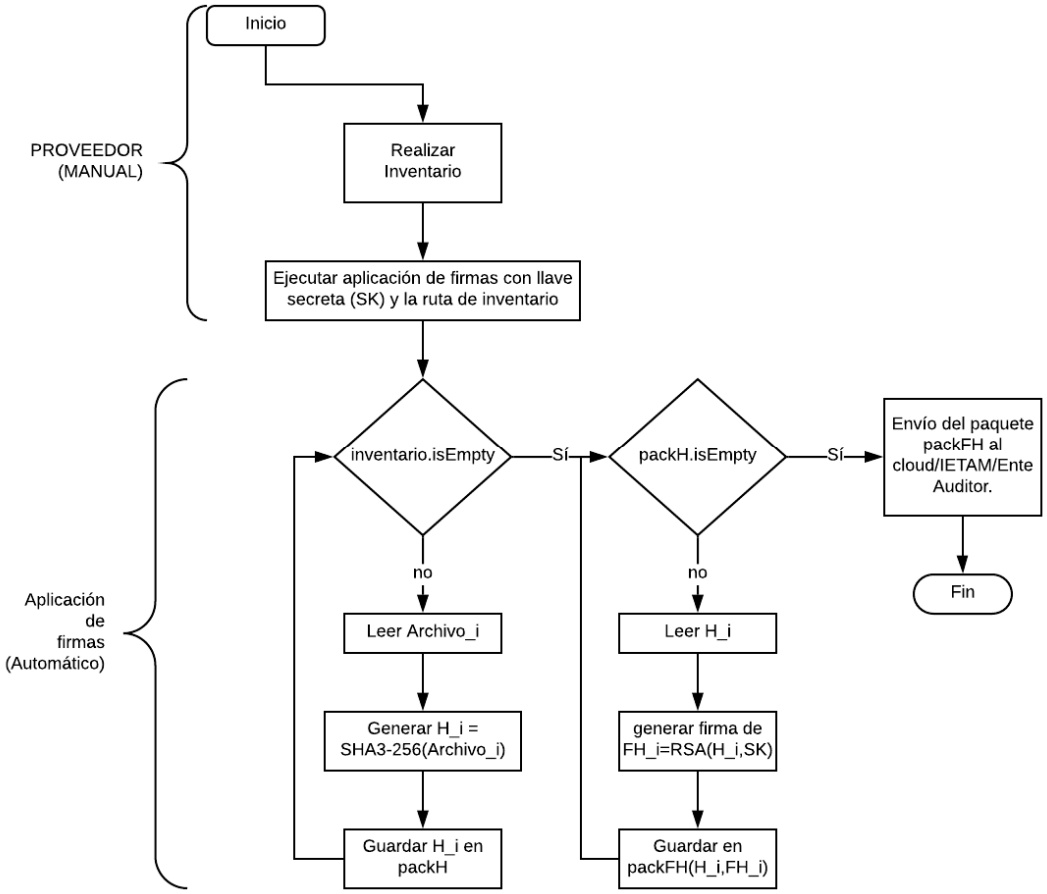


Figura 7.4 Diagrama de Flujo 4 Flujo de trabajo para la generación de las firmas de los documentos del inventario.

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

1. El personal de IETAM ejecutará la Aplicación de validación dando como entradas la llave pública (PK) y el paquete que quiere validar (Paquete simulacro 1, paquete simulacro 2, paquete simulacro 3, paquete jornada electoral o todos).
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.

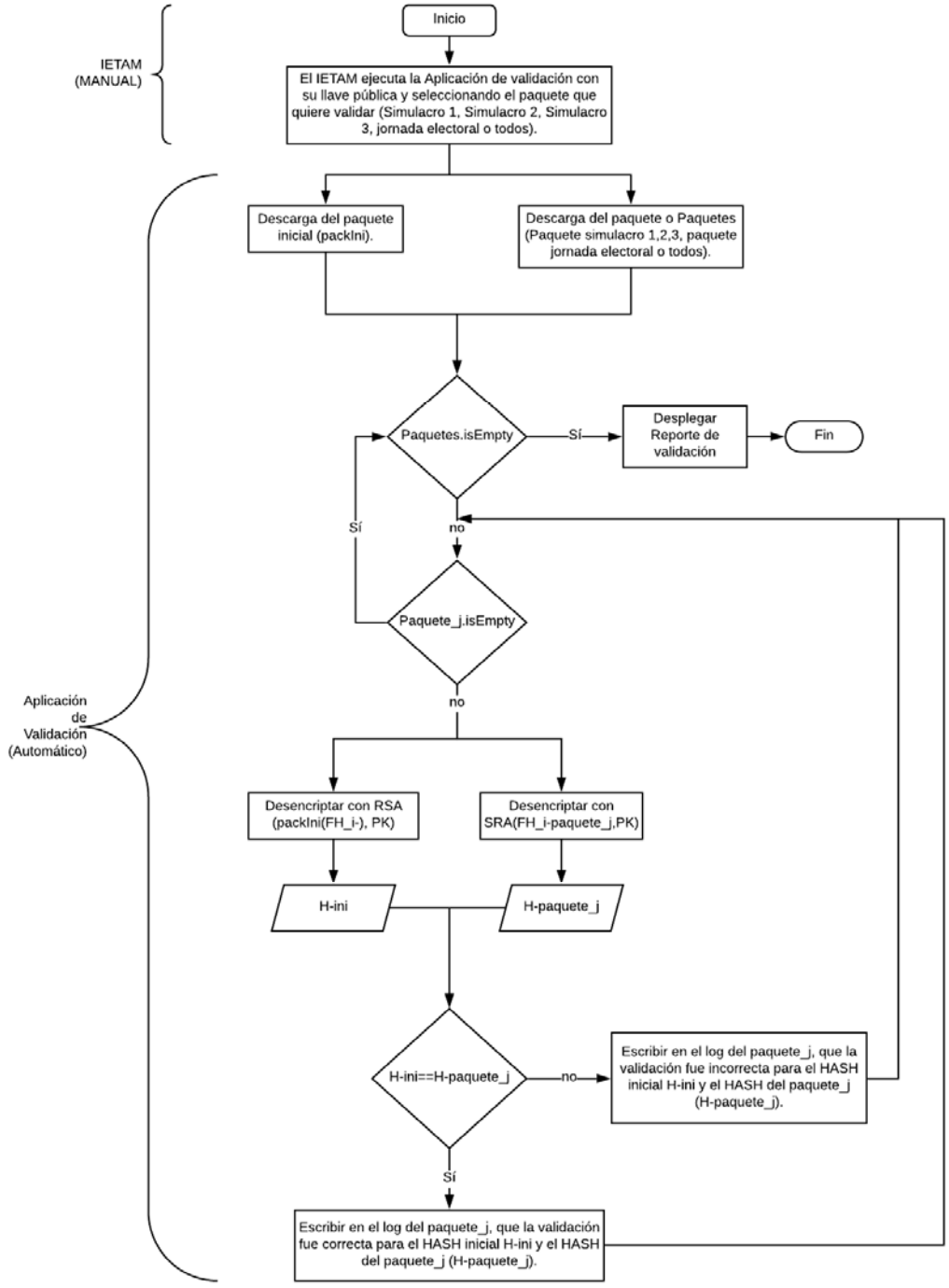


Figura 7.5 Diagrama de Flujo 5 Flujo de trabajo para la validación de las firmas iniciales con las firmas generadas durante los simulacros y la jornada electoral.

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 12, 19 y 26 de mayo de 2019, respectivamente. El procedimiento se realizará el domingo 2° de junio de 2019 en las instalaciones del IETAM, concluyendo el 3 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, a las 15:17pm del 26 de mayo de 2019.

Ciudad Victoria, Tamaulipas, 26 de Mayo de 2019

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

Siendo las 15 horas con 17 minutos del día 26 del mes de Mayo del año 2019 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 de la Mtra. María de los Ángeles Quintero Rentería en su calidad de Consejera Presidenta Provisional del Instituto Electoral de Tamaulipas, del Dr. Javier Rubio Loyola, por parte del Cinvestav Tamaulipas en su calidad de Ente Auditor 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 inicial (SHA3-256 inicial), la huella criptográfica minutos antes de iniciar a la jornada electoral (SHA3-256 del evento) y el resultado de la comparación.

Nombre del Archivo: logs.zip	**Evento: Simulacro 3** **Fecha de validación: 2019-05-26 15:17:28**
SHA3-256 Inicial	64c8982d80569b31a2abc64e868322e9f638bbfe7503e7605797f809f8a69f38
SHA3-256 del Evento	64c8982d80569b31a2abc64e868322e9f638bbfe7503e7605797f809f8a69f38
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: auditoria.zip	**Evento: Simulacro 3** **Fecha de validación: 2019-05-26 15:17:28**
SHA3-256 Inicial	d72e4ebe805a70f2b88764232842c870a4f4e494daf760f3897f9259718530a6
SHA3-256 del Evento	d72e4ebe805a70f2b88764232842c870a4f4e494daf760f3897f9259718530a6
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.

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

Nombre del Archivo: prepcasilla.zip	**Evento: Simulacro 3** **Fecha de validación: 2019-05-26 15:17:28**
SHA3-256 Inicial	e51b665cbe54db1e034fa07494682e815d6787a2f5023553293f3bb09743d970
SHA3-256 del Evento	e51b665cbe54db1e034fa07494682e815d6787a2f5023553293f3bb09743d970
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: admin.zip	**Evento: Simulacro 3** **Fecha de validación: 2019-05-26 15:17:28**
SHA3-256 Inicial	6dfbc0c6c776f76685740dce8ebaec75bbfdfa1ec4788966fea3bfdc9ce13522
SHA3-256 del Evento	6dfbc0c6c776f76685740dce8ebaec75bbfdfa1ec4788966fea3bfdc9ce13522
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.zip	**Evento: Simulacro 3** **Fecha de validación: 2019-05-26 15:17:28**
SHA3-256 Inicial	b057741c74e20a30a290a092348781eb3ba833fae30c0b1ef54e0a830f768251
SHA3-256 del Evento	b057741c74e20a30a290a092348781eb3ba833fae30c0b1ef54e0a830f768251
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: central.zip	**Evento: Simulacro 3** **Fecha de validación: 2019-05-26 15:17:28**
SHA3-256 Inicial	1e0686c547fcddf8c023671ae8148f226ba4e6b83cf83029a08ea528361f304b
SHA3-256 del Evento	1e0686c547fcddf8c023671ae8148f226ba4e6b83cf83029a08ea528361f304b
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.zip	**Evento: Simulacro 3** **Fecha de validación: 2019-05-26 15:17:28**
SHA3-256 Inicial	4ef7a89c89484df10ca288bc9c77f8eeab71cf9653f44ec7028f7095b22a87ac
SHA3-256 del Evento	4ef7a89c89484df10ca288bc9c77f8eeab71cf9653f44ec7028f7095b22a87ac
Estado	Correcto

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

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: ControladorTamaulipas.zip	**Evento: Simulacro 3 Fecha de validación: 2019-05-26 15:17:28**
SHA3-256 Inicial	f34e69cded9eeeb26bb06b21d5d68c9cd2517e82abb76ddca086f7e532886b32
SHA3-256 del Evento	f34e69cded9eeeb26bb06b21d5d68c9cd2517e82abb76ddca086f7e532886b32
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: db-tamp--2019.sql	**Evento: Simulacro 3 Fecha de validación: 2019-05-26 15:17:28**
SHA3-256 Inicial	3cf1370fdd20b251cd8fc4c8fb60bddb602d7b41d2cafb6eff0ac464067e3d2e
SHA3-256 del Evento	3cf1370fdd20b251cd8fc4c8fb60bddb602d7b41d2cafb6eff0ac464067e3d2e
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: log.txt	**Evento: Simulacro 3 Fecha de validación: 2019-05-26 15:17:28**
SHA3-256 Inicial	5385788e6bbf378b9db525e87fa648f5ccb0c34ced254280e9eca9c428bc22fb
SHA3-256 del Evento	91d1119d72901b7f8aee86238c7e8b0f23a3a463f603dd7feeccc611dd92a66e
Estado	Correcto
Observaciones	Se considera correcto porque las huellas criptográficas evaluadas para este archivo son distintas. El contenido de este archivo cambia cada que el proveedor realiza la recolección del inventario, por tal motivo deben ser distintas las huellas criptográficas.

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

Archivo	Descripción
central.zip	Compendio de Webservices para la recepción de actas.
db-tamps-2019.sql	Esquema de la base de datos central del PREP
ControladorTamaulipas.zip	Programa de captura y digitalización de actas
sitio.zip	Archivos de publicación web de resultados preliminares
generador.zip	Programa de generación de folios y contenidos estáticos
admin.zip	Programa de administración y utilerías de procesos.
auditoria.zip	Programa de auditoria de actas.

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

logs.txt	Registro de secuencia del proceso para la obtención, compresión y transmisión al servidor de auditoria.
logs.zip	Registro log en formato Zip.
prepcasilla.zip	Programa de control de proceso de Prep Casilla.

Firman la presente constancia los representantes de las entidades que intervienen, la Mtra. María de los Ángeles Quintero Rentería en su calidad de Consejera Presidenta Provisional del Instituto Electoral de Tamaulipas, el Dr. Javier Rubio Loyola, por parte del Cinvestav Tamaulipas en su calidad de Ente Auditor y el Lic. José de los Santos González Picazo en su calidad de Titular de la Instancia Interna Responsable del PREP.

Mtra. María de los Ángeles Quintero Rentería Consejera Presidenta Provisional del Instituto Electoral de Tamaulipas	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 4.

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 del IETAM y del proveedor de servicios 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 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.

8.3.2 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 al **"Plan de revisión de configuraciones a la infraestructura"** entregado previamente y el cual fue elaborado de acuerdo a 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 al siguiente calendario:

Tabla 8.1 Calendario. Nivel Plataforma Tecnológica.

Ubicación	Fecha
CCV Principal	29 de Abril y 03 de Mayo de 2019
CCV de Respaldo	29 de Abril y 03 de Mayo de 2019
CATD 1 Victoria	06 de Mayo de 2019
CATD 2 Victoria	06 de Mayo de 2019
CATD Tampico	14 de Mayo de 2019

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 el CCV principal 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 proveedor o al OPL.

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 y configurados dentro de una red privada dentro del mismo servicio.
- Las estaciones de trabajo de los CCV y de los CATD cuentan son software antivirus de uso libre (Freeware)
- Las estaciones de trabajo de los CATD no cuentan con software antivirus
- Los escáneres están conectados directamente al puerto USB de cada uno de los equipos de digitalización.

Observaciones

O3-C-3 La cuenta de usuario por default del sistema operativo es la de Administrador

Recomendaciones

R3-C-4 Es altamente recomendable delimitar la cuenta de usuario de los equipos de cómputo para el personal operativo solo con los privilegios requeridos para sus actividades y no como usuario administrador del equipo

R3-C-5 Es recomendable utilizar una solución de antivirus propietaria ya que las versiones libres no garantizan de ninguna forma la actualización de firmas contra las amenazas más recientes ni la atención ante la aparición de vulnerabilidades tipo zero-day, así como instalar este tipo de antivirus en todos los equipos tanto de los CCV como en los CATD.

R3-C-6 Es altamente recomendable para procesos futuros que 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 todos los accesos e información requerida para realizar la revisión correspondiente 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 el software Armitage+Metasploit

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 las políticas de filtrado.
- Todos los servicios de acceso remoto al equipo de seguridad perimetral del CCV están desactivados.
- Los equipos de conmutación y direccionamiento en los CATD son los módems VDSL.

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-7 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-8 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 Armitage+Metasploit.

Información recopilada

- Las estaciones de trabajo de los CATD y CCV están configuradas con el sistema operativo Microsoft Windows 7 Ultimate service pack 1
- 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-9 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-10 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.
R3-C-11 Es altamente recomendable desactivar los puertos USB que no sean requeridos por las aplicaciones y servicios durante la jornada electoral.

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 de los CATD y CCV tienen instalado el software propietario File Maker Pro 16 Advanced como requerimiento para la aplicación del sistema PREP
- Las estaciones de trabajo de los CATD y CCV tienen instalado el software propietario y IM Lock para el bloqueo de puertos físicos y el control local para el acceso a Internet.
- Las estaciones de trabajo de los CATD y CCV tienen instalado el software AnyDesk y Teamviewer para soporte técnico remoto.

Observaciones

Ninguna

Recomendaciones

R3-C-12 Es recomendable definir un procedimiento seguro por parte del personal de soporte técnico del proveedor para delimitar el uso correcto de las aplicaciones AnyDesk y Teamviewer para asistencia remota.

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, el cual protegerá 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 Principal se validó la instalación y puesta a punto de la planta de emergencia.
- En el CCV de respaldo, CATD 1 Victoria, CATD 2 Victoria y CATD Tampico se validó la instalación y puesta a punto de la planta de emergencia y realizaron las pruebas de funcionamiento con éxito.

Observaciones

O3-D-1 La planta de emergencia en el CCV principal no funcionó de manera correcta, aunque durante el simulacro 1 se identificó la falla y la solución a esta.

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 El módem en los CATD no está conectado a un SAI sino a la roseta directa del suministro de energía.

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.
R3-D-3 Es necesario conectar el modem en los CATD a un equipo SAI para su protección.

8.4 Pruebas de penetración (pentest).

8.4.1 Introducción

Las pruebas de penetración también llamadas “pen testing” 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 del proveedor de servicios del 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 de penetración se llevaron a cabo tanto desde el interior como desde el exterior de la red de datos a examinar y se consideró la siguiente infraestructura:
Aplicaciones web
Equipos de telecomunicaciones
Estaciones de trabajo

Se presentan las pruebas de penetración realizadas a la infraestructura tecnológica del proveedor de servicios. Las pruebas abarcan los diferentes dispositivos presentes en la infraestructura y 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 2 fases, la primera del 29 de abril al 6 de mayo y la segunda el 14 de mayo, ambas en 2019. En la primera fase se analizó el Centro de Captura y Verificación (CCV) principal y alterno ubicados en Cd. Victoria, Tamaulipas., así como los Centros de Acopio y Transmisión de Datos (CATD) 1 y 2 ubicados en Cd. Victoria. En la segunda fase se analizó el CATD ubicado en Tampico, Tamaulipas.

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 2019.

Las pruebas de penetración a la infraestructura del proveedor de servicios se llevarán a cabo desde el interior de las instalaciones así como desde el exterior de la red de datos y considerará como mínimo la siguiente infraestructura:

- Servidores.
- Equipos de telecomunicaciones.
- Estaciones de trabajo.
- Equipo Celular
- Personal Operativo

La planeación de las pruebas de penetración sobre la infraestructura tecnológica del proveedor de servicios del sistema PREP Tamaulipas está elaborada con base en documento *"The Open Source Security Testing Methodology Manual (OSSTMM) v2.1"* creado por el *"Institute for Security and Open Methodologies (ISECOM)"*, en sus secciones C.2, C.3, C.7 y B.3.

8.4.2 Alcance

Las pruebas de penetración a la plataforma tecnológica del proveedor de servicios fueron realizadas utilizando las herramientas: Nessus, OpenVAS y Armitage instaladas sobre una distribución del sistema operativo Linux llamada Kali, además de diversas herramientas/comandos provistos por el sistema operativo. A fin de no modificar ningún equipo del proveedor, todas las herramientas fueron desplegadas en equipos propios del ente auditor, los cuales sólo requirieron una conexión directa a los equipos de comunicaciones de la red implementada por el proveedor de servicios para realizar las pruebas.

Las herramientas utilizadas permiten ejecutar todas las tareas necesarias para realizar un análisis de vulnerabilidades confiable y reproducible de la infraestructura tecnológica, así como explotar las vulnerabilidades identificadas en el proceso a fin de verificar el nivel de riesgo de las vulnerabilidades descubiertas.

El análisis se dividió en 4 fases:

1. Extracción y recolección de información.
2. Escaneo de puertos e identificación de Servicios.
3. Búsqueda y explotación de vulnerabilidades.
4. Ingeniería Social.

Para la fase 1 se utilizaron las herramientas netdiscover y nbtscan; para la fase 2 se utilizaron las herramientas nmap, Nessus, OpenVAS y Armitage. En fase 3 se utilizó la herramienta Armitage y Metasploit; la fase 4 fue realizada de manera presencial por uno de los responsables técnicos.

8.4.3 Extracción y recolección de información

El sondeo de red sirve como introducción a los dispositivos a ser analizados. Se puede definir como una combinación de recolección de datos, obtención de información y política de control. El objetivo es construir un mapa de la red con todos los componentes que conforman la plataforma tecnológica, buscando obtener para cada dispositivo la mayor cantidad de información posible.

Resultados esperados:

- Nombres de Dominio.
- Nombres de Servidores.
- Direcciones IP.
- Mapa de Red.
- Posibles limitaciones del test.

Metodología:

1. Encontrar bloques de IPs utilizados a través de herramientas de descubrimiento.
2. Identificar vendedor de la interface de red utilizada por los dispositivos.
3. Realizar una identificación inversa de nombres a partir de las direcciones IP identificadas.

Pruebas ejecutadas:

T3-E-1. #netdiscover -r net_id/bit_mask
T3-E-2. #nbtscan -n net_id/bit_mask

8.4.4 Escaneo de puertos e identificación de servicios

En esta prueba se enumeran los puertos y servicios activos o accesibles de cada dispositivo que compone la plataforma tecnológica del proveedor. El análisis de los puertos y servicios se realizó con base en el tipo de dispositivo y de los servicios ofrecidos por éste. Una vez identificados los servicios, se intentará identificar el tipo de dispositivo, su sistema operativo, versión y paquetes de servicio o versión de actualización.

Resultados esperados:

- Puertos abiertos, cerrados y filtrados.
- Direcciones IP internas de los dispositivos activos.
- Lista de los protocolos descubiertos.
- Servicios activos.
- Tipo de Sistema Operativo.
- Paquete de Servicios o actualizaciones (parches de seguridad) instalados.

Metodología:

1. Recoger respuestas de broadcast desde la red.
2. Usar escaneos para enumerar puertos abiertos, cerrados o filtrados, para aquellos puertos TCP y UDP utilizados por defecto en todos los equipos de la red.
3. Relacionar cada puerto abierto con un servicio y protocolo.
4. Identificar el nivel de actualización (parches de seguridad) del sistema.

Pruebas Ejecutadas:

T3-E-3. #db_nmap --min-hostgroup 96 -T4 -A -v -n IP
T3-E-4. Análisis con herramienta *Nessus*
T3-E-5. Análisis con herramienta *OpenVAS*

8.4.5 Búsqueda y explotación de vulnerabilidades.

La finalidad de esta prueba es la identificación, comprensión y verificación de debilidades, errores de configuración y vulnerabilidades en un dispositivo de la infraestructura tecnológica del proveedor. La búsqueda de vulnerabilidades utilizando herramientas automáticas es una forma eficiente de determinar problemas de seguridad existentes, así como el nivel de actualización de los sistemas. Por otro lado, la explotación de vulnerabilidades se realiza con la finalidad de corroborar si es posible utilizar de manera externa las debilidades encontradas con la finalidad de tomar control o causar un daño significativo en los dispositivos de la infraestructura tecnológica del proveedor o en el proceso operativo.

Resultados esperados:

- Tipo de aplicación o servicio por vulnerabilidad.
- Niveles de actualización (parches de seguridad) de los sistemas y aplicaciones.
- Listado de posibles vulnerabilidades de denegación de servicio.
- Listado de vulnerabilidades actuales.
- Listado de sistemas internos.

Metodología:

1. Integrar en las pruebas realizadas los escáneres, herramientas de hacking y exploits utilizados actualmente (ethical-hacking).
2. Medir la red objetivo utilizando herramientas de escaneo actuales.
3. Intentar determinar vulnerabilidades por tipo de aplicación y sistema
4. Intentar ajustar vulnerabilidades a servicios.
5. Identificar todas las vulnerabilidades relativas a las aplicaciones.
6. Identificar todas las vulnerabilidades relativas a los sistemas operativos a los sistemas objetivo.
7. Verificar todas las vulnerabilidades encontradas durante la fase de búsqueda de exploits.

Pruebas Ejecutadas:

T3-E-6. Identificación adicional de vulnerabilidades mediante *Armitage.*
T3-E-7. Explotación de vulnerabilidades mediante *Armitage*.

8.4.6 Ingeniería Social

Esta prueba cubre el análisis de las vulnerabilidades desde el punto de vista de las personas, principalmente el personal operativo que participan en el proceso técnico operativo. El objetivo de cumplimiento de las pruebas de seguridad en este módulo son la concientización de seguridad del personal y la medición de brechas según el estándar de seguridad establecido en las políticas del proveedor, así como el conocimiento de la infraestructura tecnológica y las medidas de contingencias mínimas necesarias para la continuidad de la operación.

Resultados esperados:

- Nivel de conocimiento del personal operativo acerca de políticas de seguridad.
- Políticas de seguridad de usuarios.
- Extracción de información sensible de la infraestructura.
- Extracción de información sensible de controles de acceso.

Metodología:

1. Seleccionar al azar personal operativo.
2. Realizar entrevista de reconocimiento.

3. Medir el nivel de conocimiento de las políticas de seguridad.
4. Medir el nivel de conocimiento de los protocolos de contingencia.
5. Realizar preguntas con la finalidad de extraer información sensible sobre la seguridad de la infraestructura.

Pruebas Ejecutadas:

T3-E-8. Aplicación de Cuestionarios al personal contratado y capacitado por el proveedor de servicios.

8.4.7 Hallazgos de las pruebas de penetración

8.4.7.1 CCV Principal

Tabla 8.2 Resultado de pruebas en CCV principal: Nivel Plataforma Tecnológica

Prueba	Resultados
T3-E-1	• Se identificó el segmento de red 27.15.11.0/24 y el 27.15.12.0/24, en éste, se identificaron 31 dispositivos activos, los cuales corresponden a los equipos de cómputo de la marca HP Compaq y a los ruteadores marca Mikrotik. • De todos los dispositivos descubiertos fue posible extraer satisfactoriamente el fabricante de la interface de red.
T3-E-2	• Se detectó el protocolo NetBIOS activo en 1 dispositivo y por medio de éste fue posible identificar su nombre y grupo de trabajo (27.15.12.7) se recomienda revisar el equipo y desactivar el servicio.
T3-E-3	• En el equipo ruteador se identificó el siguiente puerto abierto: o 53: Generic DNS response (27.15.12.1) Se recomienda validar que el servicio solo este disponible para los equipos internos de la red. • En los equipos de cómputo no se encontraron puertos abiertos
T3-E-4 T3-E-5	• No se detectaron vulnerabilidades en los equipos analizados, pero es importante atender las recomendaciones del test T3-E-3.
T3-E-6	• Utilizando la herramienta Armitage+Metsploit+HailMary se validó que no se encontraron vulnerabilidades que pudieran ser explotadas.
T3-E-7	• Utilizando la herramienta *Armitage+Metsploit+HailMary* se validó que no se encontraron vulnerabilidades que pudieran ser explotadas. Los *exploits* utilizados forman parte de la suite estándar del *Metasploit Framework* orientados a vulnerar sistemas con el menor esfuerzo.
T3-E-8	• El personal técnico tiene bien identificado los alcances y a la manera de solucionar los posibles problemas técnicos y de seguridad que pudieran presentarse en la jornada electoral.

8.4.7.2 CCV Respaldo

Tabla 8.3 Resultado de pruebas en CCV de respaldo: Nivel Plataforma Tecnológica

Prueba	Resultados
T3-E-1	• Se identificó el segmento de red 27.15.23.0/24 y el 192.168.1.0/24, en el primero se identificaron 26 dispositivos activos, los cuales corresponden a los equipos de cómputo de la marca HP Compaq y a los ruteadores marca Mikrotik. • De todos los dispositivos descubiertos fue posible extraer satisfactoriamente el fabricante de la interface de red. • Se recomienda deshabilitar el segmento 192.168.1.0/24 por pertenecer al servicio por default del proveedor TELMEX
T3-E-2	• Se detectó el protocolo NetBIOS activo en 1 dispositivo y por medio de éste fue posible identificar su nombre y grupo de trabajo (27.15.23.23) se recomienda revisar el equipo y desactivar el servicio.
T3-E-3	• En el equipo ruteador se identificó el siguiente puerto abierto: o 53: Generic DNS response Se recomienda validar que el servicio solo esté disponible para los equipos internos de la red. • En el equipo 27.15.23.4 se identificó el siguiente puerto abierto: • 5357/tcp - Se recomienda validar si es necesario que el servicio este activo, de lo contrario desactivarlo.
T3-E-4 T3-E-5	• No se detectaron vulnerabilidades en los equipos analizados, pero es importante atender las recomendaciones del test T3-E-3.
T3-E-6	• Utilizando la herramienta Armitage+Metsploit+HailMary se validó que no se encontraron vulnerabilidades que pudieran ser explotadas.
T3-E-7	• Utilizando la herramienta Armitage+Metsploit+HailMary se validó que no se encontraron vulnerabilidades que pudieran ser explotadas. Los exploits utilizados forman parte de la suite estándar del Metasploit Framework orientados a vulnerar sistemas con el menor esfuerzo.
T3-E-8	• El personal técnico tiene bien identificado los alcances y a la manera de solucionar los posibles problemas técnicos y de seguridad que pudieran presentarse en la jornada electoral.

8.4.7.3 CATD1 Victoria (Consejo Distrital 15)

Tabla 8.4 Resultado de pruebas en CATD 1 Victoria: Nivel Plataforma Tecnológica

Prueba	Resultados
T3-E-1	• Se identificó el segmento de red 192.168.1.0/24, en éste, se identificaron 4 dispositivos activos de los cuales 3 son equipos de cómputo de la marca HP Compaq y 1 Modem VDSL marca Ping Communication. • De todos los dispositivos descubiertos fue posible extraer satisfactoriamente el proveedor de la interface de red.
T3-E-2	• Se detectó el protocolo NetBIOS activo en 1 dispositivo y por medio de éste fue posible identificar su nombre y grupo de trabajo (192.168.1.65) se recomienda revisar el equipo y desactivar el servicio.
T3-E-3	• En el equipo modem VDSL se identificaron los siguientes puertos abiertos: o 21/tcp filtered ftp o 22/tcp open ssh Dropbear sshd 2016.74 (protocol 2.0) o 23/tcp filtered telnet o 53/tcp open domain dnsmasq 2.45 o 80/tcp open tcpwrapped o 443/tcp filtered https o 49152/tcp open upnp - Se recomienda validar que los servicios 22, 53 y 443 solo estén disponibles para los equipos internos de la red. - Es altamente recomendable desactivar por completo los siguientes puertos: 21/tcp, 23/tcp, 80/tcp y 49152/tcp • En el equipo 192.168.1.67 se identificó el siguiente puerto abierto: o 9000/tcp - Se recomienda validar si es necesario que el servicio este activo, de lo contrario desactivarlo.
T3-E-4 T3-E-5	• No se detectaron vulnerabilidades en los equipos analizados, pero es importante atender las recomendaciones del test T3-E-3.
T3-E-6	• Utilizando la herramienta Armitage+Metsploit+HailMary se validó que no se encontraron vulnerabilidades que pudieran ser explotadas.
T3-E-7	• Utilizando la herramienta Armitage+Metsploit+HailMary se validó que no se encontraron vulnerabilidades que pudieran ser explotadas. Los exploits utilizados forman parte de la suite estándar del Metasploit Framework orientados a vulnerar sistemas con el menor esfuerzo.
T3-E-8	• El personal técnico tiene bien identificado los alcances y a la manera de solucionar los posibles problemas técnicos y de seguridad que pudieran presentarse en la jornada electoral.

8.4.7.4 CATD2 Victoria (Consejo Distrital 14)

Tabla 8.5 Resultado de pruebas en CATD 2 Victoria: Nivel Plataforma Tecnológica

Prueba	Resultados
T3-E-1	• Se identificó el segmento de red 192.168.1.0/24, en éste, se identificaron 4 dispositivos activos de los cuales 3 son equipos de cómputo de la marca HP Compaq y 1 Modem VDSL marca Ping Communication. • De todos los dispositivos descubiertos fue posible extraer satisfactoriamente el proveedor de la interface de red.
T3-E-2	• Se detectó el protocolo NetBIOS activo en 1 dispositivo y por medio de éste fue posible identificar su nombre y grupo de trabajo (192.168.1.65) se recomienda revisar el equipo y desactivar el servicio.
T3-E-3	• En el equipo modem VDSL se identificaron los siguientes puertos abiertos: o 21/tcp filtered ftp o 22/tcp open ssh Dropbear sshd 2016.74 (protocol 2.0) o 23/tcp filtered telnet o 53/tcp open domain dnsmasq 2.45 o 80/tcp open tcpwrapped o 443/tcp filtered https o 49152/tcp open upnp - Se recomienda validar que los servicios 22, 53 y 443 solo estén disponibles para los equipos internos de la red. - Es altamente recomendable desactivar por completo los siguientes puertos: 21/tcp, 23/tcp, 80/tcp y 49152/tcp • En el equipo 192.168.1.66 se identificó el siguiente puerto abierto: o 7070/tcp - Se recomienda validar si es necesario que el servicio este activo, de lo contrario desactivarlo.
T3-E-4 T3-E-5	• No se detectaron vulnerabilidades en los equipos analizados, pero es importante atender las recomendaciones del test T3-E-3.
T3-E-6	• Utilizando la herramienta Armitage+Metsploit+HailMary se validó que no se encontraron vulnerabilidades que pudieran ser explotadas.
T3-E-7	• Utilizando la herramienta Armitage+Metsploit+HailMary se validó que no se encontraron vulnerabilidades que pudieran ser explotadas. Los exploits utilizados forman parte de la suite estándar del Metasploit Framework orientados a vulnerar sistemas con el menor esfuerzo.
T3-E-8	• El personal técnico tiene bien identificado los alcances y a la manera de solucionar los posibles problemas técnicos y de seguridad que pudieran presentarse en la jornada electoral.

8.4.7.5 CATD Tampico

Tabla 8.6 Resultado de pruebas en CATD Tampico: Nivel Plataforma Tecnológica

Prueba	Resultados
T3-E-1	• Se identificó el segmento de red 192.168.1.0/24, en éste, se identificaron 5 dispositivos activos de los cuales 4 son equipos de cómputo de la marca HP Compaq y 1 Modem VDSL marca Ping Communication. • De todos los dispositivos descubiertos fue posible extraer satisfactoriamente el proveedor de la interface de red.
T3-E-2	• No se detectaron servicios activos en los equipos de cómputo.
T3-E-3	• En el equipo modem VDSL se identificaron los siguientes puertos abiertos: o 21/tcp filtered ftp o 22/tcp open ssh Dropbear sshd 2016.74 (protocol 2.0) o 23/tcp filtered telnet o 53/tcp open domain dnsmasq 2.45 o 80/tcp open tcpwrapped o 161/udp open o 443/tcp filtered https o 7547/tcp open soap o 49152/tcp open upnp - Se recomienda validar que los servicios 22, 53 y 443 solo estén disponibles para los equipos internos de la red. - Es altamente recomendable desactivar por completo los siguientes puertos: 21/tcp, 23/tcp, 80/tcp , 161/udp, 7547/tcp y 49152/tcp
T3-E-4 T3-E-5	• No se detectaron vulnerabilidades en los equipos analizados.
T3-E-6	• Utilizando la herramienta Armitage+Metsploit+HailMary se validó que no se encontraron vulnerabilidades que pudieran ser explotadas.
T3-E-7	• Utilizando la herramienta Armitage+Metsploit+HailMary se validó que no se encontraron vulnerabilidades que pudieran ser explotadas. Los exploits utilizados forman parte de la suite estándar del Metasploit Framework orientados a vulnerar sistemas con el menor esfuerzo.
T3-E-8	• El personal técnico tiene bien identificado los alcances y a la manera de solucionar los posibles problemas técnicos y de seguridad que pudieran presentarse en la jornada electoral.

8.4.8 Recomendaciones Generales

Tabla 8.7 Recomendaciones generales: Nivel Plataforma Tecnológica

Prueba	Recomendación
T3-E-1	R3-E-1. Es deseable que las comunicaciones entre los clientes y los servidores se realice utilizando túneles de conexión VPN, con los cuales es posible tener cifrado de los datos y un direccionamiento general para todas las sedes, seguro y con cabeceras cifradas ante cualquier atacante.
T3-E-2	R3-E-2. Instalar en los equipos de cómputo un Antivirus con licencia y garantizar sus actualizaciones. R3-E-3. Habilitar para los equipos de cómputo de los CATD un firewall que filtre todo el tráfico entrante y saliente, para evitar el acceso libre a Internet y aplicaciones.
T3-E-3 T3-E-4 T3-E-5 T3-E-6 T3-E-7	R3-E-4. Deshabilitar en los equipos de cómputo y de comunicaciones los servicios mencionados en las pruebas, que no son necesarios para el desarrollo de las actividades del sistema PREP.
T3-E-8	No aplica

9. Pruebas de denegación de servicio a sitios web del PREP y al sitio 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
  - (No se realizó, debido a las implicaciones legales que este ataque puede tener)
- 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 negación 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
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.
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.
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. El uso abusivo de infraestructura de cómputo y red no propia es lo que hace que este tipo de ataque de inundación no sea legalmente permitido.

Para la realización de los ataques se usaron 10 equipos de cómputo del Laboratorio de Redes de la Unidad Tamaulipas del Cinvestav. Los equipos cuentan con sistemas Linux, y todos sus recursos se usaron de forma dedicada para realizar cada uno de los ataques a los sitios de publicación del PREP, de los difusores oficiales y al sitio principal del IETAM. Cada ataque se programó para realizarse sobre los puertos 80 y 443 de cada uno de los sitios de publicación de los resultados y del IETAM, mientras que DNS Amplification fue lanzado hacia el puerto 53.
Los ataques SYN Flood, ICMP Flood y Slowloris se realizaron de acuerdo a lo descrito en la Tabla 9.1. En la Tabla 9.2 se describe la calendarización de los ataques Slowloris a los sitios del IETAM y del Proveedor.

Tabla 9.2 Calendarización de ataques a los sitios de publicación de resultados del PREP y sitio principal del IETAM.

Servidor (Publicación)	Puerto	Ataque	09-may	16-may	17-may	18-may	22-may
PROISI www.prep2019tamps.mx 104.20.238.130	80	SYN Flood		14:33			
		ICMP Flood				9:34	
	443	SYN Flood		15:30			
		ICMP Flood				10:24	
		Slowloris	16:00				
	53	DNS Ampl.					19:30
PROISI www.prep2019tamps.mx 104.20.237.130	80	SYN Flood		14:56			
		ICMP Flood				9:59	
	443	SYN Flood		19:30			
		ICMP Flood				10:49	
		Slowloris	16:00				
	53	DNS Ampl.					19:30

En su mayoría, los ataques se realizaron con una duración promedio de entre 20 y 30 minutos.

9.4 Resumen de resultados y hallazgos

En la Tabla 9.3 se resumen los hallazgos realizados en la ejecución de las pruebas de negación de servicios realizadas como parte de los requerimientos del IETAM.

Tabla 9.3. Resumen de los hallazgos de la pruebas de negación de servicios.

	SYN Flood	ICMP Flood	Slowloris	DNS Amplification
www.prep2019tamps.mx				
http://ietam.org.mx				

	Resistente al ataque
	No resistente al ataque
	No resistente en pruebas iniciales
	No verificado

Parte IV

10. Simulacros

Se realizaron 3 simulacros los días 12, 19 y 26 de mayo de 2019. El Ente Auditor tuvo presencia durante los tres simulacros en CCV1, CCV2, CATD Victoria, CATD Tampico (19 de mayo). En la Tabla 10.1 se presentan los indicadores más importantes de los tres simulacros.

Tabla 10.1. Simulacros realizados.

Simulacro	Fecha	Total de actas esperadas	Total de actas contabilizadas	Total de actas contabilizadas con imagen válida	Total de actas contabilizadas sin imagen válida	Avance al final del simulacro
Simulacro 1	12/05/19	4710	4456	1424	3032	30.23%
Simulacro 2	19/05/19	4694	4465	4438	27	94.54%
Simulacro 3	26/05/19	4694	4467	4274	193	91.05%

A continuación, se presentan las observaciones realizadas por el Ente Auditor a la operación del PREP durante los tres simulacros.

10.1 Comentarios y observaciones resultantes de Simulacro 1

10.1.1 Módulo de publicación de resultados

CAPA DE DATOS

- El proveedor debe inicializar la base de datos en ceros y la generación de las huellas criptográficas del inventario solicitado por el ente auditor. Es necesario que el proveedor coloque todos los archivos del inventario antes de iniciar la prueba ya que el proveedor omitió el archivo llamado Programa Remoto.zip.
- El porcentaje de efectividad del PREP es bueno, sin embargo, es necesario automatizar procesos manuales, por ejemplo cuando las actas entran a un estado inconsistente el proceso para regresarlas a un estado consistente es manual. El uso de dos archivos para un solo evento no parece ser la mejor opción a menos que exista un esquema de mapeo inequívoco que garantice que ambos archivos son tratados como un solo evento en la elección.
- El uso de dos archivos para un solo evento no parece ser la mejor opción a menos que exista un esquema de mapeo inequívoco que garantice que ambos archivos son tratados como un solo evento en la elección.
- Actas faltantes no es aceptable. Se deberían eliminar estos eventos o documentar en for fehaciente la razón por la cual dichos eventos suceden en el software del PREP
- Se requiere el Hash de origen capturado por fuente/aplicación que ha creado el acta, así como el hash del acta que ha sido depositada en el repositorio del sistema de publicación.
- No se deberían presentar inconsistencias con las huellas criptográficas de las actas publicadas por lo que esto implica para el proceso electoral.
- El origen que se registra en el log del web service debe registrarse con los nombres de las actividades del proceso técnico operativo.

CAPA DE APLICACIONES

- Valores porcentuales superiores al 100%. Se argumenta que este error es debido a las casillas especiales. Sin embargo, esto podría darse a malas interpretaciones de las personas que visualizan los resultados.
- En la actualización periódica de resultados, podría ser útil la notificación automática al usuario que una nueva actualización está disponible

CAPA DE PLATAFORMA TECNOLÓGICA

- Inicia la generación y comprobación de huellas criptográficas sin observaciones y de acuerdo al procedimiento definido.
- A las 10:08 inicia el simulacro 1 sin observaciones y con la base de datos y el portal de publicación inicializado en ceros.

10.1.2 CCV Principal

CAPA DE APLICACIONES

- Se desconoce el tratamiento de aquellas actas que exceden la lista nominal.
- No existe un mecanismo eficiente para la recuperación del sistema ante eventos inesperados (cierres de sesión, terminación de aplicación). El acta queda en un estado inválido que tiene que restaurarse a través de procesos manuales por el administrador del sistema.
- Los datos de sesión de usuario del sistema web de validación 1 y 2 se mantienen a pesar de cerrar la ejecución del navegador o apagar la computadora. (CCV)
- El sistema 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.
- El sistema no tiene un mecanismo que permita la recuperación del último estado válido del acta.
- El sistema deja iniciada la sesión del usuario debido a la memoria cache que existe en el navegador. (CCV)
- Se observó que el sistema es seguro ante un posible acuerdo entre un capturista y un verificador con fines de lucro ya que la asignación de actas a un verificador se realiza de manera aleatoria.

CAPA DE PLATAFORMA TECNOLÓGICA

- Ante ausencia de energía solo 1 de los 30 equipos instalados NO fue protegido por los sistemas UPS/SAI.
- Al habilitar nuevamente la energía solo 3 de los 30 equipos instalados (el anteriormente mencionado fue uno de ellos) se apagaron simultáneamente.

Recomendación: Revisar y en su caso habilitar un UPS más en la zona con falla y validar el correcto funcionamiento del equipo instalado originalmente.

- Al activar el suministro de la planta de emergencia los UPS no detectaron el voltaje adecuado y siguieron trabajando con las baterías. Por lo anterior se procede a cancelar la prueba a recomendación del ente auditor para continuar con el simulacro.

Recomendación: Agendar una ventana de mantenimiento para ajustar la configuración del funcionamiento de la planta de emergencia del CCV principal.

- Se retira el enlace contratado con el proveedor TELMEX y siguen operando con normalidad los equipos instalados en el CCV con el enlace dedicado contratado con el proveedor TOTALPLAY.
- Se regresa el enlace contratado con el proveedor TELMEX y siguen operando con normalidad los equipos instalados en el CCV.
- Se retira el enlace contratado con el proveedor TOTALPLAY y siguen operando con normalidad los equipos instalados en el CCV con el enlace asimétrico contratado con el proveedor TELMEX.
- Se concluye la prueba con éxito.
- Se obtienen con el apoyo del proveedor PROISI las gráficas del tráfico real de las actividades del simulacro 1.

CAPA DE INFRAESTRUCTURA DE COMUNICACIONES

- Se verificó que el sitio web el PREP utiliza "https" y no "http".
- En el momento que la energía eléctrica fue suspendida, no se registró perdida de conexión de Internet en los equipos de trabajo.
- Las pruebas de redundancia se realizaron satisfactoriamente.
- Durante las pruebas de redundancia se detectó que no se contaba con el servicio IZZI activo.
- Los certificados digitales usan una configuración RSA-2018-bits, la cual es equivalente a un nivel de seguridad de 112-bit. La recomendada debe ser 128-bits, por lo que los certificados deben actualizarse a usar RSA-3076 bits o ECC-256.
- Las contraseñas para el acceso al sitio web son generadas por medio un script. Los coordinadores son los encargados de proporcionárselas a los capturistas personalmente por medio de una tarjeta en donde se encuentran dichos datos. La longitud de la contraseña debería ser de al menos de 9 caracteres aleatorios.

10.1.3 CCV Alterno

CAPA DE APLICACIONES

- Se desconoce el tratamiento de aquellas actas que exceden la lista nominal.
- No existe un mecanismo eficiente para la recuperación del sistema ante eventos inesperados (cierres de sesión, terminación de aplicación). El acta queda en un estado inválido que tiene que restaurarse a través de procesos manuales por el administrador del sistema.
- Los datos de sesión de usuario del sistema web de validación 1 y 2 se mantienen a pesar de cerrar la ejecución del navegador o apagar la computadora. (CCV)
- El sistema 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.
- El sistema no tiene un mecanismo que permita la recuperación del último estado válido del acta.
- El sistema deja iniciada la sesión del usuario debido a la memoria cache que existe en el navegador. (CCV)
- Se observó que el sistema es seguro ante un posible acuerdo entre un capturista y un verificador con fines de lucro ya que la asignación de actas a un verificador se realiza de manera aleatoria.

CAPA DE PLATAFORMA TECNOLÓGICA

- Al realizar la prueba de funcionamiento de los UPS, 3 de 27 equipos NO fueron protegidos por falla del UPS al que estaban conectados.
- Al realizar la prueba de la planta de emergencia se pudo validar que suministró correctamente al CCV de Respaldo durante 30 minutos a partir de las 12:09, por lo cual se concluye la prueba con éxito.

Recomendación: Revisar y en su caso habilitar un UPS más en la zona con falla y validar el correcto funcionamiento.

- Se retira el enlace 1 contratado con el proveedor TELMEX y siguen operando con normalidad los equipos instalados en el CCV con el enlace 2 contratado también con el proveedor TELMEX.
- Se regresa el enlace 1 contratado con el proveedor TELMEX y siguen operando con normalidad los equipos instalados en el CCV.
- Se retira el enlace 2 contratado con el proveedor TELMEX y siguen operando con normalidad los equipos instalados en el CCV con el enlace 2 contratado con el proveedor TELMEX.
- Se concluye la prueba con éxito.

Recomendación: Es altamente recomendable tener un enlace de respaldo pero con un proveedor diferente al que provee el enlace primario y no los dos enlaces con el mismo proveedor en este caso TELMEX.

CAPA DE COMUNICACIONES

- Se verificó que el sitio web el PREP utiliza "https" y no "http".
- En el momento que la energía eléctrica fue suspendida, no se registró perdida de conexión de Internet en los equipos de trabajo.
- Las pruebas de redundancia se realizaron satisfactoriamente.
- Existe una conexión inalámbrica que no permite el acceso a Internet, sin embargo, la contraseña es la predeterminada.
- Se encontró que una computadora no contaba con acceso a Internet.
- No se encontraba activo el servicio de Totalplay.
- Riesgo Alto. Debe ser atendida ya que no se cumple con los requerimientos funcionales del PTO.
- Los certificados digitales usan una configuración RSA-2018-bits, la cual es equivalente a un nivel de seguridad de 112-bit. La recomendada debe ser 128-bits, por lo que los certificados deben actualizarse a usar RSA-3076 bits o ECC-256.
- Algunos equipos del CCV alterno no tenían acceso a internet. Dos tercios de los equipos disponibles no estaba en operación.

10.1.4 CATD Victoria

CAPA APLICACIONES

- La aplicación no verifica la orientación de la imagen, por lo que existen tomas de actas con orientación vertical.
- Se observó que cuando se desea cambiar el escáner predeterminado, es necesario reiniciar y autenticarse en la aplicación.
- Los rangos de fecha deberían estar acotados a los días de la jornada electoral. Es posible ingresar fecha posteriores y anteriores a la jornada electoral.

- 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”.
- Se desconoce el tratamiento de aquellas actas que exceden la lista nominal.
- No existe un mecanismo que informe al capturista el estado del acta que no se envió adecuadamente.
- No existe un mecanismo eficiente para la recuperación del sistema ante eventos inesperados (cierres de sesión, terminación de aplicación). El acta queda en un estado inválido que tiene que restaurarse a través de procesos manuales por el administrador del sistema.
- Como prueba adicional se ingresó un número de votos mayor al número de votantes y no se notificó ningún error.
- 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.
- El sistema 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.
- El sistema permite el cambio de escáner, para realizar tal cambio el usuario debe reiniciar la aplicación y volver a autenticarse para seleccionar un escáner diferente. Por este cambio pueden existir inconsistencia en los datos de las actas capturadas.
- El tamaño del disco puede cambiar en aquellas situaciones donde el usuario decida guardar localmente las actas que serán capturas y enviadas después. Sin embargo, estas actas, al parecer son eliminadas cuando finalizan el proceso de captura y envío.
- El sistema permite ingresar cualquier fecha en el sistema, así sea una fecha demasiado antigua o una fecha que aún no ha llegado.
- El sistema no tiene un mecanismo que permita 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 fines de lucro ya que la asignación de actas a un verificador se realiza de manera aleatoria.

CAPA PLATAFORMA TECNOLÓGICA

- Los equipos UPS funcionaron con normalidad por al menos 5 minutos sin ninguna novedad.
- A las 12:26 se conectaron los UPS a la planta eléctrica de respaldo y se observó que no le llegaba corriente a los equipos. Dicho detalle se debía a la instalación eléctrica que comunicaba la planta con los equipos, por lo cual el proveedor reemplazo la extensión y se continuo con la prueba de manera correcta.
- Al iniciar la prueba se descubrió que uno de los UPS NO funcionaba correctamente motivo por el cual se apagaron 2 de 3 equipos de cómputo, 1 de 3 equipos multifuncional y el módem de conexión a Internet. El proveedor cambio el equipo de forma inmediata y se probó que los UPS mantuvieron los equipos funcionando por al menos cinco minutos, lo cual transcurrió sin problemas.
- Después de los cinco minutos se conectaron los equipos a la planta eléctrica de respaldo y se mantuvieron así durante 30 minutos los cuales transcurrieron sin ninguna novedad.

CAPA INFRAESTRUCTURA DE COMUNICACIONES

CATD2:

- Al desconectar los UPS de la corriente eléctrica para simular el corte de energía, uno de los UPS no funcionó correctamente motivo por el cual se apagó el modem que permite la conexión al CCV.
- El proveedor cambio el equipo UPS de forma inmediata en alrededor de 3 minutos, mismo tiempo que se quedaron sin conexión los equipos del CATD.
- Como resultado de la falla anterior, el proveedor mencionó que se cuenta con servicios de banda ancha móvil que pudieran servir como alternativa a quedarse sin enlace a Internet por cable.

CATD1.

- No se tuvo ninguna incidencia crítica.
- Los capturistas no pueden acceder a internet debido a que el navegador se cierra cada vez que intentan acceder a una página web (que no sea speedtest).
- Sin embargo, se observó que dicha si se conecta un equipo de cómputo al Switch (que no sea uno de los preconfigurados) dicho equipo podría acceder a internet sin ninguna restricción.
- No se pudo verificar qué tipo de seguridad implementa la aplicación de los equipos en CATD, dado que se conectan a un servicio en la nube pero la aplicación (de escritorio) no usa HTTPS.
- Los operadores en el CATD

10.1.2 Observaciones y Comentarios de la Capa Operativa en Simulacro 1

- El CAE cuenta con un chaleco de identificación otorgado por el INE. El CAE obtuvo una capacitación antes de realizar el simulacro. El CAE cuenta con un manual de usuario. Al CAE se le asignó un dispositivo móvil en el cual tenia instalado el PREP Casilla. El CAE instaló aplicaciones innecesarias en el dispositivo móvil (WhatsApp, etc.), y hace uso de este como si fuera personal. El CAE siempre realiza la toma fotográfica en una zona oscura (sombra). El CAE al tener una duda se dirige con un técnico por parte del INE. La aplicación a la hora de tomar la fotografía dibuja un rectángulo para evadir los bordes innecesarios, pero a la hora de enviar la imagen, no se respeta ese rectángulo y la imagen sale con los bordes innecesarios.
- El acopiador, a su vez se le asigna el rol de coordinador. 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 supervisor por parte del proveedor le brindará apoyo. El acopiador es el encargado del flujo de actas, teniendo una lista en la cual registra las actas ya capturadas y el capturista correspondiente a cada una. El acopiador repartió todas las actas PREP al iniciar el simulacro. 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.
- El digitalizador deberá de contar con un gafete de identificación. El digitalizador recibirá el Acta PREP de manera personal mediante el acopiador. El digitalizador deberá de contar con las credenciales necesarias para el sistema, 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 su supervisor encargado. En caso de ser necesario, el equipo multifunción para la digitalización puede cambiarse. Si el digitalizador tiene alguna duda acerca del proceso a realizar, deberá de pedir ayuda a su supervisor, o revisar el manual de usuario que se le fue otorgado. El digitalizador obtuvo la capacitación necesaria para realizar el proceso. El rol de digitalizador y capturista lo realiza una misma persona, a excepción del capturista de PREP Casilla. 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 necesarias para el sistema, las cuales se le fueron asignadas mediante un papel impreso, cada día son credenciales diferentes. El capturista primeramente deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el supervisor a cargo. El capturista cuenta con un manual de usuario para el uso del sistema.
- El capturista cuenta con un gafete de identificación. El capturista cuenta con las credenciales para ingresar al sistema. El capturista cuenta con un manual de usuario. El capturista obtuvo una capacitación antes de realizar el simulacro. Una cantidad importante de las actas de llegaron a la captura fueron rechazadas debido a que la imagen era ilegible. Los capturistas contaban con más de una pestaña abierta para pasar de un rol a otro.
- 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. Si el verificador tiene las credenciales equivocadas deberá de pedirle ayuda al supervisor. 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. En el CCV1 todos los operadores fueron capacitados para los roles de verificador 1, verificador 2 y capturista de PREP Casilla. En el CCV2 solo se cuenta con el rol de verificador 1.
- La publicación se realiza de manera correcta, obteniendo los datos necesarios. Se publica por cada nivel de agregación de acuerdo al INE. Se encuentran disponibles las actas para su descarga. El medio de verificación (MV) de esta etapa es el formulario F5-A-7.

10.2 Comentarios y observaciones resultantes de Simulacro 2

10.2.1 Módulo de publicación de resultados

CAPA DE APLICACIÓN

- Al iniciar la jornada se presenta una pantalla que permite poner la base de datos y las aplicaciones en “ceros” como garantía del proceso. Sin embargo, sería deseable que esta pantalla incluyera las firmas digitales generadas antes de iniciar el proceso. Esto como garantía de que la versión de la base de datos y las aplicaciones corresponden a las que fueron firmadas.
- Sería conveniente indicar que el proceso de inicialización en ceros es relativo, ya que existen catálogos como la lista nominal, estados, distritos etc., que deben ser precargados en cada jornada. Se desconoce si dichos catálogos hacen parte de la misma base firmada antes de iniciar la jornada.
- En la validación de huellas, no hay garantía de que la versión activa de la base de datos es la que se utilizó en el proceso de firmas criptográficas.
- A pesar que durante el proceso de validación es posible corregir la orientación de las imágenes, todavía se visualizan imágenes con orientación vertical.
- Existen imágenes de actas con baja calidad en comparación a otras tomadas con el mismo dispositivo u otros dispositivos, los cuales tienen las mismas características relativas a la cámara.
- Las imágenes capturadas muestran algunos contornos del acta el cual no tiene valor informativo. Sería conveniente recortar la imagen para obtener exclusivamente la imagen del acta.

CAPA OPERATIVA

- La publicación se realiza de manera correcta, obteniendo los datos necesarios.
- Se publica por cada nivel de agregación de acuerdo al 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.

10.2.2 CCV Principal

CAPA DE DATOS

- Antes de iniciar el simulacro 2, el Proveedor mostró que el inventario de archivos a los cuales se le calculó las huellas criptográficas contiene cinco archivos. Sin embargo, el Proveedor no mostró el proceso, script o método utilizado para recolectar, comprimir sus aplicaciones y generar los archivos comprimidos. No fue posible entonces, por parte del ente auditor dar fe de que el contenido de los cinco archivos de los cuales se calcularon las huellas criptográficas y que las mismas correspondan a las aplicaciones utilizadas. Se recomienda que el proveedor muestre el contenido de los scripts utilizados para colectar los archivos del inventario y ejecute dicho script en presencia del Ente auditor antes del inicio del siguiente simulacro, así como la Jornada Electoral.
- Durante el simulacro 2, el proveedor omitió el paso de generar las huellas criptográficas “originales” e inició con la generación de las huellas iniciales. Debido a esta acción del proveedor, fue necesario realizar la validación de las huellas iniciales del simulacro 2 consigo mismas y así poder generar la constancia de hechos inicial, también fue necesario utilizar las huellas del inicio del simulacro como si fueran las huellas “originales” con la finalidad de poder generar las constancias de hechos intermedia y final. Es necesario que proveedor genere las huellas criptográficas "originales" antes de iniciar el siguiente simulacro justo después de realizar la recolección del inventario en parecencia del Ente Auditor. Al inicio del simulacro se realizará por segunda vez las huellas del inventario, dichas huellas serán utilizadas para compararlas con las huellas originales obtenidas antes de iniciar el simulacro. Se adjuntan como anexo las constancias pertenecientes al Simulacro 2.
- Durante el análisis de los archivos correspondientes a las actas registradas durante el simulacro dos, no fue posible realizar la descarga de múltiples imágenes. Se recomienda que el proveedor realice la carga de las fotografías e imágenes de todas las actas o indicar el motivo por el cual no se encuentran disponibles.
- Durante el análisis de las actas registradas en la base de datos junto con las imágenes descargadas del servicio del proveedor (fotografías e imágenes escaneadas), no fue posible identificar la imagen de 27 actas marcadas como contabilizadas ni 1 marcadas como no contabilizadas (adicional a las 6 marcadas como sin acta en la base de datos). Se recomienda que el proveedor realice la carga de todas las imágenes correspondientes al SHA registrado en la base de datos debido a que si carga una imagen distinta no será posible realizar la validación de las mismas.

CAPA DE APLICACIONES

- La opción de guardar imagen en el validador es adecuada, sin embargo, ya que es opcional, algunos validadores no guardan la imagen cuando ha sido cambiada su orientación. Esto provoca que se sigan observando actas con orientación vertical en el proceso de publicación.
- En captura PREP-CASILLA algunas imágenes se visualizan un poco opacas, tal vez se deba a la luminosidad del ambiente durante el proceso de la toma fotográfica.

CAPA DE PLATAFORMA TECNOLÓGICA

- Ante ausencia de energía los 30 equipos instalados fueron protegidos correctamente por los sistemas UPS/SAI.
- Al habilitar nuevamente la energía que suministra CFE los 30 equipos instalados siguieron funcionando correctamente.

Recomendaciones:

- No se tienen observaciones, las pruebas fueron realizadas de forma exitosa.

- Al activar el suministro de la planta de emergencia los UPS detectaron la energía proporcionada por el equipo y funcionaron correctamente durante 15 minutos. Posteriormente la planta de emergencia presentó una falla en la presión de aceite y el breaker del tablero de control se botó por cual se revisa el equipo y se diagnostica que tiene una falla ya sea en el sensor que regula la presión de aceite o de algún otro tipo . Por lo anterior, se decide cancelar la prueba para continuar con el simulacro.
- Durante la ejecución de esta prueba fallaron los UPS que protegen a 3 equipos de los 30 instalados.

Recomendaciones:

- Agendar una ventana de mantenimiento para reparar la falla presentada en la planta de emergencia y calendarizar pruebas de funcionamiento de esta con carga completa durante la siguiente semana.
- Revisar la carga y baterías de los UPS que fallaron con la finalidad de realizar el remplazo de los componentes necesarios o del equipo completo según sea requerido.

Resultados:

- Se retira el enlace contratado con el proveedor TOTALPLAY y siguen operando con normalidad los equipos instalados en el CCV con el enlace contratado con el proveedor TELMEX.
- Se regresa el enlace contratado con el proveedor TOTALPLAY y siguen operando con normalidad los equipos instalados en el CCV.
- Se retira el enlace contratado con el proveedor TELMEX y siguen operando con normalidad los equipos instalados en el CCV con el enlace contratado con el proveedor TOTALPLAY.
- Se concluye la prueba con éxito.

CAPA OPERATIVA

Captura y Verificación de Datos provenientes de PREP Casilla

- 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 primeramente deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el supervisor a cargo.
- El capturista NO cuenta con un manual de usuario para el uso del sistema, debe dirigirse a su Coordinador para resolver dudas.
- El capturista obtuvo la capacitación necesaria para realizar el proceso. Para ello ha realizado ensayos 3 veces a la semana
- Muchas actas recibidas fueron rechazadas debido a que la imagen era ilegible o borrosa, como consecuencia de error del CAE que manipula el PREP Casilla.

Del Cotejo de Actas

- El verificador cuenta con gafete de identificación.
- El verificador cuenta con las credenciales para tener acceso al sistema, las cuales se le fueron otorgadas en un papel impreso.
- Si el verificador tiene las credenciales equivocadas deberá de pedirle ayuda al supervisor.
- El verificador no 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 en el CCV 1 fueron capacitados para los roles de verificador 1 y capturista de PREP Casilla.
- El rol de verificador 2 sólo lo pueden tener quienes tengan más experiencia con el sistema y que hayan participado en procesos anteriores.
- Algo que se debe destacar es que NO existe un módulo que muestre el seguimiento del estado que guardan las actas en el flujo que deben seguir. Esto técnicamente es posible mediante el código hash de cada acta (cuando se digitalizan en el CATD).
- El módulo anterior permitiría también saber lo que sucede cuando un acta se "reinicia", es decir cuando el Verificador 1 y el Verificador no pueden dar por aceptable el contenido de un acta, ya sea porque es ilegible, inconsistente o imagen borrosa. En este último caso se asume que el acta se vuelve a digitalizar en el CATD de origen y vuelve a pasar por las etapas de captura y verificación. Por el momento esto no se puede ver en el sistema.

De la Publicación de Resultados

- La publicación de la información se realiza conforme lo marca el INE.

10.2.2 CCV Alterno

CAPA DE PLATAFORMA TECNOLÓGICA

- Al realizar la prueba de funcionamiento de los UPS los 27 equipos fueron protegidos correctamente por los equipos correspondientes.
- Al realizar la prueba de la planta de emergencia se pudo validar que suministró correctamente al CCV de Respaldo durante 30 minutos a partir de las 12:05, por lo cual se concluye la prueba con éxito.
- Se retira el enlace contratado con el proveedor TOTALPLAY y siguen operando con normalidad los equipos instalados en el CCV con el enlace contratado con el proveedor TELMEX.
- Se regresa el enlace 1 contratado con el proveedor TOTALPLAY y siguen operando con normalidad los equipos instalados en el CCV.
- Se retira el enlace contratado con el proveedor TELMEX y siguen operando con normalidad los equipos instalados en el CCV con el enlace contratado con el proveedor TOTALPLAY.

CAPA OPERATIVA

- En el CCV2 sólo se cuenta con el rol de verificador 1.
- Las credenciales a los operadores le fueron dictadas.

10.2.2 CATD Victoria

CAPA DE APLICACIÓN

- Los usuarios pueden acceder libremente al navegador que esté instalado en el equipo de cómputo que tienen a su disposición. Pueden buscar en Google cualquier cosa, incluyendo imágenes, sin embargo, las redes sociales están bloqueadas, al intentar acceder a ella, el navegador se cierra automáticamente.
- Los usuarios tuvieron acceso a sus teléfonos celulares durante todo el proceso de captura.
- Actas que no aparecen. Los capturistas piden ayuda a su coordinador, vía telefónica, para saber qué hacer cuando un acta no aparece para ser capturada, el coordinador les solicita a los capturistas que estas actas se “aparten”. No se indicó que se hará posteriormente con ellas para resolver el problema.
- Los usuarios tienen botellas de agua y jugos en su lugar de trabajo, pueden existir derrames de líquidos sobre los equipos de cómputo.
- Al momento de realizar el corte de energía, el técnico les solicitó que detuvieran el proceso de captura para él poder conectar el modem al UPS y después de esto ellos pudieran continuar con el proceso, debido a este suceso se retrasó el trabajo de todos los capturistas.
- Los capturistas desconocían si se podían guardar las actas localmente para su posterior envío. Corroboramos que las actas si se guardan localmente en la computadora.
- Las actas pendientes de envío aparecen en diferente color que las demás para indicarle al usuario que aún no se han enviado. Se confirmó que las actas guardadas localmente si se pueden enviar a través de un botón “enviar actas” dentro de la interfaz, el cual lleva al usuario a otra interfaz donde se encuentran todas las actas que no han sido enviadas y se comienza un proceso de envío automáticamente. Mientras este proceso es ejecutado, el capturista no puede capturar o digitalizar más actas.

CAPA DE PLATAFORMA TECNOLÓGICA

CATD1

- Al llegar a se observó que los capturistas no tenían conexión con el servidor del sistema de captura y mencionaron que tenían ese problema desde las 12:20 hrs. Se cree que dicho problema se debió a un cambio en la IP pública del módem. Por lo que se reinició el modem y se dio de alta la nueva IP solucionando el problema.
- Los equipos UPS funcionaron con normalidad por al menos 5 minutos sin ninguna novedad.
- No fue posible realizar las pruebas con la planta de emergencia dado que había una reunión en el consejo distrital donde esta ubicado el CATD y generaría ruido durante la operación de la planta lo que causaría interrupciones a las actividades de la reunión mencionada.

CATD2

- Se observo que el modem no se encontraba conectado al UPS por lo que se desconectó de la corriente eléctrica y se conectó al UPS. Derivado de dicha desconexión, la aplicación se desconectó del servidor alrededor de 10 minutos. Por lo cual los capturistas trabajaron de manera local por el mismo tiempo. Esto se debe a que el servidor tiene filtrado por IP por lo que al reiniciar el modem fue necesario registrar la nueva IP.
- Después de los cinco minutos se conectaron los equipos a la planta eléctrica de respaldo y se mantuvieron así durante 30 minutos los cuales transcurrieron sin ninguna novedad

CAPA DE INFRAESTRUCTURA DE COMUNICACIONES

- CATD 1: Se desconectó los UPS de la corriente eléctrica para simular el corte de energía. Se observo que el modem no se encontraba conectado al UPS por lo que se desconecto de la corriente eléctrica y se conecto al UPS. Derivado de dicha desconexión, la aplicación se desconecto del servidor alrededor de 10 minutos. Por lo cual los capturistas trabajaron de manera local por el mismo tiempo. Esto se debe a que el servidor tiene filtrado por IP por lo que al reiniciar el modem fue necesario registrar la nueva IP.
- CATD2: Al llegar se observo que los capturistas no tenían conexión con el servidor los capturistas mencionaron que tenían ese problema desde las 12:20. Se cree que dicho problema se debió a un cambio en la IP publica del modem. Por lo que se reinicio el modem y se dio de alta la nueva IP solucionando el problema.
- CATD2: No se realizo pruebas con la planta de energía de respaldo dado que había reunión del personal del IETAM por lo que se generaría interrupciones por el ruido

CAPA OPERATIVA

De la toma fotográfica del Acta PREP en la casilla

- El CAE cuenta con un chaleco de identificación otorgado por el INE.
- El CAE obtuvo una capacitación antes de realizar el simulacro por parte de su supervisor del INE.
- El CAE cuenta con un manual de usuario.
- Al CAE se le asignó un dispositivo móvil en el cual tenía instalado el PREP Casilla.
- El CAE al tener una duda se dirige con su supervisor por parte del INE.
- La aplicación a la hora de tomar la fotografía dibuja un rectángulo para evadir los bordes innecesarios, pero a la hora de enviar la imagen no se respeta ese rectángulo y la imagen se envía con bordes innecesarios.
- La CAE entrevistada en el simulacro 2 tiene más conocimiento que la CAE entrevistada en el simulacro 1.
- Las CAEs entrevistadas no tiene totalmente claro lo que deben hacer respecto al entorno en donde tomarán la foto, deben seguir recomendaciones más precisas para que las imágenes no salgan borrosas. Deben ser más conscientes de la importancia que la foto sea totalmente legible.
- Se debe reafirmar la capacitación que se les da por parte del INE.

10.2.2 CATD Tampico

CAPA DE APLICACIONES

- La fecha y hora de acopio en las actas son ingresados por los capturistas también en este simulacro.
- La mayoría de las actas recibidas en el CATD fueron de PREP Casilla.
- El sistema sigue permitiendo ingresar cualquier fecha de acopio sin establecer un rango para evitar posibles errores de captura.
- Existe una opción en el sistema que no se había visto, en la cual cada capturista puede ver los detalles de todas las actas capturadas en el simulacro.
- Al realizar los cortes de luz e internet al parecer el modem cambia las direcciones IPs, causando interrupción momentánea del proceso de captura.
- Aunque con menos frecuencia, todavía existen eventos en los cuales se “pierden” temporalmente actas.
- No ha sido posible validar si el sistema almacena localmente las actas no enviadas debido a algún evento fortuito, con el propósito de recuperarla y enviarla posteriormente.

CAPA OPERATIVA

Del Acopio

- 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 supervisor por parte del proveedor le brindará apoyo.
- El acopiador es el encargado del flujo de actas, en el CATD Tampico no se cuenta con la lista donde se observa que actas le corresponden a cada capturista.
- El acopiador repartió todas las actas PREP al iniciar el simulacro.
- El simulacro comenzó a las 11:10.

De la Digitalización

- El digitalizador cuenta con gafete de identificación.
- El digitalizador deberá de contar con las credenciales necesarias para el sistema, 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 su supervisor encargado.
- En caso de ser necesario, el equipo multifunción para la digitalización puede cambiarse.
- Si el digitalizador tiene alguna duda acerca del proceso a realizar, deberá de pedir ayuda a su supervisor, o revisar el manual de usuario que se le fue otorgado.
- El digitalizador obtuvo la capacitación necesaria para realizar el proceso.
- El rol de digitalizador y capturista lo realiza una misma persona.
- Al iniciar el simulacro se repartieron el total de actas entre los digitalizadores.
- El digitalizador fue el encargado de dejar constancia de fecha y hora en el acta.

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.

10.3 Comentarios y observaciones resultantes de Simulacro 3

10.3.1 Módulo de publicación de resultados

CAPA DE DATOS

- Al inicio del simulacro 3, el *proveedor* no incluyó el script utilizado para la recolección y compresión de sus aplicaciones en la carpeta creada para la concentración del inventario. En el transcurso del simulacro 3, el *proveedor* compartió dicho *script* a través de correo electrónico y el *Ente Auditor*, al revisarlo, acordó que el contenido del *script* era adecuado para llevar a cabo la recolección y compresión de las aplicaciones y servicios que hacen parte del PREP.
- El *proveedor* ejecutó el software de generación de huellas criptográficas a la carpeta de inventario llamado “original” e informó al *Ente Auditor* que había realizado un cambio en el contenido de dicho inventario. El cambio en cuestión consistía en que el archivo “logs.zip” contenía un script en

lugar del contenido comprimido del archivo "log.txt", los cuales deberían ser iguales en principio. Además, el *proveedor* indicó que la huella criptográfica del archivo "logs.zip" no debía cambiar durante la captura de las huellas criptográficas posteriores a la original. En respuesta a los cambios realizados por el *proveedor*, el *Ente Auditor a su vez,* realizó los cambios necesarios en software de obtención de huellas criptográficas para que reflejara el cambio que el *proveedor* había realizado. Se recomienda que el *proveedor* notifique con anticipación al *Ente auditor* los cambios en el inventario que desee realizar y se solicita que el *proveedor* proporcione la descripción actualizada del archivo "logs.zip".

- Durante la generación de la constancia de hechos inicial, el software de verificación de huellas criptográficas que compara las huellas criptográficas originales con las huellas del software a utilizar en el simulacro, etiqueto **seis** archivos como "No validado" de los diez archivos almacenados en el inventario, lo que significa que las huellas criptográficas de esos seis archivos no coincidían con las huellas criptográficas originales capturadas antes de iniciar el simulacro y que hacen parte del inventario etiquetado como "Original". Las inconsistencias detectadas fueron observadas por el software en la constancia de hechos. El *proveedor* realizó un análisis de los archivos recolectados y llegó a la conclusión de que la inconsistencia fue producida por archivos temporales que se guardaron dentro de los archivos comprimidos. Después de corregir el error, el *proveedor* volvió a realizar la recolección y generación de huellas criptográficas originales e iniciales. El software del *Ente Auditor* generó la constancia de hechos inicial nuevamente. En la nueva constancia de hechos, el software no observó inconsistencias marcando a cada uno de los archivos del inventario auditado como "Correcto".
- En la dirección url https://difusores.prep2019tamps.mx/entregables/38/ proporcionada por el *proveedor* para la descarga de la base de datos, se encontraba un archivo llamado "20190525_2237_PREP.zip" el cual fue generado el día 25 de mayo a las 10:37 pm, por lo cual se asume que dicho archivo fue generado antes de iniciar el *Simulacro 3 (específicamente un día antes del simulacro)*. Lo anterior representa una inconsistencia ya que se espera que el dicha URL no contenga ningún archivo. Al realizar el corte inicial de la base de datos, se generó el archivo "20190526_1041_PREP.zip". Debido a que no se esperaba la existencia de más de un archivo en esta etapa inicial del Simulacro 3, fue necesario realizar un análisis por parte del *Ente Auditor* del contenido del archivo cargado antes del simulacro 20190525_2237_PREP.zip contra el respaldo de la base de datos inicial 20190526_1041_PREP.zip generado por el PREP. Lo anterior con el fin de verificar que realmente se encontrará vacía. Después del análisis del contenido de los dos archivos, el *Ente auditor* llegó a la conclusión de que la base de datos inicial 20190526_1041_PREP.zip se encontraba vacía. Se le recomienda al *proveedor* realizar una revisión del contenido de sus sistemas de archivos para evitar que se repitan este tipo de inconsistencias debido a que no deberían existir archivos en la carpeta del URL de difusores (https://difusores.prep2019tamps.mx/entregables/38/), lo anterior sería trivial tomando en cuenta que el PREP incluye botones para el "borrado y/o puesta en ceros de la base de datos".
- Durante el análisis de los archivos correspondientes a las actas registradas durante el Simulacro 3, no fue posible realizar la descarga de múltiples imágenes (adicionales a las marcadas como "Sin acta" en la base de datos). Se recomienda que el *proveedor* realice la carga de las fotografías e imágenes de todas las actas, de no ser posible debe de indicar el motivo por el cual no se encuentran disponibles.
- Durante el análisis de las actas registradas en la base de datos junto con las imágenes descargadas del servicio del proveedor (fotografías e imágenes escaneadas) correspondientes al Simulacro 3, no fue posible identificar las imágenes de 193 actas marcadas como "contabilizadas" ni 8 marcadas como "no contabilizadas" (adicional a las 4 actas marcadas como "sin acta" en la base de datos). Se recomienda que el *proveedor* realice la carga de todas las imágenes correspondientes al SHA

registrado en la base de datos, debido a que si carga una imagen distinta, al generar el SHA de la imagen descargada se obtendrá un SHA diferente al registrado en la base de datos y no será posible realizar la validación de las actas.

CAPA DE PLATAFORMA TECNOLÓGICA

- Inicia la generación y comprobación de huellas criptográficas con modificaciones en la cantidad de archivos a auditar y en el procedimiento definido en los simulacros anteriores.
- Alrededor de las 10:30 inicia el simulacro 3 con observaciones en la generación de las huellas criptográficas, razón por la cual el proceso se retraso por un poco más de 30 minutos.

CAPA OPERATIVA

- La publicación se realiza de manera correcta, obteniendo los datos necesarios.
- Se publica por cada nivel de agregación de acuerdo al 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.

10.3.2 CCV Principal

CAPA DE APLICACIONES

- Captura PREP Casilla: El sistema dejó enviar actas al servidor sin haber iniciado formalmente la jornada (inicialización de la base de datos)
- El sistema carece de mecanismos para verificar que la jornada a dado inicio. Esto con el fin de evitar envíos innecesarios o con acta no válidas.
- El sistema carece de notificaciones que den certeza al usuario que la imagen captura fue enviada satisfactoriamente o que ocurrió algún error.
- Validación de actas: Al denegar un acta por diferentes motivos, no se da la opción al usuario que permita indicar y describir el motivo de la denegación. Esto podría servir para efectos estadísticos y de gestión de las actas.

CAPA DE PLATAFORMA TECNOLÓGICA

- Ante ausencia de energía los 30 equipos de cómputo instalados en el CCV fueron protegidos correctamente por los sistemas UPS/SAI.
- Al habilitar nuevamente la energía que suministra CFE los 30 equipos instalados siguieron funcionando correctamente.
- Al activar el suministro de la planta de emergencia los UPS detectaron la energía proporcionada y funcionaron correctamente durante 60 minutos. Durante la ejecución de esta prueba se validar de acuerdo al consumo de combustible que el equipo de emergencia tiene una capacidad de protección estimada de 24 horas.
- Se retira el enlace principal contratado con el proveedor TOTALPLAY durante 15 minutos y siguen operando con normalidad los equipos instalados en el CCV con el enlace redundante contratado con el proveedor TELMEX.
- Se regresa el enlace contratado con el proveedor TOTALPLAY y siguen operando con normalidad los equipos instalados en el CCV.
- Se obtienen las gráficas del tráfico real de las actividades del simulacro 3 con el apoyo del proveedor PROISI.

CAPA DE INFRAESTRUCTURA DE COMUNICACIONES

- Sin observaciones, se opera con normalidad de acuerdo a lo esperado en el PTO.
- En las pruebas de redundancia se desconectó el servició de Totalplay, dejando en operación únicamente el servicio de Telmex de 12:10 pm a 12:20 pm (duración de la prueba de 10 minutos); todo continúo operando con normalidad.
- Durante los cambios de servicio de red, se detectó una ligera pérdida en la conexión, la cual fue más notoria en las cámaras de vigilancia, las cuales dejaban de mostrar imagen en el monitor durante aproximadamente 10 segundos.

CAPA OPERATIVA

Captura y Verificación de Datos provenientes de PREP Casilla

- 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 primeramente deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el supervisor a cargo.
- El capturista NO cuenta con un manual de usuario para el uso del sistema, debe dirigirse a su Coordinador para resolver dudas.
- El capturista obtuvo la capacitación necesaria para realizar el proceso. Para ello ha realizado ensayos 3 veces a la semana
- Se incluyó una opción nueva al sistema de captura de PREP Casilla, que consiste en si una acta es rechazada aparece un cuadro de diálogo donde se pueden marcas las incidencias, al iniciar el simulacro si se rechazaba el acta este dialogo no aparecía, por lo que se tuvo que eliminar la memoria caché de todos los navegadores para que esta función trabajara correctamente. Se retrasó todo el proceso debido a esto.
- Muchas actas recibidas fueron rechazadas debido a que la imagen era ilegible o borrosa, como consecuencia de error del CAE que manipula el PREP Casilla.

Del Cotejo de Actas

- El verificador cuenta con 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 no 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 en el CCV 1 fueron capacitados para los roles de verificador 1 y capturista de PREP Casilla.
- El rol de verificador 2 sólo lo pueden tener quienes tengan más experiencia con el sistema y que hayan participado en procesos anteriores.
- Si alguna acta ya fue previamente capturada mediante PREP Casilla, no le permite enviarla al CRID para su verificación.
- El capturista puede clasificar el acta como “ilegible” de ser necesario, y automáticamente el sistema inhabilita cualquier opción del registro, se envía al CCV, y un verificador se encarga de validar la información.
- Algo que se debe destacar es que NO existe un módulo que muestre el seguimiento del estado que guardan las actas en el flujo que deben seguir. Esto técnicamente es posible mediante el código hash de cada acta (cuando se digitalizan en el CATD).

- El módulo anterior permitiría también saber lo que sucede cuando un acta se "reinicia", es decir cuando el Verificador 1 y el Verificador no pueden dar por aceptable el contenido de un acta, ya sea porque es ilegible, inconsistente o imagen borrosa. En este último caso se asume que el acta se vuelve a digitalizar en el CATD de origen y vuelve a pasar por las etapas de captura y verificación. Por el momento esto no se puede ver en el sistema.

De la Publicación de Resultados

- La publicación de la información se realiza conforme lo marca el INE.

10.3.3 CCV Alterno

CAPA DE APLICACIONES

- Captura PREP Casilla: El sistema dejó enviar actas al servidor sin haber iniciado formalmente la jornada (inicialización de la base de datos)
- El sistema carece de mecanismos para verificar que la jornada a dado inicio. Esto con el fin de evitar envíos innecesarios o con acta no válidas.
- El sistema carece de notificaciones que den certeza al usuario que la imagen captura fue enviada satisfactoriamente o que ocurrió algún error.
- Validación de actas: Al denegar un acta por diferentes motivos, no se da la opción al usuario que permita indicar y describir el motivo de la denegación. Esto podría servir para efectos estadísticos y de gestión de las actas.

CAPA DE PLATAFORMA TECNOLÓGICA

- Al realizar la prueba de funcionamiento de los UPS los 27 equipos de cómputo instalados en el CCV fueron protegidos correctamente, así como los equipos de comunicaciones.
- Al realizar la prueba de la planta de emergencia se pudo validar que suministró energía correctamente al CCV de Respaldo durante 30 minutos a partir de las 12:42, por lo cual se concluye la prueba con éxito a las 13:12 hrs.
- Se retira el enlace principal contratado con el proveedor TOTALPLAY por 30 minutos y siguen operando con normalidad los equipos instalados en el CCV con el enlace redundante contratado con el proveedor TELMEX.
- Se integra nuevamente el enlace contratado con el proveedor TOTALPLAY y siguen operando con normalidad los equipos instalados en el CCV.

CAPA DE INFRAESTRUCTURA DE COMUNICACIONES

- Desde el simulacro 1 se observó que se contaba con un modem de red inalámbrica cuya contraseña era la predeterminada; la contraseña está oculta con marcador permanente.

CAPA OPERATIVA

- En el CCV2 sólo se cuenta con el rol de verificador 1.
- Las credenciales a los operadores le fueron dictadas.

10.3.4 CATD Victoria

CAPA DE APLICACIONES

- Las credenciales para ingresar a la aplicación son proporcionadas de forma escrita en papel.
- La fecha de acopio ya se encuentra restringida, al parecer está condicionada a un día completo, es decir, si se ingresaba una hora pasada del día actual marcaba una alerta que decía que la fecha ingresada excedía a la fecha de la jornada (en este caso del simulacro).
- Al parecer se tuvo problemas con la inicialización de las bases de datos a 0, sin embargo este evento no fue notificado por la aplicación se permitió la captura y el envío de algunas actas sin haber iniciado la jornada.
- Esta vez se efectuó un corte de luz de 11:30 a.m a 11:51 a.m en el que los UPS funcionaron correctamente y permitieron continuar con el proceso normal como se esperaba.
- En el CATD Distrito 15 se detectaron otras dos personas trabajando sobre un sistema web del IEATAM en donde registraban actas, se desconoce el motivo

CAPA DE PLATAFORMA TECNOLÓGICA

CATD1

- Los equipos UPS funcionaron con normalidad por al menos 5 minutos sin ninguna novedad.
- No fue posible realizar las pruebas con la planta de emergencia dado que había una reunión en el consejo distrital donde esta ubicado el CATD y generaría ruido durante la operación de la planta lo que causaría interrupciones a las actividades de la reunión mencionada.

Recomendaciones:

- Dado que no fue posible durante los simulacros probar la planta de emergencia de este CATD, se recomienda al menos asegurarse previamente que el equipo móvil asignado funciona correctamente y tiene disponible el combustible requerido.

CATD2

- Los equipos UPS/SAI protegieron correctamente a todos los equipos de cómputo por 5 minutos.
- Después de los cinco minutos se conectaron los equipos a la planta eléctrica de respaldo y se mantuvieron así durante 15 minutos los cuales transcurrieron sin ninguna novedad.

CAPA DE INFRAESTRUCTURA DE COMUNICACIONES

CATD 1

- A las 11:00 horas se inicio la captura de las actas de pruebas sin ninguna novedad.
- A las 11:30 horas se desconectaron los UPS de la corriente eléctrica para simular el corte de energía. Después de los cinco minutos se conectaron los equipos a la planta eléctrica de respaldo y se mantuvo así durante 15 minutos los cuales transcurrieron sin ninguna novedad.
- A las 11:50 horas se regresaron los equipos a la corriente eléctrica convencional y se prosiguió con la captura de la actas de prueba.

CATD 2

- A las 12:00 se desconectó los UPS de la corriente eléctrica para simular el corte de energía. Los UPS funcionaron con normalidad por al menos 5 minutos sin ninguna novedad.
- No se realizaron pruebas con planta de energía de respaldo dado que había reunión del personal del IETAM por lo que se generaría interrupciones por el ruido.
- Las computadoras cuentan con acceso a internet sin embargo tienen restringido el acceso a ciertas paginas principalmente redes sociales.

CAPA OPERATIVA

De la toma fotográfica del Acta PREP en la casilla

- El CAE cuenta con un chaleco de identificación otorgado por el INE.
- El CAE obtuvo una capacitación antes de realizar el simulacro por parte de su supervisor del INE.
- El CAE cuenta con un manual de usuario, pero no lo mostró.
- Al CAE se le asignó un dispositivo móvil en el cual tenía instalado el PREP Casilla.
- El CAE al tener una duda se dirige con el responsable de Voz y Datos del INE.
- Al CAE se le otorgaron las credenciales desde que le dieron el teléfono y no han cambiado, no saben si en la jornada les otorgaran nuevas credenciales.
- La aplicación a la hora de tomar la fotografía dibuja un rectángulo para evadir los bordes innecesarios de la foto, pero a la hora de enviar la imagen no se respeta ese rectángulo y la imagen se envía con bordes innecesarios.
- La CAE indicó que sus compañeros le dijeron que era mejor tomar la foto del acta de manera manual, no con el QR.
- Se probó que haciendo la toma fotográfica de manera manual se puede tomar la foto de otra acta, si hubiera confusión, lo cual retrasaría el conteo en el CCV ya que habría que reiniciar la captura de esa acta nuevamente
- Se debe reafirmar la capacitación que se les da por parte del INE.

Del Acopio

- 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 supervisor por parte del proveedor le brindará apoyo.
- El acopiador es el encargado del flujo de actas, en el CATD Tampico no se cuenta con la lista donde se observa que actas le corresponden a cada capturista.

- El acopiador repartió todas las actas PREP al iniciar el simulacro.
- El acopiador es el encargado del flujo de actas, en el CATD del distrito 14 se cuenta con una lista de las actas en la cual se va anotando si ya ha sido capturada y el nombre del operador que realizó la digitalización y captura.
    - En el CATD del distrito 15 se tuvo que retirar el acopiador por motivos personales, por lo que las actas se tuvieron que repartir entre el total de operadores, no hubo quien sustituyera el rol del acopiador.

De la Digitalización

- El digitalizador cuenta con gafete de identificación.
- El digitalizador deberá de contar con las credenciales necesarias para el sistema, 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 su supervisor encargado.
- En caso de ser necesario, el equipo multifunción para la digitalización puede cambiarse.
- Si el digitalizador tiene alguna duda acerca del proceso a realizar, deberá de pedir ayuda a su supervisor, o revisar el manual de usuario que se le fue otorgado.
- El digitalizador obtuvo la capacitación necesaria para realizar el proceso.
- El rol de digitalizador y capturista lo realiza una misma persona.
- Al iniciar el simulacro se repartieron el total de actas entre los digitalizadores.
- El digitalizador fue el encargado de dejar constancia de fecha y hora en el acta.

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. Análisis de Riesgos

11.1 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 Aplicación, en cada uno de sus eventos y sus valoraciones de acuerdo con la metodología MAGERIT v.3.

11.2 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

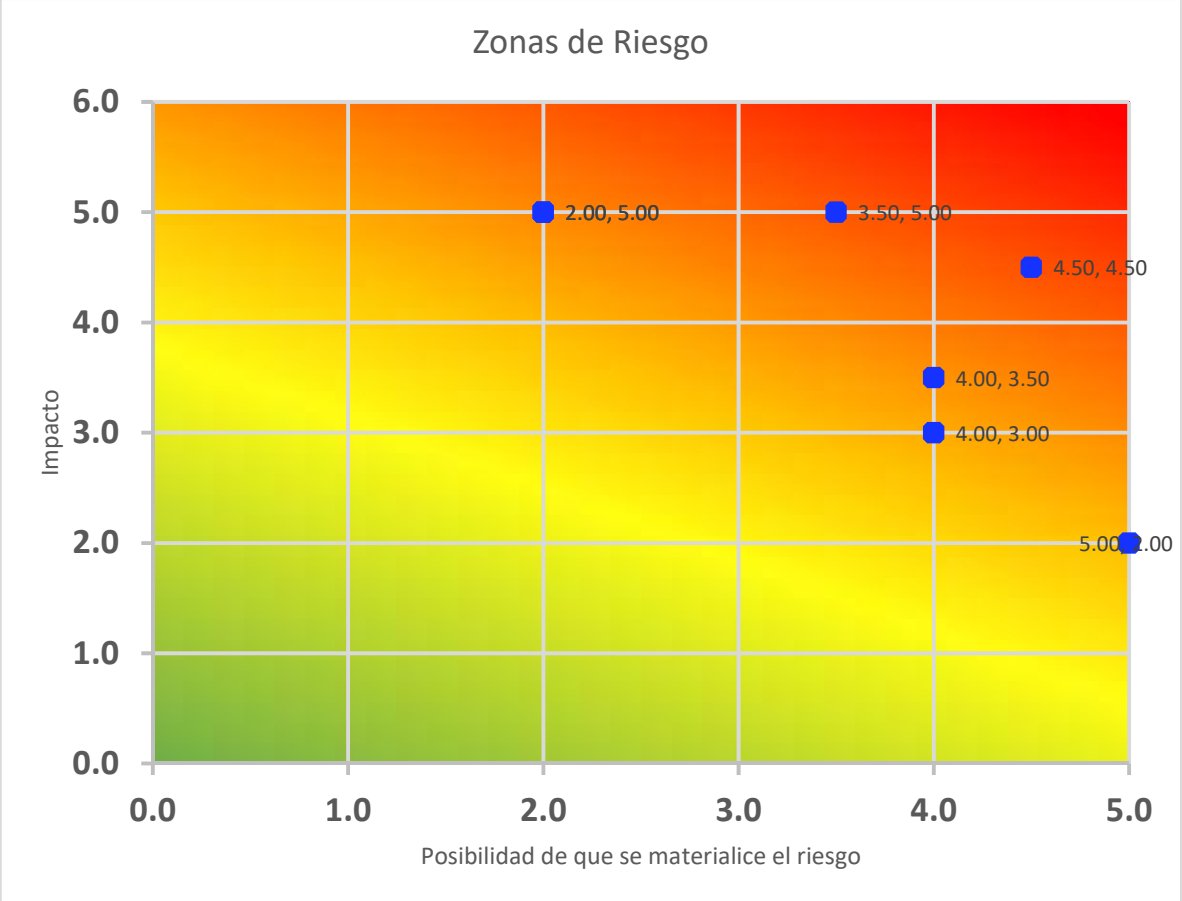


Figura 11.1 Mapa de calor. Nivel: Operativo.

11.3 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	TAREA/VULNERABILIDAD	AMENAZA	IMPACTO SOBRE LA OPERACIÓN DEL SISTEMA	POSIBILIDAD DE QUE SE MATERIALICE LA AMENAZA
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	3
	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	5
	La base de datos cumple parcialmente con las buenas prácticas.	Latencia en el proceso	1	3
	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	Intento de fraude o sabotaje	5	4

	mecanismo de versionamiento por parte del proveedor que dé garantías al 100% de la versión productiva no cambia.			
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
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	4
	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	Intento de fraude o sabotaje	5	1

	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			
	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	3
	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
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
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
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

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	2.8
ID-02	Captura de información	2.9	2.4
ID-03	Validación	3.5	2.5
ID-04	Toma Fotográfica	2.0	2.3
ID-05	Publicación de resultados	2.4	2.7
ID-06	Auditoría a los eventos del proceso	2.3	3.3
ID-10	Disponibilidad / Escalabilidad	3.0	2.7

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

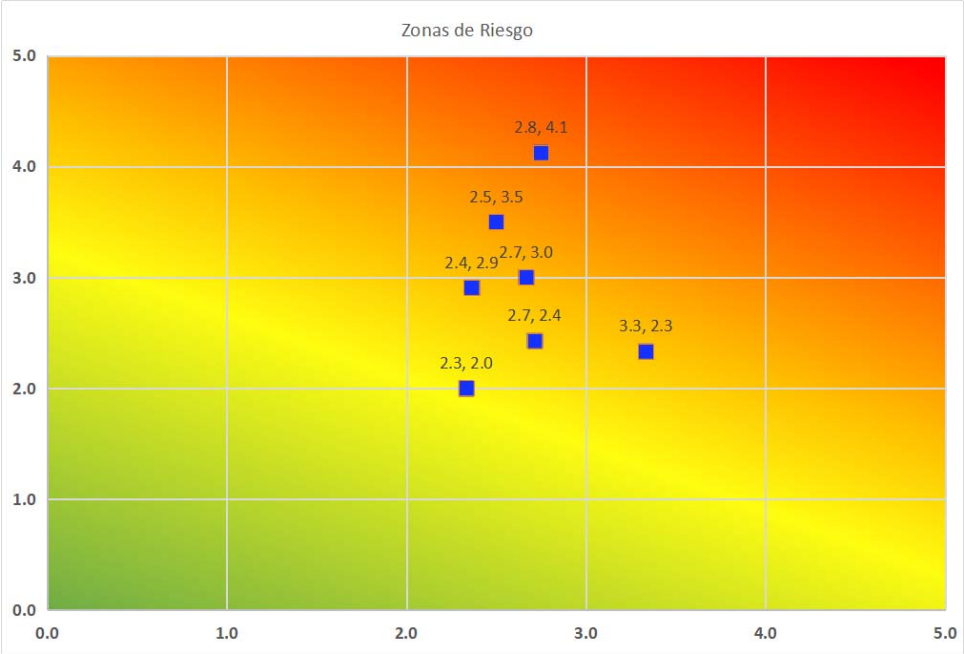


Figura 11.2 Zona de riesgos de los eventos identificados en la capa de datos y aplicación.

Del anterior diagrama se observa un nivel de riesgo considerable en los escenarios que corresponden: Inicialización y manejo de la base de datos y del sistema de archivos; Validación. Por lo anterior, se deberá poner especial atención a minimizar estos riesgos durante la Jornada Electoral.

12. Conclusiones

En el presente documento se presentaron los resultados del proceso de Auditoría al Sistema Informático y a la Infraestructura Tecnológica del Programa de Resultados Electorales para el Proceso Electoral Ordinario Local 2018-2019 (PREP) llevado a cabo entre el 3 de marzo y el 1 de junio de 2019.

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 del Instituto Electoral de Tamaulipas quien mostró disposición para obtener la información requerida.

Se han documentado observaciones específicas sobre algún paso del Proceso Técnico Operativo, sobre alguna funcionalidad del sistema informático del PREP o sobre la base de datos que lo compone, y en términos generales se han atendido la mayor parte de ellas. La observaciones que no han sido atendidas, no son críticas para la operación del PREP y son consideradas como áreas de oportunidad para procesos futuros.