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 para el Proceso Electoral Ordinario Local 2017-2018 (PREP).

Informe Final de Auditoría al PREP 2018

V5.0

Ciudad Victoria, Tamaulipas. 30 de junio de 2018.

Versión	1.0
Fecha de elaboración	Junio 08, 2018.

HISTORIAL DE VERSIONES	
Número de Versión	2.0
Fecha de actualización	Junio 18, 208.
Responsable de la actualización	Heidy Nallely Obregón Reta
Resumen de la actualización	Integración de información de las diferentes capas.
Número de Versión	3.0
Fecha de actualización	Junio 25, 208.
Responsable de la actualización	Arturo Díaz Pérez
Resumen de la actualización	Integración de información de las diferentes capas.
Número de Versión	4.0
Fecha de actualización	Junio 25, 208.
Responsable de la actualización	Arturo Díaz Pérez
Resumen de la actualización	Generación de huellas criptográficas del sistema informático.
Fecha de actualización	Junio 30, 208.
Responsable de la actualización	Arturo Díaz Pérez
Resumen de la actualización	Actualización con respecto a la atención de las observaciones realizadas durante los simulacros

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

RESPONSABLES	
De la revisión	Heidy Nallely Obregón Reta
Organización	Cinvestav-Tamaulipas
Puesto	
Firma	
De la aprobación	Arturo Díaz Pérez
Organización	Cinvestav-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.
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.
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 2018	Programa de Resultados Electorales Preliminares para el año 2018
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 2017-2018 (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 2 de abril y el 30 de junio de 2018. 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 2018.
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 2 de abril y el 8 de junio de 2018, 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 previstos entre el 09 de junio y el 30 de junio de 2018.

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

Ciudad Victoria, Tamaulipas, a los treinta días del mes de junio de dos mil dieciocho.

Dr. Arturo Díaz Pérez
Ente Auditor
Cinvestav Tamaulipas

Dictamen

Con base en la revisión llevada a cabo entre el 2 de abril y el 30 de junio de 2018 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 mínimos para la operación del PREP durante la jornada electoral del próximo 1 de julio de 2018.
2. Se ha definido un procedimiento técnico metodológico para garantizar que el sistema informático auditada es el que se utilizará durante la jornada electoral del 1 de julio.
3. El procedimiento técnico metodológico también valida que las bases de datos a usar antes del inicio del PREP, el 1 de julio de 2018, 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 negación de servicio básicos.

El presente informe se emite en Ciudad Victoria, Tamaulipas, el día treinta de junio de dos mil dieciocho.

Dr. Arturo Díaz Pérez
Ente Auditor
Cinvestav - Tamaulipas

Parte I

Informe Preliminar de Auditoría al PREP 2018

1. Introducción

En 1 de julio de 2018 se llevarán a cabo elecciones locales en el Estado de Tamaulipas en donde se elegirán a 43 presidentes municipales de los ayuntamientos de la entidad. El Instituto Electoral de Tamaulipas (IETAM) será encargado de la organización de las elecciones. Como parte de la normatividad aplicable, el IETAM estará encargado de instrumentar un Programa de Resultados Preliminares (PREP) mismo que el día de la elección tiene la función de difundir los resultados preliminares (no oficiales) de la elección. La instrumentación del PREP se debe iniciar con seis meses de anticipación al día de la jornada electoral. Los servicios de auditoría al PREP dieron inicio el pasado 2 de abril. En este periodo se ha llevado a cabo la revisión de la implementación del PREP, se han verificado tres simulacros de su operación general.

El reglamento del Instituto Nacional Electoral establece que los OPL deberán designar un ente auditor, preferentemente una institución académica con experiencia, para llevar a cabo la auditoría del PREP. La auditoría al PREP debe cubrir como mínimo las pruebas de caja negra a todos los procesos del sistema informático y el análisis de vulnerabilidades del sistema informático provisto para el PREP. El INE ha establecido las siguientes líneas de trabajo para llevar a cabo los servicios de auditoría al sistema informático y a la infraestructura tecnológica del PREP: 1) Pruebas funcionales de caja negra al sistema informático del PREP 2018, 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 describe el desarrollo de los servicios de auditoría informática al PREP 2018. Los servicios de auditoría han tomado como base los lineamientos establecidos en el documento "Proceso técnico operativo para el programa de resultados electorales preliminares para el proceso electoral ordinario 2017 – 2018 del Estado de Tamaulipas" emitido por el Instituto Electoral de Tamaulipas (IETAM) el pasado 30 de enero de 2018, en donde se describen los alcances del PREP y las especificaciones funcionales de cada uno de los procesos que componen programa. Así también, los servicios de auditoría consideran 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 han tomado en consideración el documento "Recomendación para la selección de entes auditores", emitido por el INE en marzo de 2018 particularmente en los puntos que se refieren a las recomendaciones sobre auditoría de seguridad a la infraestructura tecnológica.

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 una 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) concentración de los resultados establecidos en las actas, 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:
   iii. Pruebas funcionales de caja negra al sistema informático para evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares.
   iv. 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 2018.
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.

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 en el párrafo anterior.

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

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

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

El proceso completo de auditoría al PREP se llevó a cabo en dos fases. La **fase 1**, comprendida entre el 2 de abril y el 8 de junio de 2018, 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 previstos entre el 09 de junio y el 30 de junio de 2018. La fase 2 se completará con las actividades del día de la jornada electoral (1 de julio de 2018) y la entrega del informe final (16 de julio de 2018).

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.

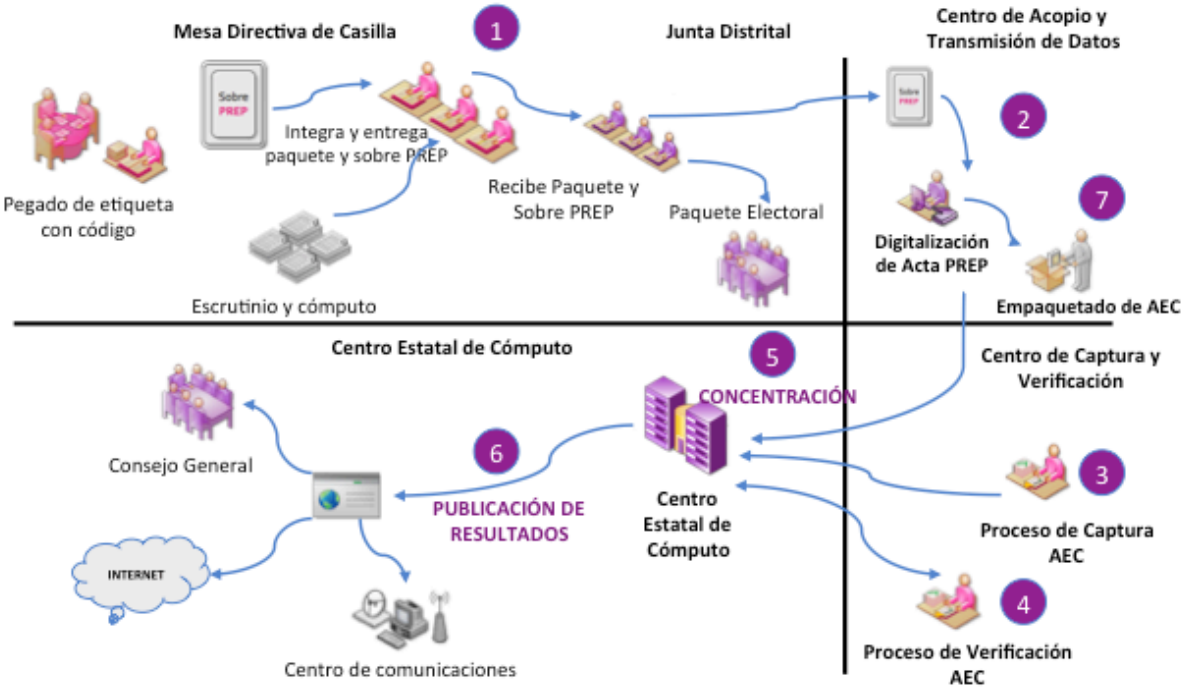

Figura 2.1. Centros de información típicos que participan en el PREP.

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.

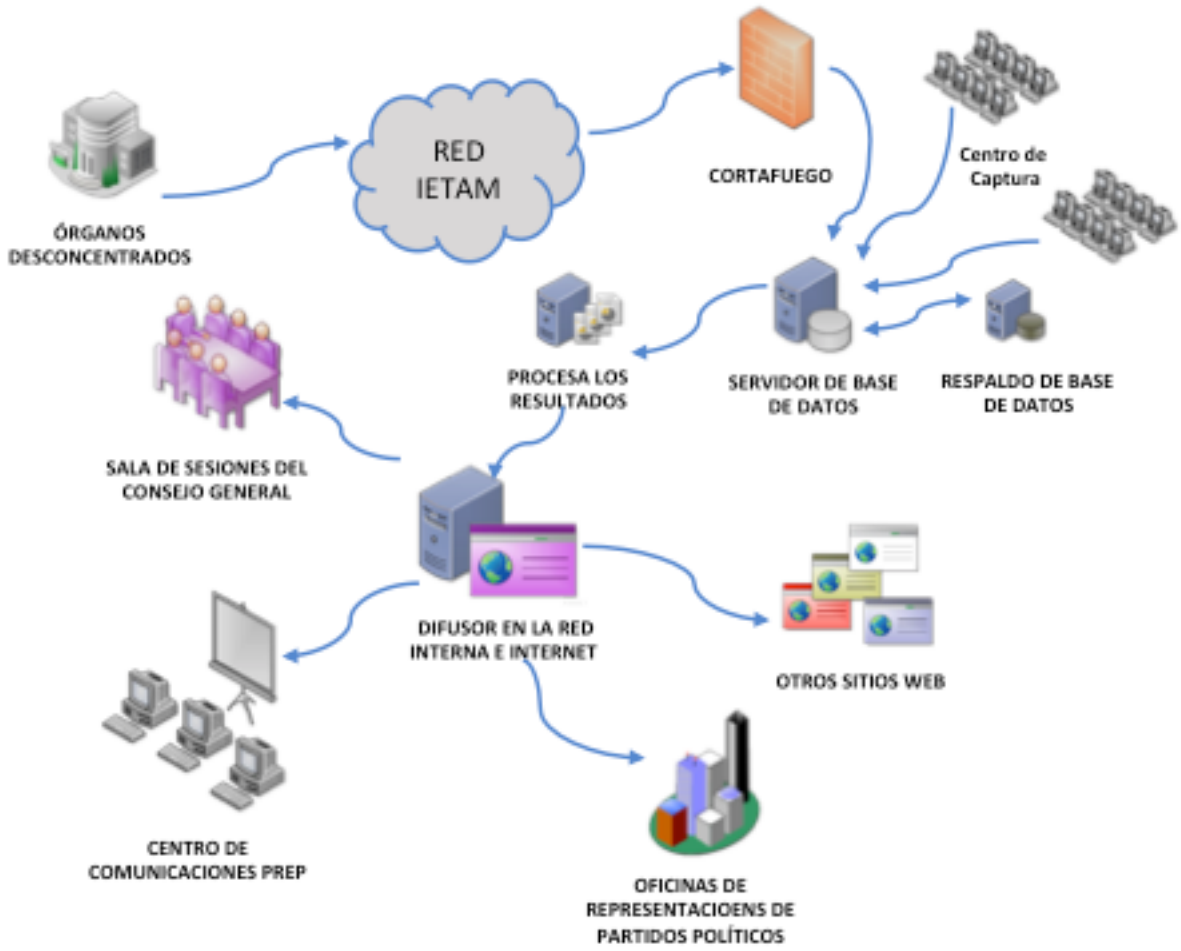

Figura 2.2. Infraestructura típica usada un un Sistema PREP.

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 5.1. Actividades detalladas de la etapa Toma Fotográfica de Acta PREP.

Fecha	Tipo de prueba	Actividades realizadas
31/mayo/2018	Pruebas preliminares	Revisión parcial al sistema informático. Etapas 2-5.
1/junio/2018	Pruebas preliminares	Revisión parcial al sistema informático. Etapas 2-5.
10/junio/2018	Simulacro 1	Revisión parcial al sistema informático. Etapas 1-6.
17/junio/2018	Simulacro 2	Revisión parcial al sistema informático. Etapas 2-6.
24/junio/2018	Simulacro 3	Revisión parcial al sistema informático. Etapas 1-6.

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 5.2. Actividades detalladas de la etapa Toma Fotográfica de Acta PREP.

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 5.3. Actividades detalladas de la etapa Acopio de Acta PREP.

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 5.4. Actividades detalladas de la etapa Digitalización de Acta PREP.

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 5.5. Actividades detalladas de la etapa Captura y Verificación de datos de Acta PREP.

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 5.6. Actividades detalladas de la etapa Cotejo de Actas PREP.

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 5.7. Actividades detalladas de la etapa Publicación de resultados.

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. 5.1)
2. Acopio de Acta PREP (Fig. 5.2)
3. Digitalización de Acta PREP (Fig. 5.3)
4. Captura y verificación de datos de Acta PREP (Fig. 5.4)
5. Cotejo de Actas PREP (Fig. 5.5)
6. Publicación de resultados (Fig. 5.6)

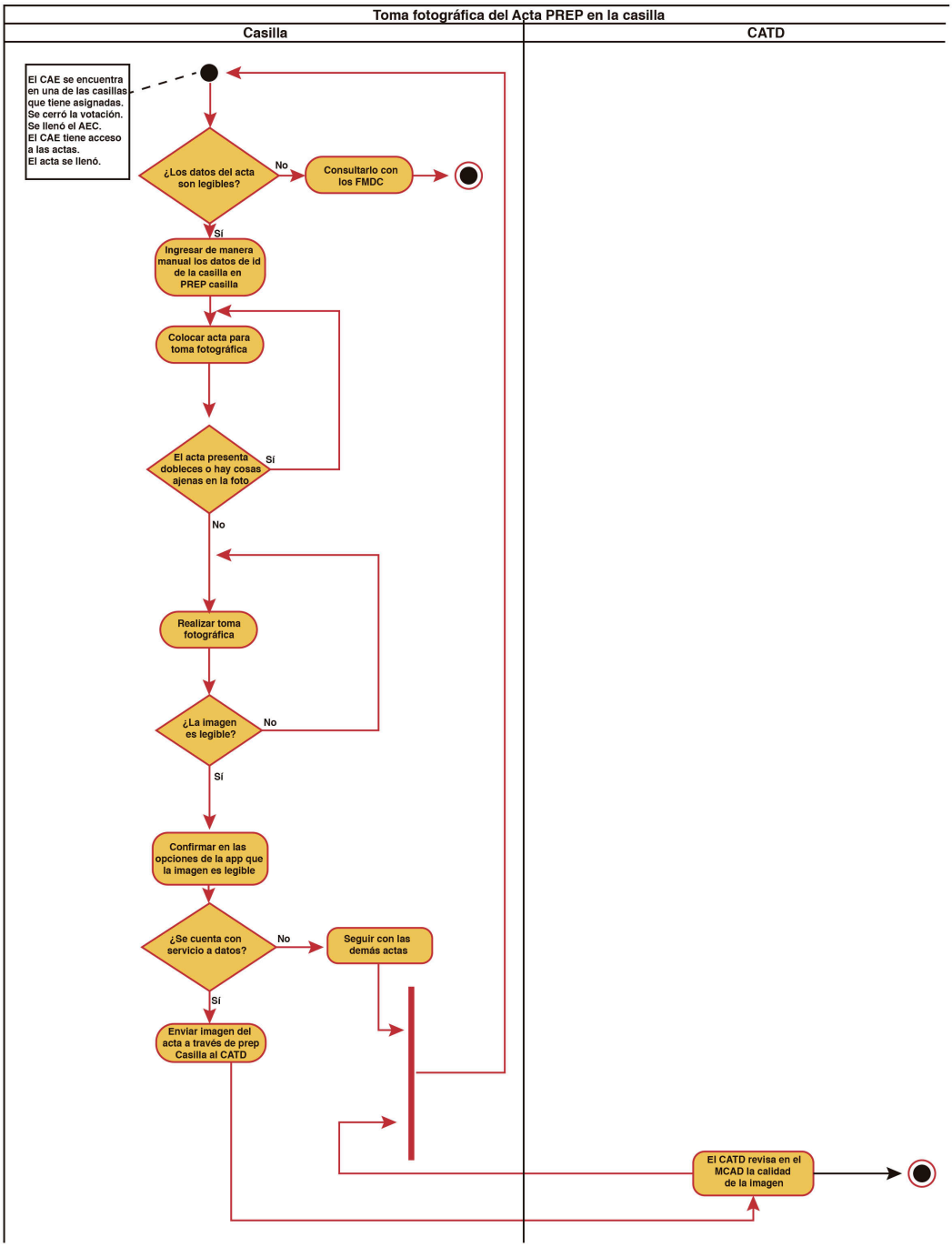

Figura 5.A.1. Toma fotográfica del Acta PREP en casilla.

Figura 5.1. Flujo de información y actividades de la etapa Toma Fotográfica del Acta PREP en casilla. Capa 5: Nivel Operación.

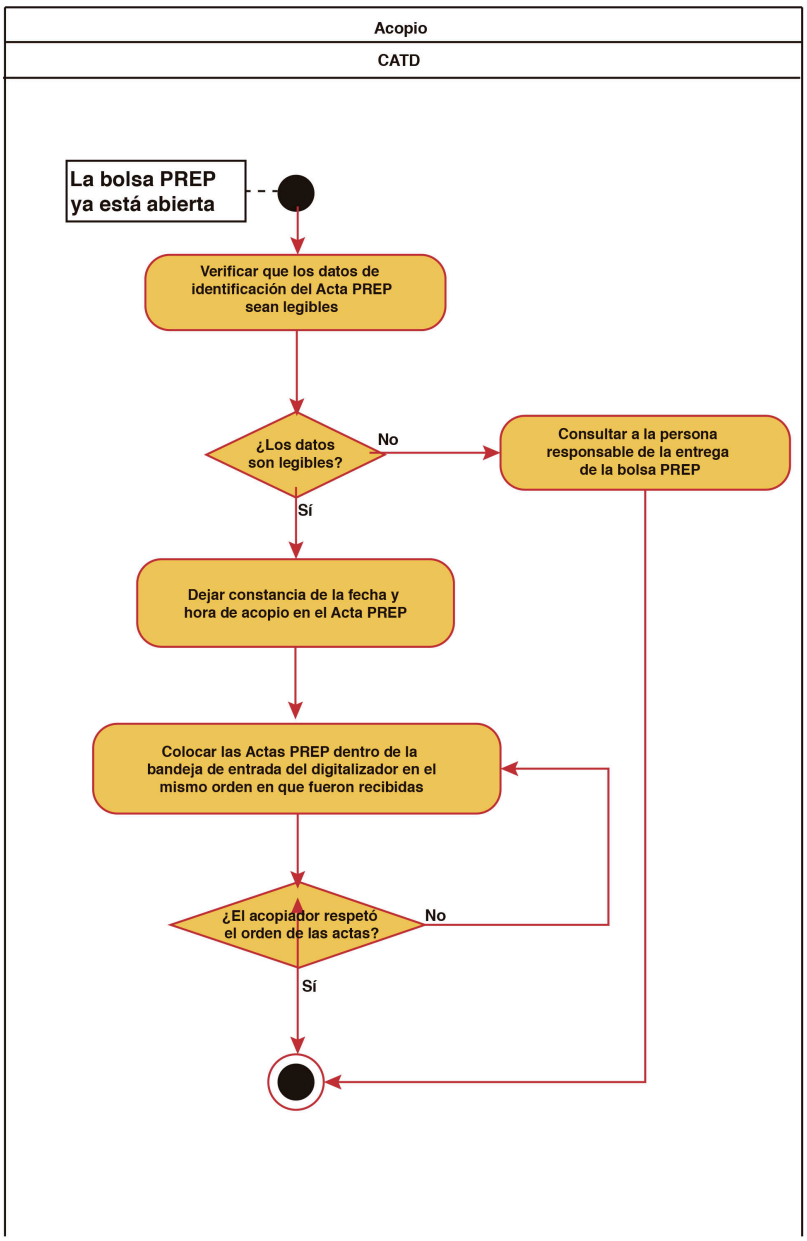

Figura 5.A.2. Acopio de Acta PREP

Figura 5.2. Flujo de información y actividades de la etapa Acopio de Acta PREP. Capa 5: Nivel Operación.

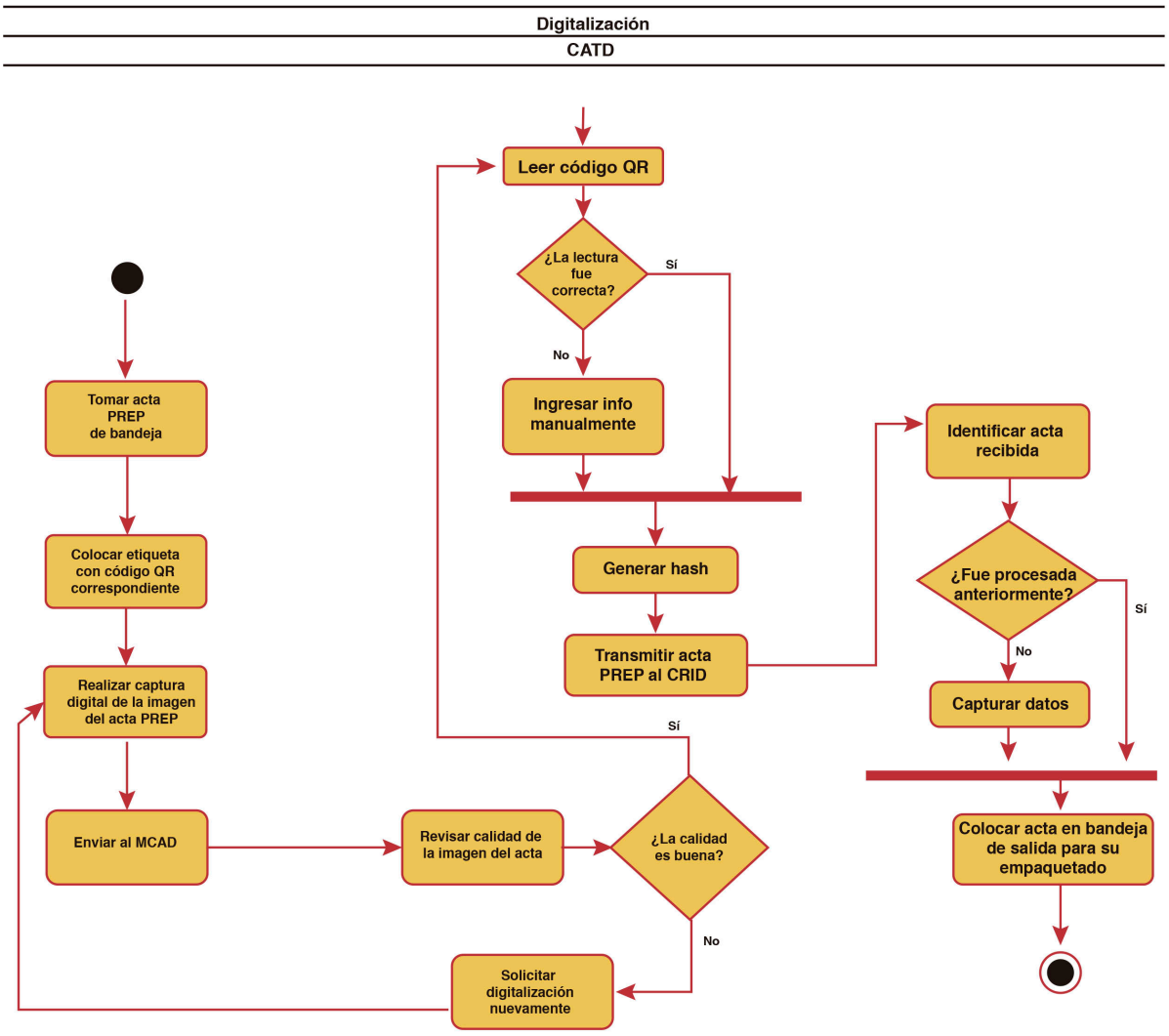

Figura 5.A.3 Digitalización de Acta PREP

Figura 5.3. Flujo de información y actividades de la etapa Digitalización de Acta PREP. Capa 5: Nivel Operación.

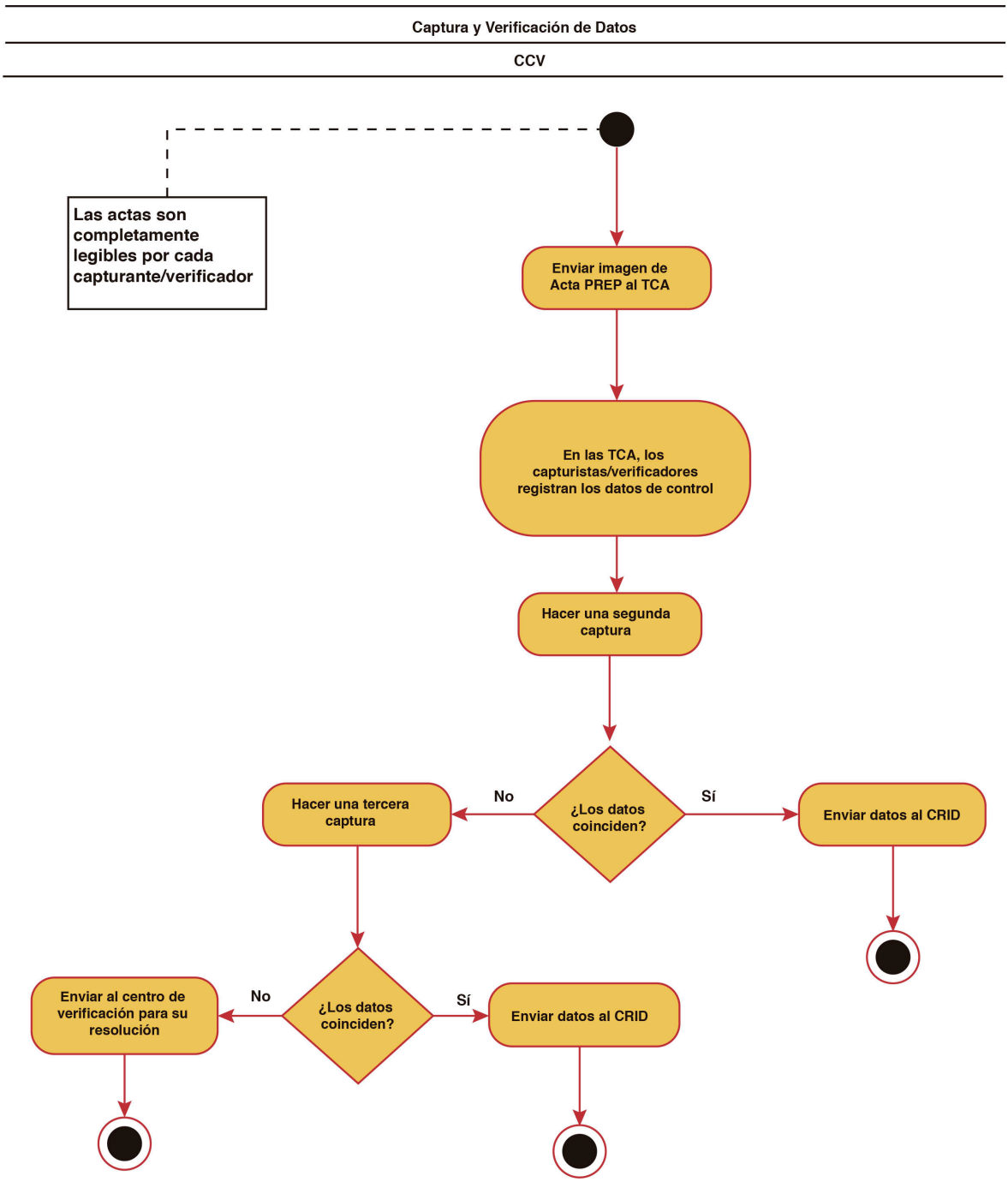

Figura 5.A.4 Captura y verificación de datos de Acta PREP

Figura 5.4. Flujo de información y actividades de la etapa Captura y verificación de datos de Acta PREP. Capa 5: Nivel Operación.

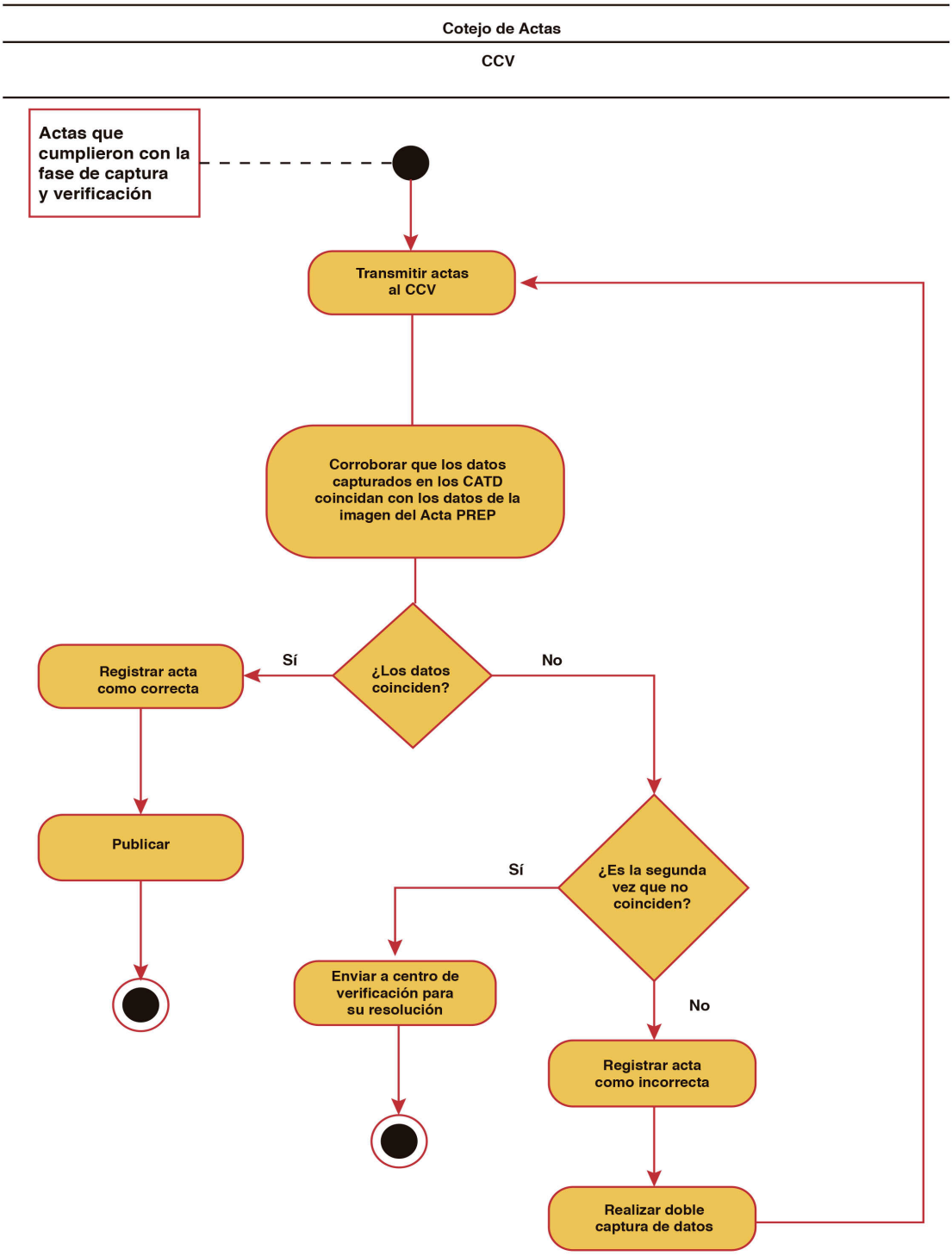

Figura 5.A.5. Cotejo de Actas PREP

Figura 5.5. Flujo de información y actividades de la etapa Cotejo de Actas PREP. Capa 5: Nivel Operación.

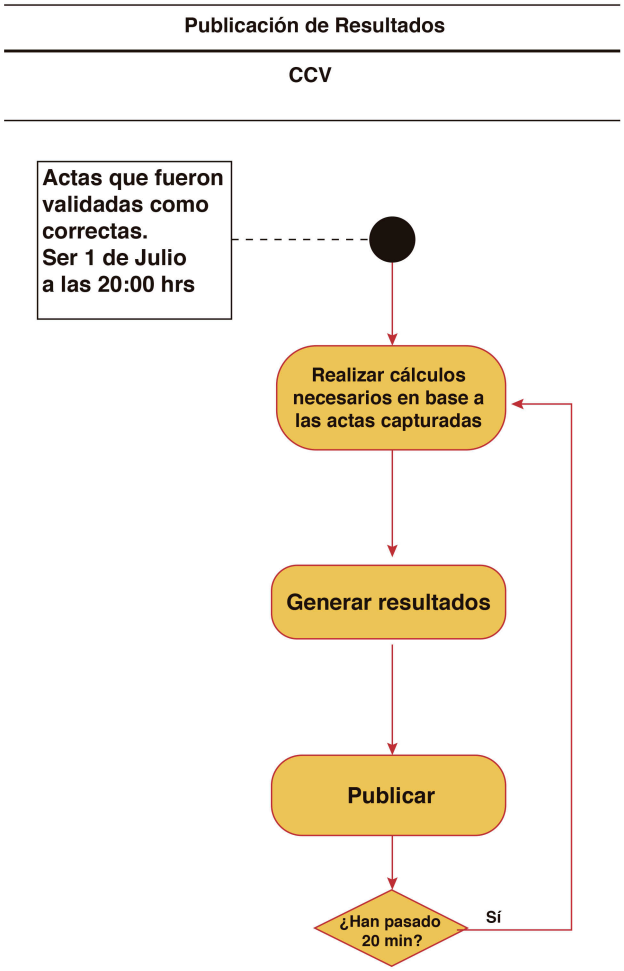

Figura 5.A.6. Publicación de resultados

Figura 5.6. 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 5.8.*

Tabla 5.8. 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.

Tabla 5.9. 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 5.10 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 5.11. 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 5.12 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.

Tabla 5.13. 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 5.14. 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 5.15. 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 5.16. 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 5.17. 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 5.18.*

Tabla 5.18. 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.

Tabla 5.19. 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 5.20. 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 5.21. 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 5.22. 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 5.23.*

Tabla 5.23. 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.

Tabla 5.24. 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 5.25. 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 5.26. 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 5.27. 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 5.28. 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:

Esta fase no se auditó debido a la falta de personal capacitado para las pruebas, que el IETAM y el INE aún no definen aspectos puntuales relacionados con la fase y que aún no se cuentan con los dispositivos móviles con los que se llevará a cabo la fase. El proveedor ya tiene desarrollada la aplicación móvil pero aún continúa haciendo modificaciones de acuerdo con sugerencias del IETAM. El medio de verificación (MV) de esta etapa es el formulario F5-A-1.

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 2017- 2018.
   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 acopiado puede tener, a su vez, 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 coordinador del IETAM o del proveedor le brindará apoyo. El acopiador es el encargado exclusivo del flujo de actas y es quien debe controlar en todo momento las actas. Si llega a tener acceso al CATD una persona ajena al proceso, el acopiador pide apoyo al oficial de seguridad encargado. El medio de verificación (MV) de esta etapa es el formulario F5-A-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. MV F5-A-2-2-B, F5-A-2-3-B.

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. MV F5-A-2-4-D, F5-A-2-4.1-D.

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. MV F5-A-2-5-B.

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. MV F5-A-2-6-B.

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. MV F5-A-2-7-A.

5.6.3 De la Digitalización

Comentario general:

El digitalizador deberá de contar con un gafete de identificación. El digitalizador recibirá el acta de manera personal mediante el acopiador. El digitalizador deberá de contar con las credenciales necesarias acceder y manipular el sistema. El digitalizador deberá de revisar el buen funcionamiento del equipo, y que el sistema informático esté actualizado a su versión más reciente. En caso de detectar un error en el equipo de cómputo o el sistema, deberá comunicarlo con su coordinador encargado, el cual si no puede resolver, deberá de ponerse en contacto con el coordinador del proveedor. En caso de ser necesario, el equipo multifunción para la digitalización puede cambiarse. Esta fase no cuenta con una bitácora donde se registre el proceso ni actividades propias del proceso. Si el digitalizador tiene alguna duda acerca de la tarea a realizar deberá de pedir ayuda a su coordinador a cargo. El medio de verificación (MV) de esta etapa es el formulario F5-A-3.

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, posicionando el Acta PREP como se lo establecieron para realizar una correcta digitalización. Queda pendiente de verificar que no quede almacenada el acta en ningún dispositivo. MV F5-A-3-8-A, F5-A-3-9-B.

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. MV F5-A-3-13-A.

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: Cuando se digitaliza el acta se escanea el código QR impreso en ella, en caso de tener una mala lectura del mismo, el digitalizador deberá de ingresar la información del acta de manera manual en el sistema. En caso de detectar un error deberá de comunicarlo con su coordinador encargado, el cual si no puede resolver, deberá de ponerse en contacto con el coordinador asignado por medio del proveedor. MV F5-A-3-14-B, F5-A-3-14.1-B, F5-A-3-14.1.1-B.

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: La generación del hash se realiza por el sistema central, una vez que la imagen del acta es recibida. MV F5-A-3-15-C, F5-A-3-15.1-C, F5-A-3-15.2-C, F5-A-3-16-C.

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. MV F5-A-3-19-B.

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

Comentario general:

El capturista deberá de estar en el TCA correspondiente, los cuales se asignan con anticipación por parte del proveedor. El capturista deberá contar con un gafete de identificación. El capturista deberá contar con las credenciales necesarias para el acceso y manipulación del sistema, las cuales estarán en un archivo de texto plano en el escritorio del equipo de cómputo. El capturista primero deberá verificar su acceso al sistema, en caso de tener un error deberá de acudir con el coordinador a cargo. El capturista cuenta con un manual de usuario para el uso del sistema informático. Quedó pendiente de verificar que no quede almacenado algún dato del acta en el equipo de cómputo; esto porque hay indicios de que se guardan las actas digitalizadas. Esta fase no cuenta con una bitácora donde se registre el proceso ni actividades propias del proceso. El medio de verificación (MV) de esta etapa es el formulario F5-A-4.

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.

Comentarios: El capturista deberá de realizar una primera solicitud de la fotografía del Acta PREP, en caso de tener un error, deberá de acudir con el coordinador a cargo. El capturista deberá verificar que la imagen sea legible, y clasificar el acta como "legible". El capturista deberá de realizar el registro de los datos asentados de la imagen del acta. El capturista deberá de solicitar el acta por segunda vez, y realizar el registro de los datos asentados en la imagen del acta. Si el acta se clasifica como "ilegible" en las dos capturas, se enviara al Centro de Verificación para su resolución. MV F5-A-4-6-A, F5-A-4-6.1-A, F5-A-4-8-A, F5-A-4-9-A, F5-A-4-10-A, F5-A-4-12-A, F5-A-4-15-A, F5-A-4-17-D, F5-A-4-17.1-D.

5.6.5 De la Captura y Verificación de Datos en el CATD

Comentario general:

El capturista deberá de estar en el TCA correspondiente, los cuales se asignan con anticipación por parte del proveedor. El capturista deberá de contar con un gafete de identificación. El capturista deberá de contar con las credenciales necesarias para el acceso y manipulación del sistema, las cuales estarán en un archivo de texto plano en el escritorio del equipo de cómputo. El capturista deberá de verificar su acceso al sistema, en caso de tener un error deberá de acudir con el coordinador a cargo. El capturista cuenta con un manual de usuario para el uso del sistema. Quedó pendiente de verificar que no quede almacenado algún dato del acta en el equipo de cómputo; esto porque hay indicios de que se guardan las actas digitalizadas. Esta fase no cuenta con una bitácora donde se registre el proceso ni actividades propias del proceso. El medio de verificación (MV) de esta etapa es el formulario F5-A-5.

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. MV F5-A-5-10-A.

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. MV F5-A-5-10-A.

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. MV F5-A-5-13-A, F5-A-5-14-B.

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. MV F5-A-5-16-B.

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. MV F5-A-5-15-A.

5.6.6 Del Cotejo de Actas

Comentario general:

El verificador deberá de contar con un gafete de identificación. El verificador encontrará sus credenciales para tener acceso y manipulación del sistema en un archivo de texto plano ubicado en el escritorio del equipo de cómputo. Las credenciales las asignará de manera anticipada el coordinador del proveedor. Si el verificador tiene las credenciales equivocadas deberá de pedirle ayuda al coordinador. El verificador cuenta con un manual de usuario para el uso del sistema informático. Quedó pendiente de verificar que no quede almacenado algún dato del acta en el equipo de cómputo usado. Esta fase no cuenta con una bitácora donde se registre el proceso ni actividades propias del proceso. El medio de verificación (MV) de esta etapa es el formulario F5-A-6.

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. MV F5-A-6-1-B, F5-A-6-1.1-B, F5-A-6-1.2-B.

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. MV F5-A-6-2-D, F5-A-6-5-A, F5-A-6-5.1-D, F5-A-6-5.3-D, F5-A-6-7-A, F5-A-6-8.1-A, F5-A-6-9-A, F5-A-6-10-A, F5-A-6-11-A.

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:

Esta fase se auditó durante los Simulacros 1, 2 y 3. 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 1 de julio de 2018 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 todo lo identificado y observado con la aplicación de los cuestionarios generados se hizo un análisis para determinar cuándo se cumplen o no las indicaciones del PTO. Esto también 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 que faciliten conocer algunos aspectos que no está claro 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

En esta sección se 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, conforme a lo establecido en el artículo 347, numeral 1, inciso a) del Reglamento de Elecciones.

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 siguiente 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 delegado por el 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, Ciudad Victoria, Tamaulipas
2. CATD 1- Fracc. Los Naranjos, Ciudad Victoria, Tamaulipas.
3. CATD 2- Oficinas IETAM, Calle Olivia Ramirez, Ciudad Victoria, Tamaulipas
4. CATD 3- Güemez, Tamaulipas
5. CATD - Tampico, Tamaulipas

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). El proceso de verificación de estas listas requirió una entrevista con el líder técnico del proyecto de desarrollo del sistema, el Ing. Guillermo Dewey. A partir de estas listas de verificación se realizó un proceso que permitió cuantificar el valor de cada atributo y establecer un perfil de calidad del sistema.

6.3.2 Nivel Datos

Para la validación de requerimientos funcionales se definió el plan de pruebas funcionales a nivel de base de datos (ANEXO 2). 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 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.

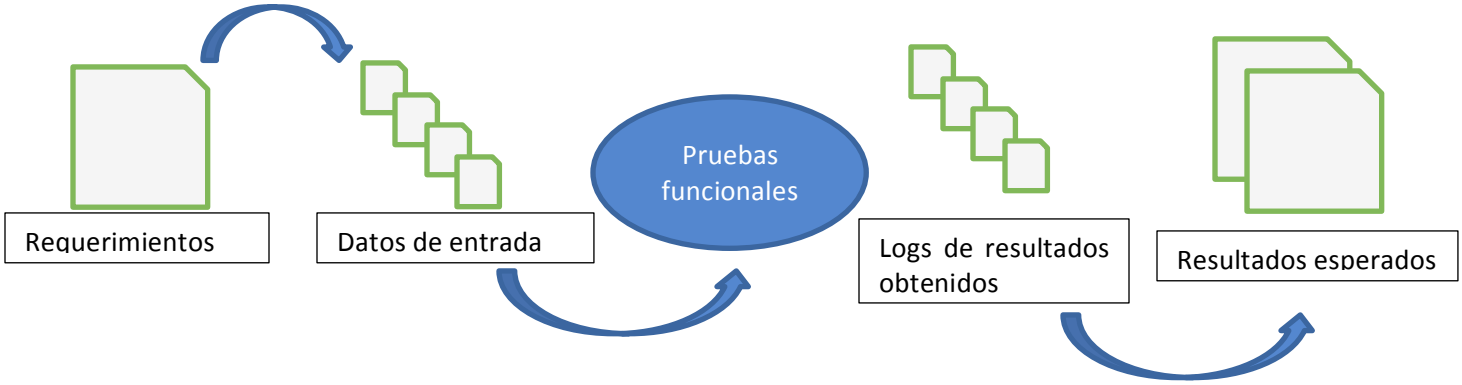

Figura 6.1 Flujo general para la validación de los requerimientos funcionales, nivel base de datos.

- 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.

- Pruebas funcionales: Hace referencia a las pruebas que harán para validar cada requerimiento funcional.

- 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 de los simulacros 1, 2, 3 y jornada electoral.

Obtenidos estos insumos se procedió de la siguiente forma:

- Se recopilaron evidencias a través de un checkList.

- Se recopilaron evidencias a través de la información generada por los web services mencionados. Esta recopilación tuvo lugar en los CCVs y CATD ubicados en Ciudad Victoria,

Tamaulipas durante las fechas programadas para la aplicación de pruebas por parte del ente auditor y los simulacros 1,2, 3 .

- El ente auditor desarrolló un script para consumir y resguardar la información que genera el web service de auditoría. Posteriormente se realizaron actividades de análisis enfocadas 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.

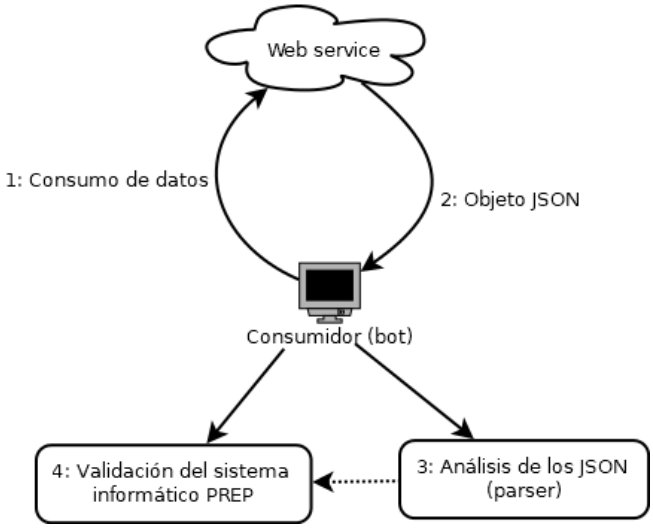

Figura 6.2 Flujo general para la validación de los requerimientos funcionales, nivel base de datos.

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 Resumen

La metodología descrita fue ejecutada por el ente auditor a través de dos equipos de trabajo especializados en el nivel de aplicación y el nivel de datos. Los integrantes de cada equipo se desplazaron a diferentes lugares donde los componentes del sistema fueron instalados previamente. En particular el equipo mencionado estuvo presente, en los CATDs de Cd. Victoria, Güemez y Tampico y los CCVs (principal y alterno también en Cd. Victoria). Esto ocurrió durante las fechas programadas para la aplicación de pruebas por parte del ente auditor y los simulacros 1, 2, 3 definidos por el IETAM.

Desde el punto de vista funcional, el sistema cumple con los lineamientos mínimos requeridos por el IETAM, sin embargo a partir de las pruebas se encontraron diferentes áreas de oportunidad las cuales se listan a continuación:

Nivel de Aplicación

- Durante los procesos de captura y validación algunas actas (alrededor de un 5%) queda en un estado inconsistente que puede afectar la efectividad y fiabilidad de los resultados publicados.
- No existe un mecanismo definido para la asignación de roles y usuarios. El proceso de 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 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.
- La eficiencia de algunos procesos puede ser mejorada, por ejemplo el proceso de validación podría implementar un mecanismo de notificaciones que informe a los validadores cuándo un acta está disponible.
- No existe un módulo del sistema que permita hacer seguimiento de algunas variables de control del proceso, como por ejemplo actas en estados inconsistentes antes de la publicación, acceso de usuarios, métricas de desempeño de los operadores, demanda del sistema.
- No existe sincronía del tiempo en todos los dispositivos involucrados en los procesos del sistema.
- Si bien la estrategia de infraestructura en la nube puede garantizar niveles de servicio adecuados, la información generada por el sistema debería estar almacenada y resguardada exclusivamente por el IETAM.
- No existe un mecanismo de liberación y versionamiento del sistema que asegure al 100% que la versiones auditadas no pueden ser cambiadas durante el simulacro de una jornada electoral.
- El proveedor no cuenta con un modelo de proceso que guie el desarrollo del sistema (SCRUM, RUP, CMMi, etc.)

Nivel Base de Datos.

- No fue posible garantizar al 100% la correspondencia entre los datos generados por el proceso operativo y los datos publicados.
- Se observaron algunos puntos de mejora en el diseño del modelo de datos (normalización, nombrado de tablas y campos).
- No existe una separación adecuada entre la capa de aplicación y la capa de datos. Seria conveniente utilizar patrones de diseño para tal fin.
- Si bien el proveedor ofreció un mecanismo (web service) para auditar algunos elementos del proceso, la información obtenida de dicho mecanismo es limitada. No es recomendable que el proveedor defina qué tipo de información es susceptible de ser auditada.
- Las actas registradas en la base de datos de publicación no tienen una correspondencia directa con las imágenes del repositorio del sistema de publicación.
- En la base de datos de publicación existen registros de imágenes de actas sin huellas criptográficas. No existe explicación u observación de por qué no se registró. También, existen registros sin fecha de acopio.
- En el repositorio de imágenes del sistema de publicación existen más imágenes de las procesadas.

En general el proceso de auditoría fue ejecutado satisfactoriamente aunque se presentaron algunos eventos que retrasaron ligeramente la planeación prevista por el ente auditor. Entre estos eventos cabe destacar:

- El proveedor entregó parcialmente y con algunos retrasos la documentación solicitada por el ente auditor.
- La documentación entregada no contiene un diseño detallado de la solución.
- No fue posible interactuar con varios integrantes del equipo de desarrollo del sistema. La interacción solo fue a través del líder técnico que si bien conoce el sistema en general, éste desconoce algunos detalles de diseño e implementación necesarios para la auditoría.
- No fue posible verificar detalladamente las buenas prácticas de diseño e implementación de los componentes del sistema tanto a nivel aplicación como de base de datos.

6.6 Resultados.

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

6.6.1 Nivel de Aplicación

Tabla 6.1. Resultados de pruebas funcionales de la aplicación del PREP.

ID PRUEBA	DESCRIPCION	DATOS ENTRADA	ACCIONES EJECUTADAS	RESULTADOS ESPERADO	RESULTADOS OBTENIDOS	OBSERVACIONES
PF-01	Nombre: -Toma Fotográfica **Precondiciones**: -Acta Física -Dispositivo Móvil con aplicación PREP Casilla. -Usuario Autenticado **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. 2. Verificar la persistencia de la fotografía	1. El mensaje de envío se obtiene a través de un código de colores: rojo, amarillo y verde.	1.La prueba se ejecutó en un dispositivo móvil no oficial. 2. Las casillas de prueba eran pre-cargadas. Se esperaría que estas estén asociadas al usuario CAE.
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	1. Cuando el capturista selecciona otro escáner es posible que se capture un acta diferente a la que se desea capturar. 2. No hay claridad del proceso de lectura de código QR.
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. La fecha y hora de captura no debería ser ingresada por el usuario. 2. 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 3. Se desconectó intencionalmente el Internet durante el proceso de envió de datos. En este caso el sistema notificó que el acta no puede ser enviada y que se

ID PRUEBA	DESCRIPCION	DATOS ENTRADA	ACCIONES EJECUTADAS	RESULTADOS ESPERADO	RESULTADOS OBTENIDOS	OBSERVACIONES
						guardará localmente
	Acciones Excepcionales	Acta Física	1. Realizar intencionalmente conteos diferentes. 2. Ingresar votos que superen la lista nominal	1. Error por diferencia entre conteos. 2. Error por exceder lista nominal	1. Error por diferencia entre conteos. 2. Error por exceder lista nominal	
PF-04	**Nombre**: -Verificación de acta **Precondiciones**: Asignación de acta previamente capturada **Módulo**: Verificación	1.Acta digitalizada (imagen y datos capturados)	1. Revisar los datos digitalizados con la imagen enviada. 2. En caso de ser correctos se enviar. 3. En caso contrario, se envía a validador 1	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 navegador o apagar la computadora. 3. No fue posible comprobar el mecanismo de asignación de las actas de un capturista a diferentes verificadores. Si existiera la posibilidad de que las actas de un capturista las revisara el mismo verificador, habría un riesgo de fraude

ID PRUEBA	DESCRIPCION	DATOS ENTRADA	ACCIONES EJECUTADAS	RESULTADOS ESPERADO	RESULTADOS OBTENIDOS	OBSERVACIONES
						electoral.
PF-05	Nombre: -Validación de acta **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	
PF-06	Nombre: -Segunda validación de acta **Precondiciones**: -Acta denegada previamente en el proceso de validación 1	Cargar acta denegada asignada (asignación automática)	1. Realizar la segunda validación corroborando que los datos capturados son realmente incorrectos. 2. Si la inconsistencia es real se envía como acta incorrecta. 3. De lo contrario el validador modifica discrecionalmente los datos y 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	
PF-07	Nombre: -Captura PREP-Casilla **Precondiciones**: -Fotografía acta PREP-Casilla					No se pudo realizar la prueba debido a que no estaban disponibles los dispositivos sobre los cuales se instalaría la aplicación de PREP-Casilla.

ID PRUEBA	DESCRIPCION	DATOS ENTRADA	ACCIONES EJECUTADAS	RESULTADOS ESPERADO	RESULTADOS OBTENIDOS	OBSERVACIONES
PF-08	Nombre: -Publicación de resultados preliminares **Precondiciones**: -Base de datos en ceros		1. Verificar que la información publicada corresponda a la definida en los lineamientos del IETAM. 2. Verificar que el formato de dicha información corresponda a lo definido por el IETAM	Todos los datos publicados corresponden a lo definido por el IETAM . Dichos datos tienen el formato predefinido por el IETAM.	Todos los datos publicados corresponden a lo definido por el IETAM . Dichos datos tienen el formato predefinido por el IETAM.	No hay observaciones respecto a los datos publicados.

6.6.2 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 antes del simulacro 1. Como resultado se tiene 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. Se tuvo como resultado que no existe una correspondencia entre la información que se registra en el log del web service de auditoría y la información que se registra en la base de datos maestra. Los resultados se encuentran en el (ANEXO 3).

Resultados de las pruebas operativas de los simulacros 1,2 y 3

A continuación, se describe los análisis que realizaron a los simulacros 1, 2 y 3

1. **Validación de la base de publicación y el repositorio de imágenes del sistema de publicación:** Este análisis esta enfocado en validar que las imágenes que fueron capturadas sean las que están registradas en el la base de datos de publicación. Para validar la correspondencia de la información de la base de datos de publicación y las imágenes del repositorio del sistema de publicación, el ente auditor desarrolló un script que descarga todas la imágenes del repositorio del sistema de publicación y obtuvo su obtuvo las huellas criptográficas (SHA256) de cada imagen y se realizó una correspondencia de las huellas criptográficas registradas por el PROVEEDOR en la base de publicación.

2. **Correspondencia la información (imágenes, datos y base de datos) en el log del web service de auditoría y la información generada durante en los simulacros 1, 2 y 3:** Este análisis esta enfocado en validar que la información registrada en el log del web service de auditoría sea suficiente para transparentar las operaciones realizadas a cada acta, durante cada simulacro y jornada electoral.

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

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

ID PRUEBA	OBSERVACIONES	CRITERIOS	SUGERENCIA
PF1. Bases de datos en ceros y huella criptográfica	Durante el simulacro 1 no se realizó la prueba. Durante el simulacro 2 se realizó la generación de las huellas criptográficas de 5 archivos. Durante el simulacro 3, solo se realizó las huellas criptográficas de 3 archivos.	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.
PF2. Verificación del nombre de archivo de imagen	Durante los 3 simulacros, el nombre de las imágenes de acta no tiene correspondencia con la clave que se encuentra en la base de datos que se publica en dicho sistema (_TAMPS_PREP_AYUn_2018)	Los datos publicados deberán ser consistentes y presentados de acuerdo con lo establecido por los lineamientos del IETAM	Guardar la imagen con el mismo identificador que se registra en la base de datos de publicación.
	En el simulacro 1 el sistema detectó que 163 imágenes no se pudieron descargar del repositorio del sistema de publicación. En el simulacro 2 el sistema detectó que 103 imágenes no se pudieron descargar del repositorio del sistema de publicación. En el simulacro 3 el sistema detectó que 143 imágenes no se pudieron descargar del repositorio del sistema de publicación.	Los datos publicados deberán ser consistentes y presentados de acuerdo con lo establecido por los lineamientos del IETAM	Es necesario que el proveedor tenga un registro de las actas que no fueron procesadas o consideradas en el proceso y una observación con el fin de descartar la perdida de las actas.
PF3. Validación de la información publicada.	En el simulacro 1, el corte del sistema PREP en su fase de publicación reportó que, solo 4268 actas de 4628 consideradas en el simulacro fueron procesadas. En simulacro 2, el corte del sistema PREP en su fase de publicación reportó que, solo 4565 actas de 4628 consideradas en el simulacro fueron procesadas. En el simulacro 3, el corte del sistema PREP en su fase de publicación reportó que, solo 4367 actas de 4628 consideradas en el simulacro fueron procesadas.	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 proceso manuales, por ejemplo cuando las actas entran a un estado inconsistente el proceso para regresarlas a un estado consistente es manual.
	En el simulacro 1 se detectó	El sistema deberá garantizar	Colocar en el campo de

PF4. Huella Criptográfica de Acta	que, para 267 actas, que existen en el repositorio del sistema de publicación, el sistema no realizó el registro su correspondiente Hash o huella criptográfica. En el simulacro 2 se detectó que, para 115 actas, que existen en el repositorio del sistema de publicación, el sistema no realizó el registro su correspondiente Hash o huella criptográfica. En el simulacro 3 se detectó que, para 261 actas, que existen en el repositorio del sistema de publicación, el sistema no realizó el registro su correspondiente Hash o huella criptográfica.	la integridad y consistencia de los datos a través de estrategias que integren personas, tecnología, procesos y buenas prácticas.	OBSERVACIÓN de la base de datos publicación el motivo por el cual no se registro la información del acta.
	En el simulacro 1 el sistema detectó 197 registros de huellas criptográficas en la base de datos (_TAMPS_PREP_AYUn_2018) que no pertenecen a ninguna de las 4268 actas recuperadas del repositorio del sistema de publicación. En el simulacro 2 el sistema detectó 103 registros de huellas criptográficas en la base de datos (_TAMPS_PREP_AYUn_2018) que no pertenecen a ninguna de las 4525 actas recuperadas del repositorio del sistema de publicación En el simulacro 3 el sistema detectó 1245. registros de huellas criptográficas en la base de datos (_TAMPS_PREP_AYUn_2018) que no pertenecen a ninguna de las 5445 actas recuperadas del repositorio del sistema de publicación. En este simulacro se detectó que en el repositorio de imágenes existía más imágenes de las que fueron capturadas.	El sistema deberá garantizar la integridad y consistencia de los datos a través de estrategias que integren personas, tecnología, procesos y buenas prácticas.	Respaldar solo aquellas imágenes que fueron procesadas en cada simulacro.
	En el simulacro 1 el sistema verificó que de las actas recuperadas 4268 actas	El sistema ofrece los mecanismos necesarios para dar cumplimiento a los	

	existe un registro válido (Hash registrado en la base de datos y el hash calculado por el sistema de verificación para cada acta coinciden). En el simulacro 2 el sistema verificó que de las actas recuperadas 4422 actas existe un registro válido (Hash registrado en la base de datos y el hash calculado por el sistema de verificación para cada acta coinciden). En el simulacro 3 el sistema verificó que de las actas recuperadas 4200 actas existe un registro válido (Hash registrado en la base de datos y el hash calculado por el sistema de verificación para cada acta coinciden).	procesos de captura, validación, cómputo y publicación señalados por el IETAM	
PF5. Validación de huella criptográfica.	Para cada uno de los simulacros el ente auditor observó que en el la base de datos (_TAMPS_PREP_AYUn_2018) solo se registra un Hash de cada acta.	Se debe garantizar la imparcialidad en el procesamiento de datos generados por el sistema respecto a afinidades políticas o intereses personales.	Se recomienda calcular 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.
PF6. Consistencia e integridad de la información registrada en el log de web service de auditoría	En los 3 simulacros de 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 de registrarse con los nombre de las actividades del proceso técnico operativo.
	En los 3 simulacros se identificó que la estampa de tiempo registrada en cada una de las actividades/operaciones realizadas a las actas no esta está sincronizada. No es imposible crear una traza en el tiempo de las operaciones realizadas a cada acta.	El sistema deberá garantizar la integridad y consistencia de los datos a través de estrategias que integren personas, tecnología, procesos y buenas prácticas.	Utilizar un único reloj para la sincronización de las aplicaciones del sistema informático PREP.

	En los 3 simulacros se identificó que la información de contenida en el log del web service de auditoría no es suficiente para hacer la correspondencia de la información en la base de datos base de datos y almacén de datos, para cada una de las aplicaciones utilizadas en el sistema informático PREP	El sistema deberá garantizar la integridad y consistencia de los datos a través de estrategias que integren personas, tecnología, procesos y buenas prácticas.	Es necesario registrar las operaciones realizadas en la bases de datos y el sistema de archivos (CRUD).
PF7. Actualización de la base de datos de publicación.	En los 3 simulacros se realizó un análisis de las base 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	
PF8. Análisis de comportamiento.	Para el simulacro 1 se identificó que el 74% de las actas procesadas fueron atendidas durante los primeros 15 minutos del total de tiempo del evento. Para el simulacro 2 se identificó que el 78.2% de las actas procesadas fueron atendidas durante los primeros 15 minutos del total de tiempo del evento. Para el simulacro 3 se identificó que el 53.4% de las actas procesadas fueron atendidas durante los primeros 15 minutos del total de tiempo del evento.		
	Para el simulacro 1 se identificó que el 7.6% de las actas procesadas su proceso operativo tardó más de 1 hora. Para el simulacro 2 se identificó que el 12% de las actas procesadas su proceso operativo tardó más de 1 hora. Para el simulacro 3 se identificó que el 27 % de las actas procesadas su proceso operativo tardó más de 1		

	hora.		

A continuación, se se presenta una gráfica donde se muestra el total de actas procesada en cada una de las actividades registradas en el log de web service de auditoría. Para los 3 simulacros.

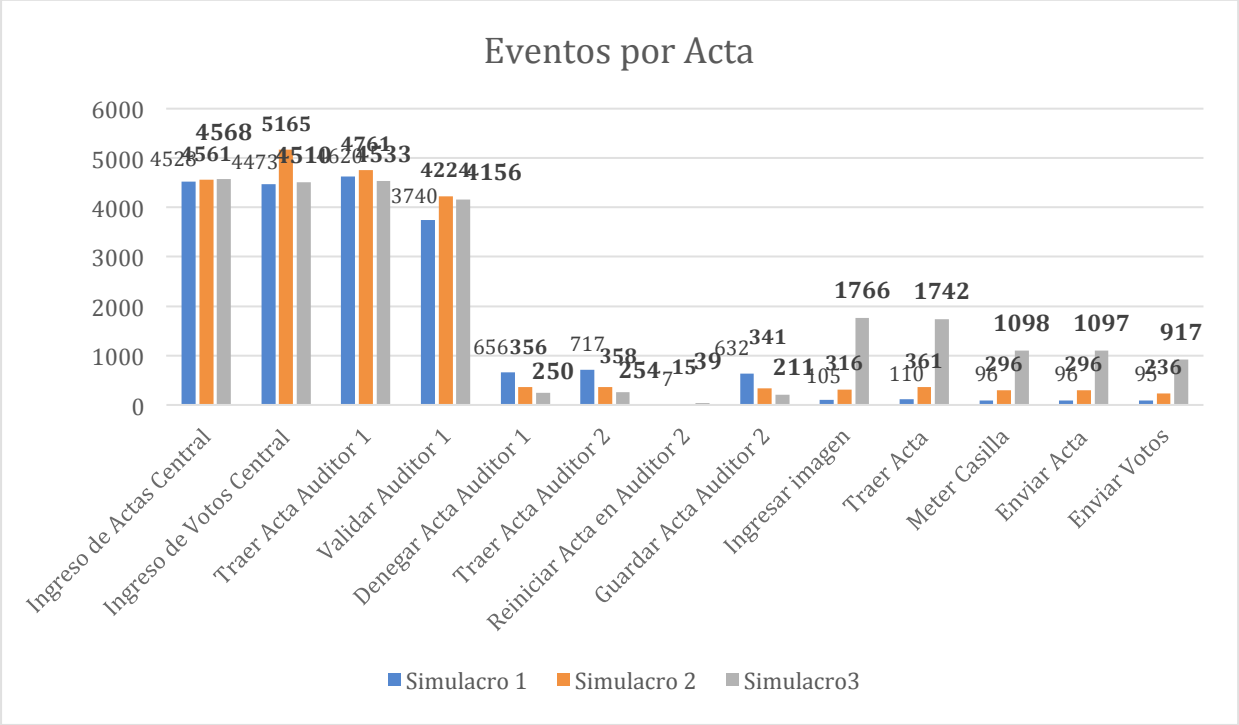

Figura 6.3. Número de eventos registrados en el web service de auditoría del PREP durante los simulacros 1, 2 y 3.

6.7 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. Sin embargo, es necesario realizar más trabajo en la correspondencia de la información desde su captura hasta su publicación.

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 realizará al inicio, durante y al final de la operación del sistema informático del PREP.

7.2 Alcance

El Ente Auditor definió 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. El procedimiento ha sido validado por el personal que el IETAM designe para tal efecto, contemplando los siguientes aspectos:

El procedimiento cuenta con un diagrama de flujo.
El procedimiento incluye los roles y responsabilidades de los involucrados los cuáles son: el proveedor del servicio, el IETAM, y el ente auditor.
El procedimiento está previsto para documentar las siguientes etapas:

a. Generación, obtención y validación de huellas criptográficas en SHA-256 del software PREP auditado.
b. Generación, obtención y validación de huellas criptográficas en SHA-256 del software PREP instalado en el ambiente productivo que operará el día de la Jornada Electoral.
c. Validación de la información inicial y final de la base de datos del PREP.
d. 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 realizar 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 aplicaciones inicializadas por el proveedor y se firman (mediante el algoritmo SHA256 para las huellas y el algoritmo RSA para la creación de llaves pública/privada). Este modelo garantiza que solo se validarán huellas criptográficas creadas por el proveedor.

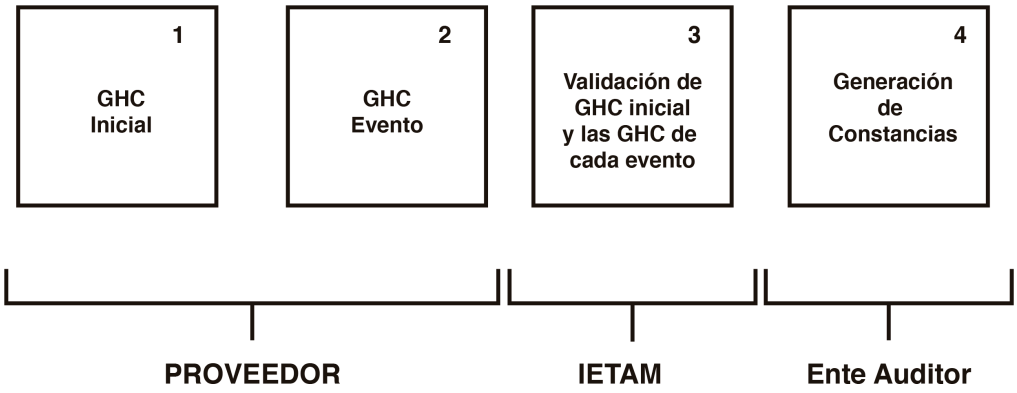

Figura 7.1. Diagrama de Flujo 1 Flujo general de trabajo para la validación de la información inicial y final de la base de datos y del software instalado en el ambiente productivo que operará en día de la jornada electoral.

En la segunda etapa (GHC Evento), el proceso se repetirá por cada evento considerado por el IETAM (simulacros y 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 Hash y su correspondiente firma. Este reporte es generado por el servicio de validación invocado por el IETAM. Esta etapa finaliza cuando el ente auditor presente el reporte (sin incidencias) al notario y se procederá a firma la correspondiente constancia. 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.

7.3.2.1 Generación de llaves para firma digital

En la actividad 1, mostrada en 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).

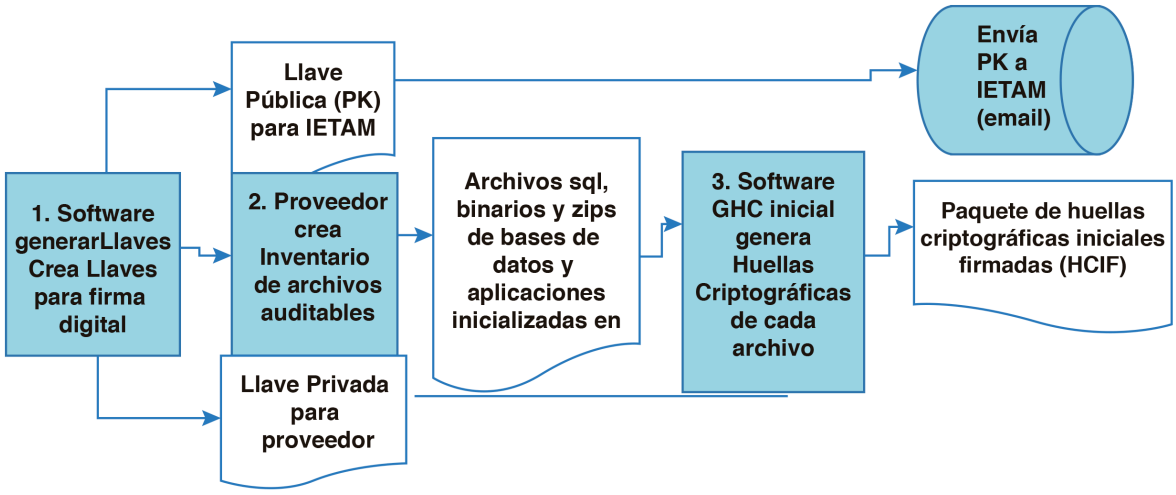

Figura 7.2 Diagrama de Flujo 2 Flujo de trabajo para la generación de huellas criptográficas iniciales de archivos del inventario firmadas por el proveedor.

El software depositará la llave SK en el lugar donde el proveedor invocó dicho software y enviará la llave pública a el ente auditor y el IETM por correo electrónico y se 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 para generar la llave PK y SK.
2. La llave SK se quedará guardada de manera local en la carpeta donde se ejecutó la aplicación, esta llave quedará al resguardo del personal del PROVEEDOR, el sistema no la enviará, el proveedor la debe conservar para ser usada en los siguientes eventos tales como simulacros o 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 ***generarLlaves***, la única operación que debe realizar el PROVEEDOR es abrir una terminar de línea de comandos y ejecutar y pegar en esa terminal el siguiente comando:

java -jar 1806ProveedorAplicacion.jar generarLlaves Llavero/ Original.

Donde ***java -jar 1806ProveedorAplicacion.jar*** es el ejecutable creado para el proveedor, ***generarLlaves*** indica la acción que el software debe realizar, ***Llavero/*** es la ruta donde se guarda la llave secreta (para no comprometer la seguridad del proveedor se sugiere crear esta carpeta) y **Original** es el nombre de la actividad que se está realizando.

7.3.2.2 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 INVENTARIO_APPS_DB, la cual deberá incluir los archivos que se listan a continuación:

1. Base de datos Maestra 1 vacía e inicializada, el PROVEEDOR realizará un dump de la base de datos con el siguiente comando (mysqldump nombre_de_Base_de_Datos > nombre_solictado.sql) o en su defecto realizará 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. Página web del sitio de publicación.
3. Aplicación para PREP Casilla
4. Módulo de captura de actas en CATD
5. Módulo de validación de actas para uso de los CCV

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.

7.3.3.3 Generación de huellas criptográficas iniciales (GHC inicial).

El PROVEEDOR ejecutará de nueva cuenta la aplicación ***1806ProveedorAplicacion.jar***, pero en esta ocasión indicará la acción a realizar (***firmarArchivos)*** y proporcionará 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 ***1806ProveedorAplicacion.jar*** dando como entrada su llave SK y la ruta donde se encuentra el inventario de archivos.
2. La aplicación en forma automática realizará las siguientes acciones:
    a. realizará un Hash de a cada documento que se encuentre en el inventario de archivos usando el algoritmo SHA256.
    b. Firmará cada HASH con la llave privada SK usando el algoritmo RSA.
    c. Enviará el conjunto de HASH's y sus firmas digitales al servicio de verificación desarrollado por el Ente Auditor y una notificación por correo electrónico será eviada al IETAM.

Para más detalles técnicos dirigirse a la Figura 7.4.

1.1. Procedimiento para ejecutar la aplicación.

Para ejecutar la aplicación detallada anteriormente, el PROVEEDOR debe abrir una terminal y ejecutar el siguiente comando:

java -jar 1806ProveedorAplicacion.jar firmarArchivos Inventario/ Llavero/LlavePrivada Original.

Donde ***java -jar 1806ProveedorAplicacion.jar*** es la aplicación de generación de huellas criptográficas, ***Inventario/*** es la ruta donde se encuentran los archivos de las bases de datos y aplicaciones 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.

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 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 1806ProveedorAplicacion.jar firmarArchivos Inventario/ Llavero/LlavePrivada S1.

Donde ***java -jar 1806ProveedorAplicacion.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 y ***S1*** indica al sistema que se está generando un lote de huellas criptográficas y firmas del evento llamado Simulacro 1. Para los siguientes eventos el único parámetros 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 aplicación 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 de IETAM ejecutará la Aplicación de validación dando como entradas la llave pública (PK) y el evento que quiere validar (simulacro 1, simulacro 2, simulacro 3, jornada electoral o todos).
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. Comparará si el HASH desencriptado del paquete generado en GHC eventos es igual al 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. Generará un reporte describiendo la validación de cada huella criptográfica y su correspondiente firma digital para cada evento contra las huellas criptográficas generados en la etapa inicial.

Para más detalles dirigirse a la figura 6.3. Diagrama de Flujo 5.
Procedimiento para ejecutar la aplicación.
Para ejecutar la aplicación detallada anteriormente, el PROVEEDOR debe de abrir la línea de comando y ejecutar el siguiente comando:

java -jar 1806IETAM.jar validar Llavero/LlavePublica Original Evento.

Donde ***java -jar 1806IETAM.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, **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.

7.3.5 Etapa 4. Generación de constancias.

En esta etapa el ente auditor realizará las siguientes actividades:

1. Imprimirá una constancia que incluirá el reporte de validación para ser firmada por parte del IETAM y Ente Auditor.
2. Imprimirá 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.
3. Firmará la constancia de hechos de la generación de huellas criptográficas.
4. Entregará 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

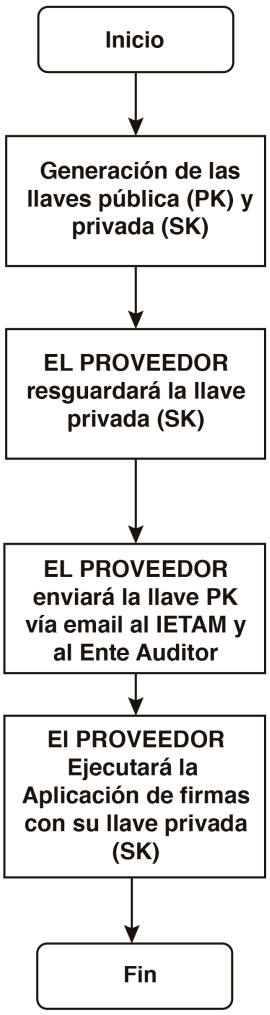

Figura 7.3 Diagrama de Flujo 3 Flujo de trabajo para la generación de las llaves pública y privada por parte del personal del PROVEEDOR.

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 SHA256 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 envió del paquete packFH al cloud (servidor del Ente Auditor) o/y vía email al IETAM y al Ente Auditor.

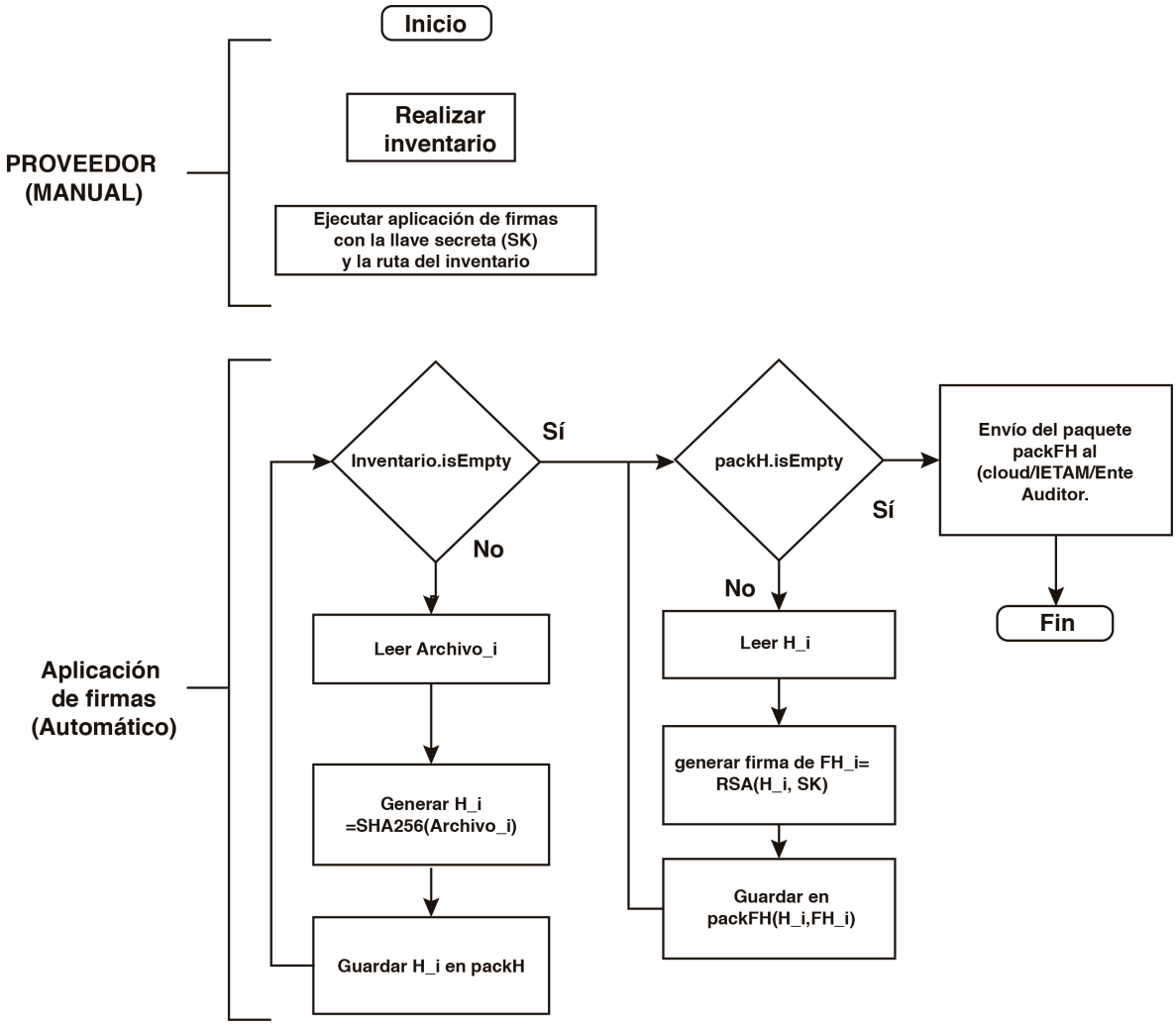

Figura 7.4 Diagrama de Flujo 4 Flujo de trabajo para la generación de las firmas de los documentos del inventario.

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 firma (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 la figura 6.2. Diagrama de Flujo 4 se muestra el flujo de trabajo de validación.

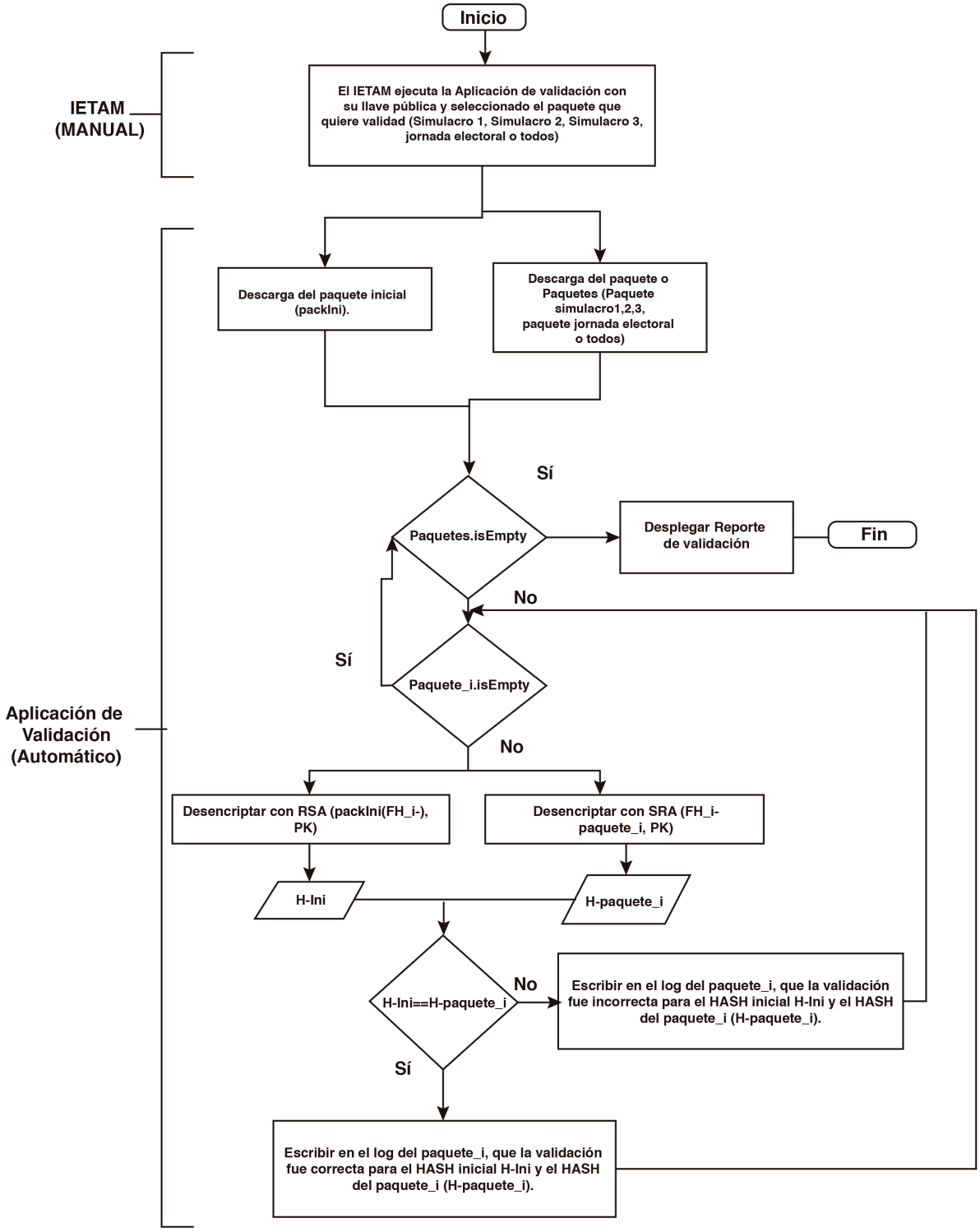

Figura 7.5 Diagrama de Flujo 5 Flujo de trabajo para la validación de las firmas iniciales con las firmas generadas durante los simulacros y la jornada electoral.

7.3.7 Resultados

El procedimiento definido se ha puesto a prueba con éxito durante los simulacros 2 y 3 llevados a cabo el 17 y 24 de junio pasados. El procedimiento se realizará el domingo 1° de julio de 2018 en las instalaciones del IETAM, concluyendo el 2 de julio y será atestiguado por un tercero con fe pública designado por el IETAM, conforme se señala en el inciso I del numeral 23, Capítulo I, Título III del Anexo 13 del Reglamento de Elecciones. En la Figura 7.6 se presenta la constancia de la generación inicial de las huellas criptográficas realizada el 30 de junio de 2018 a las 14:28 horas.

Cinvestav
Tamaulipas

Ciudad Victoria, Tamaulipas, 30 de Junio de 2018

Constancia de hechos de la generación de huellas criptográficas

Siendo las 14 horas con 20 minutos del día 30 del mes de junio del año 2018, se procedió a realizar la generación de huellas criptográficas de los módulos que integran el sistema PREP del estado de Tamaulipas, previo al inicio de la jornada electoral del 1 de julio de 2018. Este procedimiento contó con la presencia del Dr. Arturo Díaz Pérez, por parte del Cinvestav Tamaulipas en su calidad de ente auditor, el Mtro. Miguel Angel Chávez García en su calidad de Consejero Presidente del Instituto Electoral de Tamaulipasel y el Lic. José de los Santos González Picazo en su calidad de Titular de la Instancia Interna Responsable del PREP.

Nombre del archivo	sitio_tamaulipas_final.zip
SHA256	b1d33c1cb43d6de2fa67bdd922395211ed23be901532630c217e7791061d2c61
Fecha en que fueron firmados	2018-06-30 14:20:55

Nombre del archivo	prep_tamaulipas2018_final.sql
SHA256	3e9eda935d2dc659870005ade390504d613d12b91de352d9422fc8e0291a22d1
Fecha en que fueron firmados	2018-06-30 14:20:55

Nombre del archivo	casilla_final.tar.gz
SHA256	15b2eb5cb6e16f66331a5d5edacacb2faaf66a0251f318cad4ebe76801c1d88f
Fecha en que fueron firmados	2018-06-30 14:20:55

Nombre del archivo	ControladorTamaulipas.fmp12
SHA256	61c4c68b73d5132ae7949e85354258401d49f355af1c6ea52b4b07dd03064dbb
Fecha en que fueron firmados	2018-06-30 14:20:56

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

Nombre del archivo	centrales_final.tar.gz
SHA256	c52ea8d7c31bfca7fedeb3611fa780da5b0c8a6d6235831ab7f02a0b1cf16efc
Fecha en que fueron firmados	2018-06-30 14:20:56

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

Archivo	Descripción
centrales_final.tar.gz	Módulo de validación de actas.
prep_tamaulipas2018_final.sql	Base de datos central del PREP
sitio_tamaulipas_final.zip	Página web del sitio de publicación
ControladorTamaulipas.fmp12	Módulo de captura de actas en CATD
casilla_final.tar.gz	Aplicación para PREP Casilla

Firman la presente constancia los representantes de las entidades que intervienen, el Dr. Arturo Díaz Pérez, por parte del Cinvestav Tamaulipas en su calidad de ente auditor, el Mtro. Miguel Angel Chávez García en su calidad de Consejero Presidente del Instituto Electoral de Tamaulipas y el Lic. José de los Santos González Picazo en su calidad de Titular de la Instancia Interna Responsable del PREP.

Dr. Arturo Díaz Pérez Ente Auditor	Mtro. Miguel Angel Chávez García Consejero Presidente del Instituto Electoral de Tamaulipas	Lic. José de los Santos González Picazo Titular de la Instancia Interna Responsable del PREP

Figura 7.7 Constancia de Generación de Huellas Criptográficas del PREP: Página 2.

8. Análisis de vulnerabilidades a la infraestructura tecnológica

8.1 Objetivos

- 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

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, CATD-Güemez 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

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

- 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

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:

Ubicación	Fecha
CCV Principal	28 al 30 de Mayo de 2018
CATD Victoria	31 de Mayo de 2018
CATD Güemez	01 de Junio de 2018
CCV de Respaldo	05 de Junio de 2018
CATD Tampico	17 de Junio de 2018

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 y mencionadas en el numeral 4 *Alcance*.

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 en general es 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's y los CATD's no cuentan con sistema de alarmas ni con sistema de control de acceso físico automatizado.

O3-C-2 El proveedor no cuenta con un procedimiento para el monitoreo permanente del sistema de video-vigilancia ni con personal asignado para estas actividades.

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 un procedimiento y personal para el monitoreo de la operación del sistema de video-vigilancia.

R3-C-3 Es recomendable que al menos en los CCV's se implemente un sistema de control de acceso físico automatizado para todo el personal operativo que participará en la jornada electoral ya sea mediante huella digital o mediante credenciales con banda magnética por ejemplo, mediante el cual sería posible tener un mayor control de los acceso a los espacios y evidencia ante posibles incidencias de parte de personas ajenas al proveedor o al IETAM.

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 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 CCV y de los CATD cuentan son software antivirus de uso libre (Freeware)
- Los escáneres están conectados directamente al puerto USB de cada uno de los equipos de digitalización.

Observaciones

O3-C-3 El acceso al bios del equipo no tiene contraseña
O3-C-4 El acceso al sistema operativo no tiene contraseña
O3-C-5 La cuenta de usuario por default del sistema operativo es la de Administrador
O3-C-6 Los equipos móviles no estuvieron disponibles durante la revisión.

Recomendaciones

R3-C-4 Es altamente recomendable atender las observaciones O3-C-1, O3-C-2 y O3-C-3 con la finalidad de fortalecer el factor de autenticación configurado para los equipos asignando una contraseña segura y delimitar el perfil adecuado para el usuario de inicio del sistema operativo.

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.

R3-C-6 Es altamente recomendable que para procesos futuros se tengan disponibles en tiempo y forma los equipos móviles para la aplicación PREP Casilla para poder realizar la revisión de configuraciones correspondiente.

R3-C-7 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.

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 OpenVAS y Armitage.

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 switches no administrables y módems ADSL, aunque en los CATD donde los equipos de captura son mínimos solo se dispone del módem ADSL.

Observaciones

O3-C-7 El servicio de Internet en los CATD y los CCV estaba abierto durante la revisión
O3-C-8 La red inalámbrica del servicio de Internet estaba activa durante la revisión y con las credenciales por default a la vista.

Recomendaciones

R3-C-8 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.

R3-C-9 Es altamente recomendable desactivar las redes inalámbricas tanto en los CCV como en los CATD

R3-C-10 Es altamente recomendable restringir el acceso a Internet en la red de los CCV y los CATD también en los equipos de conmutación o seguridad perimetral.

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 OpenVAS y Armitage.

Información recopilada

- Los servidores en la nube están configurados con sistemas operativos Ubuntu, FreeBSD y aplicaciones open source y no se pudo tener acceso a la revisión de la configuración de los mismos.
- Las estaciones de trabajo de los CATD y CCV están configuradas con el sistema operativo Microsoft Windows 7 service pack 1
- Las estaciones de trabajo de los CATD y CCV no requieren proveer servicios activos.
- Los puertos físicos de las estaciones de trabajo están administrados localmente por el software y solo están activos aquellos que son requeridos para el funcionamiento del sistema PREP.

Observaciones

O3-C-9 La imagen del sistema operativo es la misma en todas las estaciones de trabajo
O3-C-10 Los equipos móviles no estuvieron disponibles durante la revisión.

Recomendaciones

R3-C-11 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-12 Es altamente recomendable ejecutar una actualización general mediante Windows Update en todas las estaciones de trabajo para la jornada electoral con la finalidad de que se encuentren protegidas contra vulnerabilidades de reciente descubrimiento

8.3.5.5 Revisión de la configuración de aplicaciones

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

Procedimiento de la revisión

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

Información recopilada

- Todos los servidores que serán utilizados en el proceso electoral están implementados en un servicio en la nube contratado con el proveedor Amazon y configurados dentro de una red privada dentro del mismo servicio, a los cuales no se pudo tener acceso para su revisión.
- Las estaciones de trabajo de los CATD y CCV tienen instalado el software propietario File Maker Pro 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 Professional 2010 para el bloqueo de puertos físicos y el control local para el acceso a Internet.

Observaciones

O3-C-11 El software File Maker Pro está actualmente descontinuado por el fabricante desarrollador
O3-C-12 El software IM Lock Professional 2010 tiene versiones más recientes

Recomendaciones

R3-C-13 Es recomendable utilizar versiones de File Maker Pro y IM Lock Professional 2010 más recientes con la finalidad de utilizar las mejoras realizadas a este tipo de software.

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 de forma satisfactoria.
- En el CCV de Respaldo y en el CATD Victoria se validó la instalación de la planta de emergencia pero no su funcionamiento ya que durante la revisión presentó una falla.
- En los CATD de Güemez y Tampico no estuvieron instaladas las plantas de emergencia durante la revisión. El proveedor manifestó que sería el IETAM el encargado de la instalación y operación de las plantas de emergencia y que estarían listas para la jornada electoral.

Observaciones

O3-D-1 No fue posible realizar las actividades de revisión a las plantas de emergencia de los CATD de Güemez y Tampico ya que no estuvieron disponibles durante la revisión y no fue posible realizar las pruebas funcionales de las plantas de emergencia del CATD de Victoria y del CCV de Respaldo ya que durante la revisión presentaron fallas.

Recomendaciones

R3-D-1 Es altamente recomendable para procesos futuros tener disponibles en tiempo y forma las plantas de emergencia para la realización de las actividades de revisión del funcionamiento y operación de las mismas tanto en los CCV como en los CATD.

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 por 10 minutos en promedio ante los problemas más comunes presentados en el suministro de energía eléctrica.

Observaciones

Ninguna.

Recomendaciones

R3-D-2 Es altamente recomendable tener disponibles equipos UPS adicionales como medida de prevención ante posibles fallas de los equipos ya instalados tanto en los CCV como en los CATD.

8.4 Pruebas de penetración (pentest).

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 presenta las pruebas de penetración realizadas al interior de 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 primea fase de pruebas fue programada y ejecutada del 31 de mayo al 5 de junio del presente, en esta fase se analizaron el Centro de Captura y Verificación (CCV) principal y alterno ubicados en Ciudad Victoria, así como los Centros de Acopio y Transmisión de Datos (CATD) de Ciudad Victoria y Güemez.
La segunda fase comprendió el análisis de la infraestructura del CATD ubicado en Tampico la cual se realizó el día 17 de junio de 2018.

De los centros evaluados, fue posible realizar el 100% de las pruebas de penetración que se tenían contempladas, mientras que las pruebas de ingeniería social se realizaron únicamente en los centros ubicados en Cd. Victoria. La aplicación de pruebas se dividió en 4 fases: extracción y recolección de información, escaneo de puertos e identificación de servicios, búsqueda y explotación de vulnerabilidades e Ingeniería Social.

El alcance de las pruebas se centra en la identificación de información relevante de los dispositivos de la infraestructura que pueda ser utilizada para identificar vulnerabilidades que puedan ser explotadas para acceder, modificar o corromper información privada utilizada por el dispositivo.

Del total de equipos de cómputo analizados, el 23% resultó presentan alguna vulnerabilidad media o crítica, principalmente derivadas por la falta de parches de seguridad y actualización del sistema operativo; las vulnerabilidades encontradas podrían permitir a un atacante hacerse con el control remoto del equipo lo cual puede derivar en la inutilización del mismo o en el uso indebido para intentar corromper información del PTO.

El 100% de los módems DSL analizados presentan vulnerabilidades críticas que pudieran permitir a un atacante realizar un ataque de intermediario (*man in the middle*) ya que las vulnerabilidades encontradas podrían ser utilizadas para desviar el tráfico y monitorearlo con la intención de descubrir las claves utilizadas e intentar corromper o reemplazar la información intercambiada entre los equipos de cómputo y los servidores receptores de la información.

La totalidad de las vulnerabilidades encontradas pueden ser resueltas instalando los parches y actualizaciones necesarias en los dispositivos afectados, por lo que, la recomendación principal es: utilizar las versiones más nuevas y estables de los sistemas operativos y firmware incluyendo los parches de seguridad actualizados de manera automática. Esto aunado a equipo de cómputo con las capacidades para utilizar dichos sistemas operativos. De esta manera, se reduce el riesgo dejar inoperantes las vulnerabilidades más conocidas.

Adicionalmente, es deseable que las comunicaciones estén aseguradas de punto a punto entre los servidores en la nube y los equipos de la infraestructura mediante redes privadas virtuales (VPNs), las cuales permitirían obtener servicios tales como: autenticación, confidencialidad y no repudio con una robustez a nivel criptográfico, además de permitir una mejor control y administración de los dispositivos conectados a la red.

8.4.1 Introducción

Una prueba de penetración simula las acciones de un atacante cibernético externo y/o interno que intenta detectar vulnerabilidades explotables de un sistema informático. Usando distintas herramientas y técnicas, el ejecutor de la penetración (hacker ético) intentara explotar sistemas críticos y obtener acceso a datos confidenciales.

La planeación de las pruebas de penetración sobre la infraestructura tecnológica del proveedor de servicios del sistema PREP Tamaulipas esta 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 Kali Linux además de diversas herramientas/comandos por el sistema Kali Linux. A fin de no contaminar ningún equipo del proveedor, todas las herramientas fueron desplegadas en equipos propios del auditor, los cuales sólo requirieron una conexión directa a la red del proveedor 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 de Kali Linux; para la fase 2 se utilizaron las herramientas nmap, Nessus, OpenVAS y Armitage. En fase 3 se utilizó la herramienta Armitage y; 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*.
T3-E-8. Explotación de vulnerabilidades mediante *mkbrutus.*

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-9. 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

Prueba	Resultados
T3-E-1	• Se identificó el segmento de red 10.10.2.0/24, en éste, se identificaron 39 dispositivos activos de los cuales 36 son equipos de cómputo de la marca DELL, un ruteador Mikrotik, una impresora marca Brother y un equipo CCTV-DVR Dahua. • 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 4 dispositivos, y por medio de éste fue posible identificar su nombre y grupo de trabajo.
T3-E-3	• En el equipo ruteador se identificaron 3 puertos abiertos: ○ 53: Generic DNS response ○ 8291: MikroTik WinBox ○ 2000: MikroTik bandwidth-test • En los equipos de cómputo se encontraron los siguientes puertos abiertos: ○ 135: RPC ○ 139: NetBIOS ○ 445: SMB • En el equipo CCTV-DVR se encontraron abiertos los siguientes puertos: ○ 554: Lorex IP camera RTSP ○ 80: http server • Haciendo uso del protocolo SMB activo en 4 equipos de cómputo fue posible obtener el tipo y versión de Sistema Operativo: “Windows 7 Ultimate 7601 Service Pack 1”. Usando el mismo protocolo fue posible obtener el SO del ruteador identificado como: “Linux kernel 2.6”. De la impresora fue posible obtener su nombre y modelo: “Brother

	MFC-L8900 series”
T3-E-4 T3-E-5	• De manera general se detectó el fabricante de la tarjeta de red, se logro la resolución de nombres mediante mDNS y LLMNR. • Se identificaron 4 equipos con riesgo de nivel medio relacionado con el protocolo SMB • Se identificaron 2 equipos con riesgo crítico, ambos relacionados con una falla de seguridad del servicio SMB en Windows 7 (MS17-010).
T3-E-6	• Utilizando la herramienta *Armitage* se corroboraron las vulnerabilidades encontradas mediante Nessus y OpenVAS. Aquellos equipos con servicios abiertos fueron seleccionados para ejecutar pruebas que permitieran identificar si dichas vulnerabilidades eran explotables.
T3-E-7	• Mediante la herramienta *Armitage* se ejecutaron 397 pruebas sobre el equipo CCTV-CVR, 25 sobre los equipos con NetBios y SMB; y 2 pruebas sobre el equipo de ruteo MikroTik. Ninguna prueba fue exitosa. Los *exploits* utilizados forman parte de la suit estándar del *Metasploit Framework* orientados a vulnerar sistemas con el menor esfuerzo.
T3-E-8	• Se ejecuto una prueba de rompimiento de contraseña con resultado negativo sobre el ruteador MikroTik mediante la herramienta *mkbrutus* diseñada para vulnerar equipos específicos de la compañía MikroTik utilizando el servicio del puerto 8291.
T3-E-9	• El personal de captura desconoce los protocolos de contingencias ante posibles fallas de la infraestructura tecnológica. • Es posible desempeñar más de un rol con la misma credencial.

8.4.7.2 CCV Respaldo

Prueba	Resultados
T3-E-1	• Se identificaron los segmentos de red: o En el segmento 192.168.1.0/24 se identificaron 8 dispositivos activos, 4 equipos de cómputo marca DELL, 1 Modem DSL, 1 ruteador MikroTik, 1 dispositivo móvil Sony y 1 switch administrable Cisco. o En el segmento 10.10.2.0/24 se identificaron 13 dispositivos activos, 10 equipos de cómputo marca DELL, 2 ruteadores MikroTik, 1 Modem DSL. • De todos los dispositivos descubiertos fue posible extraer satisfactoriamente el proveedor de la interface de red.
T3-E-2	• Solo se detectó el protocolo NetBIOS activo en 1 dispositivos, y por medio de éste fue posible identificar su nombre y grupo de trabajo.
T3-E-3	• En el equipo ruteador se identificaron 2 puertos abiertos: o 8291: MikroTik WinBox o 2000: MikroTik bandwidth-test • En los equipos de cómputo descubiertos en el segmento 192.168.1.0/24 se encontraron los siguientes puertos abiertos: o 135: RPC

	○ 139: NetBIOS ○ 445: SMB ○ 49152-49153: Microsoft Windows RPC • En el Switch administrable se encontraron abiertos los siguientes puertos: ○ 80: http ○ 443: SSL/http • En el modem DSL se encontraron los siguientes puertos abiertos: ○ 23: Telnet ○ 53: DNS ○ 80: Apache http ○ 49152: TCP Open UPNP • Haciendo uso del protocolo SMB activo los equipos de cómputo fue posible obtener su tipo y versión de Sistema Operativo: "Windows 7 Ultimate 7600 Service Pack 1". El ruteador MikroTik fue identificado con el SO: "Linux kernel 2.6".
T3-E-4 T3-E-5	• De manera general se detectó el fabricante de la tarjeta de red, se logro la resolución de nombres mediante mDNS y LLMNR. • Se identificó el Switch administrable con riesgos de nivel medio relacionado con el ataque de formato de cadena sobre el protocolo http y el uso de *Cipher Suites* depreciadas. • Se identificó el Modem DSL con riesgo crítico relacionado con el servicio Telnet. • Se identificó el Modem DSL con el riesgo crítico: *Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE*.
T3-E-6	• Utilizando la herramienta *Armitage* se corroboraron las vulnerabilidades encontradas mediante Nessus y OpenVAS. Aquellos equipos con servicios abiertos fueron seleccionados para ejecutar pruebas que permitieran identificar si dichas vulnerabilidades eran explotables.
T3-E-7	• Mediante la herramienta *Armitage* se ejecutaron 794 sobre el Switch administrable y 25 pruebas sobre los equipos de cómputo, ninguna fue exitosa. • Se ejecutaron 403 pruebas sobre el Modem DSL y se logró vulnerar la seguridad del Modem DSL en dos pruebas ejecutadas (linux/telnet/netgear_telnetenable y multi/realserver/describe). • Los *exploits* utilizados forman parte de la suit estándar del *Metasploit Framework* orientados a vulnerar sistemas con el menor esfuerzo.
T3-E-8	• Se ejecuto una prueba de rompimiento de contraseña con resultado negativo sobre el ruteador MikroTik mediante la herramienta *mkbrutus* diseñada para vulnerar equipos específicos de la compañía MikroTik utilizando el servicio del puerto 8291.
T3-E-9	• No había personal operativo cuando se realizó la visita a las instalaciones

8.4.7.3 CATD Victoria

Prueba	Resultados
T3-E-1	• Se identificó el segmento de red 192.168.1.0/24, en éste, se identificaron 6 dispositivos activos de los cuales 5 son equipos de cómputo de la marca DELL y 1

	Modem DSL. • 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 los 4 dispositivos, y por medio de éste fue posible identificar su nombre y grupo de trabajo.
T3-E-3	• En los equipos de cómputo se encontraron los siguientes puertos abiertos: ○ 135: RPC ○ 139: NetBIOS ○ 445: SMB ○ 554: RTSP ○ 5357: Microsoft HTTPAPI (SSDP/UPnP) ○ 2869: Microsoft HTTPAPI (SSDP/UPnP) ○ 10243: Microsoft HTTPAPI (SSDP/UPnP) ○ 49155: RPC • En el modem DSL se encontraron los siguientes puertos abiertos: ○ 23: Telnet ○ 53: DNS ○ 80: Apache http ○ 49152: TCP Open UPNP • Haciendo uso del protocolo SMB activo en los equipos de cómputo fue posible obtener el tipo y versión de Sistema Operativo: “Windows 7 Ultimate 7601 Service Pack 1”.
T3-E-4 T3-E-5	• De manera general se detectó el fabricante de la tarjeta de red, se logro la resolución de nombres mediante mDNS y LLMNR. • Se identificaron los 4 equipos con riesgo crítico relacionados con una falla de seguridad del servicio SMB en Windows 7 (MS17-010). • Se identificó el Modem DSL con riesgo crítico relacionado con el servicio Telnet. • Se identificó el Modem DSL con el riesgo crítico: *Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE*.
T3-E-6	• Utilizando la herramienta *Armitage* se corroboraron las vulnerabilidades encontradas mediante Nessus y OpenVAS. Aquellos equipos con servicios abiertos fueron seleccionados para ejecutar pruebas que permitieran identificar si dichas vulnerabilidades eran explotables.
T3-E-7	• Mediante la herramienta *Armitage* se ejecutaron 25 pruebas sobre los equipos de cómputo, ninguna fue exitosa. • Se ejecutaron 403 pruebas sobre el Modem DSL y se logró vulnerar la seguridad del Modem DSL en dos pruebas ejecutadas (linux/telnet/netgear_telnetenable y multi/realserver/describe). • Los *exploits* utilizados forman parte de la suit estándar del *Metasploit Framework* orientados a vulnerar sistemas con el menor esfuerzo.
T3-E-8	• No Aplica
T3-E-9	• Las contraseñas utilizadas por el personal operativo son distribuidas mediante llamadas telefónicas por los coordinadores, sin existir garantía de autenticación de los

	participantes. • La contraseña es complicada de memoriza provocando problemas para iniciar el proceso de captura.

8.4.7.4 CATD Güemez

Prueba	Resultados
T3-E-1	• Se identificó el segmento de red 192.168.1.0/24, en éste, se identificaron 2 dispositivos activos de los cuales 1 es un equipo de cómputo de la marca DELL y 1 Modem DSL. • De los dispositivos descubiertos fue posible extraer satisfactoriamente el proveedor de la interface de red.
T3-E-2	• No se encontró activo el protocolo NetBios.
T3-E-3	• En el equipo de cómputo no encontraron puertos abiertos: • En el modem DSL se encontraron los siguientes puertos abiertos: ○ 23: Telnet ○ 53: DNS ○ 80: Apache http ○ 49152: TCP Open UPNP • Haciendo uso del protocolo SMB activo en los equipos de cómputo fue posible obtener el tipo y versión de Sistema Operativo: “Windows 7 Ultimate 7601 Service Pack 1”.
T3-E-4 T3-E-5	• De manera general se detectó el fabricante de la tarjeta de red. • Se identificó el Modem DSL con riesgo crítico relacionado con el servicio Telnet. • Se identificó el Modem DSL con el riesgo crítico: *Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE*.
T3-E-6	• Utilizando la herramienta *Armitage* se corroboraron las vulnerabilidades encontradas mediante Nessus y OpenVAS. Aquellos equipos con servicios abiertos fueron seleccionados para ejecutar pruebas que permitieran identificar si dichas vulnerabilidades eran explotables.
T3-E-7	• Mediante la herramienta *Armitage* se ejecutaron 403 pruebas sobre el Modem DSL y se logró vulnerar la seguridad del Modem DSL en dos pruebas ejecutadas (linux/telnet/netgear_telnetenable y multi/realserver/describe). • Los *exploits* utilizados forman parte de la suit estandar del *Metasploit Framework* orientados a vulnerar sistemas con el menor esfuerzo.
T3-E-8	• No Aplica
T3-E-9	• No se aplico la prueba

8.4.7.5 CATD Tampico

Prueba	Resultados
T3-E-1	• Se identificó el segmento de red 192.168.1.0/24, en éste, se identificaron 11 dispositivos activos de los cuales 10 son equipos de cómputo de la marca DELL y 1 Modem DSL. • De todos los dispositivos descubiertos fue posible extraer satisfactoriamente el proveedor de la interface de red.
T3-E-2	• No se detectó el protocolo NetBIOS activo en los dispositivos, por lo que no fue posible identificar datos del sistema operativo.
T3-E-3	• En los equipos de cómputo se encontraron los siguientes puertos abiertos: ○ 62078: tcpwrapped ○ 2869: Microsoft HTTPAPI (SSDP/UPnP) ○ 5357: Microsoft HTTPAPI (SSDP/UPnP) • En el modem DSL se encontraron los siguientes puertos abiertos: ○ 23: Telnet ○ 53: DNS ○ 80: Apache http
T3-E-4 T3-E-5	• De manera general se detectó el fabricante de la tarjeta de red, se logro la resolución de nombres mediante mDNS y LLMNR. • Se identificó el Modem DSL con riesgo crítico relacionado con el servicio Telnet. • Se identificó el Modem DSL con el riesgo crítico: *Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE*.
T3-E-6	• Utilizando la herramienta *Armitage* se corroboraron las vulnerabilidades encontradas mediante Nessus y OpenVAS. Aquellos equipos con servicios abiertos fueron seleccionados para ejecutar pruebas que permitieran identificar si dichas vulnerabilidades eran explotables.
T3-E-7	• Mediante la herramienta *Armitage* se ejecutaron 25 pruebas sobre los equipos de cómputo, ninguna fue exitosa. • Se ejecutaron 403 pruebas sobre el Modem DSL y se logró vulnerar la seguridad del Modem DSL en dos pruebas ejecutadas (linux/telnet/netgear_telnetenable y multi/realserver/describe). • Los *exploits* utilizados forman parte de la suit estándar del *Metasploit Framework* orientados a vulnerar sistemas con el menor esfuerzo.
T3-E-8	• No Aplica
T3-E-9	• Las contraseñas utilizadas por el personal operativo son distribuidas mediante llamadas telefónicas por los coordinadores, sin existir garantía de autenticación de los participantes. • La contraseña es complicada de memoriza provocando problemas para iniciar el proceso de captura.

8.4.8 Recomendaciones Generales

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 y garantizar sus actualizaciones. R3-E-3. Habilitar en los equipos de cómputo un Firewall que filtre todo el trafico entrante.
T3-E-3	R3-E-4. Deshabilitar en los equipos de cómputo el servicio SMB.
T3-E-4	R3-E-5. Deshabilitar en los equipos de cómputo el servicio UPnP.
T3-E-5	R3-E-6. Deshabilitar en los equipos de cómputo el servicio NetBIOS.
T3-E-6	R3-E-7. Instalar en los equipos de cómputo la actualización 4012212 (MS17-010).
T3-E-7	R3-E-8. Deshabilitar en los Modem DSL el servicio Telnet. R3-E-9. Actualizar en los Modem DSL el SDK del servicio UPnP a una versión superior o igual a 1.6.18 o en su defecto deshabilitar el servicio. R3-E-10. Deshabilitar en los Modem DSL el servicio DNS.
T3-E-8	No Aplica
T3-E-9	R3-E-11. Utilizar mecanismos **criptográficos** que garanticen autenticación de los usuarios al mismo tiempo que brinden la capacidad de integridad y no repudio de la información que cada usuario registre en el sistema.

9. Pruebas de negación de servicio a sitios web del PREP y al sitio principal del OPL

9.1 Objetivo

Realizar pruebas de ataques de negación 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.

Los ataques SYN Flood, ICMP Flood y Slowloris se realizaron de acuerdo a lo descrito en la Tabla 9.2. En la Tabla 9.3 se describe la calendarización de los ataques Slowloris a los sitios de los difusores oficiales del PREP, los cuales fueron solicitados por el IETAM después del simulacro 3. En su mayoría, los ataques se realizaron con una duración promedio de 30 minutos.

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

Servidor (Publicación)	Puerto	Ataque	20-jun	21-jun
PROISI simulacro2.prep2018tamps.mx	80	SYN Flood	20:00	
		ICMP Flood	20:30	
		Slowloris	09:30	
		DNS Ampl.		09:30
	443	SYN Flood	07:00	
		ICMP Flood	07:30	
		Slowloris	10:30	
		DNS Ampl.		10:30
IETAM ietam.org.mx	80	SYN Flood		20:00
		ICMP Flood		20:30
		Slowloris	11:30	
		DNS Ampl.		11:30
	443	SYN Flood		07:00
		ICMP Flood		07:30
		Slowloris	12:30	
		DNS Ampl.		12:30

Tabla 9.3. Calendarización del ataque Slowloris a los sitios difusores de la publicación de resultados *del PREP.*

Servidor (Publicación)	Puerto	26-jun
simulacro3.prep2018tamps.mx	80 y/o 443	09:00
https://difusores.prep2018tamps.mx/		10:00
http://prep2018.hoytamaulipas.net/		11:00
http://prep.muropolitico.mx/		12:00
http://eleese.com.mx/prep/		13:00

9.4 Resumen de resultados y hallazgos

En la Tabla 5 se resumen los hallazgos realizados en la ejecución de las pruebas de negación de servicios realizadas como parte de los requerimientos del IETAM.

Tabla 5. Resumen de los hallazgos de la pruebas de negación de servicios.

	SYN Flood	ICMP Flood	Slowloris	DNS Amplification
http://simulacro2.prep2018tamps.mx				
http://ietam.org.mx				
https://difusores.prep2018tamps.mx/				
http://prep2018.hoytamaulipas.net/				
http://prep.muropolitico.mx/				
http://eleese.com.mx/prep/				
https://simulacro3.prep2018tamps.mx				
https://prep.muropolitico.mx/				
https://eleese.com.mx/prep/				

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

Cabe señalar que en el caso de los ataques DNS amplification, la valoración indicada como "Resistente" es derivada de la información recabada con el personal técnico del sitio, ya que las pruebas no se realizaron de forma práctica.

Parte IV

10. Simulacros

Se realizaron 3 simulacros los días 10, 17 y 24 de junio de 2018. El Ente Auditor tuvo presencia durante los tres simulacros en CCV1, CCV2, CATD Victoria (10 y 24 de junio), CATD Tampico (17 de junio). 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 recibidas	Avance al final del simulacro
Simulacro 1	10/06/18	4628	4332	4371	94.44%
Simulacro 2	17/06/18	4628	4481	4565	98.63%
Simulacro 3	24/06/18	4628	4297	4367	94.36%

10.1 Observaciones resultantes de los simulacros 1, 2 y 3.

10.1.1 Módulo de publicación de resultados

- Se realizó la validación de las huellas criptográficas de las aplicaciones informáticas y del estado inicial de la base de datos de acuerdo con el procedimiento acordado entre IETAM, Proveedor y Ente Auditor. Se anexa el reporte con la validación.
- El nombre con el que se recupera la imagen de acta no se puede asociar por sí mismo con el registro que corresponda en la base de datos de publicación (_TAMPS_PREP_AYUn_2018). La asociación es a través del sitio web de publicación.
- El corte del sistema PREP en su fase de publicación reportó 4565 actas recibidas de las 4628 consideradas en el simulacro.
- Mediante verificación realizada por un sistema informático, diseñado por el ente auditor se obtuvieron 4370 imágenes de actas de las 4565 actas procesadas.
- Se detectó que, para 115 actas con sus imágenes, registradas en la base de datos de publicación (_TAMPS_PREP_AYUn_2018), el sistema no realizó el registro de su correspondiente Hash o huella criptográfica.
- El sistema detectó que en 103 casos existe el registro SHA pero no encontró la imagen correspondiente en sitio web de publicación. (_TAMPS_PREP_AYUn_2018).
- El sistema detectó que 258 imágenes del sistema de publicación no se pudieron descargar.
- Se detectó que tres actas registradas en la base de datos de publicación tienen las mismas claves de casilla “280627E0305” y la misma clave de acta “280627E030502”, con imágenes diferentes.
- El ente auditor detectó que el algoritmo usado por el proveedor para crear la huella criptográfica de las actas manejadas por el sistema de publicación es el recomendado por el IETAM (SHA256).
- Mediante un análisis de las base de datos de publicación generadas cada 15 minutos, se observó que la huella criptográfica de cada archivo es distinta lo cual es indicativo que la base

de datos de publicación se actualiza.

- Se identificó que en el log del web service de auditoría se registraron 4561 actas de las 4565 de las actas capturadas.
- Se ejecutó un programa realizado por el ente auditor que realizó un proceso de scrapping sobre el sitio web de publicación pudiendo obtener sin restricción alguna el DOM del sitio y recursos como imágenes y javascript.
- Se desconoce si existe una traza de los diferentes estados por los que pasa un acta a través de todo el proceso (desde la captura hasta su contabilización).

10.1.2 CCV Principal

- La aplicación Controlador se cierra sin ningún motivo aparente.
- Las credenciales para los diferentes roles se almacenan en un block de notas compartido en el escritorio de la computadora y cualquier usuario puede acceder al mismo.
- El tiempo de respuesta entre una validación y otra no es siempre el adecuado.
- El personal de validación tiene acceso a otras aplicaciones que se conectan a Internet además de las propias de la solución del PREP.
- El validador desconoce si una nueva acta le ha sido asignada. Para saberlo éste debe realizar actualizaciones frecuentes de la página. Esto genera un número considerable de peticiones al servidor si el mismo proceso es realizado por varios validadores. Se sugiere implementar un sistema de notificaciones que le indique al usuario cuando un acta está disponible
- El validador 2 tiene la funcionalidad de modificar cualquier dato, si así lo considera.
- Los componentes del manejo de la foto no funcionan correctamente: Por ejemplo, el zoom no aumenta o no disminuye, la imagen no gira, etc.
- No está implementado un sistema de control de calidad en el trabajo que desarrolla un validador.
- En algunos casos la aplicación se detuvo justo en el momento de guardar un acta, de denegarla, etc.
- El internet inalámbrico estaba habilitado y con la contraseña por default visible en el modem. Por lo anterior, toda la red local se puede ver comprometida ante un ataque potencial iniciado por conexión inalámbrica.
- Se pudo validar la configuración de enlaces redundantes de forma exitosa desconectando por turnos los puertos de la red local.
- La prueba de desconexión del medio de comunicación a Internet fue exitosa durante el Simulacro 3.
- Se obtuvieron gráficas de análisis de tráfico entrante y saliente de cada uno de los enlaces que reflejan el comportamiento descrito en los dos puntos anteriores. Se anexan capturas de pantalla de dicho comportamiento. Se anexa reporte.
- Se pudo validar el funcionamiento de los equipos SAI (UPS) de forma exitosa hasta por 3 minutos. Sin embargo, se presentaron fallas en los UPS de la sala de coordinadores.
- Se validó que el acceso a los sitios “casilla-tamaulipas.sistemaprep.org” y “audit-

tamaulipas.sistemaprep.org" tienen acceso restringido por dirección IP.

- Se observó que el equipo de soporte técnico "Coordinadores" utiliza la versión de uso libre del software Teamviewer lo cual conlleva riesgos potenciales al estar disponible para una gran comunidad de usuarios.
- Se validó que el portal del simulacro "simulacro2.prep2018tamps.mx" utiliza el protocolo "https".
- Se validó la disponibilidad de una planta de emergencia con capacidad de 75 KVA, así como su esquema de conectividad. Se realizó la prueba de funcionamiento de la planta de emergencia de forma exitosa.
- Si bien hubo una disminución en las llamadas, sin embargo aún la mayor parte de ellas era debido a que el personal contratado para captura y verificación tenían dudas acerca del proceso de captura, lo cual hace evidente la necesidad de una capacitación mayor. Esta observación fue solventada en una revisión durante el Simulacro 3.
- Se detectó que al menos uno de los capturistas no tenía idea de cómo capturar las actas y estuvo mandando las actas mal capturadas. No se pudo identificar el CATD de procedencia. Durante el Simulacro 3, esta situación fue completamente resuelta.
- Para algunos municipios se detectó que las actas capturadas no se reflejaban rápido en el sistema de validación, duraron más de 3 horas para que éstas se pudieran reflejar. Posterior al simulacro 3, de acuerdo con el proveedor del servicio esta situación ha quedado resuelta.
- A las 10.30am 3 municipios (El Mante, Mainero y Llera) tenían problemas con la conexión a Internet, por lo que no estaban transmitiendo.
- A las 10.30am el municipio de El Mante tuvo problemas técnicos con el sistema, por lo que no pudieron digitalizar actas por PREP tradicional.
- No obstante lo anterior, en El Mante operaron con PREP Casilla capturando, llegando a tomar fotos del 93.8650% del total de las actas (153/163) para las 4pm.
- A las 10.30am Aldama estuvo transmitiendo muy lento por conexión lenta a Internet.
- A las 12pm varios municipios ya habían cerrado la transmisión de actas.
- A las 12:30pm se habían terminado de digitalizar todas las actas de Tampico, pero no se reflejaron sino hasta las 3:15pm
- A las 4:00pm se habían recibido el total de las actas de Tampico (434/434), siendo contabilizadas 419.
- Al personal de proveedor, IETAM, y auditoría, se les asignaron gafetes de identificación a la hora de acceder al CCV.
- Los capturistas/verificadores se encontraban en los TCA asignados anteriormente, y no hubo error en la asignación.
- Los capturistas/verificadores tenían la capacidad de poder operar los tres roles del CCV, siendo éstos: capturistas para las imágenes provenientes de PREP Casilla, verificadores 1 y verificadores 2.
- Los capturistas/verificadores cuentan con credenciales para un solo rol al iniciar, siendo éste el asignado, y de ser necesario se les proporciona credenciales para que puedan operar otro rol.

- Los usuarios no están asociados a la máquina o a la persona que valida por lo que un mismo usuario puede ser compartido para varias personas al mismo tiempo. Se crearon cuentas de usuario para todos los equipos con el fin de restringir el acceso a los mismos.
- Al reiniciar algunos dispositivos de red se producen errores de conectividad debido a que existen algunas direcciones IP que se asignan dinámicamente. La situación quedó resuelta mediante la configuración de los equipos.
- Los capturistas/verificadores no contaban con un manual de usuario personal para el funcionamiento del sistema, se tenía solo uno para todo el CCV. La observación ha quedado atendida posterior al simulacro 3.
- Se detectó que el sistema no cierra sesión cuando se cierra el navegador, incluso cuando se apaga el equipo por completo se mantiene la sesión abierta. El proveedor realizó la configuración necesaria para que al apagar la computadora se eliminan los datos de sesión, se dieron instrucciones a los operadores de cerrar la sesión a través de la misma aplicación, de no ser así los datos se sesión seguirán persistiendo en el navegador.
- Una gran cantidad de actas digitalizadas provenientes de CATD, se encontraban mal capturadas, había actas que la sección donde se encuentra la información del acta esta recortado, por un mal posicionamiento a la hora de realizar la digitalización. Lo anterior hace evidente la necesidad de una capacitación mayor a los capturistas y digitalizadores. Se han tomado las medidas necesarias por parte del proveedor de servicio para mantener esta situación bajo control.
- Se redujo la cantidad de capturistas/verificadores que anteriormente en el simulacro 1 no entendían correctamente la actividad que tenían que realizar, por lo cual acudían constantemente con alguno de los coordinadores disponibles por parte de proveedor. Se capacitó al personal y se distribuyeron manuales de usuario impresos para consulta.
- Los equipos que están asignados para verificador 1, tienen bloqueado el acceso de un dispositivo externo, por lo que se dificulta la instalación de un teclado para poder adaptar para el rol de verificador 2. Se ha atendido esta situación conectando teclados a todos los equipos.
- El personal del IETAM verificó los datos de resultados en la publicación.

10.1.3 CCV Alterno

- La infraestructura del CCV cuenta con 18 equipos de cómputo, 1 router MikroTik, 1 router PepLink Balance, 1 switch Cisco Small Business, 4 cámaras de circuito cerrado, 2 UPS en el rack y 5 para las terminales de captura/verificación.
- Posterior al simulacro 3, se validó el funcionamiento correcto de los dos servicios de Internet contratados: uno con Izzi, y el otro con Telmex.
- En la entrada se encuentra un guardia de seguridad que restringe el acceso físico al fraccionamiento donde se encuentran las instalaciones de este CCV; dentro del CCV no existen mecanismos de control de acceso físico al rack de componentes de red. La situación ha sido resulta posterior al Simulacro 3.

- Únicamente se utilizan cámaras de seguridad para monitorear el acceso de los capturistas/verificadores y del personal del proveedor. Se ha dispuesto de una persona encargada de controlar el acceso para el día de la jornada electoral.
- Los equipos de cómputo tienen cuentas de usuario impidiendo el acceso a las aplicaciones sin autenticación.
- El mecanismo de control de acceso a la aplicación web se basa en el uso de contraseñas generadas a partir de un script. El personal de este CCV recibe las contraseñas mediante su coordinadora, la cual tiene el listado de usuarios y contraseñas anotado en una hoja y las va dictando a cada uno de los capturistas/verificadores. Algunos verificadores anotan su usuario y contraseña en un bloc de notas y almacenan el archivo en el equipo, otros solo las anotan de forma temporal. La observación se atendió: el día de jornada se generarán nuevas contraseñas y se cuidará la distribución de éstas. Se evitará usar el archivo de bloc de notas.
- Aunque hay un encargado de soporte técnico, el acceso lógico a la administración de la red se ve limitado al acceso al software de configuración de MikroTik a cargo del administrador. En caso de presentarse una falla en el ruteador, el encargado de soporte deberá notificar al administrador de la red para que solucione el problema. Se incremento la cantidad de personal técnico para evitar este inconveniente.
- El acceso hacia el servidor de validación está filtrado mediante las IP públicas de los CCV; antes y durante el corte de energía eléctrica, el acceso al servidor desde las terminales fue intermitente, se mostraban errores de gateway incorrecto y tiempo de espera agotado, por lo que se tuvo que notificar al personal del proveedor para que atendiera la situación. La observación se atendió evitando el cambio de direcciones por falla del fluido eléctrico en el modem, mediante una UPS exclusiva.
- En el simulacro 3, los UPS se mantuvieron operando por un periodo de 3 minutos que duró el corte de energía programado.
- No se pudo realizar un escaneo oficial de puertos de red abiertos; sin embargo, mediante el navegador se pudo detectar que aún no se han filtrados los puertos dado que hay acceso a Google, Wikipedia, Facebook, Twitter (con intermitencia), Snapchat, Instagram y YouTube. Se atendió la observación cerrando los puertos para evitar el acceso a estas aplicaciones.
- Este CCV entró en operación a la 12:35PM, simulando que el CCV dejaba de operar. El CCV operó hasta las 2.00PM
- En este sitio se encontraban 12 operadores, no todos tenían identificación. Solo uno no portaba la playera de identificación. La observación ha sido solventada.

10.1.4 CATD Victoria

- La infraestructura del CATD cuenta con 5 equipos de cómputo, 5 escáneres, 1 módem, y 3 UPS.
- El servicio de Internet contratado es Telmex Infinitum 10Mbps; no existe enlace de comunicación de respaldo.

- Los equipos de cómputo están conectados mediante un switch al módem que les provee salida hacia Internet.
- No hay un área de administración de la red, el único componente de comunicaciones que se encuentra es el módem de Telmex, por lo que el control de acceso físico a esta infraestructura es inexistente. La observación ha quedado solventada.
- El internet inalámbrico estaba habilitado. Los usuarios del PREP tenían acceso al Wifi en sus equipos celulares. La contraseña del Wifi es la predeterminada y visible en el Modem DSL. Se ha realizado la configuración adecuada por lo que la observación ha sido atendida.
- Uso de celular para las dudas, usan WhatsApp para comunicarse con los coordinadores.
- Los gafetes que porta el personal del proveedor, los acopiadores y los capturistas/verificadores son usados como medida de control o monitoreo de sus entradas y salidas.
- Los equipos de cómputo no tienen cuentas de usuario de Windows configuradas, por lo que se puede acceder al escritorio de los equipos sin autenticación. Se ha realizado la configuración requerida para solventar la observación.
- El mecanismo de control de acceso a la aplicación de escritorio se basa en el uso de contraseñas generadas a partir de un script. El personal de este CATD recibe las contraseñas mediante su coordinadora de zona vía mensaje de WhatsApp. La observación se ha atendido indicando que el día de jornada se generarán nuevas contraseñas y se cuidará la distribución de estas. Se evitará usar el archivo de bloc de notas.
- No se pudo corroborar la información recabada anteriormente acerca de los mecanismos de control de acceso lógico de la aplicación PREP Casilla dado que no fue asignado algún CAE al CATD Victoria.
- Todos los operadores realizaban su trabajo de manera correcta, y estaban bien capacitados, fue muy mínima las dudas acerca de la actividad que tenían que realizar o de cómo usar el sistema.
- Los capturistas se comunican directamente con soporte técnico. Se atendió la observación Se resolvió el problema dando indicaciones para proceder en el caso de alguna incidencia.
- No fue posible validar la planta de energía ya que no se logró que ésta entrara en funcionamiento durante el periodo de prueba, indicando que se solicitará un cambio de equipo al proveedor.

10.1.5 CATD Tampico

- La infraestructura del CATD cuenta con 5 equipos de cómputo Dell, 5 escáneres, 1 módem, y 5 UPS. De momento no tienen planta de luz de emergencia, pero ya se definió que el proveedor deberá proporcionarla e instalarla al menos 1 semana antes de la fecha de la jornada electoral. Se ha atendido el requerimiento sobre la planta de energía.
- 5 digitalizadores capturistas, 2 coordinadores acopiadores, 1 jefe de grupo
- El proceso comenzó a las 9:10 am, las actas PREP ya se encontraban llenadas.
- Aunque se usaron las mismas actas del simulacro 1, se simuló la fecha del día (16 de junio 2018) en las actas.

- El total de actas para Tampico es de 434
- El servicio de Internet contratado es Telmex Infinitum 10Mbps; éste tiene velocidades promedio de carga de 1.77Mbps y 5.02Mbps de descarga.
- Si el servicio de Telmex presenta fallas se activaría banda ancha móvil como servicio de respaldo de acuerdo con el coordinador del proveedor.
- Los equipos de cómputo están conectados mediante un switch al módem que les provee salida hacia Internet.
- Se puede acceder a Internet por Wi-Fi mediante ese mismo módem utilizando la contraseña por defecto ya que, al realizar un par de escaneos de la red, se identificaron 3 dispositivos extra al iniciar la jornada de simulacro y 7 dispositivos extra al finalizar la captura de las actas. Los resultados del escaneo arrojaron que los fabricantes de los dispositivos extra son los siguientes:
  - 1 dispositivo Shanghai Wind Technologies.
  - 3 dispositivos Apple.
  - 1 dispositivo Sony Mobile Communications AB.
  - 1 dispositivo Dell.
  - 1 dispositivo no especificado.

  Se atendió la observación bloqueando redes y cambiando contraseñas.

  Se desconoce quienes son los propietarios de todos los equipos extra y si éstos corresponden únicamente a dispositivos móviles o si se trata de equipos de cómputo utilizados por el Consejo Municipal Electoral. Una vez que arribaron los integrantes del Consejo Municipal Electoral se registraron más dispositivos extra conectados a la red del CATD. Se atendió la observación bloqueando redes y cambiando contraseñas.

  No existe una red aislada para el PREP de uso exclusivo para la captura y procesamiento de la información electoral, sino que ésta es de alguna manera compartida con el Consejo Municipal Electoral. Se atendió la observación bloqueando redes y cambiando contraseñas.
- Únicamente se utilizan gafetes que porta el personal del proveedor, los acopiadores y los capturistas/verificadores como medida de control o monitoreo de sus entradas y salidas. De igual forma, se encuentran dentro de las instalaciones 2 elementos de la Policía Federal realizando tareas de vigilancia hacia el exterior. Se atendió la observación.
- Todos los operadores contaban con un gafete de identificación y se presentaron uniformados con una playera negra del proveedor.
- Los equipos de cómputo no tienen cuentas de usuario de Windows configuradas, por lo que se puede acceder al escritorio de los equipos sin autenticación. Se atendió la observación realizando la configuración requerida.
- El mecanismo de control de acceso a la aplicación de escritorio se basa en el uso de contraseñas generadas a partir de un script. El personal de este CATD recibe las contraseñas mediante su jefa de grupo y coordinadora de zona, quienes van dictando a los capturistas/verificadores sus correspondientes usuarios y contraseñas. Se atendió la

observación, creando cuentas de usuario para todos los equipos con el fin de restringir el acceso a los mismos

- La distribución de las contraseñas a la jefa de grupo y coordinadora de zona se realiza mediante imágenes vía grupo de WhatsApp donde se encuentra personal del proveedor, así como otros jefes de grupo y coordinadores de zona. Se atendió la observación dando instrucciones precisas para la distribución de contraseñas únicamente a través de los coordinadores quienes deberán asignarlas personalmente a cada operador.
- Los UPS mantuvieron encendidos 3 de los 5 equipos de cómputo, 2 escáneres y el módem durante los 5 minutos que duró la simulación del corte de energía, por lo que se pudo continuar con el proceso de captura casi de forma ininterrumpida. Se resolvió el problema de los UPS.
- Se presentó una situación de inconformidad por parte de la presidenta del Consejo Municipal Electoral debido al número de miembros del equipo del Ente Auditor. Se atendió la observación.
- Se realizaron escaneos de puertos abiertos en la red del CATD mediante un equipo externo, sin embargo, al no obtenerse resultados concluyentes para los equipos de captura de las actas y no poder acceder a éstos, se verificó desde el navegador web del mismo equipo externo los puertos de red abiertos. Como resultado se obtuvo que aún no se han filtrado los puertos puesto que hay acceso a Google, Wikipedia, Gmail, Facebook, Twitter, WhatsApp, Skype, Snapchat, Instagram y YouTube. Se atendió la observación bloqueando puertos.
- No se pudo corroborar la información recabada anteriormente acerca de los mecanismos de control de acceso lógico de la aplicación PREP Casilla dado que aún no se cuenta con los dispositivos móviles.
- El encargado de la unidad de servicio de soporte móvil tiene para respaldo y/o reemplazo 2 equipos de cómputo, 2 teclados, 1 unidad de disco, cables VGA, 2 bobinas de cable de red, conectores de red y equipo para verificar la conectividad de los cables de red. No estaban incluidos UPS de respaldo. Se atendió la observación.
- Al iniciar el proceso se les retiró el celular a los proveedores, se les entrego nuevamente al finalizar.
- Los coordinadores son los encargados de asignar las credenciales a los capturistas.
- En una ocasión las credenciales estaban erróneas, pero en seguida el coordinador le asignó nuevas. Se atendió la observación.
- Los operadores ingresaron al sistema y verificaron la versión del sistema, e iniciaron el proceso.
- Un operador estaba utilizando un teclado personal para la captura del acta, el coordinador comentó que se permitía utilizar cualquier teclado o mouse, todo con la intención de que el operador se sienta cómodo y realice un buen desempeño. Se atendió la observación dando instrucciones para usar solo el equipo autorizado.

- Todos los operadores realizaban su trabajo de manera correcta y ágil, estaban bien capacitados, fueron mínimas las dudas acerca de la actividad que tenían que realizar o de cómo usar el sistema.
- Sin embargo, se presentaron dudas una de cómo posicionar el acta PREP en el escáner.
- El personal de captura y logística del CATD demostró su destreza y capacitación para realizar todas y cada una de las actividades durante el simulacro de forma eficiente.
- Los operadores no regresan el acta PREP al acopiadora hasta terminar el proceso de captura de todas las actas que les asignaron.
- Se contaba con dos manuales de usuarios, uno para cada tipo de usuario, los dos eran para todos los operadores.
- En una ocasión un operador presentó una queja, era que su escáner a veces no funcionaba correctamente y tenía que salir y volver a entrar al sistema para que éste trabajara correctamente. El jefe de grupo no supo resolver el problema. No hubo necesidad de reiniciar el equipo. Se atendió la observación.
- Los operadores la mayoría de las ocasiones no verificaban la calidad de la imagen, ya que realizaban la captura basándose en el acta física. Se atendió la observación mediante capacitación.
- El sistema almacena localmente las actas si se pierde la conexión, ésto se guarda de manera temporal y cuando regresa la conexión a Internet ya permite al usuario enviar las actas capturadas y digitalizadas.
- Se incluyeron nuevos botones en la interfaz gráfica. Sin embargo se pudo observar que estos nuevos cambio no fueron utilizados por los operarios de la aplicación. Al parecer los usuarios desconocen la funcionalidad de estos nuevos elementos. Se atendió la observación mediante capacitación.
- Se realizó la prueba de desconexión del servicio de Internet para validar el funcionamiento del sistema aún en ausencia del mismo y el resultado fue satisfactorio.
- Se realizaron las pruebas de revisión de configuraciones a la infraestructura tecnológica y sus resultados serán incluidos en el informe en extenso del simulacro 2.
- Se realizaron las pruebas de revisión de pentest a la infraestructura tecnológica y sus resultados serán incluidos en el informe en extenso del simulacro 2.

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**

11.2 Identificación de Activos

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. En la Tabla 11.4 se presentan 14 eventos relevantes para la operación del PREP y la correcta operación del Proceso Técnico Operativo. Los primeros 9 eventos corresponden a los requerimientos funcionales propios del PREP o del PTO. Los restantes 5 activos corresponden a eventos no funcionales relevantes identificados para la correcta operación del PTO.

A continuación se presentan las vulnerabilidades y amenazas identificadas en cada uno de los eventos y su valoración de acuerdo con la metodología Mageritv3.

Tabla 11.4. Eventos relevantes funcionales y no funcionales para la operación del PREP y del PTO.

IDENTIFICACIÓN	EVENTO	DESCRIPCIÓN
ID-01	Inicialización y manejo de la base de datos y del sistema de archivos.	Acrividades relevantes previas a la operación del PREP
ID-02	Toma fotográfica	Actividades iniciales ejecutadas en el módulo PREP Casilla
ID-03	Digitalización	Actividades relacionadas con la obtención de las imágenes de las actas en los CATD
ID-04	Captura de información	Actividades propias de la captura de la información a partir de las imágenes capturadas/recibidas
ID-05	Validación	Actividades relacionadas con la validación de los resultados capturados
ID-06	Publicación de resultados	Actividades relevantes con relación a la publicación de los resultados del PREP
ID-07	Auditoría a los eventos del proceso	Registro de actividades internas realizadas en el sistema informátio
ID-08	Calidad de equipamiento y de los servicios	Vulnearabilidades observadas con respecto a la infraestructura tecnológica y de comunicaciones para la implementación del PTO
ID-09	Capacidad, técnica y entrenamiento.	Vulnerabilidades detectadas con respecto a la capacidad técnica y capacitación del equipo de trabajo que impementa el PREP
ID-10	Confiabilidad / Resiliencia.	Vulnerabilidades detectadas que afectan a la confiabilidad y continuidad del sistema ante posibles fallas u operación fuera de las especificaciones originales
ID-11	Disponibilidad / Escalabilidad	Vulnerabilidades identificadas que afectan a la continuidad del servicio
ID-12	Seguridad Informática	Vulnerabilidades identificadas con relación a la seguridad de todas las componentes tecnológicas
ID-13	Seguridad en el proceso	Vulnerabilidades identificadas con relación a la seguridad en la operación de las componentes del PTO
ID-14	Usabilidad	Vulnerabilidad identificadas con relación a la gestión del proyecto y manejo de inicidencias.

11.3 Resumen de análisis de riesgos

En la Tabla 11.5 se presenta el resumen de la valoración de los riesgos a los 14 activos funcionales y no funcionales identificados durante la revisión en el proceso de auditoría al PREP. Se indica el número de vulnerabilidades enconctradas en cada uno de los activos funcionales y no funcionales y el número de amanezas diferentes detectadas para todas las vulnerabilidades. El impacto de cada activo refleja el promedio ponderado de cada una de las vulnerabilidades y amenazas agrupadas dentro del

activo. Así también, para la probabilidad de materialización se calcula el promedio ponderado de cada una de las probabilidades de materialización de las amenazas.

Tabla 11.5. Valoración de los riesgos en los eventos funcionales y no funcionales detectados para la operación del PREP y del PTO.

IDENTIFICACIÓN	EVENTO	VULNERABILI-DADES	AMENAZAS	IMPACTO PROMEDIO	MATERIALIZA-CIÓN PROMEDIO
ID-01	Inicialización y manejo de la base de datos y del sistema de archivos.	8	4	4.1	2.8
ID-02	Toma fotográfica	6	2	2.9	2.4
ID-03	Digitalización	2	2	3.5	2.5
ID-04	Captura de información	11	3	2.0	2.3
ID-05	Validación	12	3	2.4	2.7
ID-06	Publicación de resultados	7	3	2.3	3.3
ID-07	Auditoría a los eventos del proceso	3	1	2.7	2.4
ID-08	Calidad de equipamiento y de los servicios	7	3	2.8	2.2
ID-09	Capacidad, técnica y entrenamiento.	6	2	2.8	3.3
ID-10	Confiabilidad / Resiliencia.	5	2	3.0	2.7
ID-11	Disponibilidad / Escalabilidad	3	2	3.9	2.4
ID-12	Seguridad Informática	11	5	3.8	2.5
ID-13	Seguridad en el proceso	6	3	3.3	3.3
ID-14	Usabilidad	3	2	1.0	2.0

La Figura 11.1 presenta el diagrama de calor de la ubicación de cada una de las amenazas presentes en los eventos relevantes del PREP presentados en la Tabla 11.19. Es importante destacar que, no obstante la mayoría de los impactos se encuentran en la zona amarilla, a través de las recomendaciones emitidas en la revisión de las líneas de acción es posible ubicar tales puntos en las zonas menos riesgosas para la operación del PREP.

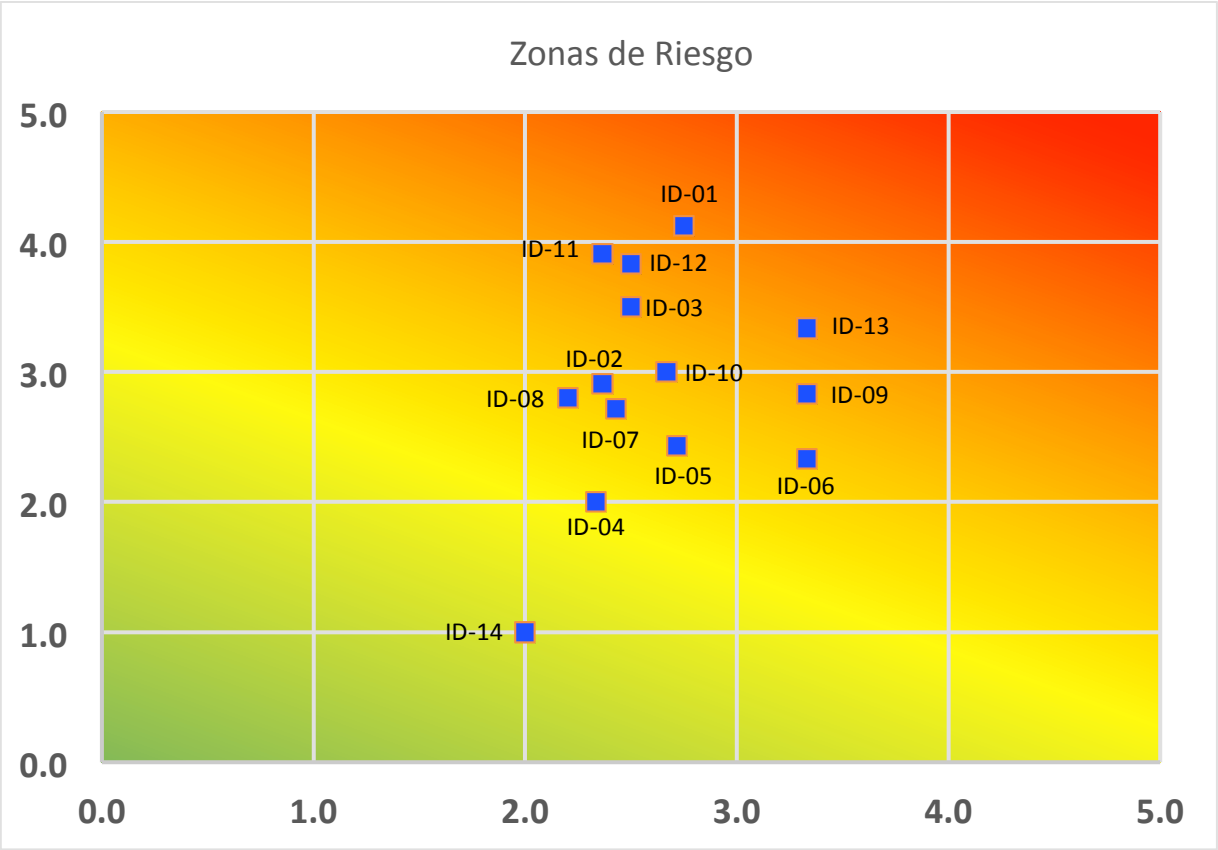

Figura 11.1. Diagrama de calor de la ubicación de los riesgos detectados en la operación del PREP.

12. Conclusiones

El presente documento presentó 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 2017-2018 (PREP) llevado a cabo entre el 2 de abril y el 30 de junio de 2018.

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 no atendidas, no son críticas para la operación del PREP y son consideradas como áreas de oportunidad para procesos futuros.