TECNOLÓGICO
DE MONTERREY®

Pruebas Funcionales de Caja Negra al Sistema Informático del SIPRE

Informes preliminares y final de las pruebas funcionales de caja negra ejecutadas al sistema informático SIPRE

Descripción breve

Este documento contiene el resultado en detalle de cada una de los resultados y observaciones identificadas en la revisión y pruebas del sistema como parte de los servicios de auditoría de seguridad para la Comisión Estatal Electoral del estado de Nuevo Leon

Jesús R. González / Juan Arturo Nolazco

jrgonza@gmail.com jnolazco@itesm.mx

Índice

Versión	Fecha	Descripción
1.0	07/Abril/2018	Documento inicial de resultados preliminares de la prueba funcional a caja negra del sistema informático SIPRE de la CEENL
1.5	11/Mayo/2018	Documento de informe de resultados preliminar con modificaciones en base a junta de inicio de actividades.
1.6	14/Mayo/2018	Cambios en la forma de clasificar hallazgos basado en OWASP e inclusión de los resultados de los requerimientos de captura del acta
1.7	28/Mayo/2018	Primera iteración Informe Preliminar de Resultados de las Pruebas Funcionales a Caja Negra
1.8	04/Junio/2018	Segunda iteración de pruebas para realizar el informe preliminar de resultados de preubas funcionales
1.9	23/Junio/2018	Ultima revisión e inclusión de los análisis de riesgo practicado sobre las pruebas ejecutadas

Dictamen elaborado por:

MSc. Jesús Raúl González Hernández en coordinación con Dr. Juan Arturo Nolazco.

1 Introdución

Este documento presenta los avances y resultados preliminares de las pruebas hechas a caja negra del sistema de captura de actas para las elecciones del 2018 para la CEENL

Este documento se dará en cada iteración de pruebas que se de para llevarlo a una aceptación del 100% por lo que estos resultados se documentarán cada vez que se lleve acabo la ejecución de pruebas.

La sección de anexos documenta en cada uno los resultados de cada iteración con las firmas por parte del ente auditor y un representante de la CEENL. La tabla de resultados tiene sección de comentarios, si hay necesidad de agregar algún tipo de recomendación adicional, esta estará incluída en esa misma sección de anexo.

Cada iteración de pruebas estará documentada en una sección de anexo de este documento con sus comentarios (si así lo requieren) y las firmas de los representantes de la entidad auditora

2 Metodología

La metodología requiere de la ejecución de las pruebas que se tienen documentadas en el documento de los planes de prueba. Los hallazgos obtenidos de la ejecución se documentarán en este documento con las recomendaciones que apliquen. Las pruebas en la metodología se separaron en dos segmentos:

- Prueba de la aplicación móvil con la comprobación de recepción de actas en sitio central
- Pruea de sitios con multifuncional con la comprobación de recepción de actas en sitio central

De acuerdo a lo requerido en el documento de Requisitos Mínimos del INE, se ejecutarán las pruebas y se documentarán resultados de estas.

- Si cumplen con las funcionalidades definidas, se documetarán como resultados finales y se presentará como tal.
- De no cumplir los criterios, entonces se documentarán las recomendaciones y resultadosasí como se acordará un tiempo para una segunda ejecución de pruebas en la cual se revisen las pruebas que no hayan cumplido con los criterios.

La sección de anexos de este documento refleja cada iteración hecha en las pruebas. Cada anexo refleja una iteración y sobre esta se documentan resultados y recomendaciones. Cada anexo debe firmarse por el representante de la entidad auditora como por un representante de la OPL.

3 Criterios utilizados para la auditoría

En la sección de anexos, se tiene la tabla que documentará los resultados de la prueba que se ejcutara. Los criterios de aceptación de cada prueba están documentados en la tabla para lo cual la prueba debe cumplir con ellos. Cada prueba puede tener uno de tres tipos de resultados que pueden ser los descritos en la tabla siguiente

Resultado Prueba	Descripcion de Criterio	Acciones
Aceptado	La prueba cumplió satisfactoriamente con los criterios de aceptación	Prueba es aceptada y se da por cerrado el inciso de esta prueba. De ser necesario ejecutar el plan de nuevo en otra iteración, esta prueba no se volverá a ejecutar.
Rechazado	La prueba no cumplió con los criterios de aceptación	Prueba no es aceptada, se documenta el resultado y recomendaciones. Esta prueba se volverá a ejecutar en la siguiente iteración para revisar la implementación de las recomendaciones dadas en el resultado de las pruebas.
Aceptado con Observaciones	La cumplió con una parte de los criterios o cumplió totalmente con observaciones.	Prueba es aceptada, pero con recomendaciones. Esto significa que las recomendaciones son solo eso, no serían obligatoria su implementación y solo queda como sugerencia o recomendación.
No Ejecutada	Prueba no fue ejcutada en el ciclo por cuestiones de tiempo o por decisión mutua	La prueba se volverá a ejecutar en otro ensayo o bien si no se ejecuta, se agregará la justificación del por que de esto.

Cada una de las pruebas a ejecutar, tiene su criterio propio. En el caso de un cumplimiento, la prueba se da por pasada y no vuelve a ejecutarse en una siguiente iteración, de ser el caso.

4 Metodología para clasificar los hallazgos

Los hallazgos que se hagan en las pruebas se clasificarán basado en el Open Web Application Security Protect Mobile (OWASP-Mobile). Esta metodología representa un consenso a nivel desarrolladores sobre los riesgos mas críticos para las a aplicaciones.

#	Clasificación	Descripción
M1	Uso impropio de la plataforma	Maluso de una caraterística de la plataforma o falla de controles de seguridad de esta.
M2	Almacenamiento inseguro de datos	ESta combina dos categorias que se habían liberado en la version previa y cubre almacenamiento inseguro de datos y fuga no-intencional de estos.
M3	Comunicación insegura	Esta clasificación cubre una mala negociación entre dos puntos por cuestiones de versions de SSL, negociación débil, comunicaciones en texto sin cifrado en activos sensibles.
M4	Autenticación insegura	Esta categoría tiene que ver con un mal proceso de autenticación en la sesión ya sea por falla al identificar el usuario, falla al mantener la identidad del usuario al ser requrida o debilidad en la gestión de la sesión.
M5	Criptografía insuficiente.	Esta clasificación tiene que ver con la aplicación de criptografía de un modo insuficiente.
M6	Autorización insegura	Esta categoría captura cualquier tipo de falla en la autorización
M7	Calidad en el Código cliente	Esta categoría tiene que ver con los problemas de implementación a nivel código en el cliente móvil.
M8	Modificaciónn de Código	ESta categoría cubre lo que viene a ser actualizaciones, parches y modificaciones locales de Código y modificaciones dinámicas de memoria.
M9	Ingeniería en reversa	Esta categoría incluye análisis del código binario para determinar su código origen, librerias, algoritmos y otros activos.
M10	Funcionalidades extrañas	Funciones escondidas de desarrollo como backdoors, controles de seguridad que no fueron inicialmente programados para ser liberados en un ambiente de producción.

Es importante notar que la prueba es sobre funcionalidad a caja negra, por lo que no se esta evaluando a detalle el código ni librearías, por lo que parte de los 10 riesgos para programación de móvil, posiblemente no apliquen.

5 Administración de Riesgos

En esta sección se describen los riesgos que se pueden ver y que se revisaron con el equipo de la CEENL para visualizar la probabilidad de ocurrencia y el impacto que potencialmente puede tener. En esta sección solo se determina la probabilidad de ocurrencia y el impacto que pueda tener. En base a esto en el documento de recomendaciones finales se establecerá el riesgo existente para cada uno de los eventos que potencialmente se pueden dar.

5.1 Administración Riesgos

Las distintas clasificaciones de amenazas y vulnerabilidades para establecer las probabilidades e impactos en los riesgos para la parte tecnológica de las casillas se describen

Análisis de Riesgo – Aplicación Móvil					
Amenaza	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Justificación**
7.2 Acceso correcto a la aplicación	Entrada de un usuario no autorizado	Clave de acceso publica	Muy Bajo	Alto	• Probabilidad Muy Baja – Los equipos se entregan preconfigurados con usuario y clave y el usuario no tiene acceso a estos datos • Impacto alto – De darse, se puede usar para dar datos falsos
7.3 Acceso incorrecto a la aplicación	Usuario puede equivocarse de acceso	Error de entrada de usuario	Muy Bajo	Alto	• Probabiidad Muy Baja – El usuario no introducirá usuario ni clave ya que vienen preconfigurados los dispositivos • Impacto Alto
7.4 Acceso a la aplicación desde dispositivo no vinculado	Tratar de vincular otro teléfono o dispositivo móvil	Traer otro dispositivo no autorizado para usarlo para escanearlo	Muy Bajo	Alto	• Probabilidad Muy Baja – Usuario no tendría cuenta aparte que no se puede usar dispositivos en esas áreas • Impacto Alto – Se podría guardar archivos basura en el repositorio
7.5 Registro de usuarios excedidos	Querer agregarse como usuario adicional a los dispositivos autorizados	Permiso de agregar teléfonos al grupo autorizado	Muy Bajo	Alto	• Probabilidad Muy Baja – No se permiten dispositivos móviles y no hay internet • Impacto Alto – Se podría guardar archivos basura en el repositorio
7.6 Registro de Actas Correctas	Subir actas con errores	Subir archivos sin control	Muy Bajo	Alto	• Probabilidad Muy Baja – Los archivos se suben con permiso desde estaciones designadas • Impacto Alto – Se puede subir basura
7.7 Carga de Archivos	Cargar achivos falsos	Permitir subir archivos sin control	Muy Bajo	Alto	• Probabilidad Muy Baja – Los archivos solo son subidos desde estaciones autorizadas y están con codigos QR • Impacto Alto – Se podría guardar archivos basura en el repositorio
7.8 Verificar que los archivos estén en el repositorio	Archivos no lleguen o no sean grabados en repositorio	Corte o error en repositorio	Muy Bajo	Crítico	• Probabilidad Muy Baja – Los archivos son subidos en automático y si hay corte, estos se reintentan subirlos • Impacto Crítico – Que no se graben actas en los repositorios
7.9 Validación de conexión segura entre el APP y el sitio central	Poder ver contenido de la transmisión entre el teléfono y el repositorio	Poder escanear la red para ver la transmisión	Muy Bajo	Alto	• Probabilidad Muy Baja – Se requiere entrar con laptop para hacer esto y no s posible conectare con equipo a la red • Impacto Alto – Se puede ver los resultados antes de publicarse
7.10 Validación de passwords	Cambiar passwords	Permisos para cambio de claves en el sistema	Muy Bajo	Medio	• Probabilida Muy Baja – Se requiere entrar a la plataforma de getión para hacer el cambio. • Impacto Medio – Se tendría que falsificar códigos escaneables y tener actas ya preparadas para poder realizar este tipo de ataque

Análisis de Riesgo – Escaner					
Amenaza	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Justificación**
8.1 Condiciones iniciales de pruebas Multifuncional	Iniciar con campos con datos en la base de datos	No vaciar la BD al inicio del proceso	**Muy Baja**	**Crítico**	• Probabilidad Muy Baja – Se requiere por protocolo reiniciar la BD y borrar todos los contenidos para lo que se tiene que ahcer de forma púbica • Impacto crítico – Los resultados pueden alterarse de forma que se pueda dar un resultado falso de las elecciones
8.2 Enlace del Multifuncional hacia sitio repositorio (Dropbox o AZURE)	Bloquear e dispotivio de conexión hacia AZURE	Enlaces saturados o bloqueados por ataques o introducción de tráfico	**Muy Baja**	**Crítico**	• Probailidad Muy Baja – Se requiere meter equipo y conectarlo a los CCV's o CATDS, lo cual no es posible. • Impacto crítico – Podría introducir datos falsos y contabilizarlos erroneamente
8.3 Integridad de acta hacia AZURE	Subir actas falsas de otro sitio u otra computadora	Acceso a puertos de red	**Baja**	**Crítica**	• Probabilidad Baja – Las acts deben estar preparadas con códigos de identificación y llenas para poder darse de alta • Impacto crítico -
8.4 Escanear actas	Poder subir otro archivo	Aceptar archivos de estaciones no autorizadas	**Muy Baja**	**Crítica**	• Probabilidad Muy Baja – el escáner hace el nombre poniendo firma SHA256 y la fecha la cual es almacenado. • Impacto Crítico – Subir documentos falsos con valores artificiales
8.5.1 Envío del acta desde el Multifuncional	Borrar actas en el repositorio de DROPBOX o AZURE	Accesos manuales al repositorio	**Muy Baja**	**Alto**	• Probabilidad Muy Baja – El acceso esta controlado y requiere privilegios de administrador para borrar documentos • Impacto Alto – Aunque pueda darse, el borrado, el acta se vuelve a capturar o reenviarse desde el origen al validarse
8.5.2 Interrupción en el envío del acta desde el Multifuncional	Corte o desconexi´n de cable de redo o eléctrico en el multifuncional	Cables expuestos y con acceso fácil	**Bajo**	**Alto**	• Probabilidad Bajo – ES posible que alguien pueda desconectarlo, pero por protocolo se vuelve a conectar y reenviar documentos al repositorio • Impacto Alto – Tiene impato en cuanto a tiempo de retraso en la recpatura o volver a escánear el acta
8.5.3 Recepción del acta	Impedir la recepción mediante bloqueo	Apagar estación o	**Bajo**	**Alto**	• Probablildad Bajo – No se ve probable, que se impida el bloqueo desde adentro del cuarto de captura, ya que no se puede meter ni conetar equipo externo • Impacto Alto – Se pueden dar datos falsos y/o retrasar la subida de actas al sistema.

Análisis de Riesgo – Escaner					
Amenaza	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Justificación**
9.1 Condiciones Iniciales de Captura	Tener condiciones alteradas para el inicio de captura	No tener procedimiento de inicialización de sistema y base de datos	**Bajo**	**Crítico**	• Probabilidad Baja – Puede por omisión no ejecutarse un protocolo de inicialización de los sistemas • Impácto crítico – Captura iniciaría con valores capturados en la base de datos
9.2 Captura de valores requeridos del Acta en la Base de datos del SIPRE	No tener los campos requeidos para captura	Falta de información en la captura que de datos erróneos en el total	**Muy Bajo**	**Crítico**	• Probabilidad Muy Baja – Las revisiones e iteraciones sobre el sistema se dieron e varias ocasiones por lo que es poco probable que no hayan los campos para los datos requeridos • Impácto crítico – No se cumpliría con los requerimietnos de captura del INE
9.3 Datos a Calcular	Resultados de los cálculos sean erróneos o falsos	No validar capturas ni campos y/o manejar los cálculos con números trunados o fuera de estándar	**Muy Bajo**	**Crítico**	• Probabilidad Muy Baja – Las revisiones e iteraciones sobre el sistema se dieron e varias ocasiones por lo que es poco probable que no hayan los campos para los datos requeridos • Impácto Crítico - arrojar datos erróneos en los cálculos finales sobre los valores requeridos del INE
9.4 Datos a Publicar	No publicar los datos requerdos por el INE en los formatos requeridos	Plataforma no publique los datos al portal público	**Muy Bajo**	**Crítico**	• Probabilidad Muy Baja – Las revisiones e iteraciones sobre el sistema se dieron e varias ocasiones por lo que es poco probable que no hayan los campos para los datos requeridos • Impacto Crítico – No se publicarían los datos requeridos por el INE en el formato requerido y/o con los valores estándar dictados en los lineamientos para las OPL's
9.5 Corrección de actas duplicadsa	Dar entrada a capturas erróneas o con interpretaciones falsas que originen resultaos alterados en el proceso de las elecciones	No validar actas que se estén capturando	**Muy Bajo**	**Crítico**	• Probabilidad Muy Bajo – Dado que las actas se llenan a mano, el sistema requiere por definición la doble captura de una acta para validar la interpretación de números escritos en las actas y que estos sean corroborados. • Impacto Crítico – De no validarse entonces se pueden dar entrada a números mal interpretados o falsos teniendo impacto en los resultados de las elecciones

Debido a las contramedidas instaladas en la plataforma AZURE, se puede llevar el riesgo a un nivel bajo dado las configuraciones que se tienen en la nube de Microsoft para evitar este tipo de ataques.

6 Observaciones Finales y Resúmen Ejecutivo

Las observaciones y recomendacions se harán sobre el anexo correspondiente de pruebas que se este realizando y bajo los criterios que se detallan por cada una de las. En esta sección se presenta un resúmen, en función de los resultados y revisión de hallazgos, da los resultados de esta y su cumplimiento, asi como hallazgos por clasificación que se de.

Los criterios que se usaron para la ejecución y presentar el resúmen se describen en la siguiente tabla los cuales son usados en todas las tablas subsecuentes.

Definición	Descripción	Acciones
Aceptado	La prueba cumplió satisfactoriamente con los criterios de aceptación	Prueba es aceptada y se da por cerrado el inciso de esta prueba. De ser necesario ejecutar el plan de nuevo en otra iteración, esta prueba no se volverá a ejecutar.
Rechazado	La prueba no cumplió con los criterios de aceptación	Prueba no es aceptada, se documenta el resultado y recomendaciones. Esta prueba se volverá a ejecutar en la siguiente iteración para revisar la implementación de las recomendaciones dadas en el resultado de las pruebas.
Aceptado con Observaciones	La cumplió con una parte de los criterios o cumplió totalmente con observaciones.	Prueba es aceptada, pero con recomendaciones. Esto significa que las recomendaciones son solo eso, no serían obligatoria su implementación y solo queda como sugerencia o recomendación.
No Ejecutada	Prueba no fue ejecutada en el ciclo por cuestiones de tiempo o por decisión mutua	La prueba se volverá a ejecutar en otro ensayo o bien si no se ejecuta, se agregará la justificación del por que de esto.
Sustituida	Prueba inicialmente diseñada pero que se intercambio por otra acción debido a cierta condición de la prueba inicial	La prueba que inicialmente se planeo no fue ejecutada dado que alguna condición de esta se debía modificar, cambiar o modificar al momento de su ejecución

6.1 Resúmen Ejecutivo Aplicación Móvil

Prueba	Criterio Para Aceptación	Resultado 10/Junio	Resultado 17/Junio	Resultado 24/Junio	Comentarios/Acciones
7.1 Condiciones iniciales de pruebas APP Móvil					
7.2 Acceso correcto a la aplicación	Entrar exitosamente a la aplicación con usuario/clave asignado.	Aceptado	Aceptado	Aceptado	El usuario no hará esta función ya que se le entrega ya configurado el teléfono y la aplicación para disminuir los errores de login.
7.3 Acceso incorrecto a la aplicación	Negar acceso a la aplicación DropBox.	Aceptado	Aceptado	Aceptado	El usuario no hará esta función ya que se le entrega ya configurado el teléfono y la aplicación para disminuir los errores de login.
7.4 Acceso a la aplicación desde dispositivo no vinculado	Negar acceso a la aplicación DropBox.	No Ejecutada	Aceptado	Aceptado	El usuario no puede acceder ya que todos los dispositivos están vinculados y firmados en Dropbox. No permite el acceso.
7.5 Registro de usuarios excedidos	Negar acceso a la aplicación DropBox.	Aceptado	Aceptado	Aceptado	El tratar de entrar en la aplicación, marca que se ha excedido el número de teléfonos asociados..
7.6 Registro de Actas Correctas	Tomar foto del acta para que esta se digitalize en formato JPG o PNG y se pueda ubicar para subir al directorio de Dropbox.	Aceptado	Aceptado	Aceptado	Al tomar la foto, la app de DropBox la sube vía SSL en formato JPG.
7.7 Carga de Archivos	Valido la existencia del archivos en formato JPG en el teléfono y se confirma que después de enviado el archivo desaparece del teléfono.	Aceptado	Aceptado	Aceptado	Se pudieron ver los archivos almacenanados en formato JPG y se borra del teléfono al ser enviados
7.8 Verificar que los archivos estén en el repositorio	Verificar que el acta este visible en el repositorio de Dropbox	Aceptado	Aceptado	Aceptado	Se visualizan las actas en Dropbox con el nombre generado en el origen con el hash del escáner.
7.9 Validación de conexión segura entre el APP y el sitio central	Validar que la conexión se hace en protocolo seguro SSL para transmisión de actas.	Aceptado	Aceptado	Aceptado	En el caso de DropBox se suben las imágenes en SSL. En el caso de AZURE, se suben en red privada sin acceso por afuera de esta red (esta configurada como una LAN independiente).
7.10 Validación de passwords	Validación de que los Passwords deben ser 8 caracteres, con mezcla de letras (caracteres minúsculas y numéricos).	Aceptado	Aceptado	Aceptado	El usuario no ve la configuración ya que se le entrega listo para usarse y al entrar no tiene que dar usuario ni clave. Aparte que el teléfono esta asociado.

6.2 Resúmen Ejecutivo En Escaner CATD

Prueba	Criterio Para Aceptación	Resultado 10/Junio	Resultado 17/Junio	Resultado 24/Junio	Comentarios/Acciones
8.1 Condiciones iniciales de pruebas Multifuncional	Documentar las condiciones iniciales.	No Ejecutada	Aceptado	Aceptado	Se encontró el siguiente ambiente: no hay WiFi disponible en los CATD's, los escanners y PC's se conectan por RJ45 solamente.
8.2 Enlace del Multifuncional hacia sitio repositorio (Dropbox o AZURE)	Tener un 90% de efectividad en pruebas de alcance con ICMP.	Aceptado	Aceptado	Aceptado	Se obtuvo un 100% de éxito en conectividad del CCV a la nube Azure la cual esta conectada vía una LAN local.
8.3 Integridad de acta hacia AZURE	Asegurar que la firma digital del archivo en estación coincida con la del archivo que se baje de AZURE para ser capturado.	Aceptado	Aceptado	Aceptado	Se encontró que el nombre del archivo es la fecha/hora/firma digital generada en SHA256 por el escáner. Archivo se bajo y se genero su llave la cual coincide.
8.4 Escanear actas	Tener el archivo del acta en formato gráfico para ser procesado y con un nombre único que lo identifique.	Aceptado	Aceptado	Aceptado	Se encontró que el formato en que se graba es JPG y el nombre se estructura: Año|mes|dia|hh|mm|<forma_digial_sha256>
8.5 Comunicación para envío desde el CATD					
8.5.1 Envío del acta desde el Multifuncional	Confirmar que el archivo de acta resida, después del envío en la BD del centro de procesamiento AZURE.	Aceptado	Aceptado	Aceptado	Se valido la existencia del acta en los repositorios de AZURE
8.5.2 Interrupción en el envío del acta desde el Multifuncional	Asegurar que el acta no queda en el centro de procesamiento y se conserva en el multifuncional para su envío posterior.	Aceptado	Aceptado	Aceptado	Se encontró que al interrumpirse su envío queda grabada para volver a intentar su envío en caso de corte.
8.5.3 Recepción del acta	Validar la recepción posterior a la caída de enlace del archivo encolado (no enviado) en el multifuncional.	Aceptado	Aceptado	Aceptado	Se confirmo que el archivo queda en fila para ser enviado posteriormente. Este se recibe correctamente volviendo a intentar su envío.

6.3 Resúmen Ejecutivo Datos de Captura para Cálculo y Publicación

Prueba	Criterio Para Aceptación	Resultado 10/Junio	Resultado 17/Junio	Resultado 24/Junio	Comentarios/Acciones
9 Datos de captura para Calcúlo y Publicación					
9.1 Condiciones Iniciales de Captura	Asegurar que la base de datos inicia la operación en limpió.	Aceptado	Aceptado	Aceptado	Se confirmo que la base de datos se limpió al inicio de la prueba y se mostraron los campos con el valor "null" el cual indica que no tienen valor.
9.2 Captura de valores requeridos del Acta en la Base de datos del SIPRE	Asegurar que los valores mínimos requeridos que exige el INE deben estar para su captura en la interfase del SIPRE.	Aceptado	Aceptado	Aceptado	Se confirmo que los valores requeridos por el INE si se están capturando en la pantalla de la aplicación de captura en el CCV. La imagen se tuvo que tomar con celular ya que no permite la estación de captura tomar una pantalla por el sistema operativo en el que reside.
9.3 Datos a Calcular	Confirmar que los datos mínimos a calcular en la interfase del SIPRE deben reflejarse.	Aceptado	Aceptado	Aceptado	Se pudo confirmar que los datos se calculan con 4 decimales truncando después de la diezmilésima. Para propósitos gráficos y dashboard de control (interno), los indicadores solamente se considera 1 decimal, pero el proceso se da calculando con 4 y se presenta al público con 4 decimales.
9.4 Datos a Publicar	Asegurarse que se presentan los datos a publicar que se mencionan en el documento de plan de pruebas como entregables mínimo.	Aceptado	Aceptado	Aceptado	Se confirmo que los archivos se publican y se generan en formato CSV para que puedan ser bajados desde el portal y se actualizan.
9.5 Corrección de actas duplicadsa	Documentar proceso mediante le cual se validan las actas duplicadas.	Aceptado	Aceptado	Aceptado	Se presentó un proceso Documentado (se encuentra en la Sección Evidencias) sobre la existencia de una mesa especializada para revisión de actas.

7 Conclusiones

Las conclusiones finales de la prueba estarán documentadas en el informe final de las pruebas de caja negra solicitada en el documento de requisitos mínimos del INE.

8 Anexo I – Tabla de cumplimiento de pruebas

Los números de las pruebas están referenciados al plan de pruebas originalmente pactado. Las condiciones y ambiente general de pruebas se puede documentar en este mismo anexo.

Pruebas Funcionales a Caja Negra CEENL 2018			
Fecha: 11/Junio/2018	**Iteración: Primer Ejercicio**		
Prueba	**Criterio Aceptación**	**Resultado**	**Comentarios**
7.1 Condiciones iniciales de pruebas APP Móvil			
7.2 Acceso correcto a la aplicación	Entrar exitosamente a la aplicación con usuario/clave asignado	Aceptado	El usuario no hará esta función ya que se le entrega ya configurado el teléfono y la aplicación para disminuir los errores de login
7.3 Acceso incorrecto a la aplicación	Negar acceso a la aplicación DropBox	Aceptado	El usuario no hará esta función ya que se le entrega ya configurado el teléfono y la aplicación para disminuir los errores de login
7.4 Acceso a la aplicación desde dispositivo no vinculado	Negar acceso a la aplicación DropBox		No es posible que acceder ya que todos los dispositivos están vinculados y firmados en Dropbox. No permite el acceso.
7.5 Registro de usuarios excedidos	Negar acceso a la aplicación DropBox	Aceptado	El tratar de entrar en la aplicación, marca que se ha excedido el número de teléfonos asociados.
7.6 Registro de Actas Correctas	Tomar foto del acta para que esta se digitalize en formato JPG o PNG y se pueda ubicar para subir al directorio de Dropbox	Aceptado	La app de DropBox toma la foto y la sube vía SSL en formatp JPG
7.7 Carga de Archivos	Visualizar archivos JPG en teléfono y después de enviarlos el archivo desaparece del teléfono	Aceptado	Los archivos se almacenan en formato JPG
7.8 Verificar que los archivos estén en el repositorio	Acta en directorio de Dropbox visible	Aceptado	Actas visibles en Dropbox con el nombre generado en el origen con el hash del escáner
7.9 Validación de conexión segura entre el APP y el sitio central	Conexión en protocolo seguro SSL para transmisión de actas	Aceptado	En el caso de DropBox se suben las imágenes en SSL. En el caso de AZURE, se suben en red privada sin acceso por afuera de esta red (esta configuada como una LAN independiente)
7.10 Validación de passwords	Passwords deben ser 8 caracteres, con mezcla de letras (caracteres minúsculas y numéricos)	Aceptado	El usuario no ve la configuración ya que se le entrega listo para usarse y al entrar no tiene que dar usuario ni clave. Aparte que el teléfono esta asociado

Hallazgos y Recomendaciones	
Clasificación	**Descripción Hallazgo o Recomendación**
M1 – Imroper Platform Usage	
M2 – Insecure Data Storage	
M3 – Insecure Communication	
M4 – Insecure Authentication	
M5 – Insufficient Cryptography	
M6 – Insecure Authorization	
M7 – Client Code Quality	
M8 – Code Tampering	
M9 – Reverse Engineering	
M10 – Extraneous Functionality	

Pruebas Funcionales a Caja Negra CEENL 2018			
Fecha: 11/Junio/2018	**Iteración: Primer Ejercicio**		
Prueba	**Criterio Aceptación**	**Resultado**	**Comentarios**
8 Casos de prueba CATD con Multifuncional			
8.1 Condiciones iniciales de pruebas Multifuncional	Documentar las condiciones iniciales		No hay WiFi en los CATD's, los escanners y PC's se conectan por RJ45
8.2 Enlace del Multifuncional hacia sitio repositorio (Dropbox o AZURE)	Pruebas de alcance con un 90% de efectividad (ICMP)	Aceptado	Azure esta conectado en LAN local y conectividad al 100% y azure esta conectado al 100% desde el CCV
8.3 Validación de integridad de acta hacia AZURE	Firma digital del archivo en estación debe coinicidir con la del archivo que se baje de AZURE para ser capturado.	Aceptado	Nombre del archivo es lafecha/hora/firma digital generada en SHA256 por el escanner. Archivo se bajo y se genero su llave la cual coincide.
8.4 Escanear actas	Archivo en formato gráfico para ser procesado y con un nombre único que lo identifique.	Aceptado	El formato en que se graba es JPG y el nombre se estructura: Año|mes|dia|hh|mm|<forma_digial_sha256>
8.5 Comunicación para envío desde el CATD			
8.5.1 Envío del acta desde el Multifuncional	Archivo de acta deberá residir, después del envío en la BD del centro de procesamiento	Aceptado	Se valido la existencia del acta en los repositorios de AZURE
8.5.2 Interrupción en el envío del acta desde el Multifuncional	Acta no queda en el centro de procesamiento y se conserva en el multifuncional para su envío posterior	Aceptado	Al interrumpirse su envío queda grabada para volver a intentar su envío en caso de corte.
8.5.3 Validación en el repositorio de recepción del acta	Recepción posterior a caída de enlace del archivo encolado (no enviado) en el multifuncional	Aceptado	El archivo queda en fila para ser enviado posteriormente. Este se recibe correctamente volviendo a intentar su envío.

Hallazgos y Recomendaciones	
Clasificación	**Descripción Hallazgo o Recomendación**
M1 – Improper Platform Usage	
M2 – Insecure Data Storage	
M3 – Insecure Communication	
M4 – Insecure Authentication	
M5 – Insufficient Cryptography	
M6 – Insecure Authorization	
M7 – Client Code Quality	
M8 – Code Tampering	
M9 – Reverse Engineering	
M10 – Extraneous Functionality	

Pruebas Funcionales a Caja Negra CEENL 2018			
Fecha: 11/Junio/2018	**Iteración: Primer Ejercicio**		
Prueba	**Criterio Aceptación**	**Resultado**	**Comentarios**
9 Datos de captura para Calcúlo y Publicación			
9.1 Condiciones Iniciales de Captura	Base de datos en limpió	Aceptado	La base de datos se limpió al inicio de la prueba y se mostraron los campos con el valor "null" el cual indica que no tienen valor.
9.2 Captura de valores requeridos del Acta en la Base de datos del SIPRE	Valores mínimos requeridos deben estar para su captura en la interfase del SIPRE	Aceptado	Los valores requeridos por el INE se están capturando en la pantalla de la aplicación de captura en el CCV. La imagen se tuvo que tomar con celular ya que no permite la estación de captura tomar una pantalla por el sisema operativo en el que reside.
9.3 Datos a Calcular	Los datos mínimos a calcular en la interfase del SIPRE deben reflejarse.	Aceptado	Los datos se calculan con 4 decimales truncando después de la diezmilésima. Para propósitos gráficos y dashboard de control (interno), los indicadores solamente se considera 1 decimal, pero el proceso se da calculando con 4 y se presenta al público con 4 decimales
9.4 Datos a Publicar	Deben presentar los datos a publicar que se mencionan en el documento de plan de pruebas como entregables mínimo.	Aceptado	Los archivos se generan en formato CSV para que puedan ser bajados desde el portal y se actualizan
9.5 Corrección de actas duplicadsa	Documentar proceso mediante le cual se validan las actas duplicadas	Aceptado	Proceso Documentado (Sección Evidencias