TECNOLÓGICO DE MONTERREY®

Comisión Estatal Electoral Nuevo León

Resumen Ejecutivo Auditoría PREP – Elecciones 2018

Resultados, hallazgos y recomendaciones de la auditoría al sistema del Programa Preliminar de Resultados Electorales de la Comisión Estatal de Nuevo León

25 Junio 2018

Tecnológico de Monterrey

COMISIÓN ESTATAL ELECTORAL NUEVO LEÓN | CEE

Índice

Pruebas Caja Negra: En 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

Pruebas Caja Negra: En Escáner 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.

Tecnológico de Monterrey

COMISIÓN ESTATAL ELECTORAL NUEVO LEÓN | CEE

Pruebas Caja Negra: En los 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.

Pruebas de Ataques de Negación de Servicio (DOS)

Prueba	Criterio Para Aceptación	Resultado 10/Junio	Resultado 17/Junio	Resultado 24/Junio	Comentarios/Acciones
7.1 Ataque volumétrico por TCP – SYN FLOOD	Verificar que no haya afectación al tráfico legítimo pudiendo detener el tráfico de ataque que se origina.	**Sustituida**	**Sustituida**	**Sustituida**	La prueba se considera **ACEPTADA** debido a la prohibición explicita de Microsoft de hacer ataques de negación de servicio en cualquier tipo. Los controles existentes en la nube de AZURE disminuyen el riesgo de este tipo de ataques
7.2 Ataque volumétrico por UDP - DNS AMPLIFICATION	Verificar que no haya afectación al tráfico legítimo pudiendo detener el tráfico de ataque que se origina.	**Sustituida**	**Sustituida**	**Sustituida**	La prueba se considera **ACEPTADA** debido a la prohibición explicita de Microsoft de hacer ataques de negación de servicio en cualquier tipo. Los controles existentes en la nube de AZURE disminuyen el riesgo de este tipo de ataques
7.3 Ataque volumétrico por ICMP – ICMP FLOOD	Verificar que no haya afectación al tráfico legítimo pudiendo detener el tráfico de ataque que se origina.	**Sustituida**	**Sustituida**	**Sustituida**	La prueba se considera **ACEPTADA** debido a la prohibición explicita de Microsoft de hacer ataques de negación de servicio en cualquier tipo. Los controles existentes en la nube de AZURE disminuyen el riesgo de este tipo de ataques
7.4 Ataque en a capa de aplicación – SLOWRIS ATTACK	Asegurar que las sesiones arrancadas simulando baja velocidad, deberán cerrarse por falta de respuesta en tiempos adecuados para no sobresaturar el servidor de WEB.	**Sustituida**	**Sustituida**	**Sustituida**	La prueba se considera **ACEPTADA** debido a la prohibición explicita de Microsoft de hacer ataques de negación de servicio en cualquier tipo. Los controles existentes en la nube de AZURE disminuyen el riesgo de este tipo de ataques

- Estas pruebas fueron sustituidas por prohibición explicita del proveedor de la nube, por lo que se opto por revisar las condiciones de protección para la CEENL las cuales son satisfactorias
- La nube de AZURE de Microsoft donde esta hosteada la aplicación de la CEENL, se describe explícitamente los procedimientos para hacer escaneos y/o análisis de seguridad de las aplicaciones. También **prohíbe explícitamente los ataques de negación de servicio (DOS)** en cualquier variante por afectar recursos compartidos de a su infraestructura.
  - https://azure.microsoft.com/en-us/services/ddos-protection/
  - https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview
- En base a esta situación se acordó **mutuamente ente el ente auditor y la CEENL no hacer este tipo de ataques** por prohibición explicita del proveedor de nube privada

Análisis de Vulnerabilidades: De la Arquitectura de Red

Prueba	Criterio Para Aceptación	Resultado 10/Junio	Resultado 17/Junio	Resultado 24/Junio	Comentarios/Acciones
4.1.1 Diseño jerárquico de la red	Revisar el diagrama de diseño de red que muestre estructura y modelo de red.	**Aceptado**	**Aceptado**	**Aceptado**	Se confirma una arquitectura jerárquica de red (Acceso, Distribución, core) de acuerdo a mejores prácticas de la industria.
4.1.2 Redundancia en conexión	Revisar la existencia de conexión alterna de salida del centro captura.	**Aceptado**	**Aceptado**	**Aceptado**	Se confirmo la existencia de dos y hasta tres accesos a Internet dependiendo del tipo de centro. (Ver evidencias para descripción).
4.1.3 Direccionamiento adecuado y eficiente	Confirmar direccionamiento segmentado por funciones, alcances y responsabilidades.	**Aceptado**	**Aceptado**	**Aceptado**	Se encontró que el direccionamiento segmentado aísla áreas de trabajo previniendo comportamientos migren de un área a otra.
4.1.4 Acceso controlado a redes en sitios de captura	Revisar el acceso a los closets de telecom que deben estar controlados y asegurados.	**Aceptado**	**Aceptado**	**Aceptado**	Se confirmo que los cuartos o closets de equipos de red están bajo llave y con acceso controlado.
4.2 Versión del los sistemas operativos sin vulnerabilidades críticas	Validar que las versiones de los switches y routers no presenten vulnerabilidades críticas ni altas.	**Aceptado**	**Aceptado**	**Aceptado**	Se confirmo que las versiones de switches y ruteadores están sin avisos de vulnerabilidades críticos o Altos para los que son los servicios que se están usando .
4.3 Soporte manual a infraestructura	Verificar que se cuente con contratos de soporte, así como soporte en sitio y vía telefónica para soporte.	**Aceptado**	**Aceptado**	**Aceptado**	Se revisaron los manuales de soporte para personal, así como el centro de ayuda telefónico .

Análisis de Vulnerabilidades: De las Estaciones de captura

Prueba	Criterio Para Aceptación	Resultado 10/Junio	Resultado 17/Junio	Resultado 24/Junio	Comentarios/Acciones
4.4.1 Acceso con privilegios mínimos	Confirmar que los usuarios tienen acceso solo a lo que requiere.	**No Ejecutada**	**No Ejecutada**	**Aceptado**	Se confirmo que el sistema operativo es de kiosko y no permite acceso a otra función fuera del portal de captura.
4.4.2 Servicios habilitados en estaciones de captura	Verificar la lista de servicios abiertos en estaciones captura.	**No Ejecutada**	**No Ejecutada**	**Aceptado**	Se encontró que las estaciones de captura tienen filtrado los puertos por lo que no servicios disponibles en estas.
4.4.3 Vulnerabilidades en las estaciones de captura	Verificar la lista de vulnerabilidades de nivel crítico y alto en las estaciones de captura.	**No Ejecutada**	**No Ejecutada**	**Aceptado**	No se encontraron puertos abiertos ni vulnerabilidades en las estaciones de trabajo de nivel crítico o alto.
4.4.4 Acceso de las estaciones de captura	Asegurarse que las estaciones de captura solo con la aplicación para captura de elecciones.	**No Ejecutada**	**No Ejecutada**	**Aceptado**	Se encontró que no hay otra aplicación cargada y no permite cargar aplicaciones al usuario operador.
4.4.5 Acceso a la infraestructura de comunicaciones	Confirmar la existencia de bloqueo de puertos TELNET, WEB, si no es así, debe haber lista de acceso. Acceso solo vía SSH.	**Aceptado**	**Aceptado**	**Aceptado**	Se escaneo desde el Internet a los routers dedicados de Internet y los puertos indicados están bloqueados.
4.4.6 Puertos dedicados	Asegurar tener habilitado Port Blocking.	**Aceptado**	**Aceptado**	**Aceptado**	Se confirma que los puertos de LAN se bloquean al conectar otra estación de trabajo y tienen horarios de activación.

Análisis de Vulnerabilidades: De los Controles de Seguridad de Operación

Prueba	Criterio Para Aceptación	Resultado 10/Junio	Resultado 17/Junio	Resultado 24/Junio	Comentarios/Acciones
4.5.1 Seguridad en Operaciones: Administración de la Capacidad	Confirmar la existencia de control de aplicaciones y/o enlace desborde para consumo ancho banda.	**No Ejecutada**	**Aceptado**	**Aceptado**	Se encontró configuraciones de desborde de tráfico en caso de caída, configurado en ruta alterna. Máximo uso de ancho de banda en CCV's no excede el 50% de las distintas capacidades.
4.5.2 Seguridad en Operaciones: Protección contra malware	Confirmar la existencia de controles para evitar la introducción de malware en la red.	**No Ejecutada**	**Aceptado**	**Aceptado**	Se encontró que el UTM Meraki MX100, posee licenciamiento de ANTIMALWARE protegiendo la infraestructura.
4.5.3 Seguridad en Operaciones: Bitácora de eventos	Asegurar la existencia de bitácoras de eventos del ambiente de red LAN y WAN.	**No Ejecutada**	**No ejecutada**	**Aceptado**	Se encontró la bitácora de eventos de los equipos MERAKI que monitorean el tráfico de la red LAN y WAN.
4.5.4 Seguridad en Operaciones: Restricciones para instalación de SW	Asegurar la existencia de controles para evitar instalación de SW no permitido en estaciones de trabajo.	**No Ejecutada**	**No ejecutada**	**Aceptado**	Se confirmo mediante escaneo desde el Internet a los routers dedicados de Internet que los puertos están bloqueados.

Análisis de Vulnerabilidades: De los Controles de Comunicaciones Seguras

Prueba	Criterio Para Aceptación	Resultado 10/Junio	Resultado 17/Junio	Resultado 24/Junio	Comentarios/Acciones
4.6.1 Comunicaciones Seguras: Controles de la Red	Asegurar que el área de captura y almacenamiento deberá estar segregado de otras áreas de TI.	**No Ejecutada**	**Aceptado**	**Aceptado**	Se confirmo que el esquema de segmentación de red permite separar las áreas operativas de las de desarrollo y operación.
4.6.2 Comunicaciones Seguras: Seguridad de los servicios de red	Confirmar que hay un control de protocolos no permitidos. Tener una lista de servicios/protocolos permitidos.	**No Ejecutada**	**Aceptado**	**Aceptado**	Se encontró que los servicios permitidos solamente son los que se ofrecen para la captura en servidores de AZURE.
4.6.3 Comunicaciones Seguras: Segregación en redes	Confirma esquema de direccionamiento con evidencia de la segregación.	**No Ejecutada**	**Aceptado**	**Aceptado**	Se confirma que las redes están segregadas en base a funciones de personal estructurado redes y subredes sobre esta base.
4.6.4 Comunicaciones Seguras: Transferencia de información	Asegurarse de tener canales seguros de transmisión de estaciones de captura hasta sistema .	**No Ejecutada**	**Aceptado**	**Aceptado**	Se revisó y encontró que se cuenta con túneles de IPSEC los cuales cifran la conexión de forma dedicada y dinámica si se requiere usar enlace alterno de la CEENL.

Análisis de Vulnerabilidades: Del Escaneo y Revisión de Configuraciones

Prueba	Criterio Para Aceptación	Resultado 10/Junio	Resultado 17/Junio	Resultado 24/Junio	Comentarios/Acciones
4.7 Robustez de la infraestructura de computo	Validar que mediante el escaneo no haya ninguna vulnerabilidad nivel alta o crítica.	**No Ejecutada**	**No Ejecutada**	**Aceptada**	Se confirmó que en el escaneo no se mostro nada y los puertos están cerrados en las estaciones de captura.
4.8 Robustez de la infraestructura de comunicaciones	Validar que mediante el escaneo no haya ninguna vulnerabilidad nivel alta o crítica.	**No Ejecutada**	**No Ejecutada**	**Aceptada**	Se confirmó mediante el escaneo con NMAP, OCS, CAT y CISCO-TORCH que los puertos se encuentran filtrados desde Internet.
4.9 Revisión de configuración de infraestructura de comunicaciones					
4.9.1 Revisión de configuración Switches LAN	Revisar que la configuración de la infraestructura de los switches cumpla los requerimientos de mejores prácticas.	**No Ejecutada**	**No Ejecutada**	**Aceptada**	Se confirmó que la configuración de los swtiches que se mostro sigue mejores practicas y recomendaciones técnicas del proveedor. No hay recomendaciones adicionales
4.9.2 Revisión de configuración Router	Revisar que la configuración de la infraestructura de router siga las recomendaciones y las mejores prácticas dadas por el fabricante.	**No Ejecutada**	**No Ejecutada**	**Aceptada**	Se reviso la configuración y versiones. Las vulnerabilidades encontradas afectan solamente cuando se hace uso de servicios y HW que no esta instalado y no se esta usando en este proyecto por lo que **no hay afectaciones para los propósitos de los servicios en las elecciones del 2018.** Existe una revisión adicional del proveedor PLANNET de quien se adquirió estos equipos y fue quien los configuro e instaló. No hay recomendaciones adicionales
4.9.3 Revisión de configuración Firewall	Revisar que la configuración de la infraestructura de Firewall cumpliendo las mejores prácticas y recomendaciones por parte del fabricante.	**No Ejecutada**	**No Ejecutada**	**Aceptada**	Se encontró que la configuración mostrada en detalle con los filtros y limitaciones de contenido suficientes para disminuir riesgos de ataques. La configuración se da e la nube y se propaga a los dispositivos implementados que se asocian con los números de serie. No hay recomendaciones adicionales

Glosario

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