TECNOLÓGICO DE MONTERREY®

Análisis de Vulnerabilidades al Sistema Informático del SIPRE

Informes preliminares y final de las pruebas y escaneos de vulnerabilidades del sistema informático SIPRE

Descripción breve

Este documento contiene el resultado y la evidencia del escaneo de vulnerabilidades a los elementos de la solución de informática 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

COMISIÓN ESTATAL ELECTORAL NUEVO LEÓN | CEE

Índice

Versión	Fecha	Descripción
1.0	16/Junio/2018	Documento inicial de resultados preliminares del análisis de vulnerabilidades del sistema informático SIPRE de la CEENL
1.5	18/Junio/2018	Resutados del primer análisis de vulnerabilidades, escaneo de red y análisis de configuraciones
1.6	25/Junio/2018	Resultados del segundo escaneo de vulnerabilidades y de redes, así como revisión en particular de los centros de operación
1.7	27/Jun/2018	Integración de escaneo en sitio y resultados
1.8	29/Jun/2018	Análisis de riesgo incluido en el informe sobre las distintas pruebas relizadas

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 los escaneos y análisis de vulnerabilidades 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 el escaneo.

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 del análisis de vulnerabilidad. Los hallazgos obtenidos de la ejecución se documentarán en este documento con las recomendaciones que apliquen.

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 documentarán como resultados finales y se presentará como tal.
- De no cumplir los criterios, entonces se documentarán las recomendaciones y resultados, así 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.

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 Administración de Riesgos

Las pruebas se realizaron y sobre estas se deterino amenazas y las vulnerabilidades sobre las que sse podrían dar con su indíce de probabilidad de ocurrencia y su impacto. La justificación se dio en base a lo observado durane la auditoría.

Análisis de Riesgo – Arquitectura de Red					
Amenaza	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Justificación**
4.1.1 Diseño jerárquico de la red	Tráfico sin distinción ni separación haciendo la red mas lenta por la catidad de tráfico que circula en ella	Tener una red plana	**Bajo**	**Medio**	• Probabilidad Baja – La aplicación no permite transferir otro tipo de archivos • Impacto Medio – La operación se seguiría dando sin problema aunque potencialmente mas lenta
4.1.2 Redundancia en conexión	Perder conectividad para captura o vista pública	Enlaces de proveedor	**Bajo**	**Crítico**	• Probabilidad Bajo – Enlaces de proveedores ofrecen alta disponibilidad • Impacto Crítico – Retrasaría la captura de actas por trasladar la operación a otro CCV
4.1.3 Direccionamiento adecuado y eficiente	Red con fallas de direccionamiento	Conflicto de direccionamiento	**Bajo**	**Alto**	• Probabilidad Baja – El conflicto de dirección puede darse • Impacto Medio – El impacto de direccionamiento no es grave
4.1.4 Acceso controlado a redes en sitios de captura	Cualquier persona entre a la red	No tener control de acceso	**Bajo**	**Alto**	• Probabilidad Baja – Cualquier usuario puede entrar a la red • Impacto Alto – Una persona con acceso a la red podría afectar la operación de esta en los CCV's
4.2 Versión de los sistemas operativos sin vulnerabilidades críticas	Modificaciones a la configuración de red	Explotación de alguna versión con vulnerabilidades que permita tener acceso	**Bajo**	**Crítico**	• Probabilidad Bajo – Acceso local es difícil por el control de acceso y hacerlo remoto es difícil por la configuración • Impacto Crítico – Acceso puede crear graves conflictos
4.3 Soporte manual a infraestructura	Falla y/o equipo defectuoso que no se pueda sustituir	Falta de contratos de soporte	**Muy Bajo**	**Alto**	• Probabilidad Bajo – La compra de equipos se hizo el 1er semestra 2018 y en esta se incluyeron 3 años de soporte • Impacto Alto – No tener sustituciónd e equipos en caso de falla puede representar una caída de servicio.

Análisis de Riesgo – Estaciones de Captura					
Amenaza	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Justificación**
4.4.1 Acceso con privilegios mínimos	Operaciones por personal no autorizado	Entrar sin control de acceso a las estaciones de captura	**Bajo**	**Medio**	• Probabilidad Baja – el acceso tiene control tanto físico para el área de captura como lógico para el accceso • Impacto Alto - Usuario externo podría meter valores no correspondientes
4.4.2 Servicios habilitados en estaciones de captura	Accesos a sitios por canales no autorizados o indebidos	Puertos abiertos en las estaciones de trabajo	**Muy Bajo**	**Alto**	• Probabilidad Muy Bajo – Por la capacidad técnica de usuarios se ve poco probabe • Impacto Alto – De darse podría crear problemas en las estaciones de captura
4.4.3 Vulnerabilidades en las estaciones de captura	Usar servicios no autorizados en las estaciones de captuura	Puertos de servicios abiertos en las estaciones de captura	**Bajo**	**Alto**	• Probabilidad Bajo – La capacidad técnica es poco probable esto. Adicionalmente las estaciones están limitadas en cuanto a lo que se puede ejecutar • Impacto Alto – De lograrse, se podría crear problemas entre las estaciones de captura y/o al sistema de captura.
4.4.4 Acceso de las estaciones de captura	Usar aplicaciones no autorizadas	Acceso sin autorización a las estaciones de captura	**Muy bajo**	**Crítico**	• Probabilidad muy Bajo – El acceso es controlado tanto físicamente como lógicamente al área y a las estaciones. • Impacto Crítico – De darse, podrían personas ejecutar funciones no permitidas o meter equipo no permitido
4.4.5 Acceso a la infraestructura de comunicaciones	Acceder al equipo de comunicaciones	cuartos de comunicaciones sin control de acceso	**Muy Bajo**	**Crítico**	• Probabilidad muy Bajo – No se permite acceso con otras computadoras al área por lo que no se ve probable suceda. • Impacto Crítico – El área permite la conexión directa a los puertos de gestión de equipos de comunicaciones
4.4.6 Puertos dedicados	Cambiar computadores en la red alámbrica	Puertos disponibles y abiertos en el área de captura	**Bajo**	**Medio**	• Probabilidad Bajo – La ocurrencia es difícil por que no se permite acceso computadoras al área de captura • Impacto Medio – Aun si así fuera, la computadora quedaría bloqueada

Análisis de Riesgo – Controles de Seguridad de Información					
Amenaza	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Justificación**
4.5.1 Seguridad en Operaciones: Administración de la Capacidad	Quedarse sin capacidad en los enlaces de captura	Enlaces llenos y no poder capturar información	**Bajo**	**Alto**	• Probabilidad Bajo – los enlaces están dimensionados para la carga de captura que se estará dando. • Impacto Alto – De llenarse los enlaces, esto traería un impacto el tiempo de captura
4.5.2 Seguridad en Operaciones: Protección contra malware	Entrada de malware a la red por las estaciones de captura	Conexión de USB o instalación de SW no permitido en estaciones	**Bajo**	**Crítico**	• Probabilidad Bajo – no se puede dar por los privilegios y el acceso que tienen • Impacto Crítico – de darse, esto podría tener consecuencias en la red no solo de captura sino de la CEENL.
4.5.3 Seguridad en Operaciones: Bitácora de eventos	No saber o controlar situaciones operativas en la infraestructura	No tener monitoreo de la infraestructura o red	**Bajo**	**Medio**	• Probabilidad Bajo – Los sistemas tienen por definición un sistema de monitoreo • Impacto Medio – No se detiene la operación aunque la visibiidad de la red quedaría limitada.
4.5.4 Seguridad en Operaciones: Restricciones para instalación de SW	Instalación de software en las estaciones de captura	Conectarse a Internet o USB para instalar SW no permitido	**Muy bajo**	**Crítico**	• Probabilidad Muy Baja – La instalación de SW es difícil que se de dado los privilegios y limitaciones en los medios para instalación de SW. • Impacto Crítico – de darse, se podría crear problemas serios no solo en la red de captura de actas, sino en toda la CEENL

Análisis de Riesgo – Controles de Comunicaciones Seguras					
Amenaza	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Justificación**
4.6.1 Comunicaciones Seguras: Controles de la Red	Poder entrar desde otros segmentos de red a la red de captura	Acceso desde otros segmentos	**Bajo**	**Critico**	• Probabilidad Bajo – dentro de la red será difícil por el control que se tiene en la red (direccionamiento, segmentación y privilegios dados en la configuración) • Impácto Crítico – De darse el impacto podría ser amplio que llegue mas alla de la red de captura y alcanar la CEENL
4.6.2 Comunicaciones Seguras: Seguridad de los servicios de red	Usar protocolos no permitidos para entrar a la red	Hacer uso de protocolos de accecso remoto para entrar a la red de captura o los sistemas de captura de AZURE	**Bajo**	**Crítico**	• Probabilidad Bajo – Estaciones y red con pocos privilegios y puertos permitidos • Impacto Crítico – De darse puede entrar a la red de AZURE y afectar la captura de actas
4.6.3 Comunicaciones Seguras: Segregación en redes	Entrada de usuarios no autorizados a la red	Redes con acceso a la red de captura o de AZURE	**Bajo**	**Crítico**	• Probabilidad Bajo – Dado el control de acceso físico y lógco, se ve fácil se de este tipo de acceso • Impacto Crítico – Puede impactar no solo a la red del CCV sino a la CEENL
4.6.4 Comunicaciones Seguras: Transferencia de información	Poder ver los resultados de capturas por cualquier persona no autorizada	Acceso a los canales de transmisión para escanearlos y ver el contenido	**Bajo**	**Alto**	• Probabilidad Bajo – El acceso a los canales de comunicación están en otra red sin acceso a los de captura y aparte esta cifrada por túnel de IPSEC • Impacto Alto – De darse, esto traería impactos en el conocimiento de la información que no se puede revelar hasta horarios determinados por el INE y afectar credibilidad de la CEENL.

Análisis de Riesgo – Escaneo y Revisión de Configuraciones					
Amenaza	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Justificación**
4.7 Robustez de la infraestructura de computo	Entrar a la infraestructura de computo de AZURE donde se captura	Accesos permitidos o sin control o monitoreo a la infraestructura de computo	**Muy Bajo**	**Crítico**	• Probabilidad Muy Bajo – La infraestructura donde esta hospedada el SW de captura es bastante robusta y dada su configuración de nube privada se ve difícil que ocurra • Impacto Crítico – De darse, el acceso la infraestructura estaría comprometida en su totalidad en cuanto al proceso de elecciones del 1º de julio
4.8 Robustez de la infraestructura de comunicaciones	Entrar a la infraestructura de redes y comunicaciones	Accesos permitidos o sin control o monitoreo a la infraestructura de comunicaciones	**Bajo**	**Crítico**	• Probabilidad Bajo – La entrada a esta infraestructura desde Internet es poco probable por los controles y proteccioens que tiene • Impacto Crítico – Su acceso puede comprometer toda la operación del proceso electoral
4.9.1 Revisión de configuración Switches LAN	Que un intruso pueda entrar al dispositivo	Huecos en la configuración que permitan tomar control y acceso a el dispositivo para modificarlo	**Bajo**	**Crítico**	• Probabilidad Bajo – La configuración de switches tiene los controles que evitaría la entrada de un intruso a los switches LAN. • Impacto Crítico – De darse, el acceso puede comprometer toda la operación de captura del proceso electoral
4.9.2 Revisión de configuración Router	Que un intruso pueda entrar al dispositivo	Huecos en la configuración que permitan tomar control y acceso a el dispositivo para modificarlo o que haya entrada en la red que conecta el ruteador	**Bajo**	**Crítico**	• Probabilidad Bajo – La configuración de los ruteadores tiene los controles que evitaría la entrada de un intruso a los ruteadores que conectan la WAN • Impacto Crítico – De darse, el acceso puede comprometer toda la operación de captura del proceso electoral
4.9.3 Revisión de configuración Firewall	Que un intruso pueda entrar al dispositivo	Huecos e la configuración que permitan tomar control y acceso al dispositivo para modificarlo o que haya entradas a la red atrás del FW	**Bajo**	**Crítico**	• Probabilidad Bajo – La configuración de los firewalls tiene los controles que evitaría la entrada de un intruso a los ruteadores que conectan la WAN • Impacto Crítico – De darse, el acceso puede comprometer toda la operación de captura del proceso electoral

5 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

5.1 Resúmen Ejecutivo: 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 .

5.2 Resúmen Ejecutivo: 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.

5.3 Resúmen Ejecutivo: Controles Seguridad Operativa

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.

5.4 Resúmen Ejecutivo: Controles Comunicación Segura

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.

5.5 Resúmen Ejecutivo: Escaneo y Revisión 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

6 Conclusiones

Las conclusiones de la prueba estarán documentadas en el informe final del análisis de vulnerabilidades solicitada en el documento de requisitos mínimos del INE.

7 Anexo I – Resúmen de 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 pueden documentar en este mismo anexo.

Pruebas del Análisis de Vulnerabilidades CEENL 2018			
Prueba	**Criterio Aceptación**	**Resultado**	**Comentarios**
4.1 Diseño y Arquitectura de Red			
4.1.1 Diseño jerarquico de la red	Diagrama muestra estructura y modelo de red	Aceptado	Arquitectura jeráquica de red (Acceso, Distribución, core) de acuedo a mejores prácticas de la industria
4.1.2 Redundancia en conexión	Conexión alterna de salida del centro captura	Aceptado	Dos y hasta tres accesos a Internet depediendo del tipo de centro. (Ver evidencias para descripción)
4.1.3 Direccionamiento adecuado y eficiente	Direccionamiento segmentado por funciones, alcances y responsabiilidades	Aceptado	Direccionamiento segmentado aisla áreas de trabajo previniendo comportamientos migren de un área a otra
4.1.4 Acceso controlado a redes en sitios de captura	El acceso a los closets de telecom debe estar controlado y asegurado	Aceptado	Los cuartos o closets de equipos de red están bajo llave y con acceso controlado.
4.2 Validación de versiones sin vulnerabilidades críticas	Versiones de los switches y routers no deben presentar vulnerabilidades críticas ni altas	Aceptado	Versiones de switches sin avisos de vulnerabilidades críticos o Altos para lo que son los servicios que se están usando
4.3 Soporte manual a infraestructura	Se cuenta con contratos de soporte, así como soporte en sitio y vía telefónica para soporte	Aceptado	Se revisaron los manuales de soporte para personal, así como el centro de ayuda telefónco
4.4 Validación de estaciones de captura			
4.4.1 Acceso con privilegios mínimos	Acceso solo a lo que requiere	Aceptado	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	Lista de servicios abiertos en estaciones captura	Aceptado	Las estaciones tienen filtrado los puertos por lo que no servicios disponibles en estas
4.4.3 Vulnerabilidades en las estaciones de captura	Lista de vulnerabilidades de nivel crítico y alto en las estaciones de captura	Aceptado	No hay puertos abiertos ni vulnerabilidades encontradas en las estaciones de trabajo
4.4.4 Acceso de las estaciones de captura	Estaciones de captura solo con la aplicación para captura de elecciones	Aceptado	No hay otra aplicación cargada y no permite cargar aplicaciones al usuario operador.
4.4.5 Acceso a la infraestructura de comunicaciones	Bloqueo de puertos TELNET, WEB, si no es así, debe haber lista de acceso. Acceso solo vía SSH	Aceptado	Escaneo desde el Internet a los routers dedicados de Internet y los puertos están bloqueados.
4.4.6 Puertos dedicados	Tener habilitado Port Blocking	Aceptado	Los puertos de LAN se bloquean al conetar otra estación de trabajo y tienen horarios de activación
4.5 Controles de seguridad de Operaciones en la red del SIPRE			
4.5.1 Seguridad en Operaciones: Administración de la Capacidad	Existencia de control de aplicaciones y/o enlace desborde para consumo ancho banda	Aceptado	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	Existencia de controles para evitar la introducción de malware en la red	Aceptado	El UTM Meraki MX100, posee licenciamiento de ANTIMALWARE protegiendo la infraestructura
4.5.3 Seguridad en Operaciones: Bitácora de eventos	Existencia de bitácoren de eventos del ambiente de red LAN y WAN	Aceptado	Existe 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	Existencia de controles para evitar instalación de SW no permitido en estaciones de trabajo	Aceptado	El sistema operativo instalado en las estaciones no permite acceder a este por parte del usuario
4.6 Controles de comunicaciones seguras			
4.6.1 Comunicaciones Seguras: Controles de la Red	El área de captura y almacenamiento deberá estar segregado de otras áreas de TI	Aceptado	El esquema de segmentación permite separar las áreas operativas de las de desarrollo y operación
4.6.2 Comunicaciones Seguras: Seguridad de los servicios de red	Control de protocolos no permitidos. Tener una lista de servicios/protocolos permitidos	Aceptado	Los servicios permitidos solamente son los que se ofrecen para la captura en servidores de AZURE
4.6.3 Comunicaciones Seguras: Segregación en redes	Mostrar esquema de direccionamiento con evidencia de la segregación	Aceptado	Redes segregadas en base a funciones de personal estructurado redes y subredes sobre esta base.
4.6.4 Comunicaciones Seguras: Transferencia de información	Tener canales seguros de transmisiónd de estaciones de captura hasta sistema	Aceptado	Se cuenta con tuneles de IPSEC los cuales cifran la conexión de forma dedicada y dinámica si se requiere usar enlace alterno de la CEENL

Pruebas del Análisis de Vulnerabilidades CEENL 2018			
Prueba	**Criterio Aceptación**	**Resultado**	**Comentarios**
4.7 Escaneo a infraestructura de computo	Que en el escaneo no haya ninguna vulnerabilidad nivel alta o crítica.	Aceptado	El escaneo no mostro nada y los puertos están cerrados en las estaciones de captura
4.8 Escaneo de infraestructura de comunicaciones	Que en el escaneo no haya ninguna vulnerabilidad nivel alta o crítica.	Aceptado	El escaneo con NMAP, OCS, CAT y CISCO-TORCH muestra los puertos filtardos desde Internet.
4.9 Revisión de configuración de infraestructura de comunicaciones			
4.9.1 Revisión de configuración Switches LAN	Recomendaciones sobre la configuración de la infraestructura de switches LAN cumpliendo los requerimientos de mejores prácticas	Aceptado	La configuración de los swtiches se mostro
4.9.2 Revisión de configuración Router	Recomendaciones sobre la configuración de la infraestructura de Routers cumpliendo los requerimientos de mejores prácticas	Aceptado	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 adquirio estos equipos y fue quien los configuro e instaló.
4.9.3 Revisión de configuración Firewall	Recomendaciones sobre la configuración de la infraestructura de Firewall cumpliendo los requerimientos de mejores prácticas	Aceptado	La configuración se mostro 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 iplementaos que se asocian con los números de serie

Hallazgos y Recomendaciones	
Severidad	**Prueba(s) Descripción Hallazgo o Recomendación**
Ninguno	
Bajo	
Medio	
Alto	
Crítico	