TECNOLÓGICO DE MONTERREY®

Instituto de Elecciones y Participación Ciudadana Chiapas (IEPC)

Resumen Ejecutivo – Reporte Final

31 Marzo 2022

Tecnológico de Monterrey

IEPC
INSTITUTO DE ELECCIONES Y PARTICIPACIÓN CIUDADANA
CHIAPAS

Resúmen General (31/Marzo)

Observaciones

Firma Digital de código

- Se confirmo la generación correcta de la firma digital del código la cual permite validar la integridad de este al inicio y durante la jornada electoral validando que sea inalterable.

PenTest/Vulnerabilidades

- Se logro cerrar las vulnerabilidades explotables de mas alta criticidad mediante las recomendaciones de configuración de los servicios que se dieron en el 2º simulacro.

Verificación de infraestructura lista para operar

- La infraestructura fue revisada así como el soporte operativo a esta tanto en el CCV como en los CATD's y cumple con las recomendaciones dadas

Por hacer

Constancia firma digital de código el día de las elecciones

- Al inicio de operación del PREP, se tomará la firma digital la cual se volverá a tomar en el transcurso de la jornada y al final de esta para asegurar la integridad del código.

Constancia de reinicio de BD el día de las elecciones

- Al inicio de la operación del PREP se correrá la rutina para reiniciar la Base de datos para dejar en ceros todos los valores de esta e iniciar la operación del PREP.

Operación de la jornada

- Durante la operación de la jornada, se documentarán hechos relevantes y/o del funcionamiento y operación del sistema PREP

Tecnológico de Monterrey

IEPC
INSTITUTO DE ELECCIONES Y PARTICIPACIÓN CIUDADANA
CHIAPAS

Pruebas Caja Negra 1/2

Prueba	Criterio Aceptación	Revisado	Comentarios
Pruebas PREP Digitalización	**SPD01 –** Control de acceso a la aplicación Móvil de digitalización mediante usuario/contraseña.	Aceptado	Se reviso el celular y se asigna cuenta y contraseña
	SPD02 – Bloqueo aplicación móvil por usuario contraseña errónea después de varios intentos	Aceptado	El usuario se bloquea y debe hablar al centro de atención, en el CCV para cambio de contraseña, la aplicación indica el teléfono.
	SPD03 – Usuario bloqueado deberá cambiarse mediante mesa de servicio	Aceptado	El usuario deberá hablar al centro de soporte al CCV
	SPD04 – Dispositivos móviles con aplicación controlada e inventariada	Aceptado	La aplicación se mantiene inventariada mediante el número único de instalación de Android.
	SPD05 – Distribución de Aplicación controlada	Aceptado	La aplicación se distribuye desde un sitio controlado por el administrador del IEPC
	S**PD06 –** Identificación con factor adicional para teléfonos móviles en el uso de la aplicación y firma de la plataforma	Aceptado	No tiene doble factor de autentificación, pero la plataforma se casa con el teléfono y el número de instalación de Android para su control e inventario. La distribución esta controlada por un portal privado de la UTSI
	SPD07 – Alta de actas por parte del equipo móvil registrado	Aceptado	Las actas se digitalizan en el teléfono. La aplicación indica cuando se tiene el acta y cuando se sincroniza hacia la BD del PREP
	SPD08 – Alta de acta equivocada (no pertenece a la casilla)	Aceptado	No lo indica ya que se determino como método para dar de alta otras actas como contingencia. La validación
	SPD09 – Transmisión de acta digitalizada al sitio o BD de Actas	Aceptado	Se sube el acta una vez tomada la foto y solicitando sincroniación. Al subirse el acta, se indica la operación y borra la fotografía del móvil
	SPD10 – Transmisión cifrada del acta digitalizada hacia el repositorio o BD del PREP (MÓVIL)	Aceptado	Se transmite vía SSL
	SPD11 – Transmisión cifrada del acta digitalizada hacia el repositorio o BD del PREP (ESCÁNER)	Aceptado	Se transmite vía SSL y la conexión es vía cable (no Wifi)
	SPD12 – Confirmación de integridad del acta digitalizada y guardada en la BD del PREP	Aceptado	Se genero la firma digital con éxito probando qu cualquier cambio puede alterar la firma
Pruebas PREP Captura	**SPC01 –** Control de acceso a la estación de captura mediante usuario/contraseña.	Aceptado	
	SPC02 – Bloqueo de usuario contraseña errónea	Aceptado	
	SPC03 – Sistema operativo de la estación de captura debe ser vigente (no estar descontinuado por el fabricante)	Aceptado	Las estaciones de captura utilizan Windows 11 con la última actualización
	SPC04 – Las estaciones de captura deberán estar conectadas a la red mediante cable y no de forma inalámbrica	Aceptado	Todas las estaciones están conectadas vía cable, no se usa WiFi
	SPC05 – Usuarios de estación de captura con privilegios mínimos de administración	Aceptado	La estación esta conectada a una VPN controlada para la captura
	SPC06 – Sistema Operativo de la plataforma de captura deberá tener negado el acceso a Internet	Aceptado	Las estaciones si tienen acceso a Internet, pero los usuarios son personal interno de IEPC Chiapas, el área de captura es chica y hay video vigilancia
	SPC07 - Las estaciones de captura solo deben tener acceso hacia las aplicaciones del PREP de la jornada 2022	Aceptado	Las estaciones solo tienen instalado el navegador y ningún otro software
	SPC08 – Sistema Operativo de la plataforma de captura no deberá permitir acceder a medios externos de almacenamiento de datos (USB, CD, CD-ROM	Aceptado	Las estaciones no tienen CD.
	Portal de captura al que acceden las estaciones de captura, deberá ser un portal en SSL y con certificado	Aceptado	El certificado es interno, la red a la que se conecta e

Pruebas Caja Negra 2/2

Prueba	Criterio Aceptación	Revisado	Comentarios
Pruebas Captura, publicación y Casos de Uso	**PCD01 –** Validar proceso de cotejo de acta digitalizada contra los campos de captura del acta	Aceptado	Este paso se lleva cuando no hay coincidencia en la 1ª y 2ª captura.
	PCD02 – El sistema PREP Local deberá considerar para la Captura los siguientes datos requeridos por parte del INE para cálculos adecuados	Aceptado	Revisados en Casos de uso
	PCD03 – Datos a calcular por la plataforma PREP en la que se debe validar que los siguientes valores se den como resultado del cálculo en cada nivel de agregación que aplique (acta, sección, distrito electoral, entidad federativa y nacional)	Aceptado	Hay inconsistencias en las actas registradas las cuales no cuadran. El domingo se encontró el error y se corregirá para el 2o simulacro
Pruebas Datos que Publicar	**PPR01 –** Resultados de porcentajes los decimales deberán calcularse a cuatro posiciones (diezmilésimas) y no deberán truncarse ni redondearse	Aceptado	Todos los números se calculan los resultados se preseentan a 4 digios
	PPR02 – El portal debe tener la liga para poder bajar los datos en formato .CSV para cargarlos en hoas de calculo	Aceptado	La base de datos se bajo en formato .csc y los datos coincidieron con los del portal que se capturaron.
	PPR03 – Datos a Publicar deberán publicar en el sitio oficial, de donde se distribuirán a los sitios replicantes de información oficial deben contener los siguientes valores	NA	En esta ocasión, no habrá replicación de contenido a otros sitios.
	PPR04 – Requerimientos de portal WEB para publicación – Interfaz Principal	Aceptado	El portal cuenta con los elementos requeridos para publicación en la interfaz principal WEB
	PPR05 – Requerimientos de portal WEB para publicación – Encabezado	Aceptado	El portal cuenta con los elementos requeridos para publicación en la interfaz principal WEB
	PPR06 – Requerimientos de portal WEB para publicación – Menú Colapsable	Aceptado	El portal cuenta con los elementos requeridos para publicación en la interfaz principal WEB
	PPR07 – Requerimientos de portal WEB para publicación – Avance entidad	Aceptado	Los requerimientos de avance en cada entidad (municipio) se encuentran el el portal WEB
	PPR08 – Requerimientos de portal WEB para publicación – Resultados Tu Casilla	Aceptado	Los requerimientos de avance en cada entidad (municipio) se encuentran el el portal WEB
	PPR09 – Requerimientos de portal WEB para publicación – Estadística de Entidad	Aceptado	Los requerimientos de avance en cada entidad (municipio) se encuentran el el portal WEB
	PPR10 – Requerimientos de portal WEB para publicación – Pie de Página (footer)	Aceptado	Los requerimientos de avance en cada entidad (municipio) se encuentran el el portal WEB
	PPR11 – Requerimientos de portal MÓVIL para publicación – Interfaz Principal	Aceptado	Los requerimientos de pie de página se encuentran presentes en el portal móvil (probado con un Android y IOS)
	PPR12 – Requerimientos de portal MÓVIL para publicación – Encabezado	Aceptado	Los requerimientos de pie de página se encuentran presentes en el portal móvil (probado con un Android y IOS)
	PPR13 – Requerimientos de portal MÓVIL para publicación – Menú Desplegable	Aceptado	Los requerimientos de pie de página se encuentran presentes en el portal móvil (probado con un Android y IOS)
	PPR14 – Requerimientos de portal MÓVIL para publicación – Menú Desplegable > Mi Casilla	Aceptado	Los requerimientos de pie de página se encuentran presentes en el portal móvil (probado con un Android y IOS)
	PPR15 – Requerimientos de portal MÓVIL para publicación – Avance Entidad	Aceptado	Los requerimientos de pie de página se encuentran presentes en el portal móvil (probado con un Android y IOS)
	PPR16 – Requerimientos de portal MÓVIL para publicación – Consulta de Votación	Aceptado	Los requerimientos de pie de página se encuentran presentes en el portal móvil (probado con un Android y IOS)
	PPR17 – Requerimientos de portal MÓVIL para publicación – Estadística Entidad	Aceptado	Los requerimientos de pie de página se encuentran presentes en el portal móvil (probado con un Android y IOS)
	PPR18 – Requerimientos de portal MÓVIL para publicación – Pie de página (footer)	Aceptado	Los requerimientos de pie de página se encuentran presentes en el portal móvil (probado con un Android y IOS)

Análisis de Vulnerabilidades 1/2

Prueba	Criterio Aceptación	Revisado	Comentarios
Revisión Configuraciones	**SPI01 –** Validar la configuración de los equipos de red siga mejores prácticas y no haya inconsistencias en esta	Aceptado	
	SPI02 – Los equipos de comunicaciones solo podrán ser accesibles desde la red interna y con protocolo seguro (SSH).	Aceptado	El escaneo solo muestra puertos de SSH, SSL para acceso desde la red interna.
	SPI03 – Equipos de ruteo y switches deberán tener versiones de sistemas operativos actualizados y bajo soporte	Aceptado	Los equipos no tienen contrato de soporte, pero se tienen equipos de respaldo en caso de alguna falla.
	SPI04 – Equipos de comunicaciones y redes deberán estar con soporte y/o sustitución en caso de falla	Aceptado	Los equipos no tienen contrato de soporte, pero se tienen equipos de respaldo en caso de alguna falla.
	SPI05 – El sistema PREP deberá contar con esquema de redundancia de comunicaciones	Aceptado	Actualmente se cuenta con 150Mbps de Internet de Telmex y se esta por instalar 200Mbps de TotalPlay. La redundancia se hace de forma manual
	SPI06 – El sistema PREP deberá contar con redundancia eléctrica en caso de caída o fallas en la red eléctrica durante la jornada electoral	Aceptado	Se tienen UPS's los cuales mantienen la operación y con los generadores eléctricos recuperan la energía en menos de un minuto. Los CATD's remotos, tienen plantas generadores, su recuperación es de aproximadamente 1 minuto.
	SPI07 – Los activos involucrados en el PREP deberán de tener habilitado la función de bitácora (logging) para guardar eventos	Aceptado	Todos la infraestructura tiene habilitado el logging para en caso de algún error, poder revisarlas y trazar el origen.
Pruebas Controles físicos	**SPI08 –** Los sistemas involucrados del PREP deberán tener un centro de control y comando que permita el monitoreo de sus sistemas	Aceptado	Todo el monitoreo se lleva acabo desde el CCV. Cualquier situación se reporta desde los CATDs. Vía telefónica al CCV Central.
	SPI09 – En los centros de captura no debe haber redes inalámbricas que conecten la infraestructura de captura o del OPL**.**	Aceptado	Las redes inalámbricas existentes son de la red del IEPCC la cual es ajena a la de captura a la cual se conectan por cable
	SPI10 – La infraestructura de los ambientes de desarrollo debe estar segregada de la infraestructura de ambientes operativos	Aceptado	El ambiente de captura PREP y publicación, son distintos a los del IEPCC
	SPI11 – El sistema debe tener recursos dedicados por lo que no debe compartir recursos con otros sistemas o plataformas ajenos al PREP en evaluación	Aceptado	Los sistemas para el PREP son dedicados y hechos por la OPL, están en otra red y el ambiente en una nube donde no se comparten.
	SPI12 – Controles de acceso físico a los centros de captura	Aceptado	Existe acceso controlado al edificio por credencial y lista de acceso la cual debe firmarse y validada por guardia.
	SPI13 – Control de acceso al sitio donde esta la infraestructura del PREP	Aceptado	Existe un control de acceso físico al IEPCC el cual esta controlado adentro de las instalaciones del IEPCC
	SPI14 – Verificar si hay control de acceso a teléfonos móviles	Aceptado	No hay control sobre celulares, pero por el tamaño del cuarto de captura, la cantidad de personas en la captura y siendo estas miembros del IEPCC hay una supervisión muy cercana.

Análisis de Vulnerabilidades 2/2

Prueba	Criterio Aceptación	Revisado	Comentarios
Hallazgos Pruebas Escaneo Vulnerabilidades de Activos	**SPV01** – Escaneo de los activos dentro de la red o segmento del PREP. Los activos deben estar justificado en cuanto a su uso	**Aceptado**	Los equipos poseen configuraciones que limitan su acceso externo. De acuerdo a la mejor práctica de seguridad.
	SPV02 – Escaneo de los puertos o servicios habilitados en los activos de la red o segmento del PREP debe estar justificado en cuanto a su uso	**Aceptado**	El sitio público tiene los puertos estrictamente requeridos para la operación del portal. El sitio interno tiene los puertos requeridos para la operación y sincronización. Adicionalmente solo se acceden por las estaciones dentro de la red privada restringida.
	SPV03 – El escaneo de servicios hecho a la infraestructura no debe no debe tener existencia de vulnerabilidades altas (7.0 – 8.9) o Críticas (9.0 – 10) basados en la clasificación estándar CVSS	**Aceptado**	Los hallazgos en la infraestructura se redujeron a menos de nivel 5 de criticidad
	SPV04 – El escaneo de servicios hechos a la infraestructura no debe tener explotaciones (exploits) desarrollados contra la infraestructura.	**Aceptado**	No se encontraron exploits en las vulnerabilidades encontradas
	SPV05 – Listar mediante un escaneo de los servidores WEB las vulnerabilidades que pueda haber en estos	**Aceptado**	Solo se encontraron dos vulnerabilidades nivel medio y bajo que no aplican para el ambiente de trabajo del IEPC Chiapas
	SPV06 – EL sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado	**Aceptado**	El sitio de publicación tiene un certificado válido
Pruebas Controles Soporte Operativo	**PRS01 –** La OPL debe tener un manual de capacitación para el personal de captura	**Aceptado**	Se entregaron manuales y operativos Se recomienda crear un manual de instalación y operación del UPS
	PRS02 – Debe haber un centro telefónico para consultas o dudas en los distintos procesos o módulos del PREP	**Aceptado**	El centro es el CCV en Tuxtla y se colgaron letreros con el teléfono a marcar para soporte
	PRS03 – Debe existir un proceso de resolución de inconsistencias al momento de captura de acta	**Aceptado**	El procedimiento es una tercera captura para inconsistencias en captura
	PRS04 – Contratos de soporte externo en caso de eventualidades sobre las plataformas operativas que se utilizan en el PREP (para sistemas desarrollados por terceros)	**Aceptado**	Se cuenta con soporte para las distintas plataformas sobre las que opera el PREP
	PRS05 – Tener los contratos con los proveedores de telecomunicaciones (primario y secundario) con los mapas de escalación de ellos para reportar eventos	**Aceptado**	Se tiene contrato con Telmex y esta pendiente i instalación de TotalPlay
	PRS06 – Tener los contratos con los proveedores de nube, así como los procedimientos de reporte en caso de eventos hacia ellos. (si se está utilizando Nube como repositorio operativo del PREP)	**Aceptado**	En el 2º simulacro se migro ambiente a AWS de forma definitiva.
	PRS07 – Tener la documentación del sistema PREP de la OPL actualizado y en resguardo por los encargados del área de tecnología de la OPL	**Aceptado**	Se compartió toda la documentación del proceso, del sistema y de la capacitación

Pruebas de Tráfico (DOS/DDOS)

Prueba	Criterio Aceptación	Revisado	Comentarios
Pruebas de ataques de DOS y DDOS	**SPN01 –** La infraestructura debe soportar un ataque volumétrico TCP-SYN FLOOD	**Aceptado**	La i infraestructura soporto un ataque de TCP-SYN FLODD de 400Mbps de una red de bots manteniendo los tiempos de respuesta por debajo de 0.5 segundos
	SPN02 – La infraestructura deberá soportar un ataque volumétrico por UDP-DNS Amplification.	**Aceptado**	Se reviso el DNS se pudo verificar que la versión que se tiene no es vulnerable a ataques de DNS Amplification
	SPN03 – LA infraestructura deberá poder soportar un ataque volumétrico por ICMP – ICMP FLOOD	**Aceptado**	La i infraestructura soporto un ataque de ICMP FLODD de 400Mbps de una red de bots manteniendo los tiempos de respuesta por debajo de 0.5 segundos
	SPN04 – La infraestructura deberá poder manejar un ataque en la capa de aplicación vía un SLOWLORIS attack	**Aceptado**	La i infraestructura soporto un ataque SLOWLORIS (RUDY) manteniendo los tiempos de respuesta por debajo de 0.5 segundos
	SPN05 – Validación de las cuotas de servicio configuradas en las subscripciones de servicios de nube (si aplica)	**Aceptado**	Los servidores en el ambiente en que se encuentran están configurados de forma correcta permitiendo detectar el ataque y manteniendo la operativodad del servicio en todo momento sin afectación en tiempos de respuesta.
	SPN06 – Revisar con la OPL la existencia de un plan o procedimiento a seguir en caso de evento de ataque de DOS	**Aceptado**	Se tienen planes de repuesta a incidentes y se así se detectará, se revisará con el proveedor
	SPN07- Validar la existencia de contratos de servicio de protección de exceso de tráfico o para blindar contra ataques DOS	**Aceptado**	La nube en que se encuentran los servidores cuenta con la protección para atraques de DOS y DDOS. Adicionalmente, mediante las pruebas, se comprobó su funcionamiento.
	SPN08 – Validar la existencia de un plan de comunicación hacia la comunidad en caso de eventos de DOS	**Aceptado**	LA comunicación hacia el púiblico se da mediante los miembros del consejo encabezados por el Consejero Presidente del IEPC con los datos e información que el área de sistemas le proporcione.