TECNOLÓGICO DE MONTERREY®

Instituto Electoral de Coahuila

Resumen Ejecutivo Auditoría – Reporte al 01 Junio 2023

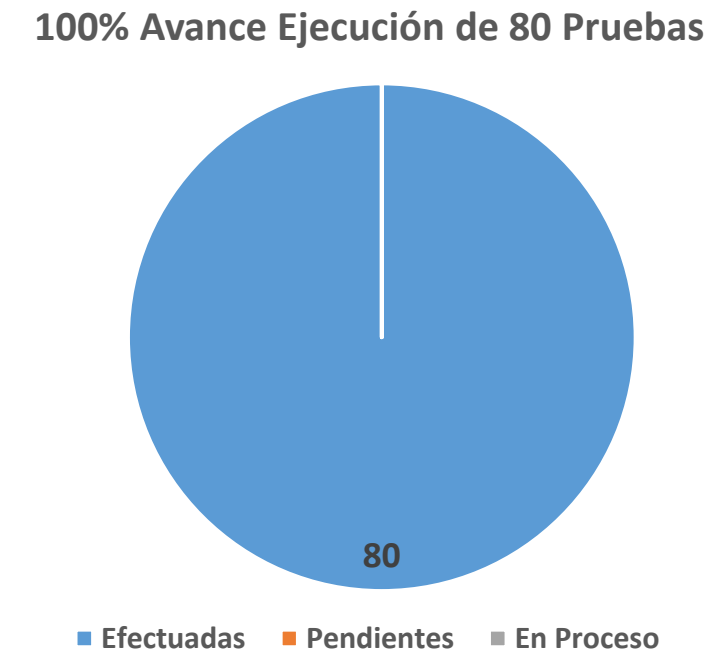
01 Junio 2023

Tecnológico de Monterrey

IEC Instituto Electoral de Coahuila

Resúmen Actividades (01/Junio)

Pruebas	Avance	Por ejecutarse
Pruebas Caja Negra	• Pruebas iniciadas, pendiente recolectar evidencias de sitios alternos y CATD's	
Pruebas Integridad y BD	• Se validó la firma digital del código y revisión del proceso de inicialización de BD	
Pruebas Vulnerabilidad	• Se realizo el escaneo de la totalidad de los servidores de publicación y de backend sin que presentaran vulnerabilidades altas o críticas. • En los escaneos no surgió ningún exploit hacia los componentes de la infraestructura.	
Pruebas Pentest	• No se han encontrado vulnerabilidades o exploits que se puedan utilizar para vulnerar la red o las aplicaciones	
Pruebas DDOS	• Se han revisado los planes existentes del proveedor así como los del IEC • Pruebas de ataques de DDOS se ejecutaron obteniendo resultados positivos sin ningún hallazgo el sitio no presento afectaciones durante el ataque	
Informe Jornada	• Revisión y seguimiento de la jornada electoral	• Actividad agendada para realizarse el día de la jornada electoral el 4 de junio durante todo el periodo que el PREP este abierto.



Tecnológico de Monterrey

IEC Instituto Electoral de Coahuila

Pruebas Aplicación1/2

Prueba	Criterio Aceptación	Revisado	Comentarios
Pruebas PREP Digitalización	**SPD01 –** Control de acceso a la aplicación Móvil de digitalización mediante usuario/contraseña.	**Aceptado**	La aplicación cuenta con usuario y contraseña para acceder a esta
	SPD02 – Bloqueo aplicación móvil por usuario contraseña errónea después de varios intentos	**Aceptado**	La aplicación móvil se bloquea después de 5 intentos
	SPD03 – Usuario bloqueado deberá cambiarse mediante mesa de servicio	**Aceptado**	El usuario debe hablar a mesa de servicio para desbloquear contraseña
	SPD04 – Dispositivos móviles con aplicación controlada e inventariada	**Aceptado**	La aplicación se inscribe a un servicio con el cual se
	SPD05 – Distribución de Aplicación controlada	**Aceptado**	La aplicación de PREP Casilla, esta controlada por medio del registro que hacen en el sistema de PROISI
	SPD06 – Identificación con factor adicional para teléfonos móviles en el uso de la aplicación y firma de la plataforma	**Aceptado**	El teléfono se autentifica con usuario, contraseña e IMEI en el programa de registro de teléfonos móviles.
	SPD07 – Alta de actas por parte del equipo móvil registrado	**Aceptado**	El móvil permite escanear el acta bajo el esquema PREP Casilla.
	SPD08 – Alta de acta equivocada (no pertenece a la casilla)	**Aceptado**	Los privilegios asignados al rol del usuario que captura no lo permiten
	SPD09 – Transmisión de acta digitalizada al sitio o BD de Actas	**Aceptado**	Se transmite al repositorio para poder ser utilizadas para captura
	SPD10 – Transmisión cifrada del acta digitalizada hacia el repositorio o BD del PREP (MÓVIL)	**Aceptado**	La transmisión se hace vía SSL (cifrado)
	SPD11 – Transmisión cifrada del acta digitalizada hacia el repositorio o BD del PREP (ESCÁNER)	**Aceptado**	La transmisión se hace vía SSL (cifrado)
	SPD12 – Confirmación de integridad del acta digitalizada y guardada en la BD del PREP	**Aceptado**	Se genera un hash 256bits en el archivo escaneado y se guarda con el acta
Pruebas PREP Captura	**SPC01 –** Control de acceso a la estación de captura mediante usuario/contraseña.	**Aceptado**	El acceso a la estación de captura cuenta con usuario/contraseña
	SPC02 – Bloqueo de usuario contraseña errónea	**Aceptado**	Se tiene que generar una nueva contraseña vía mesa de servicio
	SPC03 – Sistema operativo de la estación de captura debe ser vigente (no estar descontinuado por el fabricante)	**Aceptado**	La versión de Windows que tienen es la 11 actualmente bajo soporte.
	SPC04 – Las estaciones de captura deberán estar conectadas a la red mediante cable y no de forma inalámbrica	**Aceptado**	Todas las estaciones están cableadas, no hay ninguna con wifi
	SPC05 – Usuarios de estación de captura con privilegios mínimos de administración	**Aceptado**	Solo tienen privilegio de usuario sin permisos de administración
	SPC06 – Sistema Operativo de la plataforma de captura deberá tener negado el acceso a Internet	**Aceptado**	Se pudo validar que se siguió la recomendación del simulacro #3 ya que las estaciones de trabajo en el CCV central no tienen acceso a Internet. Se aplico filtrado en el firewall para evitar su salida a otro sitio que no sean los permitidos por la aplicación del PREP
	SPC07 - Las estaciones de captura solo deben tener acceso hacia las aplicaciones del PREP de la jornada 2022	**Aceptado**	Las estaciones de captura en los CCVs solo tienen acceso a la aplicación del PREP Adicionalmente hay supervisión para evitar que los capturistas estén haciendo algo distinto a las labores de captura.
	SPC08 – Sistema Operativo de la plataforma de captura no deberá permitir acceder a medios externos de almacenamiento de datos (USB, CD, CD-ROM	**Aprobado**	Las estaciones no tienen dispositivo de disco externo y no usa el USB
	SPC09 – Portal de captura al que acceden las estaciones de captura, deberá ser un portal en SSL y con certificado	**Aceptado**	Los sitios de captura tienen certificados internos de SSL. El certificado interno solamente se usa en aplicaciones de uso interno.

Pruebas Aplicación2/2

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**	El acta digitalizada se aprecia visualmente en el lugar de donde se tiene que capturar el numero
	PCD02 – El sistema PREP Local deberá considerar para la Captura los siguientes datos requeridos por parte del PREP para cálculos adecuados	**Aceptado**	Los datos requeridos por el INE son capturados de acuerdo a los requerimientos establecidos
	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**	Se revisaron los datos y la forma como se agregan por nivel lo cual se da correctamente
Pruebas Datos que Publicar	**PPR01 –** Resultados de porcentajes los decimales deberán calcularse a cuatro posiciones (diezmilésimas) y no deberán truncarse ni redondearse	**Aceptado**	Los formatos de número están correctos en el portal y en el archivo .CSV cuando se baja
	PPR02 – El portal debe tener la liga para poder bajar los datos en formato .CSV para cargarlos en hojas de calculo	**Aceptado**	La liga funciona correctamente pudiendo bajar el archivo en formato CSV para revisión
	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	**Aprobado**	Acuerdos con los difusores fueron hechos y el sitio principal se carga en los sitios definidos actualizándose cada 5 minutos en función del cambio de datos que haya .
	PPR04 – Requerimientos de portal WEB para publicación – Interfaz Principal	**Aceptado**	Cumple con los requerimientos dados
	PPR05 – Requerimientos de portal WEB para publicación – Encabezado	**Aceptado**	Cumple con los requerimientos dados
	PPR06 – Requerimientos de portal WEB para publicación – Menú Colapsable	**Aceptado**	Cumple con los requerimientos dados
	PPR07 – Requerimientos de portal WEB para publicación – Avance entidad	**Aceptado**	Cumple con los requerimientos dados
	PPR08 – Requerimientos de portal WEB para publicación – Resultados Tu Casilla	**Aceptado**	Cumple con los requerimientos dados
	PPR09 – Requerimientos de portal WEB para publicación – Estadística de Entidad	**Aceptado**	Cumple con los requerimientos dados
	PPR10 – Requerimientos de portal WEB para publicación – Pie de Página (footer)	**Aceptado**	Cumple con los requerimientos dados
	PPR11 – Requerimientos de portal MÓVIL para publicación – Interfaz Principal	**Aceptado**	Cumple con los requerimientos dados
	PPR12 – Requerimientos de portal MÓVIL para publicación – Encabezado	**Aceptado**	Cumple con los requerimientos dados
	PPR13 – Requerimientos de portal MÓVIL para publicación – Menú Desplegable	**Aceptado**	Cumple con los requerimientos dados
	PPR14 – Requerimientos de portal MÓVIL para publicación – Menú Desplegable > Mi Casilla	**Aceptado**	Cumple con los requerimientos dados
	PPR15 – Requerimientos de portal MÓVIL para publicación – Avance Entidad	**Aceptado**	Cumple con los requerimientos dados
	PPR16 – Requerimientos de portal MÓVIL para publicación – Consulta de Votación	**Aceptado**	Cumple con los requerimientos dados
	PPR17 – Requerimientos de portal MÓVIL para publicación – Estadística Entidad	**Aceptado**	Cumple con los requerimientos dados
	PPR18 – Requerimientos de portal MÓVIL para publicación – Pie de página (footer)	**Aceptado**	Cumple con los requerimientos dados

Tecnológico de Monterrey

Pruebas de Integridad y Reinicio de Base de datos

Prueba	Prueba	Revisado	Comentarios
Firma digital y reinicio de Base de datos	Firma de aplicación en SHA256	**Aceptado**	La firma dela aplicación SHA256 fue generada correctamente previo, durante y al final del simulacro
	Coincidencia de la firma digital	**Aceptado**	La firma coincidió correctamente en los tres ejercicios durante el simulacro y en todos los simulacros
	Inicialización de la base de datos	**Aceptado**	La base de datos se reinicio a ceros correctamente

Tecnológico de Monterrey

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**	Se compartió la configuración de los equipos que conectan a Internet y no se encontraron inconsistencias en la configuración ni en los controles de seguridad
	SPI02 – Los equipos de comunicaciones solo podrán ser accesibles desde la red interna y con protocolo seguro (SSH).	**Aceptado**	Solo permite el acceso al equipo desde la red interna del proveedor y bajo protocolo SSH
	SPI03 – Equipos de ruteo y switches deberán tener versiones de sistemas operativos actualizados y bajo soporte	**Aceptado**	La versión del equipo de red actualmente es válida y se encuentra bajo soporte
	SPI04 – Equipos de comunicaciones y redes deberán estar con soporte y/o sustitución en caso de falla	**Aceptado**	El proveedor se encarga de la solución llave en mano incluyendo sustitución de los equipos en caso de algún incidente
	SPI05 – El sistema PREP deberá contar con esquema de redundancia de comunicaciones	**Aceptado**	Se tiene dos proveedores de internet para dar soporte a la continuidad en comunicaciones
	SPI06 – El sistema PREP deberá contar con redundancia eléctrica en caso de caída o fallas en la red eléctrica durante la jornada electoral	**Aceptado**	Esta jornada, se tiene una planta de generación eléctrica para la infraestructura del PREP y la planta de generación eléctrica del edificio
	SPI07 – Los activos involucrados en el PREP deberán de tener habilitado la función de bitácora (logging) para guardar eventos	**Aceptado**	La solución del PREP esta configurada para proporcionar una bitácora de eventos para revisar la trazabilidad de estos y poder realizar un análisis post-evento
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**	El centro de comando y control esta monitoreando tanto infraestructura (su comportamiento y uso) como el proceso de captura (su avance y progreso de esta)
	SPI09 – En los centros de captura no debe haber redes inalámbricas que conecten la infraestructura de captura o del PREP**.**	**Aceptado**	La red de WiFi no forma parte de la red de los equipos de computo de captura, son redes distintas y están separadas.
	SPI10 – La infraestructura de los ambientes de desarrollo debe estar segregada de la infraestructura de ambientes operativos	**Aceptado**	Se pudo validar la separación de los ambientes se encuentran separados
	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**	Se comprobó que los elementos del sistema PREP esta dedicado a la infraestructura del IEC, no se comparte con otros sistemas u organizaciones.
	SPI12 – Controles de acceso físico a los centros de captura	**Aceptado**	Los sitios tienen control de acceso al área de procesamiento.
	SPI13 – Control de acceso al sitio donde esta la infraestructura del PREP	**Aceptado**	El acceso al sitio de captura esta controlado por dos puertas con tarjeta y otra con código para entrar.
	SPI14 – Verificar si hay control de acceso a teléfonos móviles	**Aceptado**	Existen mesas para dejar pertenencias de capturistas antes de entrar a la sala de captura por lo que no debe haber teléfonos móviles en la sala de captura. Esto fue indicado en la capacitación.

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 activos escaneados fueron revisados y justificados correctamente para la solución para el backend y frontend
	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**	Los servidores fueron escaneados y solamente tienen los puertos requeridos para operación:TCP443, TCP22, TCP80, TCP21
	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 servidores de la infraestructura del PREP fueron escaneados y no se encontraron vulnerabilidades de riesgo
	SPV04 – El escaneo de servicios hechos a la infraestructura no debe tener explotaciones (exploits) desarrollados contra la infraestructura.	**Aceptado**	En la revisión de la infraestructura no se encontraron exploits definidos para esta
	SPV05 – Listar mediante un escaneo de los servidores WEB las vulnerabilidades que pueda haber en estos	**Aceptado**	Los servidores web no presentan vulnerabilidades altas ni críticas.
	SPV06 – EL sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado	**Aceptado**	Los sitios de simulacro cuentan con certificados públicos reconocidos.
Pruebas Controles Soporte Operativo	**PRS01 –** El proveedor del sistema debe tener un manual de capacitación para el personal de captura	**Aceptado**	Manual revisado y en proceso capacitación
	PRS02 – Debe haber un centro telefónico para consultas o dudas en los distintos procesos o módulos del PREP	**Aceptado**	Centro de apoyo para sitios
	PRS03 – Debe existir un proceso de resolución de inconsistencias al momento de captura de acta	**Aceptado**	Se reviso y existe en un proceso posterior a la 3ª 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**	El proveedor PROISI esta llevando la operación del PREP y es quien lo desarrollo y quien le dará soporte. Adicionalmente se cuenta con el soporte de AWS y Cloudflare como soporte de PROISI.
	PRS05 – Tener los contratos con los proveedores de telecomunicaciones (primario y secundario) con los mapas de escalación de ellos para reportar eventos	**Aceptado**	Se cuentan con servicios de UAY Networks (primario) y de Telmex (Secundario) teniendo soporte físico en las oficinas centrales por parte de las empresas. La redundancia del enlace fue probada con éxito.
	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**	Los servicios de nube se tienen en AWS comprobando los servidores y su conectividad
	PRS07 – Tener la documentación del sistema PREP de la PREP actualizado y en resguardo por los encargados del área de tecnología de la PREP	**Aceptado**	Se entrego toda la documentación sobre el sistema, manuales de capacitación

Tecnológico de Monterrey

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**	Se inyecto tráfico por encima de 12Gbps para afectar el desempeño. El sitio de publicación no se vio afectado y los tiempos de respuesta no subieron de 250ms lo cual
	SPN02 – La infraestructura deberá soportar un ataque volumétrico por UDP-DNS Amplification.	**Aceptado**	Se ataco el DNS para afectar el desempeño de la resolución. El sitio de publicación funcionó correctamente durante el ataque confirmando que la resolución funcionaba correctamente y el tiempo de respuesta no excedía 250ms
	SPN03 – LA infraestructura deberá poder soportar un ataque volumétrico por ICMP – ICMP FLOOD	**Aceptado**	Se inyecto tráfico ICMP por exceso de 12Gbps y se pudo observar que no hubo afectación en el desempeño del sitio manteniendo los tiempos de respuesta por debajo de 250ms
	SPN04 – La infraestructura deberá poder manejar un ataque en la capa de aplicación vía un SLOWLORIS attack	**Aceptado**	Se hizo pruebas de conexión bajo un ataque tipo RUDY tratando de agotar los recursos de conexión sin éxito. El comportamiento del servidor se considera aceptado.
	SPN05 – Validación de las cuotas de servicio configuradas en las subscripciones de servicios de nube (si aplica)	**Aceptado**	Se valido con el proveedor el funcionamiento de CLOUDFLARE como servicio para protección de tráfico.
	SPN06 – Revisar con el proveedor del sistema PREP y/o el OPL la existencia de un plan o procedimiento a seguir en caso de evento de ataque de DOS	**Aceptado**	Verificar que la solución de informática que exista un manual de procedimiento a seguir en caso de un evento de ataque de negación de servicio.
	SPN07- Validar la existencia de contratos de servicio de protección de exceso de tráfico o para blindar contra ataques DOS	**Aceptado**	El servicio contratado para la protección e ataques de DDOS es CLOUDFLARE que esta antepuesto a la solución de AWS el cual detecta el tráfico y lo limita para evitar afectación en el desempeño del sitio.
	SPN08 – Validar la existencia de un plan de comunicación hacia la comunidad en caso de eventos de DOS	**Aceptado**	El plan de manejo de incidentes existe dela empresa para la comunicación hacia el OPL para alertar algún incidente. En su turno la OPL se encargaría de dar la comunicación a la ciudadanía

Tecnológico de Monterrey