TECNOLÓGICO DE MONTERREY®

Auditoría del PREP 2021 - IEES

Avance Auditoría del PREP Instituto Electoral del Estado de Sinaloa

Avance del proceso de auditoría del Programa Preliminar de Resultados Electorales (PREP) para el Instituto Electoral del Estado de Sinaloa.

05 Junio 2021

Tecnológico de Monterrey

Agenda

La auditoría fue planteada en 6 distintas líneas de revisión y al día 5 de junio se tiene el siguiente estado

#	Línea Revisión	Estado	Observaciones
1	Pruebas Caja Negra	Terminado	Todas las funcionalidades del sistema PREP, en sus distintas fases (digitalización, captura y publicación), fueron exitosas cumpliendo con los requerimientos de seguridad así como los de funcionalidad.
2	Validación Sistema Informático e Integridad PREP y BD	Terminado	Se revisaron los procesos de reinicio de BD así como el de la generación de llave de integridad, faltará ejecutarse en su momento.
3	Entregables PenTest	Terminado	Para las vulnerabilidades presentadas no hay explotaciones definidas.
4	Análisis Vulnerabilidades Infraestructura PREP	Terminado	Las vulnerabilidades encontradas fueron mitigadas con controles compensatorios.
5	Pruebas DOS a PREP	Terminado	Las pruebas se omitieron considerando que el sistema PREP está protegido por la solución empresarial CloudFlare Enterprise Plan con los módulos de Load Balancing, CDN y Enterprise Firewall, con lo que se mitigan ataques tipo DOS. El DNS no es propenso a ataques de amplificación.
6	Informe Jornada PREP	Pendiente	Se entregará hasta el 10 de junio.

Pruebas Caja Negra - Digitalización

Pruebas CATD Celular			
Controles Especificados	**Pruebas ejecutadas**	**Comentarios**	**Resultado**
SPD01 – Control de acceso a la aplicación Móvil de digitalización mediante usuario/contraseña.	Usuario deberá tener acceso al APP mediante un usuario asignado y contraseña	Se hace mediante un usuario y contraseña para la aplicación móvil.	**Aceptado**
SPD02 – Bloqueo aplicación móvil por usuario contraseña errónea después de varios intentos	El usuario deberá bloquearse después de varios intentos (mínimo 3, máximo 5) de acceder a la aplicación con la contraseña errónea	Se bloquea después de 3 intentos por un tiempo de 1 minuto.	**Aceptado**
SPD03 – Usuario bloqueado deberá cambiarse mediante mesa de servicio	Se deberá solicitar el cambio de usuario bloqueado hacia un personal con rol de administrador de usuario	Se bloquea después de 3 intentos por un tiempo de 1 minuto.	**Aceptado**
SPD04 – Dispositivos móviles con aplicación controlada e inventariada	Revisar la existencia de un inventario de activos con aplicación y sistema de control de acceso	Se cuenta con un inventario en el sistema Central PREP con la relación de cuentas y celular.	**Aceptado**
SPD05 – Distribución de Aplicación controlada	Acceso a la aplicación debe ser controlada por un solo punto de contacto para su instalación	La aplicación se instala de manera manual en cada equipo.	**Aceptado**
SPD06 – Identificación con factor adicional para teléfonos móviles en el uso de la aplicación y firma de la plataforma	Se deberá verificar que se cuente con un método de asegurarse que solo teléfonos permitidos pueden firmarse en la plataforma, adicional al usuario y clave de esta. Métodos adicionales sugeridos: Certificado, MAC, IMEI	La aplicación tiene requerimientos específicos de instalación al modelo en particular de celular. Al primer login en el sistema CATD Celular, la cuenta de acceso y el celular se relacionan, por lo que solo esa cuenta se puede usar en el mismo celular. Se utiliza el Android ID para identificar el dispositivo móvil.	**Aceptado**
SPD07 – Alta de actas por parte del equipo móvil registrado	Con usuario aceptado en la aplicación, el encargado de subir actas hará una digitalización de acta correcta	El acta asignada se logra subir correctamente.	**Aceptado**
SPD08 – Alta de acta equivocada (no pertenece a la casilla)	Con usuario aceptado en la aplicación, el encargado de subir actas hará una digitalización de un acta que no le corresponda	Solo se puede subir el acta que le corresponde.	**Aceptado**
SPD09 – Transmisión de acta digitalizada al sitio o BD de Actas	El acta digitalizada por medio móvil o escáner deberá subirse a la BD de la OPL	Se pudo verificar en el proceso de captura el acta subida a la BD.	**Aceptado**
SPD10 – Transmisión cifrada del acta hacia el repositorio o BD del PREP (sea Móvil o Escáner)	Verificar el protocolo de comunicaciones usado por la aplicación para transmitir la imagen o bien el escáner que se este usando para enviar la imagen.	El app del móvil transmite el acta por SSL hacia el repositorio de actas.	**Aceptado**
SPD11 – Transmisión cifrada del acta digitalizada hacia el repositorio o BD del PREP (ESCÁNER)	Verificar el protocolo de comunicaciones usado por el escáner para transmitir la imagen **NOTA:** *Esta prueba aplica solo si el scanner no requiere de computadora para transmitir el acta hacia la BD*	No aplica, el escáner se conecta a una laptop con el sistema y se contestó en SDP10.	**No aplica**
SPD12 – Confirmación de integridad del acta digitalizada y guardada en la BD del PREP	Hay que confirmar un esquema de generación de una llave o confirmación que verifique la integridad del acta escaneada enviada y guardada en la BD del PREP	En la validación del MRID se aplica un hash y se guarda en la base de datos y se valida en MIDAEC.	**Aceptado**

Pruebas Caja Negra - Captura

Pruebas PREP Captura			
Controles Especificados	**Pruebas ejecutadas**	**Comentarios**	**Resultado**
SPC01 – Control de acceso a la estación de captura mediante usuario/contraseña.	Usuario deberá tener acceso a la estación de captura mediante usuario/contraseña	El acceso es por usuario y contraseña y éstos son del propio sistema CVPREP. Perfiles independientes del CATD Celular y PREP Casilla.	**Aceptado**
SPC02 – Bloqueo de usuario contraseña errónea	El usuario deberá bloquearse después de varios (5) intentos de acceder a la aplicación con la contraseña errónea	Se implementó el bloqueo por 1 minuto después de 5 intentos fallidos.	**Aceptado**
SPC03 – Sistema operativo de la estación de captura debe ser vigente (no estar descontinuado por el fabricante)	El usuario administrador deberá mostrar la versión del sistema operativo instalado en la estación de captura la cual debe ser una que no este descontinuada por el fabricante	Las laptops cuentan con Windows 10 con última actualización disponible por Microsoft al momento de configurarse los equipos.	**Aceptado**
SPC04 – Las estaciones de captura deberán estar conectadas a la red mediante cable y no de forma inalámbrica	Verificar que las estaciones de captura no hagan uso de la interfase inalámbrica y estén conectadas mediante cableado.	Todas conectadas por cable y desactivando Wi-Fi. Usuario de Windows invitado, restringido la configuración, solo pueden conectar mouse. No acceso a Panel de Control ni Wi-Fi.	**Aceptado**
SPC05 – Usuarios de estación de captura con privilegios mínimos de administración	Se accederá con el usuario y verificará que no sea un usuario administrador y/o que no tenga acceso a modificar configuraciones del ambiente o del sistema operativo	Usuario “Coordinador y Digitalizador Capturista”. Mismos privilegios restringidos..	**Aceptado**
SPC06 – Sistema Operativo de la plataforma de captura deberá tener negado el acceso a Internet	Se verificará que las estaciones de captura no tengan acceso a Internet de ningún tipo	El acceso a Internet está restringido, solo permite acceso al portal de captura.	**Aceptado**
SPC07 - Las estaciones de captura solo deben tener acceso hacia las aplicaciones del PREP de la jornada 2021	Se entrar con un usuario de captura para asegurar que la estación de captura no tenga acceso a otra aplicación que no sea la del portal o aplicación de captura definido por la OPL	Las estaciones de captura sólo tienen acceso al portal CVPREP.	**Aceptado**
SPC08 – Sistema Operativo de la plataforma de captura no deberá permitir acceder a medios externos de almacenamiento de datos (USB, CD, CD-ROM	Se intentará conectar una memoria USB y/o un DVD/CDROM en la estación de captura del PREP	Las computadoras no tienen dispositivos externos, tienen bloqueado el uso de USB y el acceso al disco duro por Explorador de Windows.	**Aceptado**
SPC09 – Portal de captura al que acceden las estaciones de captura, deberá ser un portal en SSL y con certificado válido	Se consultará la información del sitio para verificar que haya un protocolo de cifrado habilitado y que haya un certificado existente	El sistema cuenta con certificado emitido por CLOUDFLARE y es válido.	**Aceptado**

Pruebas Caja Negra – Captura Datos en Cumplimiento INE

Pruebas de Captura de Datos en sistema PREP en Cumplimiento Requerimientos del INE			
Controles Especificados	**Pruebas ejecutadas**	**Comentarios**	**Resultado**
PCD01 – Validar proceso de cotejo de acta digitalizada contra los campos de captura del acta	Verificar que la plataforma PREP contenga los campos de captura y el acta digitalizada para su captura	Se reviso el sistema de captura y se tienen los campos requeridos para la captura de actas. Se solicita un acta para capturar y esta es presentada al usuario para su captura con los campos adecuados.	**Aceptado**
PCD02 – El sistema PREP Local deberá considerar para la Captura los siguientes datos requeridos por parte del INE para cálculos adecuados	Se deberá verificar que en el proceso de captura del PREP se tengan como mínimo los siguientes campos para ser llenados con los datos provenientes del acta **ID Acta PREP** • Entidad Federal • Distrito Electoral • Sección • Tipo • Número casilla • Municipio **Votos Obtenidos** • Votos obtenidos por Partido y candidatos independientes **Votos** • Total, votos • Votos nulos • Votos par candidatos no registrado	Los datos están incluidos como parte del sistema PREP.	**Aceptado**
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)	Se deberá verificar en el Sistema PREP en la captura que los siguientes datos estén siendo calculados a) Total numérico de actas esperadas; b) Total numérico de actas capturadas y su correspondiente porcentaje respecto al total de actas esperadas; c) Total numérico de actas contabilizadas y su correspondiente porcentaje respecto al total de actas esperadas; d) Total de actas fuera de catálogo; e) El porcentaje calculado de participación ciudadana; f) Total de votos por AEC, g) Agregado del total de votos, por un lado, incluyendo los votos en casillas especiales y, por el otro lado, sin incluir los votos en casillas especiales, h) Agregados a nivel nacional, circunscripción, entidad federativa, municipio o Alcaldía, distrito electoral, sección y acta, según corresponda.	Se reviso archivo CSV que se baja del portal así como los datos del portal y los datos calculados están incluidos en su totalidad.	**Aceptado**

de Monterrey

Pruebas Caja Negra – Datos Publicación

Pruebas del Proceso Publicación de Resultados (PPR)			
Controles Especificados	**Pruebas ejecutadas**	**Comentarios**	**Resultado**
PPR01 – Resultados de porcentajes los decimales deberán calcularse a cuatro posiciones (diezmilésimas) y no deberán truncarse ni redondearse	Verificar en la prueba funcional que el resultado obedece a dicho lineamiento y el calculo se realizo correctamente	La publicación del portal de resultados (en ambiente de calidad) muestra a 4 dígitos (diezmilésimas) los resultados de porcentajes.	**Aceptado**
PPR02 – El portal debe tener la liga para poder bajar los datos en formato .CSV para cargarlos en hoas de calculo	Entrar a la opción de Base de Datos y bajar el archivo en formato .CSV para verificar que pueda ser cargado por una hoja de calculo	El archivo se puede abrir desde Excel y contiene las actas contabilizadas en el ejercicio que se revisó.	**Aceptado**
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	La lista de valores a publicarse como parte de esta prueba en el sitio oficial desde donde se replicará hacia los difusores, debe incluir los siguientes valores: a) Lista nominal; b) Lista nominal de las actas contabilizadas; c) Participación ciudadana; d) Datos capturados, en el caso del total de votos asentado, únicamente se publicará en la base de datos descargable del portal del PREP. Este dato no deberá utilizarse para calcular los agregados publicados en el portal; e) Datos calculados; f) Imágenes de las Actas PREP; g) Identificación del Acta PREP con inconsistencias, así como el porcentaje de actas con inconsistencias con respecto al total de actas esperadas; h) En su caso, el resultado de las consultas populares; i) Las bases de datos con los resultados electorales preliminares, en un formato de archivo CSV y de acuerdo a la estructura establecida por el Instituto, y j) Hash o código de integridad obtenido a partir de cada imagen de las Actas PREP, con el estándar definido por el Instituto.	Se revisaron los valores en portal y están incluidos los requeridos.	**Aceptado**
PPR04 – Requerimientos de portal WEB para publicación – Interfaz Principal	Entrar a la página de publicación de la OPL para verificar la existencia de los siguientes elementos de navegación en la página principal: a) Encabezado b) Menú izquierdo colapsable. c) Avance de Entidad d) Conoce los resultados de tu casilla e) Estadística de la Entidad f) Pie de página (footer)	Se revisaron los elementos en portal y están incluidos de acuerdo con la guía de definición del INE.	**Aceptado**
PPR05 – Requerimientos de portal WEB para publicación – Encabezado	Entrar a la página de publicación de la OPL para verificar la existencia de los siguientes elementos en el encabezado a) Acceso a preguntas frecuentes b) Acceso a Centro de ayuda c) Configuración visual (tamaño y formato claro/oscuro) d) Debe incluir Logo PREP y OPL e) Boto de regreso a inicio f) Acceso directo a pestañas por elección g) Acceso a la Base de datos	Se revisaron los elementos en portal y están incluidos de acuerdo con la guía de definición del INE.	**Aceptado**

Pruebas Caja Negra – Datos Publicación

Pruebas del Proceso Publicación de Resultados (PPR)			
Controles Especificados	**Pruebas ejecutadas**	**Comentarios**	**Resultado**
PPR06 – Requerimientos de portal WEB para publicación – Menú Colapsable	Entrar a la página de publicación de la OPL y mover se hacia la esquina superior izquierda para que aparezca el menú colapsable a) Acceso directo votos por Candidatura b) Acceso directo votos por partido político y candidatura Independiente c) Detalle por casilla d) Detalle por Distrito e) Sección f) Casilla	Se revisaron los elementos en portal y están incluidos de acuerdo con la guía de definición del INE.	**Aceptado**
PPR07 – Requerimientos de portal WEB para publicación – Avance entidad	En la sección de Avance Entidad deben existir los siguientes elementos a) Actas Capturadas b) Participación Cludadana c) Indicador del Corte d) Botón Actualizar	Se revisaron los elementos en portal y están incluidos de acuerdo con la guía de definición del INE.	**Aceptado**
PPR08 – Requerimientos de portal WEB para publicación – Resultados Tu Casilla	En el portal, el usuario consultara resultados de la casilla de su interés con los siguientes elementos a) Signo Interrogación b) Campo de Sección c) Campo Primer Apellido c) Botón de Consulta d) Aviso Privacidad	Se revisaron los elementos en portal y están incluidos de acuerdo con la guía de definición del INE.	**Aceptado**
PPR09 – Requerimientos de portal WEB para publicación – Estadística de Entidad	Entrar a la página de para verificar la existencia de los totales en porcentajes, gráficos y listas: a) Actas b) Actas contabilizadas c) Lista Nominal d) Participación e) Votos f) Total, de Votos	Se verifico tanto en el portal como en los archivos de la BD para bajar que los datos requeridos están ahí como se requiere.	**Aceptado**
PPR10 – Requerimientos de portal WEB para publicación – Pie de Página (footer)	Entrar a la página de publicación de la OPL para verificar la existencia del pie de página en el portal con los siguientes elementos a) Participación b) Votos c) Total, de Votos	El footer o la parte baja (final) de la página del sitio de publicación esta incluido correctamente.	**Aceptado**
PPR11 – Requerimientos de portal MÓVIL para publicación – Interfaz Principal	Entrar a la página de publicación de la OPL para verificar la existencia de los siguientes elementos de navegación en la página principal: a) Encabezado b) Menú izquierdo colapsable. c) Avance de Entidad a) Encabezado b) Menú izquierdo colapsable. c) Avance de Entidad	El portal móvil funciona de acuerdo a lo requerido con los elementos de navegación.	**Aceptado**

Tecnológico de Monterrey

Pruebas Caja Negra – Datos Publicación

Pruebas del Proceso Publicación de Resultados (PPR)			
Controles Especificados	**Pruebas ejecutadas**	**Comentarios**	**Resultado**
PPR12 – Requerimientos de portal MÓVIL para publicación – Encabezado	Entrar a la página móvil del PREP para verificar la existencia en el encabezado de estos elementos: a) Nombre del sitio con el nombre del estado en auditoría b) Logo del PREP local c) Menú desplegable	El menú y logos están correctamente desplegados.	**Aceptado**
PPR13 – Requerimientos de portal MÓVIL para publicación – Menú Desplegable	Entrar a la página móvil del PREP y verificar en el menú desplegable los siguientes elementos: a) Tipo de Elección b) Mi casilla c) Preguntas frecuentes a) Centro Ayuda b) Tema y tamaño caracter	Las opciones y ligas hacia los distintos elementos funcionan correctamente.	**Aceptado**
PPR14 – Requerimientos de portal MÓVIL para publicación – Menú Desplegable > Mi Casilla	Entrar a la página móvil del PREP y verificar en el menú desplegable en la opción de Mi casilla los siguientes elementos: a) Aviso de Privacidad b) Instrucción c) Ejemplo de credencial para votar d) Consultar e) Aviso de privacidad al consultar f) Flecha de regreso	Las opciones y ligas hacia los distintos elementos funcionan correctamente.	**Aceptado**
PPR15 – Requerimientos de portal MÓVIL para publicación – Avance Entidad	Entrar a la página móvil del PREP en la sección de Avance Entidad y verificar la existencia de los siguientes elementos: a) Ultimo corte b) Botón actualizar	Se encontraron los elementos requeridos en el portal móvil .	**Aceptado**
PPR16 – Requerimientos de portal MÓVIL para publicación – Consulta de Votación	Entrar a la página móvil del PREP en la Consulta de Votación y verificar la existencia los siguientes elementos: a) Votos por Candidatura, Distritos o Municipios b) Votos por Partido Político y Candidatura Independiente c) Distrito, Municipio o Demarcación	La consulta se pudo hacer por distintas formas como se requiere en la prueba.	**Aceptado**
PPR17 – Requerimientos de portal MÓVIL para publicación – Estadística Entidad	Entrar a la página móvil del PREP en la Estadística Entidad y verificar la existencia de los siguientes elementos: a) Actas b) Actas contabilizadas por casillas urbanas y no urbanas c) Lista Nominal d) Participación ciudadana	La página móvil permite encontrar los distintos elementos para verificar las actas, lista nominal y participación ciudadana.	**Aceptado**
PPR18 – Requerimientos de portal MÓVIL para publicación – Pie de página (footer)	Entrar a la página móvil del PREP e ir al pie de página (sección inferior) y verificar la existencia de los siguientes elementos: a) versión de escritorio b) Leyenda c) Logos de la OPL d) Aviso de privacidad e) Nombre del Instituto Local f) versión de los servicios g) botón para compartir	Se encontraron los elementos, así como el botón para compartir.	**Aceptado**

Pruebas Caja Negra – Casos de Uso

Pruebas del Proceso Publicación de Resultados (PPR) Escenario – Gobernatura				
Controles Especificados	Casos de Uso (Escenarios PREP)	Criterio de Aceptación	Comentarios	Resultado
PFD – 01	Gubernatura – 1	Acta se digitaliza con escáner, se capturó 2 veces, al coincidir, se publica.		Aceptado
PFD – 06	Gubernatura – 2	Acta se digitaliza con PREP Casilla, todos los campos vienen en blanco por lo que se capturan con (b) indicando en blanco 2 veces, se pasa verificación y se publica más no se contabiliza.		Aceptado
PFD – 08	Gubernatura – 3	Acta se digitaliza con PREP Casilla, todos los datos ilegibles, se capturó 2 veces, coincide que se marcaron como todos los datos ilegibles, se pasa al MVEVAL quien confirma es ilegible y la publica.		Aceptado
PFD – 11	Gubernatura – 4	Acta se digitaliza con PREP Casilla, se capturó 3 veces, se solicita baja, MVEVAL acepta la baja y se pasa con prioridad a CVPREP coordinador para su captura.		Aceptado
PFD - 13	Gubernatura – 5	Acta se digitaliza con escáner, se capturó 2 veces, al coincidir, se publica y se verifica suma correcta de votos.		Aceptado

Pruebas del Proceso Publicación de Resultados (PPR) Escenario – Diputaciones				
Controles Especificados	Casos de Uso (Escenarios PREP)	Criterio de Aceptación	Comentarios	Resultado
PFD – 04	Diputaciones – 1	Acta se digitaliza con PREP Casilla, se capturó 2 veces, al coincidir, se publica.		Aceptado
PFD – 05	Diputaciones – 2	Acta se digitaliza con escáner, se detecta acta duplicada, anterior capturada en PREP Casilla, no se publica.		Aceptado
PFD – 07	Diputaciones – 3	Acta se digitaliza con escáner, se capturó 2 veces, coincide, se publica en ceros con observación de que excede la lista nominal.		Aceptado
PFD – 10	Diputaciones – 4	Acta se digitaliza con escáner, acta fuera del catálogo, no se puede identificar, no se publica, se agrega a base de datos		Aceptado

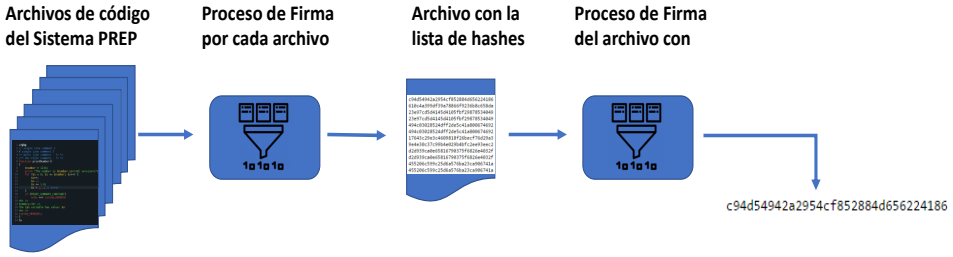
Pruebas del Proceso Publicación de Resultados (PPR) Escenario – Ayuntamientos				
Controles Especificados	Casos de Uso (Escenarios PREP)	Criterio de Aceptación	Comentarios	Resultado
PFD – 02	Ayuntamientos – 1	Acta se digitaliza con CATD Celular, se capturó 3 veces, al coincidir, se publica.		Aceptado
PFD – 03	Ayuntamientos – 2	Acta se digitaliza con escáner, se capturó 3 veces, no coincide, Coordinador MVEVAL da resolución y se publica.		Aceptado
PFD – 09	Ayuntamientos – 3	Acta se digitaliza con CATD Celular, presenta algún dato ilegible, se capturó 2 veces, al coincidir, se publica sin contabilizar el dato ilegible.		Aceptado
PFD – 12	Ayuntamientos – 4	Acta se digitaliza con CATD Celular, se capturó 2 veces, se solicita baja, MVEVAL rechaza la baja y se publica.		Aceptado

Tipo de Elección	No.	Tipo Acta PREP	Origen			Supuesto de inconsistencia							Supuestos de Captura/Verificación							
		AEC	Escaner	PREP Casilla	CATD Celular	Todos ilegibles	Todos sin dato	Algún dato ilegible	Algún sin dato	Excede LN	Fuera de catálogo	Sin inconsistencia	C1 = C2	C1 / C2	C1 o C2 = C3	C1 o C2 / C3	Cotejo: Solicita baja	Cotejo: Acepta	Cotejo: Rechaza	Resolución
Gubernatura	1	X	X									X	X							ACTA SE PUBLICA.
Ayuntamientos	2	X			X							X		X	X					ACTA SE PUBLICA.
Ayuntamientos	3	X	X						X					X	X					MVEVAL COORDINADOR DA RESOLUCIÓN.
Diputaciones	4	X		X								X	X							ACTA SE PUBLICA.
Diputaciones	5	X	X																	NO SE PUBLICA, SE DETECTA ACTA DUPLICADA (PREP CASILLA)
Gubernatura	6	X		X			X						X							SE REALIZA PUBLICACIÓN MÁS NO SE CONTABILIZA
Diputaciones	7	X	X							X			X							SE PUBLICA EN CEROS CON OBSERVACION DE EXCEDE LISTA NOMINAL
Gubernatura	8	X		X		X							X							COORDINADOR MVEVAL
Ayuntamientos	9	X			X			X						X	X					SE PUBLICA PERO NO SE CONTABILIZA EL DATO ILEGIBLE
Diputaciones	10	X	X								X									NO SE PUBLICA, SE AGREGA AL FINAL DE LA BASE DE DATOS
Gubernatura	11	X		X								X				X	X	X		SE SOLICITA BAJA DEL ACTA PUBLICADA Y ES ACEPTADA PARA REALIZAR EL CAMBIO.
Ayuntamientos	12	X			X				X				X				X		X	SE SOLICITA BAJA DEL ACTA PUBLICADA Y ESTA NO ES ACEPTADA PARA NO REALIZAR EL CAMBIO.

Tecnológico de Monterrey

Validación Sistema Informático e Integridad PREP y BD

Pruebas del PREP Digitalización (SPD)			
Controles Especificados	**Pruebas ejecutadas**	**Comentarios**	**Resultado**
IRS01 – Documentar y validar el proceso de firma digital en SHA256 del código de SW del PREP que se utilizará durante la jornada electoral	Documentar y validar el proceso	Se verificó el script que se ejecuta para generar un hash de hashes ya que se agregan las llaves de integridad de cada pieza de código en un archivo para posteriormente ejecutar sobre este archivo un nuevo hash.	**Aceptado**
IRS02 – Documentar y validar el proceso de reinicio de la base de datos para asegurar que los valores de esta sean cero y/o estén vacíos al inicio de la jornada electoral	Documentar y validar el proceso	Para reiniciar la BD existe una opción en el sistema Central PREP que al ejecutarse envía un correo al Director del Proyecto con una clave única que, al capturarse en el sistema, inicializa las tablas relacionadas, limpiando el contenido para el inicio de la jornada electoral.	**Aceptado**



Se hace búsqueda de los archivos .php dentro de los directorios del código que compone el sistma PREP

Se le genera una firma hash a cada archivo y es guardada cada firma en un archivo para obtener una firma por cada archivo

Se genera un archivo con todas las firmas digitales de cada uno de estos archivos del sistema PREP

Al archivo donde se tienen todas las firmas se le genera una firma digital hash de el archivo, un "hash de hashes"

La firma digital final es un "Hash de Hashes" que en caso de modificación de cualquier archivo, se modificaría

Tecnológico de Monterrey

Análisis Vulnerabilidades Infraestructura PREP

Resultados Preliminares Pruebas Controles Físicos			
Controles Especificados	**Pruebas ejecutadas**	**Comentarios**	**Resultado**
SPI01 – Validar la configuración de los equipos de red siga mejores prácticas y no haya inconsistencias en esta	Revisar que la configuración bloque puertos no usados, niegue por definición servicios y protocolos no utilizados	La configuración se reviso y esta hecha alineada a mejores prácticas permitiendo solamente lo estrictamente necesario.	**Aceptado**
SPI02 – Los equipos de comunicaciones solo podrán ser accesibles desde la red interna y con protocolo seguro (SSH).	Hay que confirmar que el acceso a los equipos de comunicaciones y redes solo se pueda dar por medio de SSH y no bajo otro protocolo (TELNET, HTTP u otro)	Los equipos solo pueden accederse vía SSH o mediante consola web por https.	**Aceptado**
SPI03 – Equipos de ruteo y switches deberán tener versiones de sistemas operativos actualizados y bajo soporte	Obtener las versiones de los equipos de ruteo y switcheo para confirmar que las versiones son actuales y aun disponibles (no descontinuadas)	Los equipo tienen versiones que están aun bajo soporte del fabricante.	**Aceptado**
SPI04 – Equipos de comunicaciones y redes deberán estar con soporte y/o sustitución en caso de falla	Confirmar contratos de soporte y/o equipo de reemplazo en caso de falla	Se cuenta con equipo en cold-standby en el CCV central en caso de falla se reemplaza.	**Aceptado**
SPI05 – El sistema PREP deberá contar con esquema de redundancia de comunicaciones	Entrar al equipo de comunicaciones y verificar la existencia de dos enlaces, configurados ya sea de manera activo-activo o activo-standby	Se tiene dos proveedores de servicio a Internet los cuales hacen failover en automático.	**Aceptado**
SPI06 – El sistema PREP deberá contar con redundancia eléctrica en caso de caída o fallas en la red eléctrica durante la jornada electoral	Verificar que exista una planta generadora eléctrica con UPS que mantenga ininterrumpido el flujo eléctrico en caso de falla de la red pública.	El centro principal cuenta con una planta eléctrica.	**Aceptado**
SPI07 – Los activos involucrados en el PREP deberán de tener habilitado la función de bitácora (logging) para guardar eventos	Entrar a los distintos activos y verificar la configuración y directorios donde se guarda la bitácora que esta este habilitado	Tienen habilitado la función de bitácora permitiendo tener trazabilidad a las actividades.	**Aceptado**
SPI08 – Los sistemas involucrados del PREP deberán tener un centro de control y comando que permita el monitoreo de sus sistemas	Validar la existencia de un centro que permita la visualización de la operación y su desempeño y que desde este se pueda visualizar la totalidad de los elementos del sistema PREP	El centro de comando se instala en COPREP.	**Aceptado**
SPI09 – En los centros de captura no debe haber redes inalámbricas que conecten la infraestructura de captura o del OPL.	Escanear las redes inalámbricas para asegurar que no haya acceso a la red de estaciones de captura	No hay redes inalámbricas que conectan al sistema Central PREP.	**Aceptado**
SPI10 – La infraestructura de los ambientes de desarrollo debe estar segregada de la infraestructura de ambientes operativos	Debe validarse que los ambientes de producción y de operación sean distintos y estén por separado	Los ambientes de desarrollo y producción están claramente separados entre la nube y COPREP.	**Aceptado**

Análisis Vulnerabilidades Infraestructura PREP

Resultados Preliminares Pruebas Controles Físicos			
Controles Especificados	**Pruebas ejecutadas**	**Comentarios**	**Resultado**
SPI11 – El sistema debe tener recursos dedicados por lo que no debe compartir recursos con otros sistemas o plataformas ajenos al PREP en evaluación	El ambiente operativo del PREP en evaluación no debe compartir recursos con otros sistemas o plataformas, sus recursos deben ser únicos. *Este control aplica primordialmente hacia estados donde hay terceros involucrados en el desarrollo de PREP que lo hacen para otros estados*	Ambientes exclusivos en dos zonas distintas en la nube, por lo que no se mezcla con ambientes de otros estados.	**Aceptado**
SPI12 – Controles de acceso físico a los centros de captura	El centro de captura deberá estar resguardado con entrada controlada para evitar que haya personas ajenas a los trabajos durante la jornada	El control de acceso a la entrada del edificio.	**Aceptado**
SPI13 – Control de acceso al sitio donde esta la infraestructura del PREP	Las aplicaciones que se estén utilizando para la jornada deberán estar activados sus puertos y no otros distintos a estos.	El control de acceso a la entrada del edificio y PREP público en la nube.	**Aceptado**
SPI14 – Verificar si hay control de acceso a teléfonos móviles	Debe haber un lugar donde registrar equipos móviles para control del acceso de estos	No se permitirá tener equipos móviles en las áreas de captura.	**Aceptado**

Tecnológico de Monterrey

Análisis Vulnerabilidades Infraestructura PREP

Resultados Preliminares Escaneo Vulnerabilidades de Activos			
Controles Especificados	**Pruebas ejecutadas**	**Comentarios**	**Resultado**
SPV01 – Escaneo de los activos dentro de la red o segmento del PREP. Los activos deben estar justificado en cuanto a su uso	Entrar y escanear y listando los diversos activos del PREP para la cual debe existir la justificación de cada uno de ellos por parte de la OPL	Servidores en nube son sólo los productivos y se justifica su uso.	**Aceptado**
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	Entrar y escanear y listando los diversos puertos de los activos del PREP para la cual debe existir la justificación de cada uno de ellos por parte de la OPL	Los puertos activos en los servidores son solo los necesarios.	**Aceptado**
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	Mediante escaneo vulnerabilidades obtener las vulnerabilidades de los activos (sistemas operativos y aplicaciones) relacionados con el PREP listando de por la criticidad especificada por el estándar CVSS	El escaneo arrojó vulnerabilidades sobre el servidor web y fueron compartidas con el IEES. Se cuentan con controles compensatorios.	**Aceptado**
SPV04 – El escaneo de servicios hechos a la infraestructura no debe tener explotaciones (exploits) desarrollados contra la infraestructura.	Revisar en los resultados del escaneo que no haya explotaciones publicadas contra las vulnerabilidades encontradas. De ser así se deberán listar y comprobar que estas son explotadas en los controles SPP	No se encontró ninguna explotación en los escaneos de la infraestructura.	**Aceptado**
SPV05 – Listar mediante un escaneo de los servidores WEB las vulnerabilidades que pueda haber en estos	Mediante escaneo de vulnerabilidades y/o software de tipo DAST (para pruebas dinámicas de seguridad de aplicación) obtener las vulnerabilidades de los servicios WEB	El escaneo arrojó vulnerabilidades sobre el servidor web y fueron compartidas con el IEES. Se cuentan con controles compensatorios.	**Aceptado**
SPV06 – EL sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado	Se confirmará que el sitio de publicación tenga un certificado válido y que el protocolo de SSL exista (El escaneo se hará desde Internet)	Se utiliza un certificado público para el sitio de publicación emitido por CLOUDFLARE y es válido.	**Aceptado**

Análisis Vulnerabilidades Infraestructura PREP

Resultados Preliminares Pruebas de Controles del Soporte Operativo			
Controles Especificados	**Pruebas ejecutadas**	**Comentarios**	**Resultado**
PRS01 – La OPL debe tener un manual de capacitación para el personal de captura	Verificar con la OPL la existencia de los manuales	Los manuales de capacitación si existen y es con lo que se tuvo las sesiones con los capturistas.	**Aceptado**
PRS02 – Debe haber un centro telefónico para consultas o dudas en los distintos procesos o módulos del PREP	Se revisará con la OPL la forma como se resuelven dudas o consultas en los distintos procesos del PREP	Hay un equipo que se encargará de soporte especializado el día de las elecciones y residirá en el COPREP.	**Aceptado**
PRS03 – Debe existir un proceso de resolución de inconsistencias al momento de captura de acta	Revisar con la OPL la existencia de dicha organización que permita resolver problemas de captura	Se cuenta con el módulo de verificación/validación MVEVAL.	**Aceptado**
PRS04 – Contratos de soporte externo en caso de eventualidades sobre las plataformas operativas que se utilizan en el PREP (para sistemas desarrollados por terceros)	Se deberá comprobar los contratos de soporte externo en caso de eventualidades en caso de que el sistema PREP haya sido elaborado por un tercero	Se cuentan con los contratos de soporte con Informática Electoral .	**Aceptado**
PRS05 – Tener los contratos con los proveedores de telecomunicaciones (primario y secundario) con los mapas de escalación de ellos para reportar eventos	Verificar con la OPL la existencia de contratos existentes con la matriz de escalación y tiempos de resolución por parte del proveedor de telecomunicaciones.	Los contratos se tienen con los proveedores TELMEX y METROCARRIER.	**Aceptado**
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)	Verificar con la OPL la existencia de contratos existentes con su matriz de escalación y tiempos estimados de resolución por parte del proveedor de nube (si se esta utilizando Nube como repositorio operativo del PREP)	Se tienen los contratos con los proveedores de nube y CLOUDFLARE para el manejo de contenido y protección de ataques volumétricos.	**Aceptado**
PRS07 – Tener la documentación del sistema PREP de la OPL actualizado y en resguardo por los encargados del área de tecnología de la OPL	Verificar con la OPL la existencia de dicho documento de arquitectura y modelación del sistema	Se verificó la existencia del documento actualizado.	**Aceptado**

Tecnológico de Monterrey

Pruebas DOS a PREP

Pruebas del PREP Digitalización (SPD)			
Controles Especificados	**Pruebas ejecutadas**	**Comentarios**	**Resultado**
SPN01 – La infraestructura debe soportar un ataque volumétrico TCP-SYN FLOOD	Se utilizo la herramienta LODDOS con la que se inyectará un tráfico de 3.5Gbps con 50 bots configurados para TCP-SYN FLOOD con una duración de 300ms (5 minutos) al sitio de web proporcionado	CLOUDFLARE con su red global de 67 Tbps es capaz de mitigar cualquier ataque volumétrico TCP-SYN FLOOD.	**Sustituida**
SPN02 – La infraestructura deberá soportar un ataque volumétrico por UDP-DNS Amplification.	Para evitar afectación al proveedor desde donde se origina el ataque hará una revisión de los DNS's públicos del siguiente modo: Se consultará el sitio https://www.dnsinspect.com Se deberá de verificar que la recursividad no esta habilitada	Se revisó el DNS que está ubicado en CLOUDFLARE para revisar si estaba habilitada la recursividad, se encontró que no está habilitado.	**Aceptado**
SPN03 – LA infraestructura deberá poder soportar un ataque volumétrico por ICMP – ICMP FLOOD	Se utilizo la herramienta LODDOS con la que se inyectará un tráfico de 3.5Gbps con 50 bots configurados para ICMP FLOOD con una duración de 300ms (5 minutos) al sitio de web proporcionado	CLOUDFLARE con su red global de 67 Tbps es capaz de mitigar cualquier ataque volumétrico ICMP FLOOD	**Sustituida**
SPN04 – La infraestructura deberá poder manejar un ataque en la capa de aplicación vía un SLOWLORIS attack	Se utilizo la herramienta LODDOS con la que se inyectará peticiones para establecer conexiones dejando abiertas para probar al respuesta del servidor.	Cloudflare con su red global de 67 Tbps es capaz de mitigar cualquier ataque tipo SLOWLORIS.. Todas las peticiones que recibe las pone en un buffer por lo que, en resultado, nunca llegan al origen, los servidores del OPL.	**Sustituida**
SPN05 – Validación de las cuotas de servicio configuradas en las subscripciones de servicios de nube (si aplica)	Se entrará a la consola bajo la subscripción de la OPL y verificará que haya una cuota de tráfico definida para propósitos de limitación de este a los servidores definidos	El IEES tiene contratado con CLOUDFLARE los servicios CDN, protección DOS y WAF para protección contra tráfico en exceso el cual se observa por sus características.	**Aceptado**
SPN06 – Revisar con la OPL la existencia de un plan o procedimiento a seguir en caso de evento de ataque de DOS	Verificar con el encargado de informática de la OPL que exista un manual de procedimiento a seguir en caso de un evento de ataque de negación de servicio.	El contrato existente, permite al IEES comunicarse a CLOUDFLARE como proveedor y solicitar apoyo en caso que la consola de gestión muestre algún tipo de ataque y/o tráfico sospechoso.	**Aceptado**
SPN07- Validar la existencia de contratos de servicio de protección de exceso de tráfico o para blindar contra ataques DOS	Verificar con los encargados de la OPL que existan contratos y/o servicios que ofrezcan protección contra ataques de DOS	Existe servicios de protección por medio de CLOUDFLARE como WAF para protección de ataques de tráfico .	**Aceptado**
SPN08 – Validar la existencia de un plan de comunicación hacia la comunidad en caso de eventos de DOS	Revisar con la OPL que exista un plan definido de comunicación hacia la comunidad que el área de comunicación pueda dar en caso de que se presentará este tipo de incidentes.	Se tiene definido comunicaciones en caso que sucediera un ataque de esta naturaleza.	**Aceptado**