Tecnológico de Monterrey

Auditoría del PREP 2021 - CEENL

Auditoría del PREP Comisión Estatal Electoral Nuevo Leon

Avance del proceso de auditoría del Programa Preliminar de Resultados Electorales 2021 para la Comisión Estatal de Nuevo Leon.

30 Mayo 2021

Agenda

La auditoría fue planteada en 7 distintas líneas de revisión y al día 30 de Mayo se tiene el siguiente estado

#	Línea Revisión	Estado	Comentarios
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
3	Entregables PenTest	Terminado	Para las vulnerabilidades presentadas no hay explotaciones definidas
4	Análisis Vulnerabilidades Infraestructura PREP	Terminado	Las vulnerabilidades encontradas son de nivel medio para abajo sin exploits conocidos
5	Pruebas DOS a PREP	Terminado	Pruebas sustituidas y aceptadas

Pruebas Caja Negra - Digitalización

Pruebas del PREP Digitalización (SPD)			
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	La aplicación se accede mediante usuario y contraseña en un ambiente cerrado (red privada)	**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	El usuario se bloquea después de 3 intentos y se controla la identidad mediante un gestor de identidad que se integra al servicio de autenticación.	**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 solicita bajo soporte al superior y se da hacia una mesa de apoyo para reinicialización de la clave	**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	La clave se casa con el teléfono y la aplicación de repositorio central para que no se firme en otro teléfono y no se pueda cambiar otro teléfono. El inventario se levantará hasta que se inicialicen todos los dispositivos por que se utilizará BYOD. El repositorio central gestiona la cantidad de teléfonos firmados, no permite adicionales (no se permite mas de 5 móviles con una cuenta)	**Aceptado**
SPD05 – Distribución de Aplicación controlada	Acceso a la aplicación debe ser controlada por un solo punto de contacto para su instalación	La aplicación es estándar, pero el usuario es de dominio con OKTA (dominio separado de la CEENL) y lleva sus caractetrísticas particulres (SPD04)	**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	Como el usuario de OKTA se casa con el telefono queda este como tercero de autentificaión… queda pendiente ver si se genera un certificado adicionl (ver certificado de app drobpox).	**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	En la prueba de escenarios llevada acabo el día 20/Abril/2021 se pudo verificar como el acta se sube mediante el equipo móvil. La sección 5.5 se detallan los distintos escenarios.	**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	El acta no es rechazada de origen, estas son discriminadas de forma centralizada y se hace en base a municipio y distrito local. Se comento que esta delimitación se puede modificar en caso que sea necesario digitalizarla desde otro origen	**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	En la prueba de escenarios llevada acabo el día 20/Abril/2021 se pudo verificar como el acta se puede verse en la Base de Datos ya escaneada	**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 acta se sube por la aplicación de DROPBPOX vía SSL (1.2 - verificar la versión de dropbox) El scanner sube por medio de un canal cifrado de SSL al repositorio de las 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 YA QUE EL ESCANER ES CONECTADO A UNA COMPUTADORA PARA ENVIAR LA IMAGEN Y SE CONTESTO EN EL **SPD10**	**No Aplica**
PD12 – Confirmación de integridad del cta digitalizada y guardada en la BD del REP	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	Se puede corroborar el HASH desde origen en el escáner contra el HASH del acta publicada en internet. Si la imagen se tiene que girar, por estar escaneada al revés, se calculara un nuevo HASH por el cambio en la orientación de la miágen.	**Aceptado**

Pruebas Caja Negra - Captura

Pruebas del PREP Digitalización (SPD)			
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 estos son del propio sistema SIPRE.	**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 bloquea en 3 intentos y se reinicializa por medio de mesa de servicio y es solicitado por el supervisor	**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	El 90% usa un SO en uso para la captura es PORTEUS. El 10% restante son computadoras de uso multiple para tener CATD y CCV al mismo tiempo en una windows (34 con windows y escaner y otros 8 con escanner y captura). Este 10% se maneja vía el MDM de Microsoft. Las cuentas estan dentrro del dominio de la CEENL. Las directivas y politicas son distintas a la CEENL. El sistema de captura se entra por VPN hacia la nube de AZURE para entrar al portal de captura.	**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.	los 9 ccv's son por cableado. En el resto del estado, hay estaciones por red inalámbrica. La conexión a los sistemas es por VPN	**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	El caso de PORTEUS no se permite hacer nada por que el mismo SO no lo permite. Para el caso de los windows, las políticas se centralizan vía INTUNE. Se van a distribuir 100 celulares con respaldo de Internet y/o scanner (traen el app de onedrive) y todos vienen con INTUNE	**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 filtrado de contenido se lleva acabo por las políticas de INTUNE y el software de antimalware del equipo de computo. En el caso de las estaciones con PORTEUS no se tiene acceso a Internet mas que a la red del sitio privado de captura. Adicionalmente la red filtra vía MERAKI todos los sitios de Internet	**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	La red filtra todos los sitios a Internet (no permite ninguno) solamente el de captura en todas las estaciones (es configuracióna nivel red)	**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 CD/CDROM en la estación de captura del PREP	El 90% de las estaciones con PROTEUS no tienen acceso a medios externos. El SO no lo permite En el caso del 10% en Windows se controla el acceso a medios externos vía INTUNE. Por política el uso de USB se puede habilitar por continuidad (que pasa si se quedan sin internet, ddeben poder sacar las fotos vía USB para lelvarlo a otro lado)... de cualquier manera se íde autorización a la mesa de soporte para habilitar que puedan subir las fotos vía USB	**Aceptado**
ᵖC09 – Portal de captura al que acceden s estaciones de captura, deberá ser un ɔrtal 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	Tiene certificados generados internamente, estos sitios no están publicos	**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 corrió el ejercicio de captura para algunas actas y se verificaron los campos y módulos de captura para de actas en el sistema informático PREP	**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	Se validó en la plataforma que se tienen todos los campos requeridos para la captura de la AEC	**Aceptado**
	ID Acta PREP • Entidad Federal • Distrito Electoral • Sección • Tipo • Número casilla • Municipio	Los datos existen como parte del sistema PREP	**Aceptado**
	Votos Obtenidos • Votos obtenidos por Partido y candidatos independientes		
	Votos • Total, votos • Votos nulos • Votos par candidatos no registrado		
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.		

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	Los resultados se presentan bajo requerimiento con 4 decimales (diezmilésima)	**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	Se baja el archivo en formato ZIP que contiene los archivos de captura en formato CSV para cargarse en hoja de calculo como se indica.	**Aprobado**
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 pudo confirmar la existencia de los datos a publicar en el portal.	**Aprobado**
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 confirmo la existencia de los elementos del portal para navegación	**Aprobado**
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 confirmo la existencia de los elementos del portal para navegación	**Aprobado**

Pruebas Caja Negra – Datos Publicación

Pruebas del PREP Digitalización (SPD)			
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 pudo confirmar la existencia del menú colapsable en el portal de WEB sobre la izquierda del portal	**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 Cl0udadana c) Indicador del Corte d) Boton Actualizar	Se verifico la sección de Avance entidad con sus distintos elementos	**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) Boton de Consulta d) Aviso Privacidad	Se verifico el área de resultados tu casilla para búsqueda los cuales incluyen los elementos mencionados para la búsqueda.	**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 la existencia de la sección de Estadística Entidad con los elementos mencionados publicados.	**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	Se verifico la existencia de los elementos en la sección del footer	**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	Se verifico en un celular ANDROID (MOTO g(7) plus) el funcionamiento del portal móvil con las secciones requeridas	**Aceptado**

Pruebas Caja Negra – Datos Publicación

Pruebas del PREP Digitalización (SPD)			
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	Se verifico en un celular ANDROID (MOTO g(7) plus) el funcionamiento del portal móvil con el logo y colores indicados de imagen así como el menú desplegable	**Aprobado**
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	Se verifico en un celular ANDROID (MOTO g(7) plus) el funcionamiento del portal móvil con las distintas secciones mencionadas	**Aprobado**
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 a) Consultar b) Aviso de privacidad al consltar c) Flecha de regreso	Se verifico en un celular ANDROID (MOTO g(7) plus) la sección de Mi Casilla con los requerimientos mencionados	**Aprobado**
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 verifico en un celular ANDROID (MOTO g(7) plus) la existencia de la sección del avance de entidad con los elementos requeridos	**Aprobado**
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	Se verifico en un celular ANDROID (MOTO g(7) plus) los distintos elementos en la sección de consulta de votación la cual incluye todos los mencionados	**Aprobado**
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	Se verifico en un celular ANDROID (MOTO g(7) plus) los elementos de la sección de Estadística Entidad los cuales están incluidos todos	**Aprobado**
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 verifico en un celular ANDROID (MOTO g(7) plus) los elementos del pie de página que están ubicados correctamente.	**Aprobado**

Pruebas Caja Negra – Casos de Uso

Prueba Funcional Definida (PFD) Escenario – Gobernatura			
Controles Especificados	**Casos de Uso (Escenarios PREP)**	**Criterio Aceptación**	**Resultado**
PFD – 01	Gobernatura – 1	Acta se digitaliza con escáner, se capturo 2 veces, al coincidir, se publica.	**Aceptado**
PFD – 02	Gobernatura – 2	Acta se digitaliza con móvil, se capturo 2 veces, al coincidir, se publica.	**Aceptado**
PFD – 03	Gobernatura – 3	Acta se digitaliza con escáner, se capturo 2 veces, al no coincidir, se pasa a ME para verificar, se corrige y publica	**Aceptado**
PFD – 04	Gobernatura – 4	Acta se digitaliza con escaner, QR dañado, se identifica manualmente y se captura correctamente 1ª y 2ª y se publica	**Aceptado**
PFD – 05	Gobernatura – 5	Acta fuera de catalogo sin sección o casilla. Se captura solo el dato del formato con el lo que incluya y es publicado	**Aceptado**
PFD – 06	Gobernatura – 6	Formato con elección, (sin acta) se forza capturar casillas de G1pero sin sección o casilla. Se corrige en ME y publica	**Aceptado**

Tipo de Elección	No	Tipo Acta PREP	Supuestos de digitalización		Supuestos de identificación				Supuestos de Captura/Verificación			Supuesto de inconsistencia							
		AEC	Escáner	Móvil	QR	Manual Id.	Manual Falta.	Manual Dupl.	C1 = C2	C1 / C2	Verif.	Sin inconsistencia	Todos ilegibles	Todos sin dato	Algún ilegible	Algún sin dato	Excede LN	Sin acta	Fuera de catálogo
Gubernatura	1	X	X		X				X			X							
	2	X		X	X				X			X							
	3	X	X		X					X		X							
	4	X	X			X			X			X							
	5	X	X				X		X										X
	6	X	X					X	X									X	

Pruebas Caja Negra – Casos de Uso

Prueba Funcional Definida (PFD) Escenario – Diputaciones			
Controles Especificados	**Casos de Uso (Escenarios PREP)**	**Criterio Aceptación**	**Resultado**
PFD – 07	Diputaciones – 1	Todos los campos vienen ilegibles por lo que se capturan con (i) 2 veces, se pasa a verificación y se publica	**Aceptado**
PFD – 08	Diputaciones – 2	Todos los campos vienen en blanco por lo que se capturan com (b) indicando en blanco 2 veces, se pasa verificación y se publica	**Aceptado**
PFD – 09	Diputaciones – 3	Se capturan los datos con valores y los que estén ilegibles se capturan con (i) indicando ilegible. Se capturan 2 veces y se publica	**Aceptado**
PFD – 10	Diputaciones – 4	Se capturan los datos con valores y los que estén en blancos se capturan con (b) indicando en blanco. Se capturan 2 veces y se publica	**Aceptado**
PFD – 11	Diputaciones – 5	Los datos exceden la lista nominal por lo que se captura, pero no se contabiliza y se publica.	**Aceptado**
PFD – 12	Diputaciones – 6	Las dos capturas se equivocan en el mismo dato y se identifica en la verificación. Se corrige y se publica	**Aceptado**

Tipo de Elección	No	Tipo Acta PREP	Supuestos de digitalización		Supuestos de identificación				Supuestos de Captura/Verificación			Supuesto de inconsistencia							
		AEC	Escáner	Móvil	QR	Manual Id.	Manual Falta.	Manual Dupl.	C1 = C2	C1 / C2	Verif.	Sin inconsistencia	Todos ilegibles	Todos sin dato	Algún ilegible	Algún sin dato	Excede LN	Sin acta	Fuera de catálogo
Diputaciones	1	X	X		X				X				X						
	2	X	X		X				X					X					
	3	X	X		X				X						X				
	4	X	X		X				X							X			
	5	X	X		X				X								X		
	6	X		X	X				X		X	X							

Pruebas Caja Negra – Casos de Uso

Prueba Funcional Definida (PFD) Escenario – Ayuntamientos			
Controles Especificados	**Casos de Uso (Escenarios PREP)**	**Criterio Aceptación**	**Resultado**
PFD – 13	Ayuntamientos – 1	Acta se digitaliza con móvil, se capturo 2 veces, al coincidir, se publica.	**Aceptado**
PFD – 14	Ayuntamientos – 2	Los campos ilegibles se capturan con (i) para clasificarlos como ILEGIBLES	**Aceptado**
PFD – 15	Ayuntamientos – 3	Los campos en blanco se capturan con (b) para clasificarlos como en BLANCO, como no coinciden valores, se pasa a ME y se publica	**Aceptado**
PFD – 16	Ayuntamientos – 4	Acta se digitaliza con escáner, se capturo 2 veces, al coincidir, se publica.	**Aceptado**
PFD – 17	Ayuntamientos – 5	Acta se digitaliza con móvil, se capturo 2 veces, al coincidir, se publica.	**Aceptado**
PFD – 18	Ayuntamientos – 6	Formato “Sin Acta” se captura bajo esa clasificación	**Aceptado**

Tipo de Elección	**No**	**Tipo Acta PREP**	**Supuestos de digitalización**		**Supuestos de identificación**				**Supuestos de Captura/Verificación**			**Supuesto de inconsistencia**							
		AEC	**Escáner**	**Móvil**	**QR**	**Manual Id.**	**Manual Falta.**	**Manual Dupl.**	**C1 = C2**	**C1 / C2**	**Verif.**	**Sin inconsistencia**	**Todos ilegibles**	**Todos sin dato**	**Algún ilegible**	**Algún sin dato**	**Excede LN**	**Sin acta**	**Fuera de catálogo**
Ayuntamientos	**1**	X		X	X				X			X							
	2	X	X		X				X						X				
	3	X	X		X					X						X			
	4	X	X		X				X			X							
	5	X		X	X				X			X							
	6	X	X			X			X									X	

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	El proceso se encuentra como parte del código el cual se corre cada 10 minutos generando una firma digital por segmento de código y almacenando esta en un archivo para posteriormente generar una firma digital del archivo que contiene todas las firmas. Es un Hash de Hashes en SHA256.	**Aceptada**
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	El procedimiento para reinicio de la base de datos, se hace mediante un módulo en la administración de la aplicación del PREP en donde se genera una jornada de trabajo la cual reinicia el sistema. La comprobación se hace presentando la consola de la base de datos mostrando esta vacía en el momento de inicio de la jornada electoral	**Aceptada**

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 administra desde la nube, por ser equipos del fabricante MERAKI. El filtrado, acceso y uso de puertos va de acuerdo a mejores prácticas así como el diseño jerárquico de la red.	**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 que se usan son MERAKI se acceden vía consola web cifrado SSL. El sitio requiere MFA vía celular para accederlo	**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 sistemas operativos de los equipos de red están bajo soporte	**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	Los equipos tienen soporte del proveedor	**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 instalados en los CCV's hasta 3 proveedores de comunicaciones. Dos en redundancia automática y un tercero manual	**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.	Se tiene instalados UPS's con duración de 4hrs para continuar la operación.	**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	Los activos están habilitados con funciones de bitácora para trazabilidad de acciones.	**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	Se tendrá un sistema de control donde se monitorea el funcionamiento de red, servidores y estaciones de captura	**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	Si las hay y las tienen los supervisores para movilidad en el soporte. El acceso a esta esta restringido	**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	La infraestructura de la comisión esta separada de la del PREP. Los equipos y enlace son distintos.	**Aceptado**
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*	Los sistemas son de uso exclusivo del PREP	**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	Los accesos están controlados por personas que requieren identificación de acceso.	**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.	Las estaciones de captura están con acceso limitado habiendo personal verificando la entrada de personal a las instalaciones mediante identificación y gafete de capturista	**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	Los teléfonos móviles están dados de alta mediante el sistema INTUNE como MDM el cual los tiene inventariados y controlados para su uso.	**Aceptado**

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	La infraestructura de la CEENL se encuentra hosteada en los servicios de AZURE de Microsoft y algunos de estos se adquirieron como servicios por lo que no se escanean. Solo se escanearon los servidores que están operando como parte de la solución. Se listaron servidores de WEB para captura (servidores internos). La infraestructura restante, se compro como SaaS por lo que no es escaneable ya que son servicios	**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 únicos puertos detectados son el 443 para SSL	**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	Se detecto una vulnerabilidad en los servicios de WEB que fue ya compartida hacia el equipo del CEENL respecto a la posibilidad de inyección de SQL sobre servidores de WEB Se requiere modificar dicha versión y/o agregar controles para quitar esta vulnerabilidad	**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	Fuera de la vulnerabilidad encontrada de inyección de SQL, no hay otra que sea explotable	**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	Solo se encontró la vulnerabilidad de Inyección de SQL. Las BD y DNS's no se pueden escnear ya que son SaaS por lo que se adquirieron como servicios de AZURE donde esta montada la aplicación de PREP.	**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)	Los sitios internos tienen certificados hechos de forma interna. El sitio público tendrá un certificado público reconoible.	**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	Se reviso el manual con el equipo de la CEENL y se verifco la capacitación que se proporciona con el manual	**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	El centro se establecerá en las oficinas centrales de la CEENL	**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 le denomina la Mesa Especializada para resolución de dudas sobre las capturas	**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 tiene contrato de soporte con: MIGESA para soporte de Microsoft PLANNET para soporte de CISCO TrustNet para soporte de DropBox	**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.	Se nos compartió los accesos que tienen hacia tres proveedores, donde dos se configuran en automático y un tercero es manual. Los documentos muestran el proceso de escalación del proveedor, en caso de incidentes.	**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)	Los contratos con el proveedor de nube (Microsoft) para AZURE soporte pro-direct y aparte se tiene contrato con MIGESA para soporte local.	**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	Los contratos con proveedores	**Aceptado**

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 realizará una inundación de tráfico al sitio de publicación mediante el uso de hping: `root@kali:~# hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source <Sitio_Prueba>`	La nube de AZURE prohibe hacer ataques de DOS y DDOS en su infraestructura: https://docs.microsoft.com/en-us/azure/security/fundamentals/pen-testing La prueba requerida de TCP-SYN Flood es un ataque deprotocolo https://docs.microsoft.com/en-us/azure/ddos-protection/types-of-attacks	**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:
	1. Se consultará el sitio https://openresolver.com
	Se escaneará el DNS para verificar que la recursividad está habilitada
	Usando el software NMAP para hacer el escaneo al DNS mediante el comando:
	`nmap -sU -p 53 -sV -P0 --script "dns-recursion" x.x.x.x <x.x.x.x` siendo la dirección del servidor de DNS>. Esto deberá arrojar un resultado similar al siguiente:
	`PORT STATE SERVICE VERSION`
	`53/udp open domain ISC BIND "version"`
	`*|_dns-recursion: Recursion appears to be enabled*`
		La nube de AZURE prohibe hacer ataques de DOS y DDOS en su infraestructura: https://docs.microsoft.com/en-us/azure/security/fundamentals/pen-testing
		
		Se reviso el DNS que esta ubicado en AZURE para revisar si estaba habilitada la recursividad, se encontró que no esta habilitad
			Aceptado

SPN03 – LA infraestructura deberá poder soportar un ataque volumétrico por ICMP – ICMP FLOOD	El ataque se hace utilizando el comando hping3 seleccionando la opción de flood `root@kali:~# hping3 --flood --rand-source --icmp -p 80 (direccion_IP)`	La nube de AZURE prohibe hacer ataques de DOS y DDOS en su infraestructura: https://docs.microsoft.com/en-us/azure/security/fundamentals/pen-testing La prueba requerida de ICMP-Flood es un ataque deprotocolo https://docs.microsoft.com/en-us/azure/ddos-protection/types-of-attacks	**Sustituida**
SPN04 – La infraestructura deberá poder manejar un ataque en la capa de aplicación vía un SLOWLORIS attack	se hará con la herramienta **`slowhttptest`** la cual se puede configurar para generar este tipo de conexiones incompletas `root@kali:~# slowhttptest -c 1000 -H -g -o Trafico_slowloris -i 10 -r 200 -t GET -u http://sitio.remoto.mx -x 24 -p 3`	AZURE como portal ofrecen protección contra distintos tipos de ataques de protocolo: https://docs.microsoft.com/en-us/azure/ddos-protection/types-of-attacks La prueba requerida de SLOWLORIS es de aplicación	**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 esquema de protección de azure para DOS/DDOS solo permite configuración básica y estándar y no permite configuración de cuotas de tráfico. https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview	**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.	Se valido la existencia del plan de seguridad para la CEENL el cual se definen los principios de seguridad así como las acciones a realizar en caso de incidentes de seguridad, incluyendo ataques de negación de servicio	**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	El contrato existente de AZURE existe con Microsoft. Se valido en el análisis de infraestructura https://docs.microsoft.com/en-us/azure/ddos-protection/manage-ddos-protection El plan de servicio de protección DDOS es por subscripción y se dará al inicio de junio, ya que el plan es mensual.	**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.	El plan de reacción se detalla en el plan de seguridad para realizar comunicación en caso de ser necesario	**Aceptado**