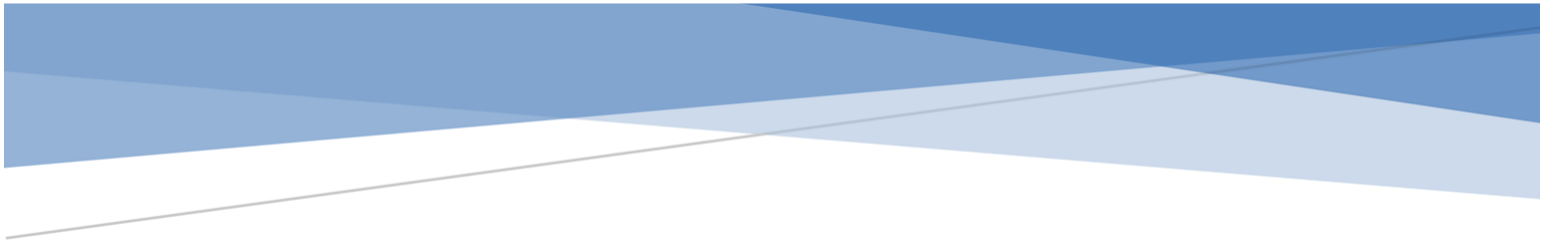

Tecnológico de Monterrey

Informe de Pruebas al Sistema Informático del PREP

Informe sobre las pruebas ejecutadas sobre el sistema informático del IEPC Guerrero al 5 de junio de 2021

Descripción breve

Este documento contiene el resultado final de cada una de los resultados y observaciones identificadas en la revisión y pruebas del sistema como parte de los servicios de auditoría de seguridad para el IEPC Guerrero

Ignacio Cendejas
Marco Otilio Peña
Gualberto Aguilar
Jesús R. González
coord_audit_prep@servicios.tec.mx
Juan Arturo Nolazco
jnolazco@itesm.mx

1 Introducción

Este documento presenta los resultados finales de las pruebas hechas al sistema de captura de actas para las elecciones del 2021 para el **IEPC Guerrero**, la auditoría se condujo sobre 5 líneas de revisión

Línea Revisión	Estado	Observaciones
Pruebas Caja Negra	Terminado	Las funcionalidades del sistema PREP, en sus distintas fases (digitalización, captura y publicación), se cumplieron con observaciones en los requerimientos de seguridad, así como los de funcionalidad
Validación Sistema Informático e Integridad PREP y BD	Terminado	Se revisaron los procesos de reinicio de BD, proceso de generación de llave de integridad faltará ejecutarse en su momento.
Entregables Pentest	Terminado	Para las vulnerabilidades presentadas, se declara que se aceptan los riesgos con las acciones especificadas por el IEPC
Análisis Vulnerabilidades Infraestructura PREP	Terminado	Las vulnerabilidades encontradas son de nivel medio para abajo, para los CATD, se declara que se los riesgos se aceptan al ser un sistema privado, cerrado, controlado sin acceso desde el exterior
Pruebas DOS a PREP	Terminado	Pruebas no realizadas por términos de servicio de proveedor. Se tiene contrato de protección contra DOS por parte del proveedor.
Informe Jornada PREP	Pendiente	

2 Criterios utilizados para la auditoría

Cada prueba puede tener uno de tres tipos de resultados que pueden ser los descritos en la tabla siguiente

Resultado Prueba	Descripción de Criterio	Acciones
Aceptado	La prueba cumplió satisfactoriamente con los criterios de aceptación	Prueba es aceptada y se da por cerrado el inciso de esta prueba. De ser necesario ejecutar el plan de nuevo en otra iteración, esta prueba no se volverá a ejecutar.
Rechazado	La prueba no cumplió con los criterios de aceptación	La prueba no es aceptada, se documenta el resultado y recomendaciones. Esta prueba se volverá a ejecutar en la siguiente iteración para revisar la implementación de las recomendaciones dadas en el resultado de las pruebas.
Aceptado con Observaciones	La cumplió con una parte de los criterios o cumplió totalmente con observaciones.	Prueba es aceptada, pero con recomendaciones. Esto significa que las recomendaciones son solo eso, no serían obligatoria su implementación y solo queda como sugerencia o recomendación.

Cada una de las pruebas a ejecutar, tiene su criterio propio. En el caso de un cumplimiento, la prueba se da por pasada y no vuelve a ejecutarse en una siguiente iteración, de ser el caso.

3 Metodología para clasificar los hallazgos

Los hallazgos que se hagan en las pruebas se clasificarán basado en el Open Web Application Security Protect Mobile (OWASP-Mobile). Esta metodología representa un consenso a nivel desarrolladores sobre los riesgos más críticos para las aplicaciones.

Es importante notar que la prueba es sobre funcionalidad a caja negra, por lo que no se está evaluando a detalle el código ni librerías, por lo que parte de los 10 riesgos para programación de móvil, posiblemente no apliquen.

4 Pruebas de Caja Negra

En esta sección se encuentran los resultados con los comentarios dados, si es que los hubo, durante la ejecución de pruebas y el resultado obtenido en base a los criterios de aceptación.

4.1 Pruebas PREP Digitalización

Pruebas del Proceso Publicación de Resultados (PPR)				
Controles Especificados	**Pruebas ejecutadas**	**Criterio de Aceptación**	**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 de digitalización tiene un acceso controlado por usuario/contraseña		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	Después de 5 intentos máximo, deberá bloquearse el usuario que intenta acceder	Se hace la prueba directamente en dispositivo, después de 5 intentos fallidos se bloquea de manera temporal	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	El cambio se hará en una mesa de servicio que atienda estos requerimientos	Se requiere llevar dispositivo físico a mesa de servicio	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 OPL deberá tener un sistema central de inventario de teléfonos con la aplicación en uso	Se muestra evidencia de inventario de teléfonos y asignaciones	Aceptado
SPD05 – Distribución de Aplicación controlada	Acceso a la aplicación debe ser controlada por un solo punto de contacto para su instalación	La aplicación deberá estar manejada centralmente y no distribuida públicamente	La instalación de la aplicación se realiza de manera manual en cada uno de los dispositivos	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	Equipo móvil debe contar un tercer factor, adicional al usuario y contraseña; para firmarse en la aplicación y/o red para escanear actas.	Se utiliza ID generado por API de Android para validar contra inventario de dispositivos autorizados, al momento de iniciar se muestra ID	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 deberá marcar como aceptada y subida. Se podrá verificar en la BD en uso del PREP		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 deberá ser rechazada e indicar que no corresponde a su asignación	El acta se puede digitalizar en con tipo de acta equivocada, se tiene homologado el procedimiento de respuesta en el CATD, falta reforzar su aplicación	Aceptado con observaciones
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	verificar en la BD en uso del PREP		Aceptado

SPD10 – Transmisión cifrada del acta digitalizada hacia el repositorio o BD del PREP (MÓVIL)	Verificar el protocolo de comunicaciones usado por la aplicación móvil para transmitir la imagen	La transmisión del archivo deberá darse por SSL (TLS1.2 o mayor) o vía IPSEC. Para el caso del móvil puede darse vía Wifi o datos del servicio celular contratado	Se utiliza URL cifrado con certificado SSL verificado	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*	La transmisión del archivo deberá darse por SSL (TLS1.2 o mayor) o vía IPSEC Para Escáner debe ser conexión por cable (no Wifi)	Escáner conectado directamente	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	El hash o llave generada debe coincidir entre el archivo escaneado y el guardado en la BD	Hash se confirma en base de datos CSV	Aceptado

4.2 Pruebas PREP Captura

Pruebas del Proceso Publicación de Resultados (PPR)				
Controles Especificados	**Pruebas ejecutadas**	**Criterio de Aceptación**	**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	La estación de captura deberá requerir usuario/contraseña para accederlo y no debe ser compartido el usuario.		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	Después de 5 intentos máximo, deberá bloquearse el usuario que intenta acceder a la estación de captura	Aplicación se bloquea después de 5 intentos	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 esté descontinuada por el fabricante	La versión debe estar dentro de las versiones soportadas por el fabricante del sistema operativo	Se tiene última versión de sistema operativo CentOS 8 Stream	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.	Las estaciones de captura deberán estar interconectadas físicamente por cableado		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	El usuario de captura no podrá modificar variables ni		Aceptado

	modificar configuraciones del ambiente o del sistema operativo	configuraciones de la estación de captura.		
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	Las estaciones de captura no tendrán acceso a Internet.		Rechazado
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	El usuario no debe tener acceso a otra aplicación que no sea la de captura definida por la OPL	Se tiene acceso a aplicaciones no críticas sin afectación a proceso PREP	Aceptado, con observaciones
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	La estación de captura no reconocerá el USB y no permitirá la conexión a este La estación de captura no deberá aceptar el CD/CDROM en la estación.		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 servidor donde se capture la información deberá contar con un certificado y tener habilitado el cifrado SSL (TLS1.2 al menos)	El portal de captura es solo accesible desde la red local	Aceptado

4.3 Pruebas Captura Datos en Cumplimiento requerimientos INE

Las siguientes pruebas están alineadas a los requerimientos mínimos del INE en cumplimiento a los anexos del Reglamento de Elecciones actualizado al 26 de febrero del 2021

Pruebas de Captura de Datos en sistema PREP en Cumplimiento Requerimientos del INE				
Controles Especificados	**Pruebas ejecutadas**	**Criterio de Aceptación**	**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	Debe haber visualización del acta para su captura en la plataforma del 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 **ID Acta PREP** ● Entidad Federal **Boletas** ● Boletas Sobrantes	Los datos mencionados deberán tener campo de captura para que puedan ser adquiridos durante el proceso de captura.		Aceptado

	• Distrito Electoral • Sección • Tipo • Número casilla • Municipio	• Personas que votaron • Representantes Partidos políticos e independientes acreditados que votaron • Total, votos sacados de urna			
	Votos Obtenidos • Votos obtenidos por Partido y candidatos independientes				
	Votos • Total, votos • Votos nulos • Votos por candidatos no registrado	**Acta** Imagen del acta			

Pruebas de Captura de Datos en sistema PREP en Cumplimiento Requerimientos del INE				
Controles Especificados	**Pruebas ejecutadas**	**Criterio de Aceptación**	**Comentarios**	**Resultado**
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.	Los datos deberán estar siendo calculados para su publicación		Aceptado

4.4 Pruebas Datos Que Publicar

Los datos se deberán publicar en el sitio oficial, de donde se distribuirán a los sitios replicantes de información oficial deben contener los siguiente

Pruebas del Proceso Publicación de Resultados (PPR)				
Controles Especificados	**Pruebas ejecutadas**	**Criterio de Aceptación**	**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 cálculo se realizó correctamente	La publicación esté dada a 4 dígitos sin redondearse		Aceptado
PPR02 – El portal debe tener la liga para poder bajar los datos en formato .CSV para cargarlos en hojas 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	Que el archivo exista, coincida y pueda cargarse en la hoja de calculo	Se tiene un retraso aproximado de 20 minutos para la muestra de último corte, durante ese periodo, se muestra el error. **Not Found** **The requested URL was not found on this server.**	Aceptado, con observaciones
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 con la estructura establecida por el Instituto, y	Estos valores deberán estar incluidos en el portal de publicación del PREP de la OPL bajo auditoría.	Se tienen problemas de comunicación por causas geográficas o climáticas entre algunos CATD y el sitio centralizado de publicación/difusión. Un porcentaje pequeño de actas capturadas por medio de la aplicación móvil no se mostraron en el último simulacro. Para una parte de las actas, se tiene un retraso para el despliegue de la digitalización, durante ese tiempo se muestra un error de archivo no encontrado. La descarga de base de datos en formato CSV tiene un retraso aproximado de 20 minutos contra el corte relacionado, durante ese tiempo se muestra error de descarga.	Aceptado, con observaciones

	j) Hash o código de integridad obtenido a partir de cada imagen de las Actas PREP, con el estándar definido por el Instituto.			

Pruebas del Proceso Publicación de Resultados (PPR)				
Controles Especificados	**Pruebas ejecutadas**	**Criterio de Aceptación**	**Comentarios**	**Resultado**
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)	Los elementos deberán existir dentro del portal siguiendo los lineamientos y guías establecidos por el 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) Botón de regreso a inicio f) Acceso directo a pestañas por elección g) Acceso a la Base de datos	Los elementos deberán existir dentro del portal con los colores y guías que se establecen en el anexo de este documento		Aceptado
PPR06 – Requerimientos de portal WEB para publicación – Menú Colapsable	Entrar a la página de publicación de la OPL y moverse 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	Los elementos deberán existir dentro del portal con los colores y guías que se establecen en el anexo de este documento		Aceptado

Pruebas del Proceso Publicación de Resultados (PPR)				
Controles Especificados	**Pruebas ejecutadas**	**Criterio de Aceptación**	**Comentarios**	**Resultado**
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) Botón Actualizar	Los elementos deberán existir dentro del portal con los colores y guías que se establecen en el anexo de este documento		Aceptado
PPR08 – Requerimientos de portal WEB para publicación – Resultados Tu Casilla	En el portal, el usuario consultará resultados de la casilla de su interés con los siguientes elementos a) Signo Interrogación b) Campo de Sección c) Campo Primer Apellido d) Botón de Consulta e) Aviso Privacidad	Los elementos deberán existir dentro del portal con los colores y guías que se establecen en el anexo de este documento		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	Los elementos deberán existir dentro del portal con los colores y guías que se establecen en el anexo de este documento		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	Los elementos deberán existir dentro del portal con los colores y guías que se establecen en el anexo de este documento		Aceptado

Pruebas del Proceso Publicación de Resultados (PPR)				
Controles Especificados	**Pruebas ejecutadas**	**Criterio de Aceptación**	**Comentarios**	**Resultado**
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 d) Encabezado e) Menú izquierdo colapsable. f) Avance de Entidad	Los elementos deberán existir dentro del portal con los colores y guías que se establecen en el anexo de este documento	El menú colapsable está del lado derecho	Aceptado, con observaciones
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	Los elementos deberán existir dentro del portal con los colores y guías que se establecen en el anexo de este documento		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 d) Centro Ayuda e) Tema y tamaño caracter	Los elementos deberán existir dentro del portal con los colores y guías que se establecen en el anexo de este documento	"Mi casilla" se encuentra dentro de la opción "Avance entidad" "Preguntas frecuentes" y "Centro de ayuda" se encuentran en pie de página Faltan tema y tamaño de carácter El portal móvil es un sitio *responsivo*	Aceptado con observaciones
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	Los elementos deberán existir dentro del portal con los colores y guías que se establecen en el anexo de este documento	"Mi casilla" se encuentra dentro de la opción "Avance entidad" Faltan elementos **b**, **c**, **e** y **f**	Aceptado con observaciones

Pruebas del Proceso Publicación de Resultados (PPR)				
Controles Especificados	**Pruebas ejecutadas**	**Criterio de Aceptación**	**Comentarios**	**Resultado**
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) Actas capturadas b) Participación Ciudadana c) Último corte d) Botón actualizar	Los elementos deberán existir dentro del portal con los colores y guías que se establecen en el anexo de este documento		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	Los elementos deberán existir dentro del portal con los colores y guías que se establecen en el anexo de este documento		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	Los elementos deberán existir dentro del portal con los colores y guías que se establecen en el anexo de este documento		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	Los elementos deberán existir dentro del portal con los colores y guías que se establecen en el anexo de este documento	Faltan elementos a y f.	Aceptado, con observaciones

4.5 Casos de Uso

Estos casos de uso se probaron sobre ambiente controlado de pruebas en red local (pruebas de laboratorio)

Pruebas del Proceso Publicación de Resultados (PPR) Escenario – Gobernatura				
Controles Especificados	**Casos de Uso (Escenarios PREP)**	**Criterio de Aceptación**	**Comentarios**	**Resultado**
PFD – 01	Gobernatura – 1	C1 y C2 coinciden	Sin comentarios.	Aceptado
PFD – 02	Gobernatura – 2	C1 o C2 igual a C3	Sin comentarios.	Aceptado
PFD – 03	Gobernatura – 3	C1 y C2 coinciden	Sin comentarios.	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	C1 o C2 igual a C3		Aceptado
PFD – 05	Diputaciones – 1	Captura en aplicación móvil, C1 y C2 coinciden	Prueba realizada en red local de pruebas preliminares, captura sale rotada 90 grados	Aceptado
PFD – 06	Diputaciones – 1	Captura en aplicación móvil, C1 o C2 coinciden con C3	Prueba realizada en red local de pruebas preliminares	Aceptado

Pruebas del Proceso Publicación de Resultados (PPR) Escenario – Ayuntamientos				
Controles Especificados	**Casos de Uso (Escenarios PREP)**	**Criterio de Aceptación**	**Comentarios**	**Resultado**
PFD – 07	Ayuntamientos – 1	Captura en aplicación móvil, no coinciden las 3 capturas, se turna a CCV para resolución	Prueba realizada en red local de pruebas preliminares	Aceptado
PFD – 08	Ayuntamientos – 2	Captura en aplicación móvil, C1 coincide con C2	Prueba realizada en red local de pruebas preliminares	Aceptado
PFD – 09	Ayuntamientos – 3	No coinciden las 3 capturas, se turna a CCV para resolución	Sin comentarios.	Aceptado

5 Validación Sistema Informático e Integridad PREP y BD

Al momento de presentación de este reporte no se ha realizado la verificación de código a través de hash debido a modificaciones en configuración y código para subsanar observaciones sobre el último simulacro.

La base de datos se mostró en ceros para el sitio de difusión durante el último simulacro. El IEPC declara que el proceso de puesto en cero de la base de datos empieza en los CATD y luego se refleja en el sitio principal, por lo que, si el sitio principal se muestra en ceros, significa que los CATD están en ceros también.

6 Pruebas sobre infraestructura de CATD

Se hicieron pruebas sobre 6 CATD. La configuración de todos y cada uno de los CATD es similar, por lo que los resultados presentados aplican a todos los CATD analizados.

Dado que la configuración de las computadoras en cada CATD es idéntica, las herramientas Medusa, Zap y OpenVAS se ejecutan sobre una máquina seleccionada aleatoriamente, con el entendido de que los resultados aplican a todas las computadoras.

Teniendo conexión directa a la red local de cada CATD se corrieron las siguientes pruebas:

- Detección de puertos de red abiertos
- Vulnerabilidad de contraseñas
- Vulnerabilidad de aplicación web

Se hacen escaneos de vulnerabilidad sobre la aplicación web de acopio, digitalización, captura y validación utilizando la herramienta ZAP. Se reportan vulnerabilidades de criticidad alta y media. Todas las vulnerabilidades encontradas son solventables por medio de configuración y actualización. Se recomienda atacar las vulnerabilidades medias y altas por medio de aplicación de las configuraciones y actualizaciones adecuadas.

Acción tomada por IEPC: No aplica, se declara que es un sistema privado, controlado, cerrado y sin acceso del exterior. Se declara aceptación de riesgo.

Vulnerabilidades de sistema operativo

Se hacen escaneos de vulnerabilidades sobre el sistema operativo anfitrión de una computadora del centro de acopio. Se reportan vulnerabilidades de criticidad alta y media. Todas las vulnerabilidades encontradas son solventables por medio de configuración y actualización. Se recomienda atacar las vulnerabilidades medias y altas por medio de aplicación de las configuraciones y actualizaciones adecuadas.

Acción tomada por IEPC: No aplica, se declara que es un sistema privado, controlado, cerrado y sin acceso del exterior. Se declara aceptación riesgo.

6.1 Pruebas sobre infraestructura de sistema de difusión en nube

Se hicieron pruebas sobre la dirección IP pública disponible. Se reportan vulnerabilidades de criticidad alta y media.

Vulnerabilidades encontradas en servidor de nube

Acción tomada por IEPC: Se endurece versión específica de servidor Web Apache y se declara que el riesgo de falla por configuración o funcionalidad por cambio de versión es mayor que el riesgo de explotación.

Otras vulnerabilidades encontradas

Acción tomada por IEPC:

- Se configura certificado de seguridad en dominio https://prep2021-gro-opl.mx/
- IEPC declara que listado de carpetas se deshabilitará para jornada electoral

7 Análisis Vulnerabilidades Infraestructura PREP

En esta sección se presenta un resumen, en función de los resultados y revisión de hallazgos, da los resultados de esta y su cumplimiento, así como hallazgos por clasificación que se dé.

7.1 Pruebas Revisión Configuraciones

Para estas pruebas, en adición a que el personal técnico de la **IEPC Guerrero** proporcione la configuración en línea de comando o por interfase gráfica para revisión, el ente auditor utilizó las herramientas necesarias para detectar mediante escaneos a los activos, las vulnerabilidades que puedan existir en los activos que pertenecen al PREP

Resultados Preliminares Revisión de Configuraciones				
Prueba	**Pruebas ejecutadas o descripción**	**Criterio de Aceptación**	**Comentarios**	**Resultado**
SPI01 – Validar que la configuración de los equipos de red siga mejores prácticas y no haya inconsistencias en esta	Revisar que la configuración bloquee puertos no usados, niegue por definición servicios y protocolos no utilizados	La configuración debe tener incorporada la limitación de protocolos, direcciones que no se estén usando en la jornada electoral 2021		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)	Acceso a los equipos de comunicaciones (FW, SW, Router) solo debe ser posible desde la red interna de la OPL	El acceso a la configuración de los equipos de comunicaciones es a través de WUI	Aceptado con observaciones
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)	Las versiones de estos equipos deben estar aun en soporte por el fabricante	Los dispositivos son nuevos y tienen el último firmware disponible del fabricante, pero ya están fuera de producción	Aceptado con observaciones
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	Deberá haber un contrato de soporte por un tercero o bien equipo en frio que pueda instalarse en caso de falla.	Se tienen dispositivos de repuesto disponibles por región	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	Existencia de redundancia de sistemas de comunicaciones para continuidad de captura. Verificar tiempos de convergencia (desde caída hasta recuperación) durante simulacro	Se tienen enlaces con proveedores diferentes	Aceptado
SPI06 – El sistema PREP deberá contar con redundancia eléctrica en caso de caída o fallas en la	Verificar que exista una planta generadora eléctrica con UPS que mantenga ininterrumpido el flujo eléctrico en caso de falla de la red pública.	Existencia de planta eléctrica para en caso de corte. Verificar tiempos de corte (desde caída hasta recuperación) durante simulacro	Se cuenta con plantas generadoras de gasolina para emergencia	Aceptado

red eléctrica durante la jornada electoral				
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 esté habilitada	La función de bitácora deberá estar habilitada y sus archivos creados		Aceptado

7.2 Pruebas Controles Físicos

Resultados Preliminares Pruebas Controles Físicos				
Prueba	**Pruebas ejecutadas o descripción**	**Criterio de Aceptación**	**Comentarios**	**Resultado**
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	Existencia de un centro o grupo que se dedique a monitorear el funcionamiento adecuado de los sistemas del PREP	Se tiene un grupo dedicado a soporte en Oficinas Centrales 3er piso	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	De haber redes inalámbricas en los centros de captura, estas redes no pueden tener acceso a la red de captura	Se hizo escaneo de redes Wifi	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 deben ser distintos y debe haber una clara segregación lógica y/o física entre estos ambientes.	Centro de desarrollo se encuentra en el IPN, fuera de IEPC	Aceptado
SPI11 – El sistema debe tener recursos dedicados por lo que no debe compartir recursos con otros sistemas o	El ambiente operativo del PREP en evaluación no debe compartir recursos con otros sistemas o plataformas, sus recursos deben ser únicos.	Validación que el ambiente es único y que no hay compartición de recursos con otras plataformas.	Se tiene contrato con Google Cloud a través de un *partner*. La infraestructura virtual es de uso exclusivo del PREP Gro.	Aceptado

plataformas ajenos al PREP en evaluación	Este control aplica primordialmente hacia estados donde hay terceros involucrados en el desarrollo de PREP que lo hacen para otros estados			
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 puede ser manual (registro), tarjeta, o pase para apertura automática	Se mostró procedimiento documentado en el Plan de Seguridad del PREP	Aceptado
SPI13 – Control de acceso al sitio donde está 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 deberán contar con el mínimo de privilegios y un control de contenido y de navegación en Internet	Se mostró procedimiento documentado en el Plan de Seguridad del PREP	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	Registro de equipos móviles para evitar tenerlos en el área de captura	Se mostró procedimiento documentado en el Plan de Seguridad del PREP	Aceptado

7.3 Pruebas Escaneo Vulnerabilidades de Activos

Resultados Preliminares Escaneo Vulnerabilidades de Activos				
Prueba	**Pruebas ejecutadas o descripción**	**Criterio de Aceptación**	**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	Todos los activos listados deberán estar justificados con el servicio que desempeña dentro de la función del PREP		Ver **pruebas CATD**
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	Todos los puertos o servicios listados en los distintos activos deberán estar justificados con el servicio que desempeña dentro de la función del PREP		Ver **pruebas CATD**
SPV03 – El escaneo de servicios hecho a la infraestructura no debe no debe tener existencia de	Mediante escaneo vulnerabilidades obtener las vulnerabilidades de los activos (sistemas operativos y aplicaciones) relacionados con el	Las aplicaciones y los sistemas operativos no deben tener vulnerabilidades críticas ni altas. Si tienen nivel medio, deberá existir contramedidas para esta. La lista completa		Ver **pruebas CATD**

vulnerabilidades altas (7.0 – 8.9) o Críticas (9.0 – 10) basados en la clasificación estándar CVSS	PREP listando de por la criticidad especificada por el estándar CVSS	de vulnerabilidades debe estar notificada hacia la parte responsable del OPL.		
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	En la obtención de la lista de vulnerabilidades no debe haber ninguna explotación existente para estas.		Ver **pruebas CATD**
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	Los hallazgos de este escaneo no deberán ser de severidad crítica o alta. De haber nivel medio, deberá existir contramedidas para esta. La lista completa de vulnerabilidades debe estar notificada hacia la parte responsable del OPL.		Ver **pruebas CATD**
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)	Certificado expedido e instalado y protocolo de cifrado deberá ser TLS1.2 o mayor	Certificado configurado en https://prep2021-gro-opl.mx/	Aceptado

7.4 Pruebas CATD

Se hicieron pruebas iguales en los CATD de los distritos 03, 04, 07, 08, 19 y 24. Los resultados aplican a todos los CATD, con ciertas excepciones marcadas.

Dominio: Comunicaciones		
Controles Especificados	**S/N/Número**	**Comentarios**
Enlaces funcionando	Si, 2 enlaces	2 enlaces exclusivos para PREP, enlace de oficina disponible como 3ª redundancia

Firewall/Router/Modem/BAMSim	Si, 1 firewall	Firewall/Gateway con balanceo de carga/*failover* para 2 enlaces.
Equipos de comunicaciones accesibles desde la LAN por protocolo seguro	Si	
Conexión VPN	Si	OpenVPN configurada en cada nodo en la máquina virtual
Configuración enlaces: (A-A), (A-P)	A - P	
Centro de ayuda/apoyo de TI con comunicación hacia los distintos centros en el estado	Si	Soporte centralizado

Dominio: Físico		
Controles Especificados	**S/N/Número**	**Comentarios**
Cuenta con No-Break o UPS (por equipo o general)	Si, 6 UPS	Verificar si los UPS tienen capacidad suficiente para respaldar el equipo conectado por el tiempo requerido para accionar el procedimiento de encendido de las plantas de respaldo. Hay que considerar que, en espacios reducidos, mal ventilados o con mala disipación de temperatura, un UPS puede fallar por la sobre demanda de un CPU queriendo disipar más temperatura.
Equipos con conexión por cable	Si, todos	

Equipos sin tarjeta inalámbrica o desactivada	Si, todos	Todos los equipos tienen desactivadas las tarjetas inalámbricas
Cantidad de equipos en el CATD	9 computadoras, 3 escáner	
Cuenta con Scanner adecuado a las AEC	Si	La calidad y velocidad de escaneado es adecuada para la digitalización de las boletas
Cuenta con adecuación para conectar planta eléctrica en caso de falla de energía	Si	Procedimiento manual, se cuenta con 2 plantas eléctricas de emergencia
Control de acceso de personas a los CATD	Si	Se tiene la política de restringir el acceso a solamente las personas que participarán en el PREP.
Control de dispositivos móviles en el CATD que no pertenezcan al proceso	Si	Se tiene la política de recoger todos los equipos móviles de las personas que participarán en el PREP.
Instalaciones adecuadas, seguras	Si	Espacio dedicado exclusivo para el ejercicio del PREP, con instalación eléctrica y de comunicaciones adecuadas a las necesidades del equipo computacional instalado y del sistema de distribución de información configurado.
Mobiliario completo	Si	

Dominio: Físico		
Controles Especificados	**S/N/Número**	**Comentarios**
Acceso de usuario limitado al equipo	Si	El usuario tiene acceso a otras aplicaciones no críticas sin afectación para proceso PREP

Usuario sin permiso de navegación en internet	No	Usuario con acceso sin restricciones a internet
Acceso de usuario solo a la aplicación del PREP	Si	El usuario tiene acceso a otras aplicaciones no críticas sin afectación para proceso PREP
Equipos sin carpetas compartidas	Si	
Restricción de acceso a Internet	No	Usuario con acceso sin restricciones a internet
Restricción a funciones administrativas en las computadoras de capturistas	Si	Si, se requiere contraseña de administrador
Restricción de acceso a otras aplicaciones	Si	El usuario tiene acceso a otras aplicaciones no críticas sin afectación para proceso PREP
Restricción a almacenamiento externo (USB/CD/DVD)	Si	
Redes inalámbricas restringidas	Si	No se tienen redes inalámbricas conectadas a la red de PREP
Sistema operativo actualizado	Si	Actualización no crítica pendiente

Dominio: Físico		
Controles Especificados	**S/N/Número**	**Comentarios**
Procedimiento de acción por contingencia eléctrica	Si	

Procedimiento de acción por caída de red	Si	
Procedimiento de verificación de hash	No aplica	Proceso automático y centralizado
Procedimiento de verificación de base de datos vacía	Si	

Se recomienda homologación, documentación y distribución de procedimientos de contingencia entre todos los CATD para evitar el riesgo de interpretación errónea o acción discrecional por parte del personal a cargo.

7.5 Pruebas Soporte Operativo

Resultados Preliminares Pruebas de Controles del Soporte Operativo				
Prueba	Criterio Aceptación	Criterio Aceptación	**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	Debe haber un manual disponible para el personal de captura	Se mostró manual de capacitación	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	Debe haber un grupo de personas que atiendan llamadas de aclaración de dudas o consultas de las distintas fases del proceso del PREP	El centro se encuentra en las oficinas centrales de IEPC	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	Existencia de una mesa de servicio o de soporte para resolución de problemas o dudas en los distintos procesos del PREP, así como resolución de las inconsistencias al momento de la captura.	Se tiene procedimiento documentado en el Manual de Operación y se tiene un Centro de Ayuda en el sitio web	Aceptado
PRS04 – Contratos de soporte externo en caso de eventualidades sobre las plataformas operativas que	Se deberá comprobar los contratos de soporte externo en caso de eventualidades en caso de que el	Existencia de un contrato de soporte válido durante la fecha de la jornada electoral para el soporte del a plataforma PREP de la OPL.	Sistema elaborado por tercero, pero el soporte lo da el IEPC	No aplica

se utilizan en el PREP (para sistemas desarrollados por terceros)	sistema PREP haya sido elaborado por un tercero			
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.	Tener contrato válido con soporte y con los procesos de reporte en caso de eventos, así como los niveles de servicio para resolución de incidentes en caso de que se llegue a reportar algo	Se tiene convenio de atención con Telmex y CFE, evidencia disponible por oficio y correo electrónico	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)	Tener contrato válido con soporte y con los procesos de reporte en caso de eventos, así como los niveles de servicio para resolución de incidentes en caso de que se llegue a reportar algo	Se tiene soporte extendido con Xertica, *partner* de Google Cloud	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	Mostrar evidencia de la existencia del documento	Se envía documentación del sistema	Aceptado

8 Planeación de las pruebas

La infraestructura del centro de difusión se encuentra ubicada en un centro de datos con acceso compartido perteneciente a Google Cloud Platform. Se hace uso de servidores virtuales y redes privadas virtuales para implementar la arquitectura completa del sitio de difusión y publicación de resultados.

IMPORTANTE: Realizar ataques de negación de servicio dedicado o distribuido hacia infraestructura que no es propia sin la debida autorización se considera un delito.

8.1 Excepciones

La política de uso aceptable de Google Cloud Platform (Acceptable Use Policy – AUP) restringe las pruebas de negación de servicio por la posible interferencia del servicio para terceros usuarios, y las considera una falta mayor a los Términos de Servicio del contrato, pudiendo incluso caer en condiciones de indemnización monetaria o de índole legal. Debido a esta situación y con la autorización debida por el responsable del PREP en IEPC Guerrero, las pruebas DOS no se llevarán a cabo contra la infraestructura del sitio de difusión del PREP.

Se revisa el esquema de protección que Google Cloud Platform ofrece a través de su producto Cloud Armor para infraestructura virtual hospedada en sus centros de datos, así como los controles complementarios a tener en el manejo de un ataque DOS/DDOS.

9 Conclusiones

Al final del último simulacro se tienen las siguientes observaciones:

1. Dos distritos no se pudieron conectar por cuestiones climáticas y geográficas, considerar que esta situación puede repetirse durante la jornada electoral. El IEPC declara que puede tomar medidas alternativas ante estas situaciones.
2. Se observaron algunos casos de actas cargadas por medio de la aplicación móvil donde no se desplegó la imagen digitalizada en el sitio.
3. Hay un desfase de los tiempos de sincronización entre el despliegue en sitio de publicación, el despliegue de las actas digitalizadas y el archivo de base de datos en CSV, por lo tanto, la información electoral puede mostrar inconsistencias por esta diferencia en sincronización.