TECNOLÓGICO DE MONTERREY

# Instituto Estatal Electoral de Hidalgo

Auditoría de Infraestructura Tecnológica y Sistema Informático del PREP

**Reporte Final de Auditoría**

Tecnológico de Monterrey

HIDALGO IEE INSTITUTO ESTATAL ELECTORAL

# ALCANCE Y CONCLUSIONES DE LA AUDITORÍA

Una vez que se ha concluido la Auditoría al sistema del Programa de Resultados Electorales Preliminares (PREP) para los procesos electorales ordinario y extraordinario 2020-2021 en el estado de Hidalgo, se concluye que existen controles de seguridad implementados que mitigan los riesgos de vulnerabilidad. Además, durante la ejecución de pruebas y simulacros se pudo determinar que el sistema cumple las expectativas para las cuales fue desarrollado.

Relativo a los seis controles marcados como rechazados, éstos no reflejan una vulnerabilidad existente sino la ausencia de una evaluación formal. Lo anterior debido a que por motivos de confidencialidad de datos contractuales del proveedor, no se presentaron las evidencias comprobatorias al considerarse reservadas. La Auditoría fue planteada en 6 distintas líneas de revisión:

| No. | Tipo de prueba | Estatus | Comentarios |
|---|---|---|---|
| 1 | Pruebas de Caja Negra | Terminado | Informe final entregado |
| 2 | Validación del Sistema Informático | Terminado | Informe final entregado |
| 3 | Vulnerabilidad y Configuraciones | Terminado | Informe final entregado |
| 4 | Pruebas de Penetración | Terminado | Informe final entregado |
| 5 | Pruebas DoS | Terminado | Informe final entregado |
| 6 | Informe de Jornada Electoral | Terminado | Se entregará el día 10 de junio (Posterior a la Jornada Electoral) |

# PRUEBAS DE CAJA NEGRA

# PRUEBAS DE CAJA NEGRA

Pruebas 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 | El acceso es a través de usuario y 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 | El mecanismo de autenticación actual envía un mensaje después de 3 intentos erróneos de autenticación, bloqueando el acceso al teléfono. | **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 | Existe una mesa de servicio a nivel nacional para dar soporte de forma centralizada | **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 | El proveedor tiene instalado un sistema de Gestión de Dispositivos Móviles (MDM) para gestionar el inventario de teléfonos con la aplicación en uso | **Aceptado** |
| **SPD05 –** Distribución de Aplicación controlada | Acceso a la aplicación debe ser controlada por un solo punto de contacto para su instalación | La instalación es llevada a cabo por el proveedor de forma centralizada, no existe ningún sitio público de descarga. | **Aceptado** |
| **SPD06 –** Identificación con factor adicional para teléfonos móviles en el uso de la aplicación y firma de la plataforma | Se deberá verificar que se cuente con un método de asegurarse que solo teléfonos permitidos pueden firmarse en la plataforma, adicional al usuario y clave de esta. Métodos adicionales sugeridos: Certificado, MAC, IMEI | La seguridad para la autenticación de la aplicación quedará a cargo de un Sistema de Gestión de Dispositivos Móviles (MDM). | **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 | Se ha podido cotejar el correcto funcionamiento de la aplicación. | **Aceptado** |

# PRUEBAS DE CAJA NEGRA

Pruebas PREP Digitalización (SPD)

| Controles Especificados | Pruebas ejecutadas | Comentarios | Resultado |
|---|---|---|---|
| **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 | Se ha podido cotejar el correcto funcionamiento de la aplicación. Ver Caso de Uso PFD-10 “Acta fuera de catálogo” | **Aceptado** |
| **SPD09 –** Transmisión de acta digitalizada al sitio o BD de Actas | El acta digitalizada por medio móvil o escáner deberá subirse a la BD de la OPL | Se ha podido cotejar el correcto funcionamiento de la aplicación. | **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 esté usando para enviar la imagen. | Por motivos de confidencialidad de datos contractuales del proveedor, no se presentó la evidencia comprobatoria con los detalles de la conexión. | **Rechazado** |
| S**PD11 –** 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<br><br>**NOTA:** *Esta prueba aplica solo si el scanner no requiere de computadora para transmitir el acta hacia la BD* | No aplica debido a que el escenario en el que el escáner pueda transmitir de forma autónoma un acta digitalizada no está contemplado | **Aceptado** |
| **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 | Se genera un hash al momento de la digitalización y al momento de su almacenamiento en la BD. Ambos deben coincidir y esto se puede cotejar de forma visual a través del sitio de publicación. | **Aceptar** |

# PRUEBAS DE CAJA NEGRA

Pruebas PREP Captura (SPC)

| 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 a través de usuario y contraseña | **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 | El mecanismo de autenticación actual no permite el acceso al equipo después de varios (5) intentos erróneos, sin embargo, no se bloquea.<br>**Se recomienda implementar un mecanismo de bloqueo de la aplicación después de varios (5) intentos erróneos para elevar el nivel de seguridad**. | **Aceptado con observaciones** |
| **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 | El sistema operativo (SO) instalado en las estaciones de captura tiene soporte vigente con el fabricante | 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 están conectadas por red cableada hacia la estación de telecomunicaciones local | **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 usuario de captura tiene acceso únicamente a la aplicación de captura de actas digitalizadas, todos los demás privilegios le son negados a través de una configuración personalizada del sistema operativo | **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 | Las estaciones de trabajo cuentan únicamente con acceso a la red local, no tienen acceso a internet. Además, tampoco cuentan con ninguna aplicación que pudiera hacer uso de la conexión a internet en caso de que esta existiera. | **Aceptado** |

# PRUEBAS DE CAJA NEGRA

Pruebas PREP Captura (SPC)

| Controles Especificados | Pruebas ejecutadas | Comentarios | Resultado |
|---|---|---|---|
| **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 de captura tiene acceso únicamente a la aplicación de captura de actas digitalizadas, todos los demás privilegios le son negados a través de una configuración personalizada del sistema operativo | **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 | Las estaciones de captura cuentan tienen puertos USB habilitados.<br>**Se recomienda que los puertos USB no utilizados sean deshabilitados por SO para elevar el nivel de seguridad** | **Aceptado con observaciones** |
| **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 | La aplicación de captura de actas digitalizadas utiliza un certificado de seguridad para transmitir el archivo hacia el servidor central | **Aceptado** |

# PRUEBAS DE CAJA NEGRA

## Pruebas de Captura de Datos (PCD)

| 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 | Los campos que contiene un acta se capturan dentro del flujo del sistema | **Aceptado** |
| **PCD02 –** El sistema PREP Local deberá considerar para la Captura los siguientes datos requeridos por parte del INE para cálculos adecuado | 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.<br>**ID Acta PREP**<br>• Entidad Federal, Distrito Electoral, Sección, Tipo , Número casilla, Municipio<br>**Boletas**<br>• Boletas Sobrantes, Personas que votaron, Representantes Partidos políticos e independientes acreditados que votaron, Total, votos sacados de urna<br>**Votos Obtenidos**<br>• Votos obtenidos por Partido y candidatos independientes<br>**Votos**<br>• Total, votos, Votos nulos, Votos par candidatos, No registrados<br>**Acta**<br>• Imagen del acta | Los datos referidos son capturados en diferentes etapas del proceso PREP | **Aceptado** |

# PRUEBAS DE CAJA NEGRA

Pruebas de Captura de Datos (PCD)

| Controles Especificados | Pruebas ejecutadas | 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<br>a) Total numérico de actas esperadas;<br>b) Total numérico de actas capturadas y su correspondiente porcentaje respecto al total de actas esperadas;<br>c) Total numérico de actas contabilizadas y su correspondiente porcentaje respecto al total de actas esperadas;<br>d) Total de actas fuera de catálogo;<br>e) El porcentaje calculado de participación ciudadana;<br>f) Total de votos por AEC,<br>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,<br>h) Agregados a nivel nacional, circunscripción, entidad federativa, municipio o Alcaldía, distrito electoral, sección y acta, según corresponda. | Conforme se realiza la captura de las actas, estos valores se van actualizando en los diferentes puntos del portal de publicación | **Aceptado** |

# PRUEBAS DE CAJA NEGRA

Casos de Uso

| Controles Especificados | Casos de Uso (Escenarios PREP) | Criterio de Aceptación | Resultado |
|---|---|---|---|
| PFD – 01 | Diputaciones – 1 | Acta se digitaliza con escáner, se folia, 1ª y 2ª captura iguales, se publica | Aceptado |
| PFD – 03 | Diputaciones – 2 | Acta se digitaliza con escáner, se folia, 1ª, 2ª y 3ª captura diferentes, 4ª captura igual a la 3ª, se publica | Aceptado |
| PFD – 05 | Diputaciones – 3 | Todos los campos ilegibles, envío a validación (foliación), 1ª y 2ª captura iguales, se verifican datos ilegibles, se publica | Aceptado |
| PFD – 07 | Diputaciones – 4 | Algunos datos ilegibles, 1ª y 2ª captura iguales colocando "i" en ilegibles, se verifican datos ilegibles, se publica | Aceptado |
| PFD – 09 | Diputaciones – 5 | Los datos exceden LN, 1ª y 2ª captura iguales, se publica, NO se contabiliza | Aceptado |
| PFD – 10 | Diputaciones – 6 | Acta fuera de catálogo, envío a validación, NO se publica, NO se contabiliza, aparece en el archivo CSV del sitio de publicación | Aceptado |
| PDF – 14 | Diputaciones – 7 | Acta se digitaliza con escáner, se folia, 1ª y 2ª captura iguales, se publica | Aceptado |
| PDF – 16 | Diputaciones – 8 | Acta se digitaliza con escáner, se folia, 1ª y 2ª captura iguales, se publica | Aceptado |
| PDF – 18 | Diputaciones – 9 | Acta se digitaliza con escáner, se folia, 1ª y 2ª captura iguales, se publica | Aceptado |
| PDF – 20 | Diputaciones – 10 | Acta se digitaliza con escáner, se folia, 1ª y 2ª captura iguales, se publica | Aceptado |
| PDF – 22 | Diputaciones – 11 | Acta se digitaliza con escáner, se folia, 1ª y 2ª captura iguales, se publica | Aceptado |
| PDF – 24 | Diputaciones – 12 | Acta con QR se digitaliza con móvil, se folia 2 veces, 1ª y 2ª captura iguales, se publica | Aceptado |
| PDF – 25 | Diputaciones – 13 | Acta sin QR se digitaliza con móvil, se folia 2 veces capturando datos de acta manualmente, 1ª y 2ª captura iguales, se publica | Aceptado |
| **Controles Especificados** | **Casos de Uso (Escenarios PREP)** | **Criterio de Aceptación** | **Resultado** |
| PFD – 02 | Ayuntamientos – 1 | Acta de digitaliza con escáner, 1ª y 2ª captura diferentes, 3ª captura igual a 1ª o 2ª, se publica | Aceptado |
| PFD – 04 | Ayuntamientos – 2 | Acta se digitaliza con escáner, se folia, 1ª, 2ª ,3ª y 4ª captura diferentes, envío a proceso de validación, se publica | Aceptado |
| PFD – 06 | Ayuntamientos – 3 | Todos los campos vaciós, 1ª y 2ª captura con "b" iguales, envío a proceso de validación, se publica | Aceptado |
| PFD – 08 | Ayuntamientos – 4 | Algunos datos vaciós, 1ª y 2ª captura iguales colocando "b" en vacios, se verifican datos vacíos, se publica | Aceptado |
| PFD – 11 | Ayuntamientos – 5 | Paquete No Entregado, envío a validación, se publica, NO se contabiliza | Aceptado |
| PFD – 12 | Ayuntamientos – 6 | Paquete sin sobre, envío a validación, se publica, NO se contabiliza | Aceptado |
| PFD – 13 | Ayuntamientos – 7 | Casilla no instalada, envío a validación, se publica, NO se contabiliza | Aceptado |
| PFD – 15 | Ayuntamientos – 8 | Acta se digitaliza con escáner, se folia, 1ª y 2ª captura iguales, se publica | Aceptado |
| PFD – 17 | Ayuntamientos – 9 | Acta se digitaliza con escáner, se folia, 1ª y 2ª captura iguales, se publica | Aceptado |
| PFD – 19 | Ayuntamientos – 10 | Acta se digitaliza con escáner, se folia, 1ª y 2ª captura iguales, se publica | Aceptado |
| PFD – 21 | Ayuntamientos – 11 | Acta se digitaliza con escáner, se folia, 1ª y 2ª captura iguales, se publica | Aceptado |
| PFD – 23 | Ayuntamientos – 12 | Acta se digitaliza con escáner, se folia, 1ª y 2ª captura iguales, se publica | Aceptado |

# PRUEBAS DE CAJA NEGRA 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 cálculo se realizó correctamente | Se revisaron los números publicados en los diferentes elementos de la interfaz y en todos se reflejaban los porcentajes correctos, sin truncamientos ni redondeos. | **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 | Existe el enlace para poder descargar la base de datos, los cuales se encuentran en formato .zip y dentro traen los .csv correspondientes. | **Aceptado** |
| **PPR03 –** Datos a Publicar deberán publicar en el sitio oficial, de donde se distribuirán a los sitios replicantes de información oficial deben contener los siguientes valores | La lista de valores a publicarse como parte de esta prueba en el sitio oficial desde donde se replicará hacia los difusores, debe incluir los siguientes valores:<br><br>a) Lista nominal;<br>b) Lista nominal de las actas contabilizadas;<br>c) Participación ciudadana;<br>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;<br>e) Datos calculados;<br>f) Imágenes de las Actas PREP;<br>g) Identificación del Acta PREP con inconsistencias,<br>h) En su caso, el resultado de las consultas populares;<br>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<br>j) Hash o código de integridad obtenido a partir de cada imagen de las Actas PREP, con el estándar definido por el | Todos los elementos se encuentran conforme a los requerimientos y manuales | **Acepado** |

# PRUEBAS DE CAJA NEGRA

Publicación de Resultados (PPR)

| Controles Especificados | Pruebas ejecutadas | 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:<br>a) Encabezado<br>b) Menú izquierdo colapsable.<br>c) Avance de Entidad<br>d) Conoce los resultados de tu casilla<br>e) Estadística de la Entidad<br>f) Pie de página (footer) | Todos los criterios se encuentran dentro de la interfaz web de la página de publicación | **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<br>a) Acceso a preguntas frecuentes<br>b) Acceso a Centro de ayuda<br>c) Configuración visual (tamaño y formato claro/oscuro)<br>d) Debe incluir Logo PREP y OPL<br>e) Boto de regreso a inicio<br>f) Acceso directo a pestañas por elección<br>g) Acceso a la Base de datos | El acceso a preguntas frecuentes despliega una barra donde se muestran las preguntas. Todo funciona correctamente. Las preguntas frecuentes no tienen modo oscuro, y hay algunos elementos la interfaz que no cambian de tamaño de letra. | **Aceptado con observaciones** |
| **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<br>a) Acceso directo votos por Candidatura<br>b) Acceso directo votos por partido político y candidatura Independiente<br>c) Detalle por casilla<br>d) Detalle por Distrito<br>e) Sección<br>f) Casilla | Todos los elementos se encuentran conforme al centro de ayuda y los prototipos navegables referidos | **Aceptado** |

# PRUEBAS DE CAJA NEGRA

Publicación de Resultados (PPR)

| Controles Especificados | Pruebas ejecutadas | Comentarios | Resultado |
|---|---|---|---|
| **PPR07** – Requerimientos de portal WEB para publicación – Avance entidad | En la sección de Avance Entidad deben existir los siguientes elementos<br><br>a) Actas Capturadas<br>b) Participación Ciudadana<br>c) Indicador del Corte<br>d) Botón Actualizar | El avance de la entidad tiene todos los elementos requeridos. | **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<br><br>a) Signo Interrogación<br>b) Campo de Sección<br>c) Campo Primer Apellido<br>d) Botón de Consulta<br>e) Aviso Privacidad | Todos los elementos se encuentran. Se determinó que el campo de primer apellido ya no sería requerido para este periodo de elecciones | **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:<br><br>a) Actas<br>b) Actas contabilizadas<br>c) Lista Nominal<br>d) Participación<br>e) Votos<br>f) Total de Votos | Se despliegan todos los elementos correctamente. | **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<br><br>a) Leyenda<br>b) Nombre del Instituto Electoral del Estado<br>c) Aviso de privacidad | Cumple con todos los elementos requeridos | **Aceptado** |

# PRUEBAS DE CAJA NEGRA

Publicación de Resultados (PPR)

| Controles Especificados | Pruebas ejecutadas | 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:<br>a) Encabezado<br>b) Menú izquierdo colapsable.<br>c) Avance de Entidad<br>d) Encabezado<br>e) Menú izquierdo colapsable.<br>f) Avance de Entidad | La página móvil tiene los elementos y se despliegan correctamente en Safari para iOS y Chrome para Android | **Aceptado** |
| **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:<br>a) Nombre del sitio con el nombre del estado en auditoría<br>b) Logo del PREP local<br>c) Menú desplegable | Se muestran correctamente los elementos dentro de Safari para iOS y Chrome para Android | **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:<br>a) Tipo de Elección<br>b) Mi casilla<br>c) Preguntas frecuentes<br>d) Centro Ayuda<br>e) Tema y tamaño caracter | Se encuentran todos los elementos requeridos en la interfaz | **Aceptado** |
| **PPR14** – Requerimientos de portal MÓVIL para publicación – Menú Desplegable > Mi Casilla | Entrar a la página móvil del PREP y verificar en el menú desplegable en la opción de Mi casilla los siguientes elementos:<br>a) Aviso de Privacidad<br>b) Instrucción<br>c) Ejemplo de credencial para votar<br>d) Consultar<br>e) Aviso de privacidad al consultar<br>f) Flecha de regreso | Se encuentran todos los elementos requeridos en la interfaz | **Aceptado** |

# PRUEBAS DE CAJA NEGRA

Publicación de Resultados (PPR)

| Controles Especificados | Pruebas ejecutadas | 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:<br>a) Actas capturadas<br>b) Participación Ciudadana<br>c) Ultimo corte<br>d) Botón actualizar | Todos los elementos se muestran correctamente. | **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:<br>a) Votos por Candidatura, Distritos o Municipios<br>b) Votos por Partido Político y Candidatura Independiente<br>c) Distrito, Municipio o Demarcación | Todos los elementos se encuentran en la interfaz y funcionan correctamente | **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:<br>a) Actas<br>b) Actas contabilizadas por casillas urbanas y no urbanas<br>c) Lista Nominal<br>d) Participación ciudadana | Todos los elementos aparecen correctamente. | **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:<br>a) Versión de escritorio<br>b) Leyenda<br>c) Logos de la OPL<br>d) Aviso de privacidad<br>e) Nombre del Instituto Local<br>f) versión de los servicios<br>g) botón para compartir | Se encuentran todos los elementos requeridos de la interfaz, | **Aceptado** |

# VALIDACIÓN DEL SISTEMA

# VALIDACIÓN DEL SISTEMA

| 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 procedimiento de generación de la firma digital SHA256 ha sido documentado | **Aceptado** |
| **IRS02 –** Documentar y validar el proceso de reinicio de la base de datos para asegurar que los valores de esta sean cero y/o estén vacíos al inicio de la jornada electoral | Documentar y validar el proceso | El procedimiento de reinicio de la base de datos ha sido documentado | **Aceptado** |

# VULNERABILIDAD Y CONFIGURACIONES

# VULNERABILIDAD Y CONFIGURACIONES

## Revisión de Configuraciones (SPI)

| Prueba | Pruebas ejecutadas o descripción | 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 | Los equipos de captura han sido escaneados en busca de vulnerabilidades y se ha podido cotejar que bloquean puertos no usados, y no exponen servicios y protocolos no utilizados | 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 sistemas solo pueden ser accedidos dentro de la red interna | 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 equipos de comunicaciones tienen versiones de software que incluyen actualizaciones de seguridad ante vulnerabilidades conocidas. | 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 | La solución tecnológica cuenta con equipo de respaldo (en frío) para sustitución del equipo de comunicaciones en caso de falla. | 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 cuenta con enlaces en fibra óptica de con diferente proveedor y diferente salida | Aceptado |
| **SPI06 –** El sistema PREP deberá contar con redundancia eléctrica en caso de caída o fallas en la red eléctrica durante la jornada electoral | Verificar que exista una planta generadora eléctrica con UPS que mantenga ininterrumpido el flujo eléctrico en caso de falla de la red pública. | El proveedor tiene instalados equipos UPS en todos los equipos de cómputo. Se ha podido cotejar la instalación y correcto funcionamiento de la planta de energía, ante eventos de corte del suministro de luz. | Aceptado |
| **SPI07 –** Los activos involucrados en el PREP deberán de tener habilitado la función de bitácora (logging) para | Entrar a los distintos activos y verificar la configuración y directorios donde se guarda la bitácora | Todos los equipos de comunicaciones tienen las bitácoras activadas | Aceptado |

# VULNERABILIDAD Y CONFIGURACIONES

## Controles Físicos (SPI)

| Prueba | Pruebas ejecutadas o descripción | 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 | Se cuenta con un monitoreo propio activo 24/7 | 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 | Todos los equipos se conectan vía cable. | Aceptado |
| **SPI10 –** La infraestructura de los ambientes de desarrollo debe estar segregada de la infraestructura de ambientes operativos | Debe validarse que los ambientes de producción y de operación sean distintos y estén por separado | Los ambientes de producción y de operación son distintos y existe una clara segregación física entre estos ambientes. | 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 servidores de comunicaciones, bases de datos y publicación son exclusivos para PREP Hidalgo | Aceptado |
| **SPI12 –** Controles de acceso físico a los centros de captura | El centro de captura deberá estar resguardado con entrada controlada para evitar que haya personas ajenas a los trabajos durante la jornada | El centro de captura está resguardado con entrada controlada para evitar que haya personas ajenas a los trabajos durante la jornada electoral | Aceptado |
| **SPI13 –** Control de acceso al sitio donde se encuentra la infraestructura del PREP | Las aplicaciones que se estén utilizando para la jornada deberán estar activados sus puertos y no otros distintos a estos. | El usuario de captura tiene acceso únicamente a la aplicación de captura de actas digitalizadas, todos los demás privilegios le son negados a través de una configuración personalizada el Sistema Operativo | Aceptado |

# VULNERABILIDAD Y CONFIGURACIONES

## Escaneo de Vulnerabilidades de Activos

| Prueba | Pruebas ejecutadas o descripción | 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 | El escaneo de equipos locales encontró que todos los activos están justificados y no tienen vulnerabilidades.<br><br>Se tiene conocimiento de la existencia de 4 activos en la nube. Sin embargo, por motivos de confidencialidad de datos contractuales del proveedor, no se presentó la evidencia comprobatoria para evaluar su vulnerabilidad. | Rechazado |
| **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 | El escaneo de equipos locales encontró que todos los activos están justificados y no tienen vulnerabilidades.<br><br>Se tiene conocimiento de la existencia de 4 activos en la nube. Sin embargo, por motivos de confidencialidad de datos contractuales del proveedor, no se presentó la evidencia comprobatoria para evaluar su vulnerabilidad. | Rechazado |
| **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 | Las aplicaciones instaladas en el servidor de comunicaciones incluyen actualizaciones de seguridad ante vulnerabilidades conocidas. | 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 nivel alto o crítico. De ser así se deberán listar y comprobar que estas son explotadas en los controles SPP | Las aplicaciones instaladas en el servidor de comunicaciones incluyen actualizaciones de seguridad ante vulnerabilidades conocidas. | Aceptado |

# VULNERABILIDAD Y CONFIGURACIONES

## Escaneo de Vulnerabilidades de Activos

| Prueba | Criterio Aceptación | Comentarios | Resultado |
|---|---|---|---|
| **SPV05** – Listar mediante un escaneo de los servidores WEB las vulnerabilidades que pueda haber en estos | 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. | Se realizó el escaneo de las páginas web de publicación de resultados. En estos sitios no se encontraron vulnerabilidades.<br><br>Se tiene conocimiento de la existencia de 4 activos en la nube. Sin embargo, por motivos de confidencialidad de datos contractuales del proveedor, no se presentó la evidencia comprobatoria para evaluar su vulnerabilidad. | Rechazado |
| **SPV06** – EL sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado | Certificado expedido e instalado y protocolo de cifrado deberá ser TLS1.2 o mayor | El sitio de publicación tiene activado un certificado SSL válido | Aceptado |

# VULNERABILIDAD Y CONFIGURACIONES

Pruebas de Soporte Operativo

| Prueba | Pruebas ejecutadas o descripción | 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 | El proveedor cuenta con un manual disponible para el personal de captura | 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 | Existe una mesa de servicio centralizada disponible para resolver dudas y consultas | 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 | Existe una mesa de servicio centralizada disponible para resolver dudas y consultas | 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 | Existe un contrato entre el proveedor y el IEEH para la prestación de servicios para la implementación y desarrollo del PREP 2021. | 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 tiene contrato con Telmex | 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 está utilizando Nube como repositorio operativo del PREP) | Existe un contrato con los proveedores en la nube que contemplan mecanismos técnicos en caso de fallas | 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 | La documentación de arquitectura y modelación del sistema existe y está resguardada por el OPL Hidalgo | Aceptado |

# PRUEBAS DoS

## PRUEBAS DoS Ataque Volumétrico por TCP

| Prueba | Pruebas ejecutadas o descripción | Comentarios | Resultado |
|---|---|---|---|
| **SPN01 –** La infraestructura debe soportar un ataque volumétrico TCP-SYN FLOOD | Se documentará el nivel de tráfico y el desempeño del servidor bajo esta situación | No se permite que los clientes realicen por sí solos evaluaciones de seguridad de la infraestructura o de los servicios, incluyendo Denegación de servicio (DoS), DoS distribuida (DDoS) o DoS simulada. | **Sustituida** |

## PRUEBAS DoS Ataque Volumétrico por UDP

| Prueba | Pruebas ejecutadas o descripción | Comentarios | Resultado |
|---|---|---|---|
| **SPN02 –** La infraestructura deberá soportar un ataque volumétrico por UDP-DNS Amplification. | En cualquiera de los dos casos, el resultado deberá ser que la recursividad no está habilitada en el DNS | No se permite que los clientes realicen por sí solos evaluaciones de seguridad de la infraestructura de AWS o de los servicios de AWS, incluyendo Denegación de servicio (DoS), DoS distribuida (DDoS) o DoS simulada.<br>Se tiene evidencia de que los DNS del sitio no permiten recursividad. | **Aceptado** |

## PRUEBAS DoS Ataque Volumétrico por ICMP

| Prueba | Pruebas ejecutadas o descripción | Comentarios | Resultado |
|---|---|---|---|
| **SPN03 –** La infraestructura deberá poder soportar un ataque volumétrico por ICMP – ICMP FLOOD | Se documentará el nivel de tráfico recibido para verificar que el servidor ha sido inundado de paquetes desde la dirección origen | No se permite que los clientes realicen por sí solos evaluaciones de seguridad de la infraestructura o de los servicios, incluyendo Denegación de servicio (DoS), DoS distribuida (DDoS) o DoS simulada. | **Sustituida** |

## PRUEBAS DoS Ataque a la capa de aplicación

| Prueba | Pruebas ejecutadas o descripción | Comentarios | Resultado |
|---|---|---|---|
| **SPN04 –** La infraestructura deberá poder manejar un ataque en la capa de aplicación vía un SLOWLORIS attack | Se documentará la respuesta y desempeño del servidor con este tipo de ataques. | La tecnología utilizada en el sitio de publicación cierra automáticamente las conexiones de los atacantes de lectura o escritura lentas (Slowloris) | **Sustituida** |

# PRUEBAS DoS

## Controles compensatorios

| Prueba | Pruebas ejecutadas o descripción | Comentarios | Resultado |
|---|---|---|---|
| **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 sitio de publicación es estático y no tiene conexión otro tipo de infraestructura, lo cual sugiere un bajo riesgo. Sin embargo, por motivos de confidencialidad de datos contractuales del proveedor, no se presentó la evidencia comprobatoria para evaluar su vulnerabilidad. | **Rechazado** |
| **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 cuenta con servicio de protección DoS contratado por parte del proveedor. | **Aprobado** |
| **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 sitio de publicación es estático y no tiene conexión otro tipo de infraestructura, lo cual sugiere un bajo riesgo. Sin embargo, por motivos de confidencialidad de datos contractuales del proveedor, no se presentó la evidencia comprobatoria para evaluar su vulnerabilidad. | **Rechazado** |
| **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 OPL Hidalgo cuenta con procedimientos internos de comunicación en caso de eventos adversos durante la jornada electoral | **Aprobado** |