# Informe final público de la auditoría al sistema informático PREP San Luis Potosí 2024

Resumen final del proceso de auditoría del Programa Preliminar de Resultados Electorales 2024 para el Organismo Público Local Electoral.

30 de mayo 2024

# Líneas de revisión auditoría

**La auditoría fue planteada en 6 distintas líneas de revisión y al día 30 de mayo se tiene el siguiente estado:**

| # | Línea Revisión | Estado | Observaciones |
|---|---|---|---|
| 1 | Pruebas Caja Negra | Terminado | Todas las funcionalidades del sistema PREP, en sus distintas fases (digitalización, captura y publicación), fueron exitosas cumpliendo con los requerimientos de funcionalidad marcados. |
| 2 | Análisis Vulnerabilidades Infraestructura PREP | Terminado | Las vulnerabilidades encontradas son de nivel bajo o medio sin exploits conocidos. |
| 3 | Pruebas PenTest | Terminado | Para las vulnerabilidades presentadas no hay explotaciones definidas a realizar. |
| 4 | Revisión de configuraciones de la infraestructura | Terminado | Se llevo a cabo la revisión de configuraciones y la implementación de buenas prácticas en los equipos que conforman la infraestructura del PREP. |
| 5 | Pruebas DDOS a PREP | Terminado | Pruebas volumétricas realizadas, sin impacto. En todos los casos, no hay afectación en tiempos de respuesta del servidor de publicación. En todas las pruebas, los tiempos de respuesta no exceden 200ms El DNS no es propenso a ataques de amplificación. |
| 6 | Validación Sistema Informático e Integridad PREP y BD | En Proceso | Se revisaron los procesos de reinicio de la Base de datos así como el de la generación de llave de integridad durante los tres simulacros del sistema. Falta la entrega de los hashes finales del sistema informático para resguardo y la ejecución del proceso al inicio de la jornada electoral el 02 de junio. |

# Criterios para asignar un resultado

## Criterios utilizados para la auditoría

Los criterios de aceptación de cada prueba están documentados en la tabla para lo cual la prueba debe cumplir con ellos. 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 ejecuta nuevamente. |
| Rechazado | La prueba no cumplió con los criterios de aceptación | Prueba no es aceptada, se documenta el resultado y recomendaciones. Esta prueba se vuelve a ejecutar en la siguiente iteración para revisar la implementación de las recomendaciones dadas en el resultado de las pruebas. |
| Aceptado con Observaciones | La prueba cumplió con una parte de los criterios o cumplió totalmente y se incluyen observaciones del auditor. | La prueba es aceptada, pero con recomendaciones. Esto significa que las recomendaciones son solo eso, no sería obligatoria su implementación y solo queda como sugerencia o recomendación. |

# Pruebas de caja negra

# Pruebas Caja Negra - Contexto

Las pruebas tienen como base el Open Web Application Security Project (OWASP). Esta metodología representa un consenso a nivel desarrolladores sobre los riesgos más críticos en desarrollos de software. Los puntos generales revisados se ubican en alguno de los siguientes apartados:

| Clasificación | Descripción |
|---|---|
| Uso impropio de la plataforma | Mal uso de alguna característica de la plataforma o falla de controles de seguridad de esta. |
| Almacenamiento inseguro de datos | Almacenamiento inseguro de datos y fuga no-intencional de estos. |
| Comunicación insegura | Esta clasificación cubre una mala negociación entre dos puntos por cuestiones de versiones de SSL, negociación débil, comunicaciones en texto sin cifrado en activos sensibles. |
| Autenticación insegura | Esta categoría tiene que ver con un mal proceso de autenticación en la sesión ya sea por falla al identificar el usuario, falla al mantener la identidad del usuario al ser requerida o debilidad en la gestión de la sesión. |
| Criptografía insuficiente | Esta clasificación tiene que ver con la falla o falta de aplicación de criptografía. |
| Autorización insegura | Esta categoría captura cualquier tipo de falla en la autorización. |
| Calidad en el Código cliente | Esta categoría tiene que ver con los problemas de implementación a nivel código en los clientes móviles. |
| Modificación de Código | Esta categoría cubre actualizaciones, parches, modificaciones locales de código y modificaciones dinámicas de memoria. |
| Funcionalidades extrañas | Funciones escondidas de desarrollo, controles de seguridad que no fueron inicialmente programados para ser liberados en un ambiente de producción. |

# Pruebas Caja Negra – 1/3

| Pruebas | Control revisado | Resultado |
|---|---|---|
| Pruebas Aplicación Móvil | **SPD01** – Control de acceso a la aplicación móvil de digitalización mediante usuario/contraseña. | Aceptado |
| | **SPD02** – Bloqueo aplicación móvil por usuario con contraseña errónea. | Aceptado |
| | **SPD03** – Usuario bloqueado deberá cambiarse mediante mesa de servicio. | Aceptado |
| | **SPD04** – Dispositivos móviles con aplicación controlada. | Aceptado |
| | **SPD05** – Distribución de aplicación controlada. | Aceptado |
| | **SPD06** – Identificación con factor adicional para teléfonos móviles en el uso de la aplicación y firma de la plataforma. | Aceptado |
| | **SPD07** – Alta de actas por parte del equipo móvil registrado. | Aceptado |
| | **SPD08** – Alta de acta equivocada (no pertenece a la casilla). | Aceptado |
| | **SPD09** – Transmisión de acta digitalizada al sitio o BD de actas. | Aceptado |
| | **SPD10** – Transmisión cifrada del acta hacia el repositorio o BD del PREP (sea móvil o escáner). | Aceptado |
| | **SPD11** – Transmisión cifrada del acta digitalizada hacia el repositorio o BD del PREP (escáner). | Aceptado |
| | **SPD12** – Confirmación de integridad del acta digitalizada y guardada en la BD del PREP. | Aceptado |

# Pruebas Caja Negra – 2/3

| Pruebas | Control revisado | Resultado |
|---|---|---|
| Pruebas Estación de Captura | **SPC01** – Control de acceso a la estación de captura mediante usuario/contraseña. | Aceptado |
| | **SPC02** – Bloqueo de usuario con contraseña errónea. | Aceptado |
| | **SPC03** – Sistema operativo de la estación de captura debe ser vigente (no estar descontinuado por el fabricante). | Aceptado |
| | **SPC04** – Las estaciones de captura deberán estar conectadas a la red mediante cable y no de forma inalámbrica. | Aceptado |
| | **SPC05** – Usuarios de estación de captura con privilegios mínimos de administración. | Aceptado |
| | **SPC06** – Sistema Operativo de la plataforma de captura deberá tener negado el acceso a Internet y el acceso remoto. | Aceptado |
| | **SPC07 -** Las estaciones de captura solo deben tener acceso hacia las aplicaciones del sistema de elecciones. | Aceptado |
| | **SPC08** – Sistema Operativo de la plataforma de captura no deberá permitir acceder a medios externos de almacenamiento de datos (USB, CD, CD-ROM). | Aceptado |
| | **SPC09** – Portal de captura al que acceden las estaciones de captura, deberá ser un portal en SSL y con certificado válido. | Aceptado |
| | **SPC10** - Estaciones de captura de voto deben bloquearse. | Aceptado |
| Pruebas Captura Datos | **PCD01** – Validar proceso de cotejo de acta digitalizada contra los campos de captura del acta. | Aceptado |
| | **PCD02** – El sistema PREP Local deberá considerar para la captura los siguientes datos requeridos por parte del OPL para cálculos adecuado. | Aceptado |
| | **PCD03 –** Datos a calcular por la plataforma PREP en la que se debe validar que los siguientes valores se den como resultado del cálculo en cada nivel de agregación que aplique (acta, sección, distrito electoral, entidad federativa y nacional). | Aceptado |

# Pruebas Caja Negra – 3/3

| Pruebas | Control revisado | Resultado |
|---|---|---|
| Pruebas PREP Digitalización | **PPR01 –** Resultados de porcentajes, los decimales deberán calcularse a cuatro posiciones (diezmilésimas) y no deberán truncarse ni redondearse. | Aceptado |
| | **PPR02 –** El portal debe tener la liga para poder bajar los datos en formato .CSV para cargarlos en hojas de cálculo. | Aceptado |
| | **PPR03 –** Datos a Publicar se deberán publicar en el sitio oficial, de donde se distribuirán a los sitios replicantes de información oficial. Deben contener los valores. | Aceptado con observaciones |
| | **PPR04 –** Requerimientos de portal WEB para publicación – Interfaz Principal. | Aceptado |
| | **PPR05** – Requerimientos de portal WEB para publicación – Encabezado. | Aceptado |
| | **PPR06 –** Requerimientos de portal WEB para publicación – Menú Colapsable. | Aceptado |
| | **PPR07** – Requerimientos de portal WEB para publicación – Avance entidad. | Aceptado |
| | **PPR08 –** Requerimientos de portal WEB para publicación – Resultados Tu Casilla. | Aceptado |
| | **PPR09 –** Requerimientos de portal WEB para publicación – Estadística de Entidad. | Aceptado |
| | **PPR10 –** Requerimientos de portal WEB para publicación – Pie de Página (footer). | Aceptado |
| | **PPR11 –** Requerimientos de portal MÓVIL para publicación – Menú Colapsable | Aceptado con observaciones |
| | **PPR12 –** Requerimientos de portal MÓVIL para publicación – Mi Sección | Aceptado |
| | **PPR13 –** Requerimientos de portal MÓVIL para publicación – Avance Entidad. | Aceptado |
| | **PPR14 –** Requerimientos de portal MÓVIL para publicación – Consulta de Votación. | Aceptado |
| | **PPR15–** Requerimientos de portal MÓVIL para publicación – Estadística Entidad. | Aceptado |
| | **PPR16–** Requerimientos de portal MÓVIL para publicación – Pie de página (footer). | Aceptado |
| | **PPR17** – Requerimiento de actas de Voto anticipado. | Aceptado |

# Análisis de vulnerabilidades

# Análisis Vulnerabilidades Infraestructura PREP

| Pruebas | Control revisado | Resultado |
|---|---|---|
| Red de backend de sitio de publicación | **SPV01** – Escaneo de los activos dentro de la red o segmento del PREP. Los activos deben estar justificado en cuanto a su uso. | Aceptado |
| | **SPV02** – Escaneo de los puertos o servicios habilitados en los activos de la red o segmento del PREP debe estar justificado en cuanto a su uso. | Aceptado |
| | **SPV03** – El escaneo de servicios hecho a la infraestructura no debe no debe tener existencia de vulnerabilidades altas (7.0 – 8.9) o Críticas (9.0 – 10) basados en la clasificación estándar CVSS. | Aceptado |
| | **SPV04** – El escaneo de servicios hechos a la infraestructura no debe tener explotaciones (exploits) desarrollados contra la infraestructura. | Aceptado |
| | **SPV05** – Listar mediante un escaneo de los servidores WEB las vulnerabilidades que pueda haber en estos. | Aceptado |
| | **SPV06** – EL sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado. | Aceptado |
| Red de CATD | **SPV01** – Escaneo de los activos dentro de la red o segmento del PREP. Los activos deben estar justificado en cuanto a su uso. | Aceptado |
| | **SPV02** – Escaneo de los puertos o servicios habilitados en los activos de la red o segmento del PREP debe estar justificado en cuanto a su uso. | Aceptado |
| | **SPV03** – El escaneo de servicios hecho a la infraestructura no debe no debe tener existencia de vulnerabilidades altas (7.0 – 8.9) o Críticas (9.0 – 10) basados en la clasificación estándar CVSS. | Aceptado |
| | **SPV04** – El escaneo de servicios hechos a la infraestructura no debe tener explotaciones (exploits) desarrollados contra la infraestructura. | Aceptado |
| | **SPV05** – Listar mediante un escaneo de los servidores WEB las vulnerabilidades que pueda haber en estos. | Aceptado |
| | **SPV06** – EL sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado. | Aceptado |

# Análisis Vulnerabilidades Infraestructura PREP

| Prueba | Control revisado | Resultado |
|---|---|---|
| Red CCV | **SPV01** – Escaneo de los activos dentro de la red o segmento del PREP. Los activos deben estar justificado en cuanto a su uso. | Aceptado |
| | **SPV02** – Escaneo de los puertos o servicios habilitados en los activos de la red o segmento del PREP debe estar justificado en cuanto a su uso. | Aceptado |
| | **SPV03** – El escaneo de servicios hecho a la infraestructura no debe no debe tener existencia de vulnerabilidades altas (7.0 – 8.9) o Críticas (9.0 – 10) basados en la clasificación estándar CVSS. | Aceptado |
| | **SPV04** – El escaneo de servicios hechos a la infraestructura no debe tener explotaciones (exploits) desarrollados contra la infraestructura. | Aceptado |
| | **SPV05** – Listar mediante un escaneo de los servidores WEB las vulnerabilidades que pueda haber en estos. | Aceptado |
| | **SPV06** – EL sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado. | Aceptado |

# Revisión de configuraciones

# Revisión de Configuraciones 1/6

| Pruebas | Control revisado | Resultado |
|---|---|---|
| Red Backend Sitio Publicación | **SPI01 –** Validar la configuración de los equipos de red siga mejores prácticas y no haya inconsistencias en esta. | Aceptado |
| | **SPI02 –** Los equipos de comunicaciones solo podrán ser accesibles desde la red interna y con protocolo seguro (SSH). | Aceptado |
| | **SPI03 –** Equipos de ruteo y switches deberán tener versiones de sistemas operativos actualizados y bajo soporte. | Aceptado |
| | **SPI04 –** Equipos de comunicaciones y redes deberán estar con soporte y/o sustitución en caso de falla. | Aceptado |
| | **SPI05 –** El sistema PREP deberá contar con esquema de redundancia de comunicaciones. | Aceptado |
| | **SPI06 –** El sistema PREP deberá contar con redundancia eléctrica en caso de caída o fallas en la red eléctrica durante la jornada electoral. | Aceptado |
| | **SPI07 –** Los activos involucrados en el PREP deberán de tener habilitado la función de bitácora (logging) para guardar eventos. | Aceptado |
| | **SPI08 –** Los sistemas involucrados del PREP deberán tener un centro de control y comando que permita el monitoreo de sus sistemas. | Aceptado |
| | **SPI09 –** En los centros de captura no debe haber redes inalámbricas que conecten la infraestructura de captura o del OPL**.** | Aceptado |
| | **SPI10 –** La infraestructura de los ambientes de desarrollo debe estar segregada de la infraestructura de ambientes operativos. | 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. | Aceptado con observaciones |
| | **SPI12 –** Control de acceso al sitio donde está la infraestructura del PREP. | Aceptado |

# Revisión de Configuraciones 2/6

| Pruebas | Control revisado | Resultado |
|---|---|---|
| Red Backend Sitio Publicación | **SPV01** – Escaneo de los activos dentro de la red o segmento del PREP. Los activos deben estar justificado en cuanto a su uso. | Aceptado |
| | **SPV02** – Escaneo de los puertos o servicios habilitados en los activos de la red o segmento del PREP debe estar justificado en cuanto a su uso. | Aceptado |
| | **SPV03** – El escaneo de servicios hecho a la infraestructura no debe no debe tener existencia de vulnerabilidades altas (7.0 – 8.9) o Críticas (9.0 – 10) basados en la clasificación estándar CVSS. | Aceptado |
| | **SPV04** – El escaneo de servicios hechos a la infraestructura no debe tener explotaciones (exploits) desarrollados contra la infraestructura. | Aceptado |
| | **SPV05** – Listar mediante un escaneo de los servidores WEB las vulnerabilidades que pueda haber en estos. | Aceptado |
| | **SPV06** – EL sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado. | Aceptado |
| | **PRS01 –** El OPL debe tener un manual de capacitación para el personal de captura. | Aceptado |
| | **PRS02 –** Debe haber un centro telefónico para consultas o dudas en los distintos procesos o módulos del PREP. | Aceptado |
| | **PRS03 –** Debe existir un proceso de resolución de inconsistencias al momento de captura de acta. | 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). | Aceptado |
| | **PRS05 –** Tener los contratos con los proveedores de telecomunicaciones (primario y secundario) con los mapas de escalación de ellos para reportar eventos. | 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). | Aceptado |
| | **PRS07 –** Tener la documentación del sistema PREP del OPL actualizado y en resguardo por los encargados del área de tecnología del OPL. | Aceptado |

# Revisión de Configuraciones 3/6

| Pruebas | Control revisado | Resultado |
|---|---|---|
| Red CATD | **SPI01 –** Validar la configuración de los equipos de red siga mejores prácticas y no haya inconsistencias en esta. | Aceptado |
| | **SPI02 –** Los equipos de comunicaciones solo podrán ser accesibles desde la red interna y con protocolo seguro (SSH). | Aceptado |
| | **SPI03 –** Equipos de ruteo y switches deberán tener versiones de sistemas operativos actualizados y bajo soporte. | Aceptado |
| | **SPI04 –** Equipos de comunicaciones y redes deberán estar con soporte y/o sustitución en caso de falla. | Aceptado |
| | **SPI05 –** El sistema PREP deberá contar con esquema de redundancia de comunicaciones. | Aceptado |
| | **SPI06 –** El sistema PREP deberá contar con redundancia eléctrica en caso de caída o fallas en la red eléctrica durante la jornada electoral. | Aceptado |
| | **SPI07 –** Los activos involucrados en el PREP deberán de tener habilitado la función de bitácora (logging) para guardar eventos. | Aceptado |
| | **SPI08 –** Los sistemas involucrados del PREP deberán tener un centro de control y comando que permita el monitoreo de sus sistemas. | Aceptado |
| | **SPI09 –** En los centros de captura no debe haber redes inalámbricas que conecten la infraestructura de captura o del OPL**.** | Aceptado |
| | **SPI10 –** La infraestructura de los ambientes de desarrollo debe estar segregada de la infraestructura de ambientes operativos. | 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. | Aceptado |
| | **SPI12 –** Controles de acceso físico a los centros de captura. | Aceptado |
| | **SPI13 –** Control de acceso al sitio donde está la infraestructura del PREP. | Aceptado |
| | **SPI14 –** Verificar si hay control de acceso a teléfonos móviles. | Aceptado con observaciones |

# Revisión de Configuraciones 4/6

| Pruebas | Control Revisado | Resultado |
|---|---|---|
| Red CATD | **SPV01** – Escaneo de los activos dentro de la red o segmento del PREP. Los activos deben estar justificado en cuanto a su uso. | Aceptado |
| | **SPV02** – Escaneo de los puertos o servicios habilitados en los activos de la red o segmento del PREP debe estar justificado en cuanto a su uso. | Aceptado |
| | **SPV03** – El escaneo de servicios hecho a la infraestructura no debe no debe tener existencia de vulnerabilidades altas (7.0 – 8.9) o Críticas (9.0 – 10) basados en la clasificación estándar CVSS. | Aceptado |
| | **SPV04** – El escaneo de servicios hechos a la infraestructura no debe tener explotaciones (exploits) desarrollados contra la infraestructura. | Aceptado |
| | **SPV05** – Listar mediante un escaneo de los servidores WEB las vulnerabilidades que pueda haber en estos. | Aceptado |
| | **SPV06** – EL sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado. | Aceptado |
| | **PRS01 –** El OPL debe tener un manual de capacitación para el personal de captura. | Aceptado |
| | **PRS02 –** Debe haber un centro telefónico para consultas o dudas en los distintos procesos o módulos del PREP. | Aceptado |
| | **PRS03 –** Debe existir un proceso de resolución de inconsistencias al momento de captura de acta. | 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). | Aceptado |
| | **PRS05 –** Tener los contratos con los proveedores de telecomunicaciones (primario y secundario) con los mapas de escalación de ellos para reportar eventos. | 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). | Aceptado |
| | **PRS07 –** Tener la documentación del sistema PREP del OPL actualizado y en resguardo por los encargados del área de tecnología del OPL. | Aceptado |

# Revisión de Configuraciones 5/6

| Pruebas | Control Revisado | Resultado |
|---|---|---|
| Red CCV | **SPI01 –** Validar la configuración de los equipos de red siga mejores prácticas y no haya inconsistencias en esta. | Aceptado |
| | **SPI02 –** Los equipos de comunicaciones solo podrán ser accesibles desde la red interna y con protocolo seguro (SSH). | Aceptado |
| | **SPI03 –** Equipos de ruteo y switches deberán tener versiones de sistemas operativos actualizados y bajo soporte. | Aceptado |
| | **SPI04 –** Equipos de comunicaciones y redes deberán estar con soporte y/o sustitución en caso de falla. | Aceptado |
| | **SPI05 –** El sistema PREP deberá contar con esquema de redundancia de comunicaciones. | Aceptado |
| | **SPI06 –** El sistema PREP deberá contar con redundancia eléctrica en caso de caída o fallas en la red eléctrica durante la jornada electoral. | Aceptado |
| | **SPI07 –** Los activos involucrados en el PREP deberán de tener habilitado la función de bitácora (logging) para guardar eventos. | Aceptado |
| | **SPI08 –** Los sistemas involucrados del PREP deberán tener un centro de control y comando que permita el monitoreo de sus sistemas. | Aceptado |
| | **SPI09 –** En los centros de captura no debe haber redes inalámbricas que conecten la infraestructura de captura o del OPL**.** | Aceptado |
| | **SPI10 –** La infraestructura de los ambientes de desarrollo debe estar segregada de la infraestructura de ambientes operativos. | 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. | Aceptado |
| | **SPI12 –** Controles de acceso físico a los centros de captura. | Aceptado |
| | **SPI13 –** Control de acceso al sitio donde está la infraestructura del PREP. | Aceptado |
| | **SPI14 –** Verificar si hay control de acceso a teléfonos móviles. | Aceptado con observaciones |

# Revisión de Configuraciones 6/6

| Pruebas | Control Revisado | Resultado |
|---|---|---|
| Red CCV | **SPV01** – Escaneo de los activos dentro de la red o segmento del PREP. Los activos deben estar justificado en cuanto a su uso. | Aceptado |
| | **SPV02** – Escaneo de los puertos o servicios habilitados en los activos de la red o segmento del PREP debe estar justificado en cuanto a su uso. | Aceptado |
| | **SPV03** – El escaneo de servicios hecho a la infraestructura no debe no debe tener existencia de vulnerabilidades altas (7.0 – 8.9) o Críticas (9.0 – 10) basados en la clasificación estándar CVSS. | Aceptado |
| | **SPV04** – El escaneo de servicios hechos a la infraestructura no debe tener explotaciones (exploits) desarrollados contra la infraestructura. | Aceptado |
| | **SPV05** – Listar mediante un escaneo de los servidores WEB las vulnerabilidades que pueda haber en estos. | Aceptado |
| | **SPV06** – EL sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado. | Aceptado |
| | **PRS01 –** El OPL debe tener un manual de capacitación para el personal de captura. | Aceptado |
| | **PRS02 –** Debe haber un centro telefónico para consultas o dudas en los distintos procesos o módulos del PREP. | Aceptado |
| | **PRS03 –** Debe existir un proceso de resolución de inconsistencias al momento de captura de acta. | 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). | Aceptado |
| | **PRS05 –** Tener los contratos con los proveedores de telecomunicaciones (primario y secundario) con los mapas de escalación de ellos para reportar eventos. | 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). | Aceptado |
| | **PRS07 –** Tener la documentación del sistema PREP del OPL actualizado y en resguardo por los encargados del área de tecnología del OPL. | Aceptado |

# Pruebas de Negación de Servicio

# Pruebas de Negación de Servicio a PREP

El objetivo de estas pruebas es validar la resiliencia y funcionamiento de la plataforma informática bajo un ataque de tráfico en varios escenarios que afecten el funcionamiento de ésta.

| **Resultados de los ataques volumétricos ejecutados en el sistema PREP SLP 2024** | |
|---|---|
| Prueba | Resultado |
| SPN01 – La infraestructura debe soportar un ataque volumétrico TCP | Aceptado |
| SPN02 – La infraestructura deberá soportar un ataque volumétrico por UDP-DNS | Aceptado |
| SPN03 – La infraestructura deberá poder soportar un ataque volumétrico por ICMP | Aceptado |
| SPN04 – La infraestructura deberá poder manejar un ataque en la capa de aplicación | Aceptado |

# Pruebas DOS a PREP

Controles compensatorios validados

| Resultados de los controles compensatorios asociados a la protección de ataques de Negación de Servicio | |
|---|---|
| **Prueba** | **Resultado** |
| SPN05 – Validación de las cuotas de servicio configuradas en las suscripciones de servicios de nube | Aceptado |
| SPN06 – Existencia de un plan o procedimiento a seguir en caso de evento de ataque de DOS | Aceptado |
| SPN07- Existencia de contratos de servicio de protección de exceso de tráfico o para blindar contra ataques DOS | Aceptado |
| SPN08 – Existencia de un plan de comunicación hacia la comunidad en caso de eventos de DOS | Aceptado |

# Validación de sistema informático

# Validación de Sistema Informático y Base de Datos

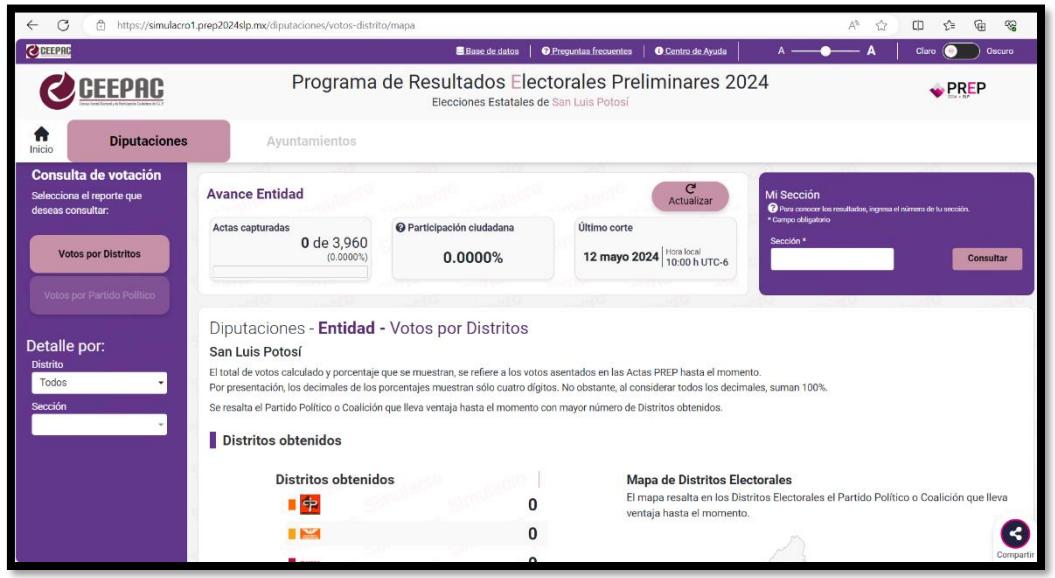
```
# Generar hash SHA256 recursivo y lista de archivos para la carpeta sitio en el servidor remoto
sitio_hash=$(get_remote_recursive_hash "$REMOTE_SITIO_FOLDER_PATH")

# Generar hash SHA256 recursivo y lista de archivos para la carpeta frontend en el servidor remoto
frontend_hash=$(get_remote_recursive_hash "$REMOTE_FOLDER_PATH")

# Generar hash SHA256 recursivo y lista de archivos para la carpeta admin en el servidor remoto
admin_hash=$(get_remote_recursive_hash "$REMOTE_ADMIN_FOLDER_PATH")
```

*Los procesos de integridad generan como resultado final un hash de hashes, uno específico para el sitio, otro específico para aplicativo y otro para el sitio de administración.*

*Proceso Hash del sistema informático*




*Validación de proceso de inicialización de la Base de datos*

Tecnológico de Monterrey

CEEPAC

# Pruebas de Integridad y BD

| Prueba | Control | Resultado |
|---|---|---|
| **Integridad y Base de datos** | Validación de procedimiento de integridad mediante hash | Aceptado |
| | Validación de proceso de puesta en cero de la base de datos | Aceptado |
| | Constancia de hechos de la generación de huellas criptográficas (día de la jornada) | **Pendiente** |
| | Constancias de hechos de la validación de los programas y de las bases de datos (día de la jornada) | **Pendiente** |

- Las pruebas de revisión de firma digital y reinicio de base de datos se han llevado acabo en los tres simulacros previos a la jornada electoral. Los procedimientos correspondientes de prueba de integridad y puesta en cero de la base de datos se analizaron previamente para validar que cumplan con los requerimientos que garantizan que el código no se modificará en momento alguno durante la jornada electoral y que la base de datos se encuentra vacía y lista para recibir la información de las actas.
- Unos días antes de la jornada electoral se tiene que generar el hash final, compartir con el ente auditor y notario para resguardo. Se validará que este concuerde antes de habilitar el sistema PREP el domingo 02 de junio, durante el funcionamiento del sistema y al cerrar el ejercicio.

# Observaciones de avances en simulacros

# Comentarios generales durante simulacros

- **Simulacro 01 – CCV SLP, CATD Distrito 5 CME, Fraccionamiento Tangamanga, SLP**
  - Algunos CATD se encontraban con dudas, se atendieron en el centro de control. Se presentaron algunos detalles con la aplicación PREP casilla, las actas no contaban aún con código de barras. Se generó un apagón no planeado en Lagunillas y se activó el protocolo de la planta de energía. Se contó con 1 CCV, 73 CATD, 495 CAEL, 110 Digitalizadores y 110 capturistas. Se realiza proceso de “corte de luz” y “corte de enlace” en CCV sin inconvenientes.

- **Simulacro 02 – CCV SLP, CATD Distrito 8 CDE, Valle de Jacarandas, SLP**
  - Se percibe una mejor organización de los coordinadores de los CATD, las actas ya cuentan con identificador, se siguen presentando detalles con la aplicación PREP casilla y desde los CATD se terminan de escanear algunas actas. Nuevamente se llevan a cabo pruebas exitosas de desconexión de internet y falla eléctrica en CCV. Se presentaron problemas de energía en CATD de Tamanzuchale. Se dañó un switch del CCV y se instaló uno temporal, se aprovechó para reforzar el procedimiento de continuidad de servicio. En el CCV se presentó una falla de luz y se volvió a ejecutar el protocolo con la planta de energía la cuál se quedó funcionando el resto del ejercicio sin problema.

- **Simulacro 03 – CCV SLP, CATD Distrito 2 CME, Mexquitic de Carmona, SLP**
  - El personal se observa más familiarizado con el proceso debido a la experiencia de los simulacros anteriores, se logra más eficiencia en la velocidad de digitalización y captura, siendo el simulacro que termina más temprano (3:20 PM ). Se recomienda concentrar esfuerzos en la exactitud de captura y verificación el día de la jornada electoral. Se ejecuta simulacro de CATD violentado y cambio de sitio para continuar con el proceso. PREP casilla siguió presentando algunas fallas que fueron localizadas y se establece el compromiso de funcionalidad para la jornada electoral.

# Conclusiones

Como resultado de las pruebas realizadas hasta el día de hoy, se concluye que los servidores e infraestructura pertenecientes al sistema PREP del estado de San Luis Potosí cuentan con nivel de riesgo bajo debido a la configuración robusta de la tecnología implicada y los controles de protección aplicados.

**El sistema cumple con los requerimientos funcionales solicitados por el INE y se encuentra en condiciones adecuadas para su correcta operación durante la jornada electoral de este 02 de junio del presente año.**

Jessica Izquierdo

M.C. Jessica Izquierdo
Ente Auditor PREP SLP
30 de mayo, 2024

Tecnológico de Monterrey

CEEPAC
Consejo Estatal Electoral y de Participación Ciudadana de S.L.P.