



**TECNOLÓGICO  
DE MONTERREY®**

# **Informe Final de Configuraciones de la Infraestructura del Sistema Informático del PREP**

**Informe preliminar de las pruebas y escaneos de vulnerabilidades,  
así como de configuraciones del sistema informático del PREP del  
IEE Sinaloa**

## **Descripción breve**

Este documento contiene el resultado y la evidencia del escaneo de vulnerabilidades a los elementos de la solución de informática como parte de los servicios de auditoría de seguridad del sistema preliminar de resultados para el IEE Sinaloa

**Roberto Luis Iriarte / Raime Alejandro Bustos**

roberto@iriarte.net

raime.bustos@tec.mx

**Jesús R. González / Juan Arturo Nolasco**

jrgonza@gmail.com

jnolasco@itesm.mx

## Índice

1	Introducción	2
2	Resultados Generales	2
2.1	Criterios utilizados para la auditoría	2
2.2	Pruebas Escaneo Vulnerabilidades de Activos y Configuración	3
3	Comentarios	4

Versión	Fecha	Descripción
1.0		
1.1	14/Abr/2021	Documento inicial preliminar de configuración e infraestructura

Dictamen elaborado por:

MSc. Jesús Raúl González Hernández en coordinación con el Dr. Juan Arturo Nolasco, Ing. Roberto Luis Iriarte Pablos y MSE Raime Alejandro Bustos Garde

## 1 Introducción

Este documento presenta los avances y resultados preliminares de la revisión de configuraciones y de los escaneos y análisis de vulnerabilidades del PREP para la jornada electoral del 2021

Este documento se dará en cada iteración de pruebas que se de para llevarlo a una aceptación del 100% por lo que estos resultados se documentarán cada vez que se lleve a cabo el escaneo.

La sección de anexos documenta en cada uno los resultados de cada iteración con las firmas por parte del ente auditor y un representante del **IEE Sinaloa**.

Cada iteración de pruebas estará documentada en una sección de anexo de este documento con sus comentarios (si así lo requieren) y las firmas de los representantes de la entidad auditora

## 2 Resultados Generales

### 2.1 Criterios utilizados para la auditoría

Las tablas de la sección 2.2 documentarán resultados en función de los criterios de aceptación dados. 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	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.

### 2.2 Pruebas Escaneo Vulnerabilidades de Activos y Configuración

Prueba	Resultado	Prueba	Resultado
<b>SPI01</b> – Validar la configuración de los equipos de red siga mejores prácticas y no haya inconsistencias en esta	<b>Aceptado</b>	<b>SPV01</b> – Escaneo de los activos dentro de la red o segmento del PREP. Los activos deben estar justificado en cuanto a su uso	<b>Aceptado</b>
<b>SPI02</b> – Los equipos de comunicaciones sólo podrán ser accesibles desde la red interna y con protocolo seguro (SSH).	<b>Aceptado</b>	<b>SPV02</b> – 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	<b>Aceptado</b>
<b>SPI03</b> – Equipos de ruteo y switches deberán tener versiones de sistemas operativos actualizados y bajo soporte	<b>Aceptado</b>	<b>SPV03</b> – El escaneo de servicios hecho a la infraestructura no debe tener existencia de vulnerabilidades altas (7.0 – 8.9) o Críticas (9.0 – 10) basados en la clasificación estándar CVSS	<b>Aceptado</b>
<b>SPI04</b> – Equipos de comunicaciones y redes deberán estar con soporte y/o sustitución en caso de falla	<b>Aceptado</b>	<b>SPV04</b> – El escaneo de servicios hechos a la infraestructura no debe tener explotaciones (exploits) desarrollados contra la infraestructura.	<b>Aceptado</b>
<b>SPI05</b> – El sistema PREP deberá contar con esquema de redundancia de comunicaciones	<b>Aceptado</b>	<b>SPV05</b> – Listar mediante un escaneo de los servidores WEB las vulnerabilidades que pueda haber en estos	<b>Aceptado</b>
<b>SPI06</b> – El sistema PREP deberá contar con redundancia eléctrica en caso de caída o fallas en la red eléctrica durante la jornada electoral	<b>Aceptado</b>	<b>SPV06</b> – El sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado	<b>Aceptado</b>
<b>SPI07</b> – Los activos involucrados en el PREP deberán de tener habilitado la función de bitácora (logging) para guardar eventos	<b>Aceptado</b>	<b>PRS01</b> – La OPL debe tener un manual de capacitación para el personal de captura	<b>Aceptado</b>
<b>SPI08</b> – Los sistemas involucrados del PREP deberán tener un centro de control y comando que permita el monitoreo de sus sistemas	<b>Aceptado</b>	<b>PRS02</b> – Debe haber un centro telefónico para consultas o dudas en los distintos procesos o módulos del PREP	<b>Aceptado</b>
<b>SPI09</b> – En los centros de captura no debe haber redes inalámbricas que conectan la infraestructura de captura o del OPL.	<b>Aceptado</b>	<b>PRS03</b> – Debe existir un proceso de resolución de inconsistencias al momento de captura de acta	<b>Aceptado</b>
<b>SPI10</b> – La infraestructura de los ambientes de desarrollo debe estar segregada de la infraestructura de ambientes operativos	<b>Aceptado</b>	<b>PRS04</b> – Contratos de soporte externo en caso de eventualidades sobre las plataformas operativas que se utilizan en el PREP (para sistemas desarrollados por terceros)	<b>Aceptado</b>
<b>SPI11</b> – El sistema debe tener recursos dedicados por lo que no debe compartir recursos con otros sistemas o plataformas ajenos al PREP en evaluación	<b>Aceptado</b>	<b>PRS05</b> – Tener los contratos con los proveedores de telecomunicaciones (primario y secundario) con los mapas de escalación de ellos para reportar eventos	<b>Aceptado</b>
<b>SPI12</b> – Controles de acceso físico a los centros de captura	<b>Aceptado</b>	<b>PRS06</b> – 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)	<b>Aceptado</b>
<b>SPI13</b> – Control de acceso al sitio donde está la infraestructura del PREP	<b>Aceptado</b>	<b>PRS07</b> – Tener la documentación del sistema PREP de la OPL actualizado y en resguardo por los encargados del área de tecnología de la OPL	<b>Aceptado</b>
<b>SPI14</b> – Verificar si hay control de acceso a teléfonos móviles	<b>Aceptado</b>		