



**TECNOLÓGICO  
DE MONTERREY®**

## **Informe de la Aplicación de Recomendaciones a la Infraestructura del Sistema Informático del PREP**

**Informe de la Aplicación de Recomendaciones dadas sobre la  
infraestructura del sistema informático del PREP del IEE Sinaloa**

### **Descripción breve**

Este documento contiene el resultado de la aplicación de recomendaciones dadas por el auditor en la revisión de la configuración de la Infraestructura de 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 Nolazco  
jrgonza@gmail.com jnolazco@itesm.mx

## Índice

1 Resumen Ejecutivo	2
2 Objetivos	3
3 Alcance	4
4 Criterios utilizados para la auditoría	4
5 Observaciones Preliminares	5
5.1 Hallazgos Pruebas Revisión Configuraciones	5
5.1.1 Recomendaciones Revisión de Configuraciones	6
5.2 Hallazgos Pruebas Escaneo Vulnerabilidades de Activos	8
5.2.1 Recomendaciones Escaneo Vulnerabilidades de Activos	9
5.3 Hallazgos Pruebas Controles físicos	9
5.3.1 Recomendaciones Controles Físicos	9
5.4 Hallazgos Pruebas Revisión de infraestructura	9
5.4.1 Recomendaciones Infraestructura	10
5.5 Hallazgos Pruebas Soporte Operativo	11
5.5.1 Recomendaciones Soporte Operativo	11

<b>Versión</b>	<b>Fecha</b>	<b>Descripción</b>
1.0		

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 Resumen Ejecutivo

Este documento presenta el resultado de aplicación de recomendaciones basadas en la revisión de configuraciones de la infraestructura del PREP del **IEE Sinaloa** para la jornada electoral del 2021

#	Prueba	Resultado	Recomendación
6.1	a) La infraestructura de red deberá estar segregada entre las distintas partes del proceso del PREP	Aceptado	
	b) Validar la configuración de los equipos de red siga mejores prácticas y no haya inconsistencias en esta	Aceptado	
	c) Los equipos de comunicaciones sólo podrán ser accesibles desde la red interna y con protocolo seguro (SSH).	Aceptado	Deshabilitar acceso por http
	d) Equipos de ruteo y switches deberán tener versiones de sistemas operativos actualizados y bajo soporte	Aceptado	Actualizar el firmware de switch Switch Cisco SG220-26P y Firewall Sonicwall NSA 2650
	e) Servidores deberán tener versiones de sistemas operativos actualizados y bajo soporte	Aceptado	
	f) Aplicaciones deberán tener versiones de sistemas operativos actualizados y bajo soporte	Aceptado	
	g) Validar los parámetros de configuración de las aplicaciones en uso para la jornada electoral y determinar recomendaciones	Aceptado	
	h) Estaciones de captura deberán tener versiones de sistemas operativos actualizados actualizados y bajo soporte	Aceptado	
	i) Las estaciones de captura solo deben tener acceso hacia las aplicaciones del PREP de la jornada 2021	Aceptado	
	j) Los usuarios de las estaciones de captura en las estaciones de captura no deberán ser de administrador	Aceptado	
	k) Usuarios de estaciones de captura, no deben poder bajar, instalar Software que no esté ya instalado en las estaciones de captura	Aceptado	
6.2	a) El escaneo de sistemas operativos de servidores no haya vulnerabilidades de nivel alto o crítico	Aceptado	Actualizar librería openssl en CentOS 7.9
	b) El escaneo de servidores solo debe tener activos los servicios que presten el día de la jornada electoral <b>IEE Sinaloa</b>	Aceptado	

	c) El escaneo de servidores no debe arrojar ninguna vulnerabilidad de nivel alto o crítico	<b>Aceptado</b>	Actualizar Apache HTTP Server o aplicar controles compensatorios
<b>6.3</b>	a) Controles de acceso físico a los centros de captura	<b>Aceptado</b>	
	b) Control de acceso al sitio donde está la infraestructura del PREP	<b>Aceptado</b>	
	c) Verificar si hay control de acceso a teléfonos móviles	<b>Aceptado</b>	
<b>6.4</b>	a) Verificar funcionamiento del esquema de redundancia de comunicaciones	<b>Aceptado</b>	
	b) Verificar existencia y funcionamiento de redundancia eléctrica para continuidad de operaciones	<b>Aceptado</b>	
	c) Hay que asegurar que los equipos de comunicaciones tengan soporte de sustitución o que haya algún equipo sustituto	<b>Aceptado</b>	
	d) El escaneo de servidores no debe arrojar ninguna vulnerabilidad de nivel alto o crítico	<b>Aceptado</b>	Actualizar Apache HTTP Server o aplicar controles compensatorios
	e) Verificar que los equipos tengan configurados capacidades de bitácora para analizar eventos que se presenten	<b>Aceptado</b>	
	f) Existencia de estaciones de control y monitoreo del sistema	<b>Aceptado</b>	
	g) En los centros de captura no debe haber redes inalámbricas que conecten la infraestructura de captura o del <b>IEE Sinaloa</b> a esta.	<b>Aceptado</b>	
<b>6.5</b>	a) Manual de capacitación para los equipos de captura	<b>Aceptado</b>	
	b) Línea de soporte para aclarar dudas en la captura	<b>Aceptado</b>	
	c) Proceso de resolución e inconsistencias en captura de actas	<b>Aceptado</b>	
	d) Proceso para crecimiento de capacidad de infraestructura en caso de requerir	<b>Aceptado</b>	

## 2 Objetivos

Este documento documenta los resultados preliminares de las pruebas para poder hacer la implementación de controles o medidas para poder cerrar los hallazgos en cuanto a vulnerabilidades y disminuir la superficie de riesgo que el PREP del **IEE Sinaloa** pueda tener al terminar la primera revisión.

## 3 Alcance

El alcance de las pruebas se estructura en la sección 6 de este documento en base a las siguientes partes:

- Revisión Configuraciones – Configuraciones y parámetros de los equipos involucrados en el PREP
- Escaneos de Activos – Revisión de vulnerabilidades de los sistemas operativos y aplicaciones
- Revisión de infraestructura – Revisión de infraestructura que soporta al PREP
- Controles físicos – Validación de controles físicos de la infraestructura e instalaciones
- Soporte Operativo – Revisión de los controles de soporte operativo a la operación del PREP

## 4 Criterios utilizados para la auditoría

Las tablas de la sección 6 documentaron resultados en función de los criterios de aceptación dados. En la sección de anexos se encuentra la evidencia de dichas pruebas. 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.

## 5 Observaciones Preliminares

Las observaciones y recomendaciones se harán sobre el anexo correspondiente de pruebas que se esté realizando y bajo los criterios que se detallan por cada una de las pruebas. En esta sección se presenta un resumen, en función de los resultados y revisión de hallazgos, de los resultados de ésta y su cumplimiento, así como hallazgos por clasificación que se de.

### 5.1 Hallazgos Pruebas Revisión Configuraciones

Para estas pruebas, en adición a que el personal técnico de la **IEE Sinaloa** proporcione la configuración en línea de comando o por interfaz gráfica para revisión, el Ente Auditor usará las herramientas necesarias (no intrusivas) para detectar mediante escaneos a los activos, las vulnerabilidades que puedan existir en los activos que pertenecen al PREP.

<b>Resultados Preliminares Revisión Configuraciones IEE Sinaloa 2021</b>			
<b>Prueba</b>	<b>Criterio Aceptación</b>	<b>Resultado</b>	<b>Comentarios</b>
a) La infraestructura de red deberá estar segregada entre las distintas partes del proceso del PREP	Debe existir segregación entre los distintos segmentos que ejecutan las partes del proceso PREP, por lo menos: Prueba, Captura, procesamiento y publicación	<b>Aceptado</b>	Los servidores productivos no comparten recursos con otros ambientes de prueba.
b) Validar la configuración de los equipos de red siga mejores prácticas y no haya inconsistencias en esta	LA configuración debe tener incorporada la limitación de protocolos, direcciones que no se estén usando en la jornada electoral 2021	<b>Aceptado</b>	Solo están habilitados los servicios y puertos necesarios para la función del sistema y del propio servidor.
c) Los equipos de comunicaciones sólo podrán ser accesibles desde la red interna y con protocolo seguro (SSH).	Acceso a los equipos de comunicaciones (FW, SW, Router) solo debe ser posible desde la red interna del <b>IEE Sinaloa</b>	<b>Aceptado</b>	El acceso a los firewalls y router son por consola web, se contaba con acceso por http, se deshabilitó durante la auditoría quedando solo por conexión segura https.
d) Equipos de ruteo y switches deberán tener versiones de sistemas operativos actualizados y bajo soporte	Las versiones de los Firewalls, switches y routers deben ser actuales y aun disponibles	<b>Aceptado</b>	A recomendación de Ente Auditor se actualizó el firmware del firewall SonicWall.
e) Servidores deberán tener versiones de sistemas operativos actualizados y bajo soporte	Las versiones de los sistemas operativos de servidores deben ser actuales y aun disponibles	<b>Aceptado</b>	Servidores con última versión de mayo de CentOS 7.9.
f) Aplicaciones deberán tener versiones de sistemas operativos actualizados y bajo soporte	Las versiones de las aplicaciones deben ser actuales y aun disponibles	<b>Aceptado</b>	Actualizar Apache HTTP Server o aplicar controles compensatorios.
g) Validar los parámetros de configuración de las aplicaciones en uso para la jornada electoral y determinar recomendaciones	Los parámetros de la aplicación deben seguir la mejor práctica de configuración de la aplicación para su operación.	<b>Aceptado</b>	Parámetros de configuración siguen las mejores prácticas.
h) Estaciones de captura deberán tener versiones de sistemas operativos actualizados actualizados y bajo soporte	La versión de sistema operativo en la estación de captura debe ser actuales y aun disponibles	<b>Aceptado</b>	Estaciones con Windows 10 y parches liberados en marzo 2021.

i)	Las estaciones de captura solo deben tener acceso hacia las aplicaciones del PREP de la jornada 2021	No debe haber acceso a Internet en las estaciones de captura de los centros de captura	<b>Aceptado</b>	Equipos sin acceso a internet, ni a otras aplicaciones.
j)	Los usuarios de las estaciones de captura en las estaciones de captura no deberán ser de administrador	El usuario de la estación de captura no deberá tener privilegios de administrador	<b>Aceptado</b>	Utilizan una cuenta de invitado para acceder a la laptop.
k)	Usuarios de estaciones de captura, no deben poder bajar, instalar Software que no este ya instalado en las estaciones de captura	El usuario de captura no debe poder instalar o bajar aplicaciones en la estación de captura.	<b>Aceptado</b>	Equipos sin acceso a Internet ni con privilegios de administrador.

## 5.1.1 Recomendaciones Revisión de Configuraciones

Recomendaciones Preliminares Revisión Configuraciones IEE Sinaloa 2021	
Prueba	Recomendación
l) La infraestructura de red deberá estar segregada entre las distintas partes del proceso del PREP	No hay recomendación
m) Validar la configuración de los equipos de red siga mejores prácticas y no haya inconsistencias en esta	No hay recomendación
n) Los equipos de comunicaciones sólo podrán ser accesibles desde la red interna y con protocolo seguro (SSH).	Deshabilitar el acceso por http. Se realizó en presencia de Ente Auditor
o) Equipos de ruteo y switches deberán tener versiones de sistemas operativos actualizados y bajo soporte	Se recomendó actualizar Switch Cisco SG220-26P en versión de firmware 1.1.4.1 a la última es 1.1.4.8 y Firewall Sonicwall NSA 2650, v6.5.1-5-6n actualizar a SonicOS 6.5.4.7-83n
p) Servidores deberán tener versiones de sistemas operativos actualizados y bajo soporte	No hay recomendación
q) Aplicaciones deberán tener versiones de sistemas operativos actualizados y bajo soporte	Se recomienda actualizar el Apache Web Server a la última versión, 2.4.48
r) Validar los parámetros de configuración de las aplicaciones en uso para la jornada electoral y determinar recomendaciones	No hay recomendación
s) Estaciones de captura deberán tener versiones de sistemas operativos actualizados actualizados y bajo soporte	Actualizar parches a los últimos disponibles para Windows 10
t) Las estaciones de captura solo deben tener acceso hacia las aplicaciones del PREP de la jornada 2021	No hay recomendación
u) Los usuarios de las estaciones de captura en las estaciones de captura no deberán ser de administrador	No hay recomendación

---

v) Usuarios de estaciones de captura, no deben poder bajar, instalar Software que no esté ya instalado en las estaciones de captura	No hay recomendación
---	----------------------

## 5.2 Hallazgos Pruebas Escaneo Vulnerabilidades de Activos

### Resultados Preliminares Escaneo Vulnerabilidades de Activos IEE Sinaloa 2021

Prueba	Criterio Aceptación	Resultado	Comentarios
a) El escaneo de sistemas operativos de servidores no haya vulnerabilidades de nivel alto o crítico	Los sistemas operativos de servidores no debe haber vulnerabilidades críticas ni altas. Si tienen nivel medio, deberá existir contramedidas para esta	<b>Aceptado</b>	Servidores con CentOS v7.9 2009.
b) El escaneo de servidores solo debe tener activos los servicios que presten el día de la jornada electoral IEE Sinaloa	Las aplicaciones que se estén utilizando para la jornada deberán estar activados sus puertos y no otros distintos a estos.	<b>Aceptado</b>	Aplicaciones y puertos sólo los necesarios para la operación y monitoreo del sistema PREP.
c) El escaneo de servidores no debe arrojar ninguna vulnerabilidad de nivel alto o crítico	Las aplicaciones no deben tener vulnerabilidades críticas ni altas. Si tienen nivel medio, deberá existir contramedidas para esta	<b>Aceptado</b>	Vulnerabilidades críticas en Apache HTTP Server, se mitigan con controles compensatorios.

Para las vulnerabilidades encontradas en la sección 5.2. se arreglarán en función a la criticidad especificada por el estándar CVSS 3.1 (<https://www.first.org/cvss/specification-document>)

CVSS Score	
0 - 1	Bajo
1 - 2	
2 - 3	
3 - 4	
4 - 5	Medio
5 - 6	
6 - 7	
7 - 8	
8 - 9	Alto
9 - 10	Crítico

La documentación de vulnerabilidades por activo se puede hacer en la siguiente tabla

Dirección IP	CVSS Score	Descripción
prepsinaloa.info 10.3.0.224 10.3.0.222	CVE-2014-0231	mod_cgid denial of service
prepsinaloa.info 10.3.0.224 10.3.0.222	CVE-2016-8743	important: Apache HTTP Request Parsing Whitespace Defects
prepsinaloa.info 10.3.0.224 10.3.0.222	CVE-2017-3169	important: mod_ssl Null Pointer Dereference

prepsinaloa.info 10.3.0.224 10.3.0.222	CVE-2019-0217	important: mod_auth_digest access control bypass
prepsinaloa.info 10.3.0.224 10.3.0.222		TLS Version 1.0 Protocol Detection
prepsinaloa.info 10.3.0.224 10.3.0.222	CVE2016-0734	Web Application Potentially Vulnerable to Clickjacking
prepsinaloa.info 10.3.0.224 10.3.0.222	CVE-2014-0226	Race condition in the mod_status module in the Apache HTTP Server
prepsinaloa.info 10.3.0.224 10.3.0.222	CVE-2021-31618	The vulnerability exists due to a NULL pointer dereference error in mod_http2 in Apache HTTP server

### 5.2.1 Recomendaciones Escaneo Vulnerabilidades de Activos

Recomendaciones Escaneo Vulnerabilidades de Activos IEE Sinaloa 2021	
Prueba	Recomendaciones
d) El escaneo de sistemas operativos de servidores no haya vulnerabilidades de nivel alto o crítico	Se recomienda actualizar versión del firmware de switches y firewalls
e) El escaneo de servidores solo debe tener activos los servicios que presten el día de la jornada electoral <b>IEE Sinaloa</b>	No hay recomendación
f) El escaneo de servidores no debe arrojar ninguna vulnerabilidad de nivel alto o crítico	Se recomendó actualizar Apache Web Server en servidores PREP y Central PREP

## 5.3 Hallazgos Pruebas Controles físicos

Resultados Preliminares Controles físicos IEE Sinaloa 2021			
Prueba	Criterio Aceptación	Resultado	Comentarios
a) 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	<b>Aceptado</b>	Control de acceso con tarjeta y registro sanitario de temperatura y de registro de asistencia.
b) 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.	<b>Aceptado</b>	Estaciones de captura sin Wi-Fi, sin acceso a recursos del sistema operativo ni navegación por Internet.
c) Verificar si hay control de acceso a teléfonos móviles	Debe haber un lugar donde registrar equipos móviles para control del acceso de estos	<b>Aceptado</b>	Está establecido la política que prohíbe el uso de celular durante el PREP, se recogerán para resguardo al principio del turno del Capturista y se le regresará solo al final del mismo.

### 5.3.1 Recomendaciones Controles Físicos

Recomendaciones Preliminares Controles físicos IEE Sinaloa 2021	
Prueba	Recomendaciones
d) Controles de acceso físico a los centros de captura	Sin recomendaciones
e) Control de acceso al sitio donde está la infraestructura del PREP	Sin recomendaciones
f) Verificar si hay control de acceso a teléfonos móviles	Sin recomendaciones

## 5.4 Hallazgos Pruebas Revisión de infraestructura

Resultados Preliminares Infraestructura IEE Sinaloa 2021			
Prueba	Criterio Aceptación	Resultado	Comentarios
a) Verificar funcionamiento del esquema de redundancia de comunicaciones	Existencia de redundancia de sistemas de comunicaciones para continuidad de captura. Verificar tiempos de convergencia (desde caída hasta recuperación)	<b>Aceptado</b>	Se realizaron pruebas de redundancia de comunicaciones el día 5 de junio 2021.

b)	Verificar existencia y funcionamiento de redundancia eléctrica para continuidad de operaciones	Existencia de planta eléctrica para en caso de corte. Verificar tiempos de corte (desde caída hasta recuperación)	<b>Aceptado</b>	La prueba de redundancia eléctrica se realizó el día 5 de junio, 2021.
c)	Hay que asegurar que los equipos de comunicaciones tengan soporte de sustitución o que haya algún equipo sustituto en caso de falla	Existencia de contrato de soporte de proveedor o bien equipo de respaldo	<b>Aceptado</b>	Cuentan con equipo en resguardo para atender una incidencia.
d)	El escaneo de servidores no debe arrojar ninguna vulnerabilidad de nivel alto o crítico	Las aplicaciones no deben tener vulnerabilidades críticas ni altas. Si tienen nivel medio, deberá existir contramedidas para esta	<b>Aceptado</b>	Vulnerabilidades críticas en Apache HTTP Server se mitigan con controles compensatorios.
e)	Verificar que los equipos tengan configurados capacidades de bitácora para analizar eventos que se presenten	Los sistemas deben tener configurados las bitácoras para capturar los eventos que se presenten en los elementos del PREP	<b>Aceptado</b>	Servidores y equipos de telecomunicaciones con bitácoras habilitadas.
f)	Existencia de estaciones de control y monitoreo del sistema	El <b>IEE Sinaloa</b> debe tener una estación y herramientas que este monitoreando el funcionamiento de los sistemas y redes que componen el PREP	<b>Aceptado</b>	Se cuenta con un centro de mando donde se monitorea el funcionamiento de los sistemas.
g)	En los centros de captura no debe haber redes inalámbricas que conecten la infraestructura de captura o del <b>IEE Sinaloa</b> a esta.	Inventariar redes existentes y verificar que su único acceso sea hacia la red pública	<b>Aceptado</b>	No hay redes inalámbricas que se conecten al sistema Central PREP.

## 5.4.1 Recomendaciones Infraestructura

Recomendaciones Preliminares Infraestructura IEE Sinaloa 2021	
Prueba	Recomendaciones
h) Verificar funcionamiento del esquema de redundancia de comunicaciones	Sin recomendaciones
i) Verificar existencia y funcionamiento de redundancia eléctrica para continuidad de operaciones	Sin recomendaciones
j) Hay que asegurar que los equipos de comunicaciones tengan soporte de sustitución o que haya algún equipo sustituto en caso de falla	Sin recomendaciones
k) El escaneo de servidores no debe arrojar ninguna vulnerabilidad de nivel alto o crítico	Se recomendó actualizar Apache HTTP Server, deshabilitar TLS 1.1 e inferior, deshabilitar DES/3DES y aplicar un parche en sistema operativo CentOS
l) Verificar que los equipos tengan configurados capacidades de bitácora para analizar eventos que se presenten	Sin recomendaciones
m) Existencia de estaciones de control y monitoreo del sistema	Sin recomendaciones
n) En los centros de captura no debe haber redes inalámbricas que conecten la infraestructura de captura o del <b>IEE Sinaloa</b> a esta.	Sin recomendaciones

## 5.5 Hallazgos Pruebas Soporte Operativo

### Resultados Preliminares Controles físicos IEE Sinaloa 2021

Prueba	Criterio Aceptación	Resultado	Comentarios
a) Manual de capacitación para los equipos de captura	Los sistemas operativos de servidores no debe haber vulnerabilidades críticas ni altas. Si tienen nivel medio, deberá existir contramedidas para esta	Aceptado	Cumple, se cuenta con una guía rápida para Capturista.
b) Línea de soporte para aclarar dudas en la captura	Las aplicaciones que se estén utilizando para la jornada deberán estar activados sus puertos y no otros distintos a estos.	Aceptado	Mesa de ayuda con teléfonos IP atendiendo en extensión 3500.
c) Proceso de resolución e inconsistencias en captura de actas	Existencia de una mesa de soporte para revisar inconsistencias en capturas de datos de las actas	Aceptado	Se cuenta con el módulo de verificación/validación MVEVAL.
d) Proceso para crecimiento de capacidad de infraestructura en caso de requerirlo	Proceso de crecimiento de capacidad en infraestructura en caso de ser requerido	Aceptado	Se cuenta con Plan de Continuidad.

### 5.5.1 Recomendaciones Soporte Operativo

#### Recomendaciones Preliminares Controles físicos IEE Sinaloa 2021

Prueba	Recomendaciones
e) Manual de capacitación para los equipos de captura	Se cuenta con guía rápida para capturista, se recomienda elaborar manuales para MRID, MIDAEC, PREP Casilla, CATD Celular, MVEVAL
f) Línea de soporte para aclarar dudas en la captura	Sin recomendaciones
g) Proceso de resolución e inconsistencias en captura de actas	Sin recomendaciones
h) Proceso para crecimiento de capacidad de infraestructura en caso de requerirse	Sin recomendaciones