



### INFORME FINAL DE LAS PRUEBAS FUNCIONALES DE CAJA NEGRA DEL SISTEMA INFORMÁTICO PREP SINALOA

- Introducción

El presente documento tiene como objetivo el evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares que se utilizará en la elección local, el día de la jornada electoral.

Estas pruebas permiten conocer el conjunto de condiciones de entrada que ejerciten todos los requisitos funcionales del PREP. En ellas se ignora la estructura de control, concentrándose en los requisitos funcionales del sistema y ejercitándolos. Es decir, se basa en verificar que los datos de entrada (plasmados en las AEC) sean los que se reflejan en la publicación, Pagina Web Publica del PREP.

- Metodología

La revisión se realizó en tres etapas para analizar el funcionamiento de la aplicación en relación con las fases del proceso técnico operativo, priorizando la digitalización, captura, verificación y publicación de resultados, determinando los flujos completos e interacción entre los diversos módulos. Para el caso del Instituto Electoral del Estado de Sinaloa (IEES) son: acopio, digitalización, captura, verificación, publicación y cotejo, debiendo cumplirse cada una de ellas en el orden señalado.

Se utilizaron Casos de Prueba considerando los procesos declarados para cada módulo.

- Criterios utilizados para la auditoría

Los marcados por el protocolo de Auditoría del Sistema informático del PREP UNAM, Versión 5, del 23 de enero de 2018.

- Resumen Ejecutivo

Se utilizaron los equipos instalados por la empresa en el CATD, y se permitió acceso a los servidores para las pruebas de los modulos de Digitalización, Captura y Validación (MCAD, CAPREP, VERIPREP) y de Publicación de Resultados (SIPREP).

Se aplicaron los casos de prueba para cada módulo, donde se detectaron problemas en los tiempos de captura, lo cual retrasaba el tiempo de publicación, pero no afectaba a la funcionalidad requerida.

Posterior a la revisión de los modelos de entrada y salida, fue necesario supervisar en las oficinas del COPREP, los modulos de Monitor PREP, Central PREP, PREP Casilla, Módulo Coordinador, y SILPREP.

Durante los simulacros se determinó que existían diferencias de criterio del personal en las AEC con incidencias, pero no corresponden a errores del Software del PREP.



Así mismo, problemas que se presentaron en la captura de algunos CATD Municipales, se debieron a problemas de infraestructura y no de funcionalidad.

- Resultados

El sistema informático permite la captura, digitalización y publicación de los datos asentados en la Actas de Escrutinio y Cómputo que se reciben en los Centros de Acopio y Transmisión de Datos.

El sistema informático integra los procesos de captura, validación, transmisión, recepción, consolidación y difusión de los resultados electorales preliminares de las elecciones, en el marco de la normatividad vigente.

El sistema informático apoya las funciones en los CATD.

Se maneja la Integridad en el registro de la información: Que a partir de un Acta de Escrutinio y Cómputo en papel, se genera una imagen digital completa y legible de ésta y es almacenada sin alteraciones en su contenido y publicada para consulta; Que la imagen digital del Acta de Escrutinio y Cómputo, así como sus datos capturados manualmente son debidamente asociados a la casilla, sección y distrito que corresponda; Que los resultados del Acta de Escrutinio y Cómputo capturados son asociados fielmente al partido, coalición o rubro en el cual se registren.

Para la revisión de desempeño se consideró el universo válido de información de un distrito muestra: únicamente se verificó que el sistema implemente dicha validación o restricción a partir de un catálogo de información el cual deberá tener cargada previamente la información de las casillas válidas.

También se consideró la Contabilización de actas y presentación de resultados acumulados.

Por lo que se considera adecuado para operar el día de la jornada electoral.



---

**INFORME FINAL DE LAS PRUEBAS DE PENETRACIÓN A LA INFRAESTRUCTURA TECNOLÓGICA Y DE LA REVISIÓN DE CONFIGURACIONES DE INFRAESTRUCTURA DE SINALOA.**

- Resumen ejecutivo

Las pruebas realizadas consisten en la ejecución de herramientas informáticas para identificar potenciales vulnerabilidades, y posteriormente en la aplicación de diversas técnicas para intentar explotarlas e identificar así el impacto que tienen sobre la infraestructura, determinar el nivel de exposición de información sensible.

Evaluar la configuración actual de los sistemas operativos de los dispositivos que conforman la infraestructura, a través de la comparación con buenas prácticas internacionales de seguridad informática.

La revisión de configuraciones se enfoca en el sistema operativo de servidores, consolas y dispositivos, por lo que no considera los servicios y aplicaciones que se ejecuten en los mismos. Así mismo se verificó la velocidad de las conexiones de internet y que se contara con una conexión de respaldo para el envío de datos.

Todos los hallazgos y oportunidades de mejora que se obtienen, como resultado de la ejecución del pentest y de la revisión de configuraciones, se analizan y se clasifican.

A partir de los informes de las pruebas de penetración y de la revisión de configuraciones, se verificó la aplicación de las medidas de mitigación aplicadas por el Instituto a fin de identificar la persistencia de los hallazgos reportados en la infraestructura de TI.

Utilizando el software Nessus Profesional se realizó un escaneo para establecer los activos sobre los que se realizarán las pruebas y la revisión de configuraciones. Se consideraron los siguientes aspectos: clasificación de los activos por funcionalidad y aspectos técnicos; condiciones de operación actual de los activos a evaluar.

Una vez determinados los activos a analizar, se utilizaron además las siguientes herramientas para el pentest: OWASPZAP 2.7, Amap, Metasploit, Dmitry, Grabber y SQLmap, hping3, SlowHttpTest.

Para los horarios de pruebas se considero el horario de servicio de COPREP y de los CATD.

Una vez determinado lo anterior, se designaron los activos primordiales a revisar.

El servicio de pruebas de penetración y análisis de vulnerabilidad para la infraestructura tecnológica tiene como objeto obtener información relacionada con los activos evaluados, conocer el nivel de exposición de información sensible y documentar los hallazgos.

La primera etapa de las pruebas consisten en la identificación de vulnerabilidad en objetivos específicos, así como en otros que podrían proporcionar acceso a información del PREP, intentando explotar vulnerabilidad identificadas para determinar el impacto



potencial en caso de que alguna fuera aprovechada por un usuario malintencionado. El tiempo de pruebas para cada uno de los activos es limitado, por lo que se definió un plan de pruebas. Entre las vulnerabilidades que tratan de explotarse se encuentran:

1. Instalaciones por defecto
2. Errores o huecos de seguridad en el software.
3. Configuraciones débiles o vulnerables
4. Vulnerabilidades que permiten a un atacante remoto acceder de forma no autorizada a información sensible.
5. Vulnerabilidades que permitan a un atacante remoto modificar de forma no autorizada el contenido o la visualización del mismo en un activo de información.
6. Vulnerabilidades que provoquen afectaciones a la disponibilidad de los recursos de TIC
7. Modificaciones no autorizadas en el contenido de repositorios de documentos (Base de Datos)
8. Verificación de cuentas sin algún tipo de autenticación, cuentas por defecto y contraseñas débiles por medio de ataques de diccionario o fuerza bruta.

Para las pruebas de penetración se consideran dos escenarios: pruebas externas y pruebas internas. En las pruebas externas se evalúan los objetivos que pueden ser accedidos desde internet y se ejecutan a través de éste mismo medio desde ubicaciones externas a la organización; las pruebas internas incluyen los objetivos que son accesibles sólo desde la red interna y se ejecutan en las instalaciones de la organización.

- Alcance

La revisión de las configuraciones de la infraestructura incluye las visitas a los CATD y la determinación de pruebas de conectividad, en VPNs, Firewalls, etc.

Para la revisión de la infraestructura se revisaron las instalaciones de los CATD: Distrital 2 Ahome, Distrital 3 Ahome, Distrital 4 Ahome y Guasave, Distrital 5 Ahome, Distrital 7 Guasave, Distrital 8 Guasave, Distrital 9 Alvarado y Angostura, Distrital 11 Navolato, Distrital 12 Culiacán, Distrital 13 Culiacán, Distrital 14 Culiacán, Distrital 15 Culiacán, Distrital 16 Culiacán, Distrital 17 Culiacán, Distrital 18 Culiacán, Distrital 19 Cruz de Eola, Distrital 20 Mazatlán, Distrital 21 Mazatlán, Distrital 22 Mazatlán, Distrital 23 Mazatlán, Distrital 24 Rosario y Escuinapa, Municipal Navolato, Municipal Mazatlán, el IEES, las instalaciones del COPREP, y los servidores en la nube.

- Resultado de la Verificación.

Se atendieron los hallazgos de manera satisfactoria para la infraestructura, en materia de configuraciones de infraestructura y, las pruebas de penetración determinaron que la infraestructura es adecuada para operar en un riesgo bajo.

Cabe aclarar que esta revisión se basa en clasificación de riesgos, y la auditoría pretende mitigar al máximo los hallazgos que se encontraron. Sin embargo la tecnología avanza rápidamente día con día y nuestra estimación no implica que se llegue a un 0% de riesgo.

El siguiente es un compilado fotográfico de los lugares donde se realizó revisión de infraestructura.





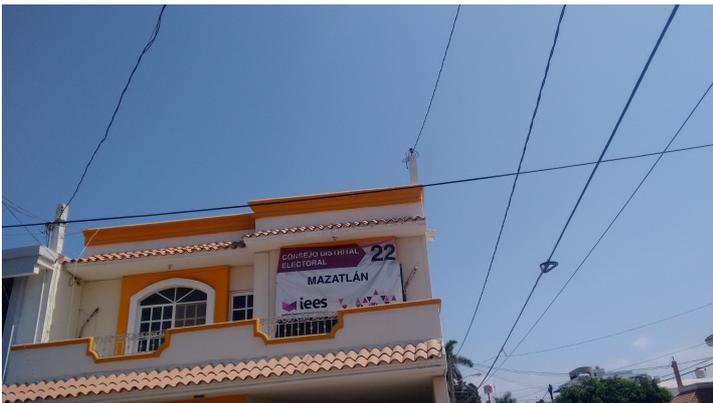
# Centro de Física Aplicada y Tecnología Avanzada de la UNAM







# Centro de Física Aplicada y Tecnología Avanzada de la UNAM







---

**INFORME FINAL DEL ANÁLISIS DE VULNERABILIDAD A LA INFRAESTRUCTURA  
TECNOLÓGICA DEL PREP SINALOA**

- **Introducción**

Simultáneamente al proceso de revisión de configuración de infraestructura y pruebas de penetración de la infraestructura del PREP, se realizó un escaneo de vulnerabilidades. Una vez identificados los puntos de vulnerabilidad el análisis se enfocó primordialmente en servidores, aplicaciones web, equipos de telecomunicaciones y estaciones de trabajo (estos últimos en el COPREP).

Una vez determinado los activos a analizar se utilizaron además las siguientes herramientas para el pentest: OWASPZAP 2.7, Amap, Metasploit, Dmitry, Grabber y SQLmap, hping3, SlowHttpTest. Se realizó ataque desde el interior y el exterior tratando de cambiar los datos en el AEC, los datos de la Base de datos o inutilizar los equipos para que no se pudiera realizar alguno de los procesos del PREP.

- **Resultados Generales**

Se determinó que los servidores están protegidos adecuadamente.

Las aplicaciones web no pueden modificarse desde fuera de las instalaciones y el personal del PREP no tiene posibilidades de alterar el contenido de las mismas

Los equipos de telecomunicaciones sólo pueden fallar por desconexión física, pero la empresa cuenta con, al menos, una conexión de respaldo en cada CATD y en el caso de tres municipios se sugirió contratar adicionalmente una tercer conexión de tipo Satelital. Resistieron los ataques internos de negación de servicio.

Se revisaron las instalaciones del COPREP y en las mismas se encontró que, a pesar de los ataques, la estaciones de trabajo de los coordinadores siguieron trabajando sin problemas. Adicional a esto, se tiene como plan de contingencia el mover a un sitio alternativo en caso de una falla total en las instalaciones del Instituto.

Para cada instalación se generó un reporte como el siguiente y solo se entregaron a la empresa aquellos que eran necesario mitigar.

En el ejemplo que se muestra en la siguiente pagina, la empresa mitigó los dos activos críticos al actualizar las versiones de los programas utilizados. Esto se verificó y se aprobó.



COPREP10  
Mon, 30 Apr 2018 11:02:30 CDT

### TABLE OF CONTENTS

#### Vulnerabilities by Host

- 10.1.0.15
- 10.1.0.16
- 10.1.0.21
- 10.1.0.22
- 10.1.0.23
- 10.1.0.24
- 10.1.0.25
- 10.1.0.26
- 10.1.0.28
- 10.1.0.30
- 10.1.0.61
- 10.1.0.70
- 10.1.0.98
- 10.1.0.100
- 10.1.0.152
- 10.1.0.153
- 10.1.0.154
- 10.1.0.171
- 10.1.0.172
- 10.1.0.173
- 10.1.0.174
- 10.1.0.201
- 10.1.0.250
- 10.1.0.254

#### Remediations

- [Suggested Remediations](#)

#### Vulnerabilities by Host

### 10.1.0.15



#### Scan Information

Start time: Mon Apr 30 09:16:29 2018  
 End time: Mon Apr 30 09:18:51 2018

#### Host Information

Netbios Name: CHECADOR-PC  
 IP: 10.1.0.15



---

## INFORME DE RESULTADOS DE PRUEBA DE NEGACION DE SERVICIO A SITIOS WEB DEL PREP SINALOA

- Introducción

El acceso a los servicios de internet, ha permitido que más personas puedan obtener información para desarrollar ataques en la web. Esto ha generado amenazas entre las que las cibernéticas son un factor importante; por esta razón es necesario que los datos contenidos en el PREP tengan una validación de disponibilidad.

La auditoría tiene como objetivo asegurar la correcta y continua disponibilidad del servicio web de los sitios de publicación de resultados del PREP, durante el período de operación.

- Pruebas realizadas

Para los ataques se utilizaron las instalaciones del CFATA y la conexión a internet de la Red Niba.

Se realizaron ataques en la capa de aplicación (HTTP) con diversos escenarios de SLOWLORIS ATTACK como son:

- a. Slow headers: consiste en enviar las cabeceras HTTP incompletas (sin el CRLF final que indica el final del header) de tal forma que el servidor no considera las sesiones establecidas y las deja abiertas, afectando al número de conexiones máximas configuradas.
- b. Range (Apache killer): se crean numerosas peticiones superponiendo rangos de bytes en la cabecera (HTTP ranges), agotando los recursos de memoria y CPU del servidor.
- c. Slow read: en este caso se envían peticiones HTTP legítimas, pero se ralentiza el proceso de lectura de la respuesta, retrasando el envío de ACK (HTTP es TCP).

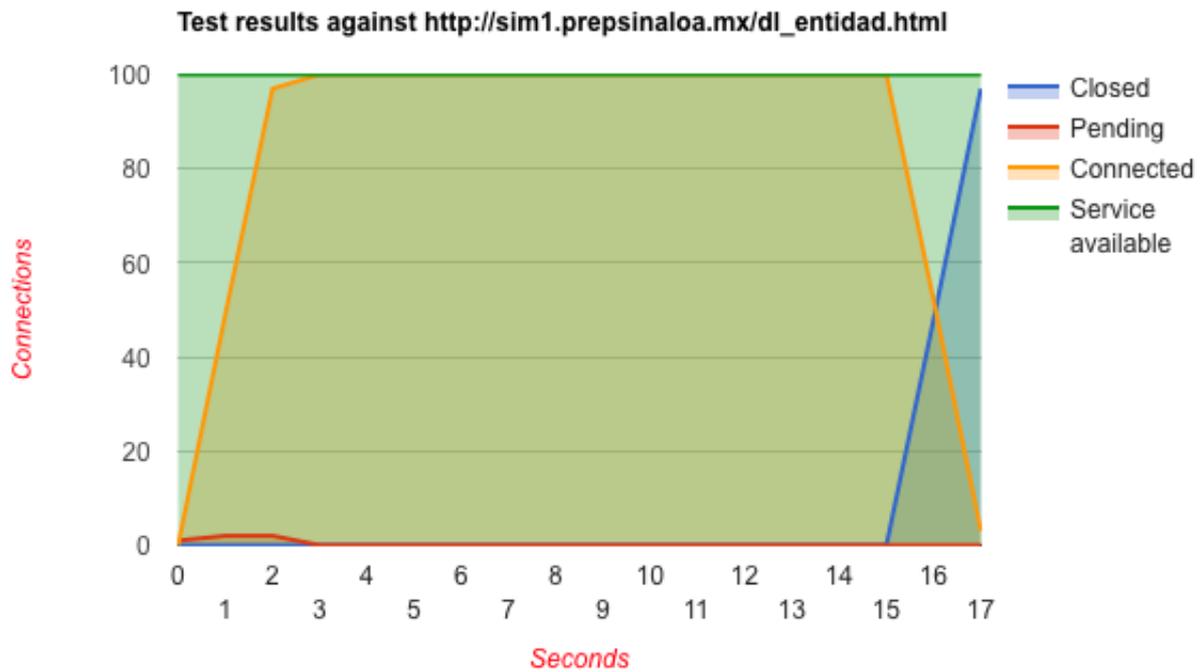
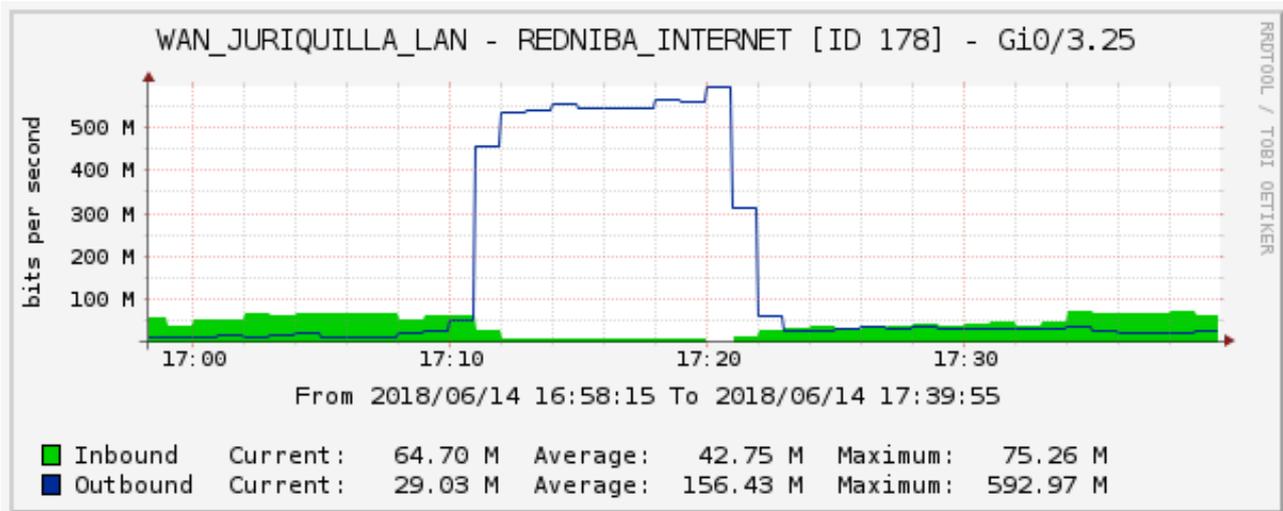
Se realizaron ataques volumétricos por los protocolos TCP (con SYN FLOOD), UDP (con DNS Amplification), ICMP con (ICMP Flood); empleando IP aleatorias, para que no se identificara el atacante. Al mismo tiempo se simuló tráfico legítimo.

El servidor analizado fue el de [sim1.prepsinaloa.mx](http://sim1.prepsinaloa.mx) y, para el ataque slowloris, se inició con la página /dl\_entidad.html, el cual fue previamente escaneado para obtener sus vulnerabilidades y explotarlas durante el ataque.

- Resultados

1. El escaneo no proporcionó información de vulnerabilidades.
2. El servicio conservó su continuidad ante el ataque de slowloris.
3. La página continuó respondiendo adecuadamente ante el tráfico de red, de hasta 592.97M.

Se muestran las gráficas de resultados del ataque volumétrico y un ejemplo del slowloris .



ATENTAMENTE

VOBO

M. EN C. GUILLERMO VÁZQUEZ SÁNCHEZ  
RESPONSABLE TÉCNICO DE LA AUDITORIA

DR. JOSE LUÍS ARAGÓN VERA  
DIRECTOR DEL CFATA