

Instituto Electoral del  
Estado de Querétaro

# Informe Final de Auditoría al Programa de Resultados Electorales Preliminares del Instituto Electoral del Estado de Querétaro

## 2021

4 de junio de 2021



---

**INFORME FINAL DE LAS PRUEBAS FUNCIONALES DE CAJA NEGRA DEL SISTEMA  
INFORMÁTICO PREP QUERÉTARO 2021**

---

- **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, Página Web Pública 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 Querétaro (IEEQ) son: acopio, digitalización, captura, verificación, y publicación, 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, en su última versión.

- **Resumen Ejecutivo**

Se utilizaron los equipos instalados en los CATD y CCV, además se permitió acceso a los servidores para las pruebas de los módulos de Acopio, Captura y Validación, y de Publicación de Resultados.

Se aplicaron los casos de prueba para cada módulo, donde se detectaron problemas en la publicación, las cuales fueron reparadas hasta el 2 de junio.

Posterior a la revisión de los modelos de entrada y salida, fue necesario supervisar en las oficinas del CCV, los módulos de Acopio, Captura, Validación y Supervisión.



- 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, el cual solo incluye el acopio, la digitalización y transmisión.

El sistema maneja la Integridad en el registro de la información: que a partir de un Acta de Escrutinio y Cómputo en papel, se genere una imagen digital completa y legible de ésta y sea 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; sean debidamente asociados a la casilla, sección y distrito que corresponda; que los resultados del Acta de Escrutinio y Cómputo capturados sean 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.

Durante los tres simulacros se hicieron cambios, que se reportan en el informe de configuración de la infraestructura.

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 QUERÉTARO 2021**

---

- Resumen ejecutivo

Las pruebas realizadas consistieron 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 y determinar el nivel de exposición de información sensible.

Se evaluó la configuración 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 enfocó en el sistema operativo de servidores, consolas y dispositivos, por lo que no se consideraron los servicios y aplicaciones que se ejecutan 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 obtuvieron, como resultado de la ejecución del pentest y de la revisión de configuraciones, se analizaron y se clasificaron.

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 CCV 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, tuvo 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 consistió en la identificación de vulnerabilidad en objetivos específicos, así como en otros que podrían proporcionar acceso a información del PREP, intentando explotar las vulnerabilidades 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 trataron 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 alcanzados 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 15 CATD Distritales, 12 CATD Municipales, las instalaciones del CCV, CCV Alterno, 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 opera en un riesgo bajo, mientras no se realicen cambios a las configuraciones. Dichos cambios tardan 27 minutos en restablecer la publicación en el sitio público.

Los últimos cambios se realizaron durante las pruebas del 3 de Junio, se recomienda que no se realicen cambios sin validarse previamente pues implicaría el retraso del inicio de la publicación.

En caso de presentarse el supuesto anterior, la información en los backend se mantiene segura y el contenido en la base de datos también, solo se afecta la visualización del portal público.

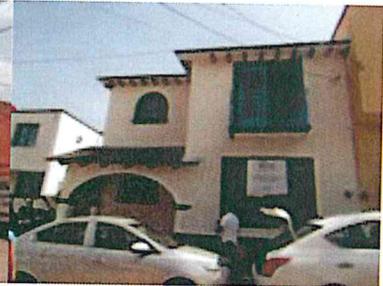
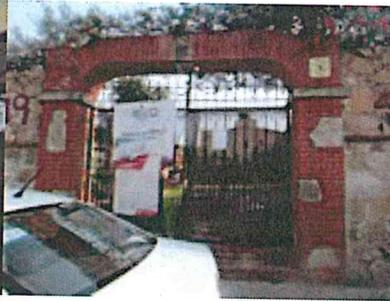
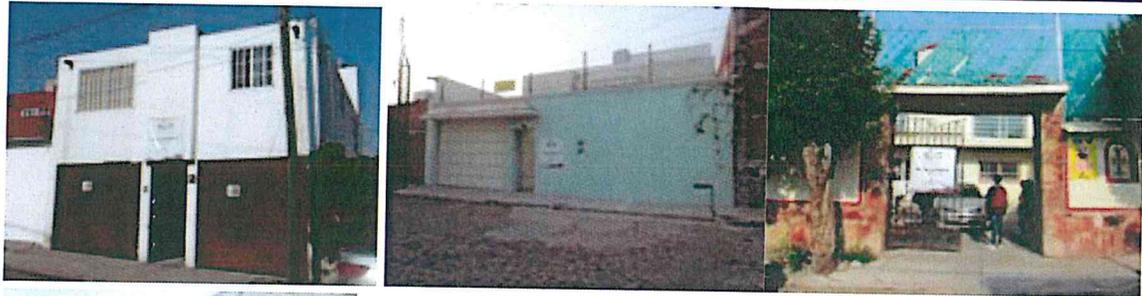
Cabe aclarar que esta revisión se basa en clasificación de riesgos, y la auditoría pretende mitigar al máximo los hallazgos que se encontraron. Sin embargo la tecnología avanza rápidamente día con día y nuestra estimación no implica que se llegue a un 0% de riesgo.

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



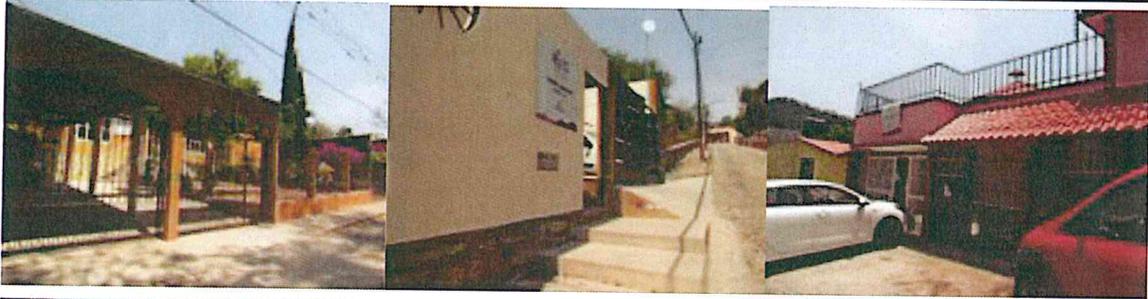


# Centro de Física Aplicada y Tecnología Avanzada de la UNAM





# Centro de Física Aplicada y Tecnología Avanzada de la UNAM





---

INFORME FINAL DEL ANÁLISIS DE VULNERABILIDAD A LA INFRAESTRUCTURA  
TECNOLÓGICA DEL PREP QUERETARO 2021

---

- 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 CCV).

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 realizaron ataques 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 cuenta con al menos, una conexión de respaldo en cada CATD y uso de datos 4G. Resistieron los ataques internos de negación de servicio.

Se revisaron las instalaciones del CCV y en las mismas se encontró que, a pesar de los ataques, la estaciones de trabajo de todo el personal siguieron trabajando sin problemas.

Para cada instalación se generó un reporte como el siguiente y solo se entregaron aquellos que eran necesario mitigar. No se presentaron riesgos en los CATD.

**Todos los hallazgos fueron atendidos y revisados a mas tardar en el tercer simulacro.**



## XXX.XX.X.1

Crítico	Alto	Medio	Bajo	Información

### Vulnerabilities

#### 51192 - SSL Certificate Cannot Be Trusted -

##### Synopsis

The SSL certificate for this service cannot be trusted.

##### Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

##### Solution

Purchase or generate a new SSL certificate for this service.

##### Risk Factor

Medium

##### CVSS Base Score

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

##### Plugin Information

Published: 2010/12/15, Modified: 2020/04/27



## INFORME DE RESULTADOS DE PRUEBA DE NEGACION DE SERVICIO A SITIOS WEB DEL PREP QUERETARO 2021

- 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 y Telmex. Fungiendo como testigos el personal de Telecomunicaciones del Campus Juriquilla.

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 no malintencionado con el que se simuló tráfico legítimo.

Se analizaron tres veces los servidores `ieeq2021sc.southcentralus.cloudapp.azure.com` y, para el ataque slowloris, se inició con la página `/home/inicio`, el cual fue previamente escaneado para obtener sus vulnerabilidades y explotarlo durante el ataque.

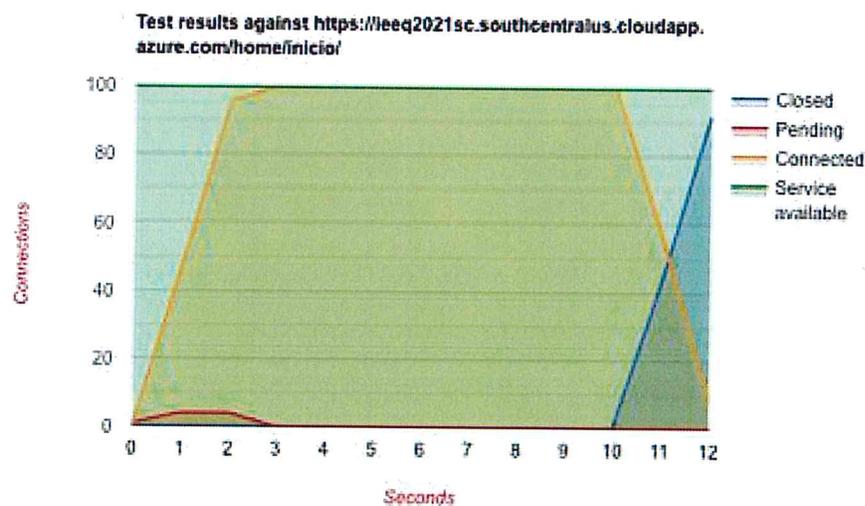
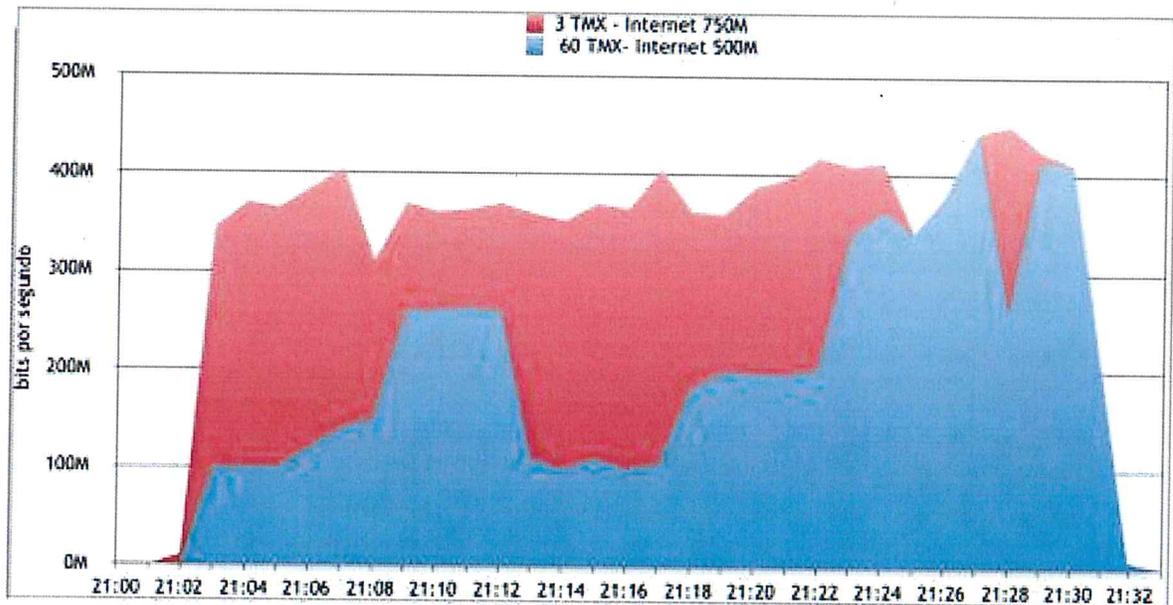
- Resultados

1. El escaneo no proporcionó información de vulnerabilidades.
2. El servicio conservó su continuidad ante el ataque de slowloris, y en algunos casos fueron bloqueadas al detectarse.



3. La página al llegar a los 450M continuó respondiendo adecuadamente ante el tráfico de red, se iniciaron nuevos ataques a bases de datos y el servicio continuó funcionando.

Se muestran las gráficas de resultados del ataque volumétrico y un ejemplo del slowloris. Realizados el 12 de Mayo de 2021





**Centro de Física Aplicada y  
Tecnología Avanzada de la UNAM**



ATENTAMENTE

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

VOBO

DR. JOSÉ LUIS ARAGÓN VERA  
DIRECTOR DEL CFATA