INSTITUTO TECNOLÓGICO DE LA PAZ

Departamento de Sistemas y Computación

Informe final de la Auditoría Informática al Sistema Informático y a la Infraestructura tecnológica del PREP (Programa de Resultados Electorales Preliminares).

30 de junio 2018

Destinatario:

M.G.T.I. Mario Yee Castro.

Director de la Unidad de Cómputo y Servicios Informáticos. Instituto Estatal Electoral de Baja California Sur.

Nombre de la Auditoria:

Auditoría Informática de los sistemas de información que son utilizados en la implementación del PREP, con la finalidad de evaluar la integridad en el procesamiento de la información conforme a la normatividad en términos de funcionalidad.

Objetivo de la auditoria.

Realizar una auditoría con el fin de evaluar el sistema de información e infraestructura, para verificar el cumplimiento de normas y especificaciones y asegurar la adecuada aplicación de los controles del sistema de información, en términos de calidad, funcionalidad, análisis de vulnerabilidades de la infraestructura tecnológica de acuerdo a los Lineamientos del Programa de Resultados Electorales Preliminares (PREP).

Antecedentes

Esta auditoría se apegará a lo dispuesto en el marco de las actividades para la implementación y operación del Programa de Resultados Electorales Preliminares (PREP) para el Proceso Local Electoral 2017-2018, donde se establece que se requiere que se lleve a cabo una auditoría al sistema informático y a la infraestructura tecnológica del PREP, de conformidad con lo dispuesto en la sección cuarta, del capítulo II del Reglamento de Elecciones del INE, así como del título II, capítulo III, de su Anexo 13 relativo a los Lineamientos del PREP

Alcance:

Comprende todas las actividades del plan de auditoria al sistema PREP que operará previo al fin de la jornada electoral del día 1 de julio de 2018 para el estado de Baja California Sur, comprendiendo pruebas de funcionalidad de caja negra, validaciones del sistema informático PREP y de su Base de Datos, análisis de

vulnerabilidades a su infraestructura tecnológica pruebas de denegación de Servicios distribuidos (DDoS).

Objetivos particulares:

- Verificar infraestructura e instalaciones físicas del el Centro Estatal De Cómputo del PREP.
- Aplicar listas de verificación con respecto a los controles de seguridad marcados en la norma ISO/IEC 27002-3013.
- Confirmar la correspondencia en cuanto a la información de los manuales de procedimientos y la operación real.
- Corroborar la correspondencia en cuanto a la información de los planes de contingencia y seguridad y la operación real.
- Verificar instalaciones y plan de continuidad de las actividades en el Centro Estatal de Cómputo del PREP cuando surja una falla de corriente eléctrica.
- Ejecutar pruebas de validación al PREP.
- Realizar análisis de vulnerabilidades e inyección de código al sistema PREP.
- Hacer un ataque de negación de servicios al sistema web.

Periodo de revisión.

Del 28 de Mayo al 28 de Junio del presente año con respecto a las actividades arriba mencionadas.

Dirección:

Calle Revolución entre Constitución y 5 de mayo.

Limitaciones del proceso de auditoría.

El equipo auditor tuvo acceso a los catálogos parciales, manuales de procedimientos y planes de contingencia y seguridad, SIN ACCESO a código de los programas, por lo que la presente auditoria se limitará a pruebas de funcionalidad y penetración, propuestos como pruebas de caja negra.

Procedimientos de auditoria realizados.

El procedimiento llevado a cabo por el ente auditor se especifica en cada una de las fases de la auditoria.

Fase 1. Planeación de la auditoria

Se llevó a cabo una entrevista inicial con el representante de la empresa PODERNET en esta ciudad, el Ing. Cesar Jiménez, quien proporcionó una descripción de las instalaciones, sus áreas de operación, su infraestructura y procedimientos de seguridad y emergencia en caso de incidentes.

Se nos proporcionó una visita por todas las áreas de las instalaciones a fin de constatar el estado de las instalaciones físicas, instalaciones de conectividad y comunicaciones, eléctricas y de seguridad.

Se utilizó por parte del equipo auditor en esta primera revisión, la recopilación de información basados en; observación, revisión y análisis de manuales y planes, así como la comprobación de las siguientes listas de verificación correspondientes a los controles que marca la norma oficial y aplicados a esta etapa:

- Lista de Verificación Seguridad Física y ambiental.
- Lista de Verificación Seguridad en las telecomunicaciones.
- Lista de Verificación Identificación de los componentes informáticos.
- Lista de Verificación Control de acceso
- Lista de Verificación en términos de funcionalidad y calidad.

Se realizaron las siguientes actividades para la ejecución de las mismas:

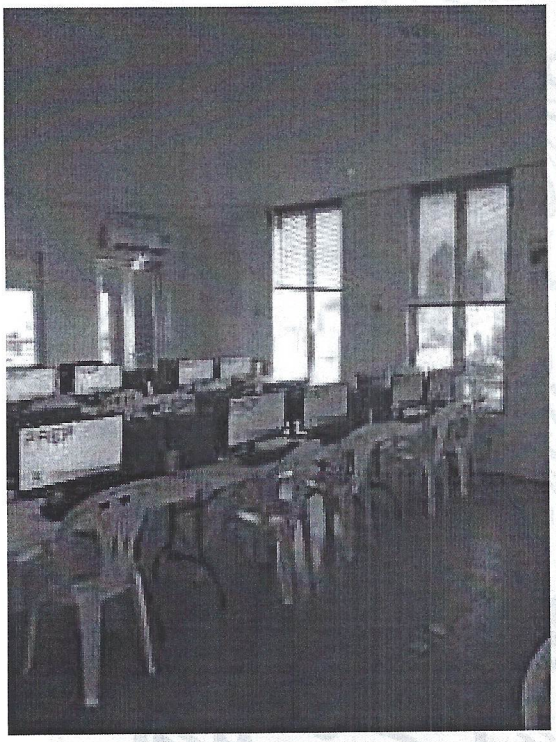
- Identificación de actividades de control y seguridad de los sistemas.
- Identificación de los componentes del Sistema Informático e infraestructura.
- Recopilación de información en términos de funcionalidad y calidad.
- Recopilación de información en términos de seguridad.
- Identificación de los componentes del Sistema Informático e infraestructura del CCV.
- Recopilación de información en términos de funcionalidad y calidad durante el primer simulacro el día 10 de junio del 2018.

- Recopilación de información en términos de seguridad durante el primer simulacro el día 10 de junio del 2018.

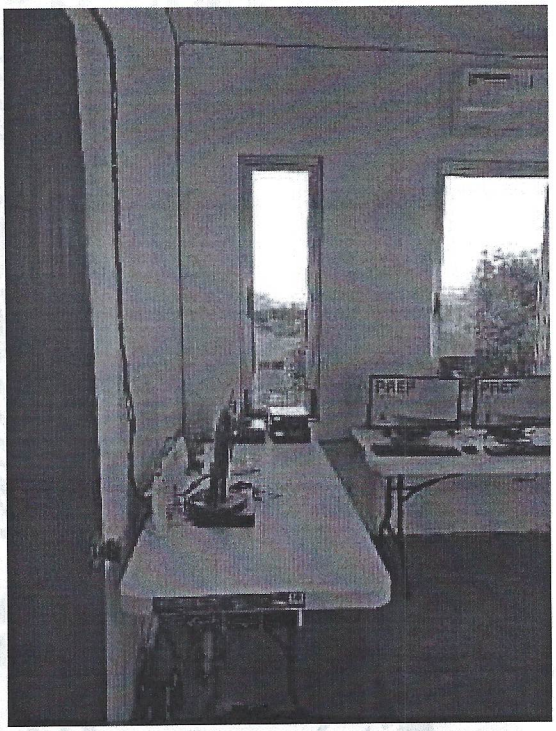
Hallazgos u observaciones encontradas.

En las instalaciones no se contaba con los siguientes puntos:

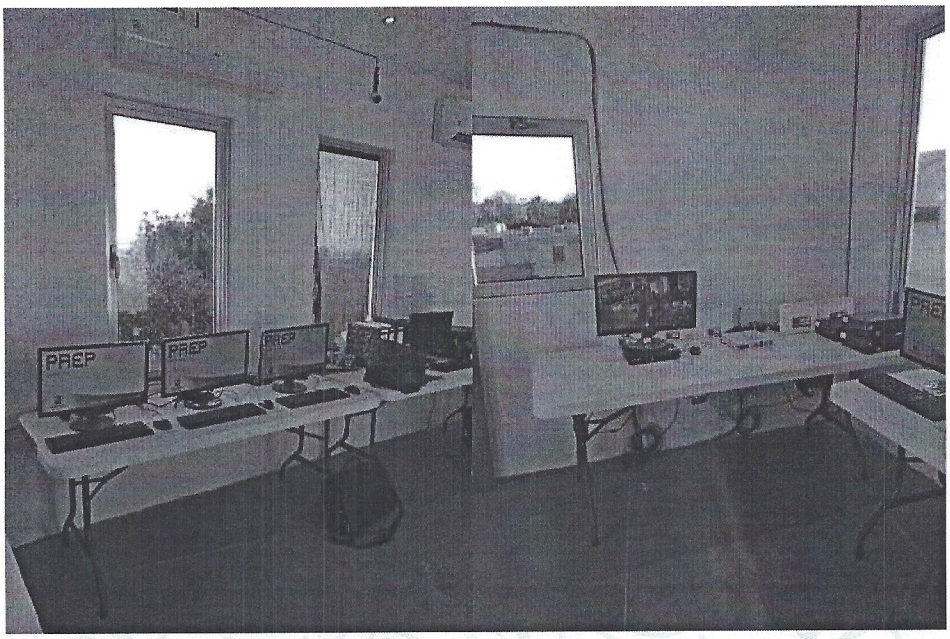
- Extinguidores
- Implementación del control de acceso a instalaciones.
- Delimitación de áreas de trabajo.
- Se observó a su vez que se cuenta con sistema de video vigilancia pero no se cuenta con un operador del mismo.



Área sin delimitar



Ausencia de extintores.



Sistema de video vigilancia sin operador.

En el marco del primer simulacro, se observó lo siguiente:

- Se comprobó la recepción automática satisfactoria de las imágenes correspondientes a las actas digitalizadas.
- Se examinó el manejo de los foliadores (cuatro) a las actas recibidas.
- Se probó el proceso de Captura de las actas que fueron digitalizadas y foliadas en las áreas correspondientes.
- Se constató el manejo de las actas recibidas en el área de Captura.
- Se corroboró el proceso de digitalización de actas en el CATD del distrito 02.
- No se pudo verificar el proceso de PREP casilla.

Se concluye esta fase constatando que los hallazgos encontrados fueron atendidos en tiempo y forma por la empresa auditada.

Delimitación de áreas de trabajo y extintores.

Fase 2. Pruebas de funcionalidad y caja negra.

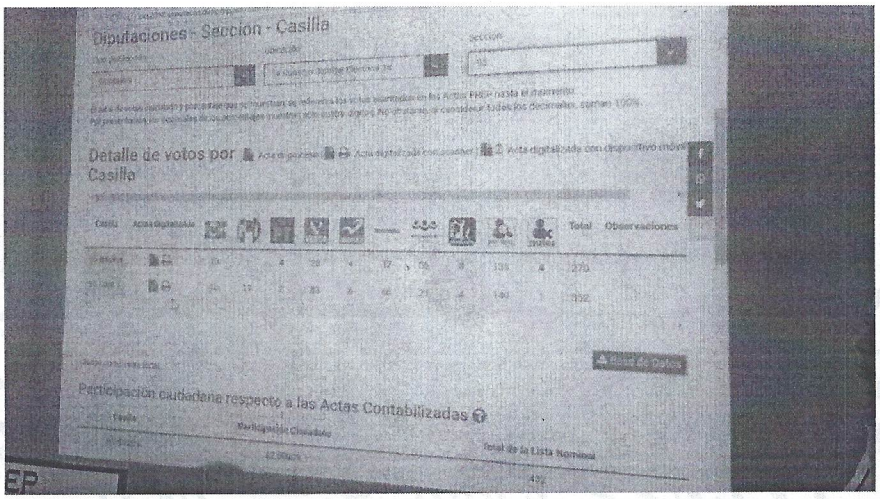
Las pruebas de caja negra consisten en probar las funciones que el sistema debe realizar y que las ejecute eficientemente. Durante las pruebas se verifican que las salidas que resulten del procesamiento de los datos de entradas sean las esperadas. El objetivo de esta auditoria fue comprobar que las imágenes de las actas de escrutinio y cómputo son procesadas de manera íntegra por el sistema informático PREP y que los diversos reportes de resultados preliminares sean desplegados de acuerdo a las especificaciones dadas.

Actividades Principales

- Revisión de manuales de seguridad y análisis de riesgo propuesto por la empresa PoderNet.
- Durante el primer simulacro, identificar factores de riesgo dentro del personal operador del sistema.
- Realizar pruebas de acceso al sistema de captura.
- Realizar pruebas de digitalización de al menos 30 actas establecidas como actas de pruebas.
- Realizar pruebas de captura de la información tomadas de la imagen digitalizada.
- Realizar pruebas de validación de los datos obtenidos en la captura.
- Revisar la información de salida del cómputo realizado y compararlo con las actas para así verificar su disponibilidad.

Las pruebas funcionales de caja negra se realizaron en dos momentos:

El primer momento fue del 11 al 17 de junio del presente año y como resultado de este se emitió un informe preliminar que fue entregado el 18 de junio del 2018. Los casos de prueba se diseñaron previamente en un plan de pruebas y se ejecutaron en un ambiente simulado para la operación del PREP que fue provisto por la empresa PoderNet. Se probaron y confirmaron los requerimientos para los distintos módulos del sistema: Digitalización tanto para PREP casilla como vía CATD, Foliación, Captura, Verificación, Validación y el despliegue de resultados electorales vía Web.



Procedimientos de auditoria realizados.

Se llevó a cabo una revisión de los manuales de operación de cada uno de los módulos del sistema, así como la revisión de los manuales de seguridad.

Pruebas de caja negra PREP.

Se llevó a cabo la actividad de digitalización de 30 actas por parte del ente auditor para probar cada uno de los módulos del PREP.

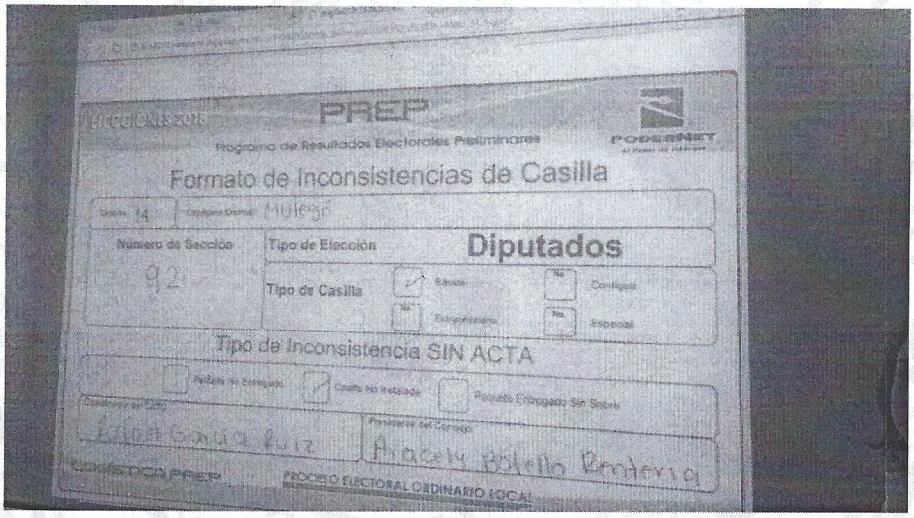
Se operaron los siguientes módulos:

- Digitalización de actas.
  Se digitalizaron 30 actas de diferentes candidaturas.
- Foliación.
  Se verificó la recepción de las 30 actas y se procedió a generar su foliación. Se utilizaron actas con código QR y actas sin código QR.
- Captura de actas.

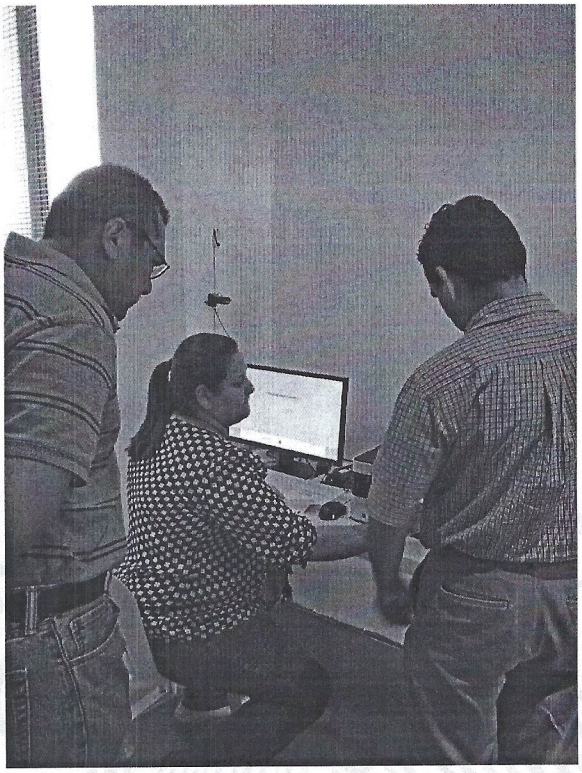
Se capturó los valores de las actas que fueron foliadas, se simularon errores en algunas actas para verificar el procedimiento y validación que se aplica.

- Validación de actas con errores.
  Las actas que se identificaron con errores de captura se validaron correctamente, en la captura de algunas actas se forzó nuevamente la captura con errores, hasta que ya fueron capturadas correctamente.

El segundo momento fue durante los simulacros realizados los días 10, 17 y 24 de junio de los corrientes. Las observaciones resultantes de estos fueron incluidas en los informes entregados los días 11, 18 y 21 de junio. Se realizaron listas de verificación, control de entradas y salidas, verificaciones aritméticas, entre otros durante estos.
Se contabilizaron los resultados obtenidos durante el simulacro para constatar que los totales fueran los correctos, así como los porcentajes.



En las distintas etapas se aplicaron técnicas para la recopilación de información como la observación, revisión de documentación, entrevistas, muestreo, simulación y revisión de prototipos funcionales.



Como resultado de la ejecución de las pruebas funcionales de caja negra se le hicieron llegar las observaciones al IEE y se verifico durante el transcurso de la auditoria que fueran atendidas. La respuesta de la empresa PoderNet fue atender correctamente cada una de ellas.

Hallazgos u observaciones encontradas

- Dada la revisión de los manuales de seguridad, se verifico que tienen contemplado un análisis de riesgo basado en el ISO27005. Por lo que se constata que llevan a cabo una administración del riesgo, así como un plan de contingencias.
- Se pudo verificar el manejo de los foliadores (cuatro) a las actas recibidas.
- Se verifico el proceso de Captura de las actas que fueron digitalizadas y foliadas en las áreas correspondientes.
- Se pudo constatar el manejo de las actas recibidas en el área de Captura.
- No se pudo verificar el proceso de PREP casilla.
- Se observó que los procesos principales que componen el sistema PREP interactúan adecuadamente y arrojan resultados suficientes en base a las

actividades realizadas durante el segundo simulacro del día 18 de junio de los corrientes.

- Durante la ejecución de las listas de verificación al CATD:
  - No se observó control de acceso alguno.
  - Se constató que en cuanto a infraestructura tecnológica física de los CATD se cumple satisfactoriamente por parte de la empresa PoderNet.
- Durante las visitas realizadas al CCV:
  - Se constató que en respuesta a la observación: Se recomienda llevar una bitácora de visitantes en el CCV. Se atendió dicha recomendación por parte de la empresa PoderNet.
  - Se verificó que la empresa PoderNet atendió la recomendación del Primer Informe de este ente auditor referente a: Indicar quienes integran el personal de Guardia de Seguridad y la ubicación de la bitácora de vigilancia, así como sus funciones regulares y por excepción.

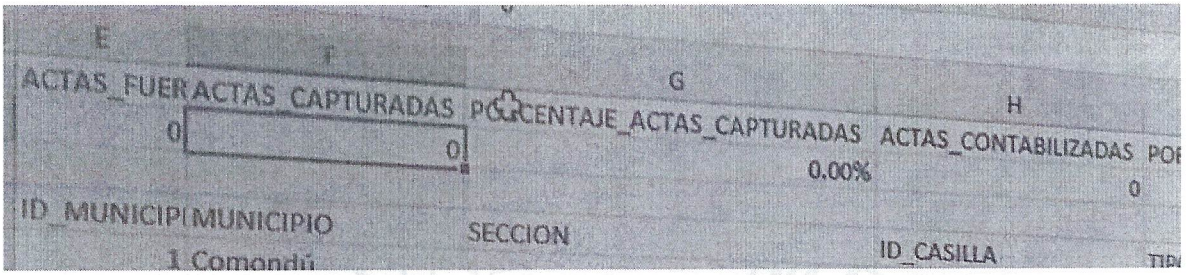
Como resultado de las pruebas de caja negra se concluye que el sistema PREP cumple con los criterios funcionales establecidos en los lineamientos del PREP y que además los ejecuta manera íntegra. El sistema PREP es robusto, eficaz, eficiente, completo, confiable e íntegro. Sus resultados corresponden a los esperados en función de las entradas y en ningún momento incluye procedimientos que alteren de manera injustificada la información de las Actas de Escrutinio y Cómputo de tal forma que se pudiera influir en los resultados preliminares. Una vez dicho esto podemos confirmar que el sistema PREP es funcional y cumple satisfactoriamente con los lineamientos del PREP.

Fase 3. Validación del sistema informático del PREP 2018 y su base de datos.

El día 30 de junio se llevó a cabo el primer paso de la validación del sistema PREP con la presencia del notario Hugo Carlos Mendoza Nuñez, adscrito a la notaria No. 26 de esta ciudad de La Paz, arrojando la cadena siguiente:

```
FECHA: sábado 30 de junio de 2018 13:00 horas (UTC -6)
EDO:Baja California Sur
VERSION:25.6
HASH:f77ea927158a3bad73384f6e9f078269448370171f84d9059f3a2149900e40db
```

Siendo las 17:00 hrs del 1 de julio del presente, se llevo a cabo la verificacion de la cadena hash de fecha 30 de junio, obteniendose un hash nuevo a la hora citada, dando fe legal el Lic. Hugo Carlos Mendoza Nuñez Notario adscrito a la notaria pública No. 26 de esta ciudad de La Paz. Asi mismo, se corroboró ante el notario, que la base de datos se encontrara en ceros.



Se concluye por parte del ente auditor que el sistema PREP cumple con los requisitos establecidos en el lineamiento sobre confidencialidad, integridad y disponibilidad, constatando que tanto las cadenas hash son las mismas en las dos tomas, asi como la base de datos comienza en ceros.

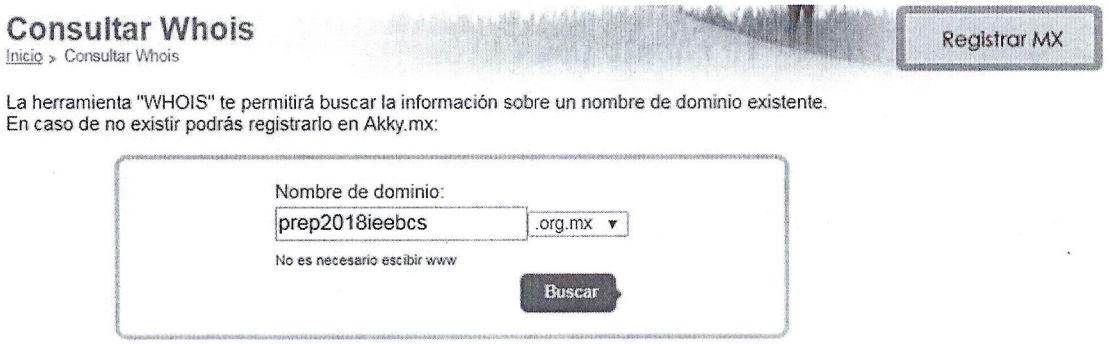
Fase 4.

Análisis de vulnerabilidades a la infraestructura tecnológica.

Actividades realizadas

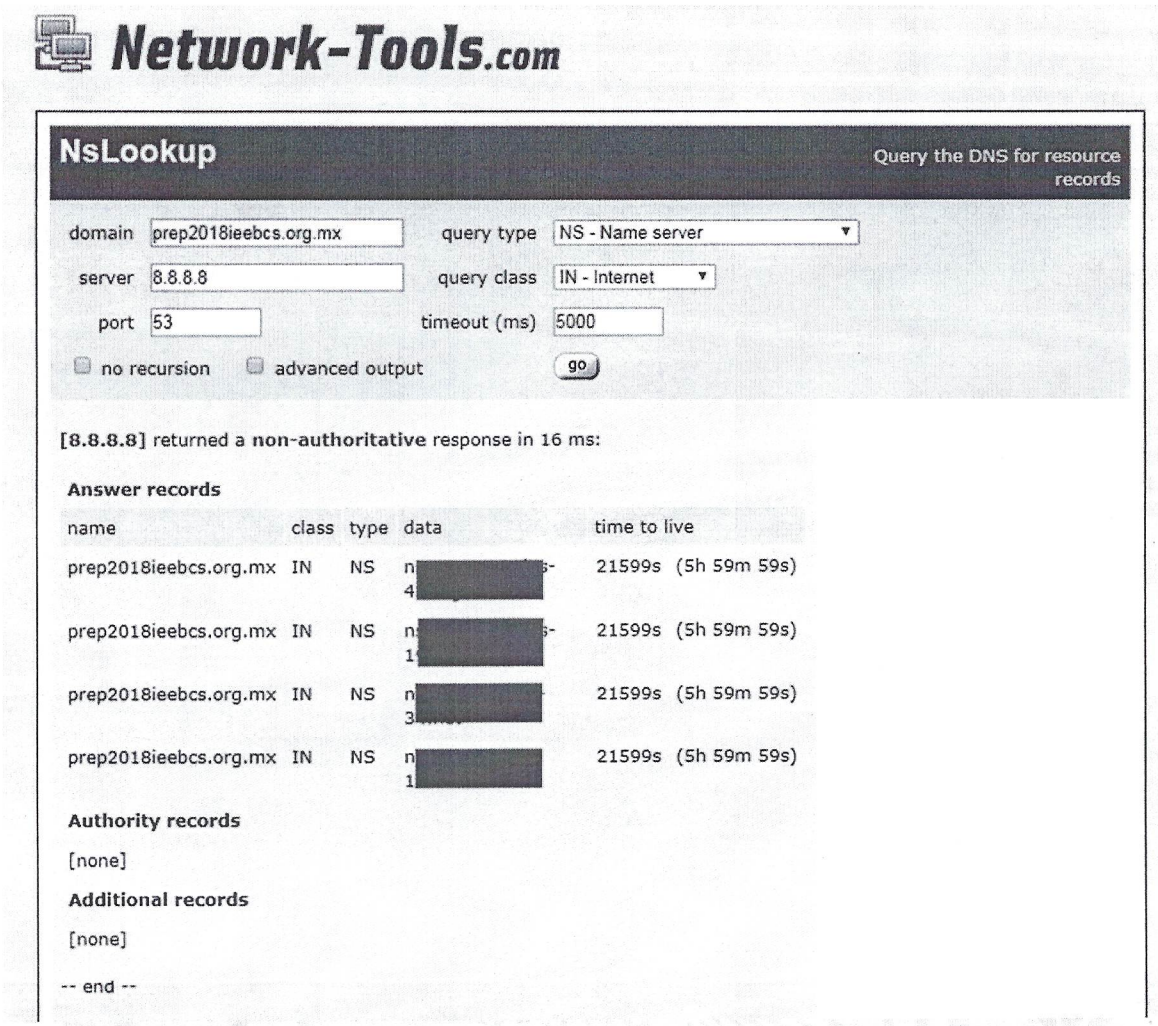
Se ejecutó un análisis de vulnerabilidades al sistema PREP2018 utilizando herramientas especializadas para ello.

En primera instancia y de acuerdo a los registros internacionales "whois" del dominio prep2018ieeebcs.org.mx el cual será la identificación oficial para el PREP 2018 del proceso electoral 2017-2018 del estado de Baja California Sur, tenemos la siguiente información: (fuente https://www.akky.mx/jsf/whois/whois.jsf




```
Domain Name (Nombre de dominio): prep2018ieebcs.org.mx
Registry Domain ID (ID del dominio en Registry): DOMAIN_25000005663064-MX
Registrar WHOIS Server (Servidor WHOIS del Registrar): whois.akky.mx
Registrar URL (URL del Registrar): http://www.akky.mx
Updated Date (Fecha de ultima modificacion): 2018-06-09T12:52:14-0500
Creation Date: 2018-06-05T09:23:47-0500
Registrar Registration Expiration Date (Fecha de expiracion en el Registrar): 2019-06-(
Registrar (Registrar): Akky. Una division de NIC Mexico
Registrar IANA ID (Registrar IANA ID): 1705
Registrar Abuse Contact Email (Correo electronico para reporte de abusos): abuse@akky.r
Registrar Abuse Contact Phone (Telefono para reporte de abusos): +52.8188642625
Domain Status: clientTransferProhibited
Registry Registrant ID (Registrante - ID en Registry): CONTACT_1528208627UKBB-MX
Registrant Name (Registrante - Nombre): Administrador de Dominio Podernet
Registrant Organization (Registrante - Organizacion):
Registrant City (Registrante - Ciudad): Mexico
Registrant State/Province (Registrante - Estado/Provincia): Ciudad de Mexico
Registrant Country (Registrante - Pais): MX
Registry Admin ID (Administrativo - ID en Registry): CONTACT_1528208627ZAT1-MX
Admin Name (Administrativo - Nombre): Administrador de Dominio Podernet
Admin Organization (Administrativo - Organizacion):
Admin City (Administrativo - Ciudad): Mexico
Admin State/Province (Administrativo - Estado/Provincia): Ciudad de Mexico
Admin Country (Administrativo - Pais): MX
Registry Tech ID (Tecnico - ID en Registry): CONTACT_1528208627EALW-MX
Tech Name (Tecnico - Nombre): Administrador de Dominio Podernet
Tech Organization (Tecnico - Organizacion):
Tech City (Tecnico - Ciudad): Mexico
Tech State/Province (Tecnico - Estado/Provincia): Ciudad de Mexico
Tech Country (Tecnico - Pais): MX
Name Server (DNS): ns-95.awsdns-11.com
Name Server (DNS): ns-1693.awsdns-19.co.uk
Name Server (DNS): ns-785.awsdns-34.net
Name Server (DNS): ns-1368.awsdns-43.org
DNSSEC (DNSSEC): no firmado
```

Esto, nos arroja información referente al registro del dominio a nivel internacional e información sobre el dueño y administrador del mismo. Así mismo, en el mismo tenor de búsqueda se observa que la redundancia como parte primordial de la seguridad del sistema, esta soportado con 4 servidores de dominio.



Network-Tools.com

NsLookup — Query the DNS for resource records

domain: prep2018ieebcs.org.mx | query type: NS - Name server
server: 8.8.8.8 | query class: IN - Internet
port: 53 | timeout (ms): 5000
no recursion | advanced output | go

[8.8.8.8] returned a **non-authoritative** response in 16 ms:

Answer records

name	class	type	data	time to live
prep2018ieebcs.org.mx	IN	NS	n[redacted]	21599s (5h 59m 59s)
prep2018ieebcs.org.mx	IN	NS	n[redacted]	21599s (5h 59m 59s)
prep2018ieebcs.org.mx	IN	NS	n[redacted]	21599s (5h 59m 59s)
prep2018ieebcs.org.mx	IN	NS	n[redacted]	21599s (5h 59m 59s)

Authority records

[none]

Additional records

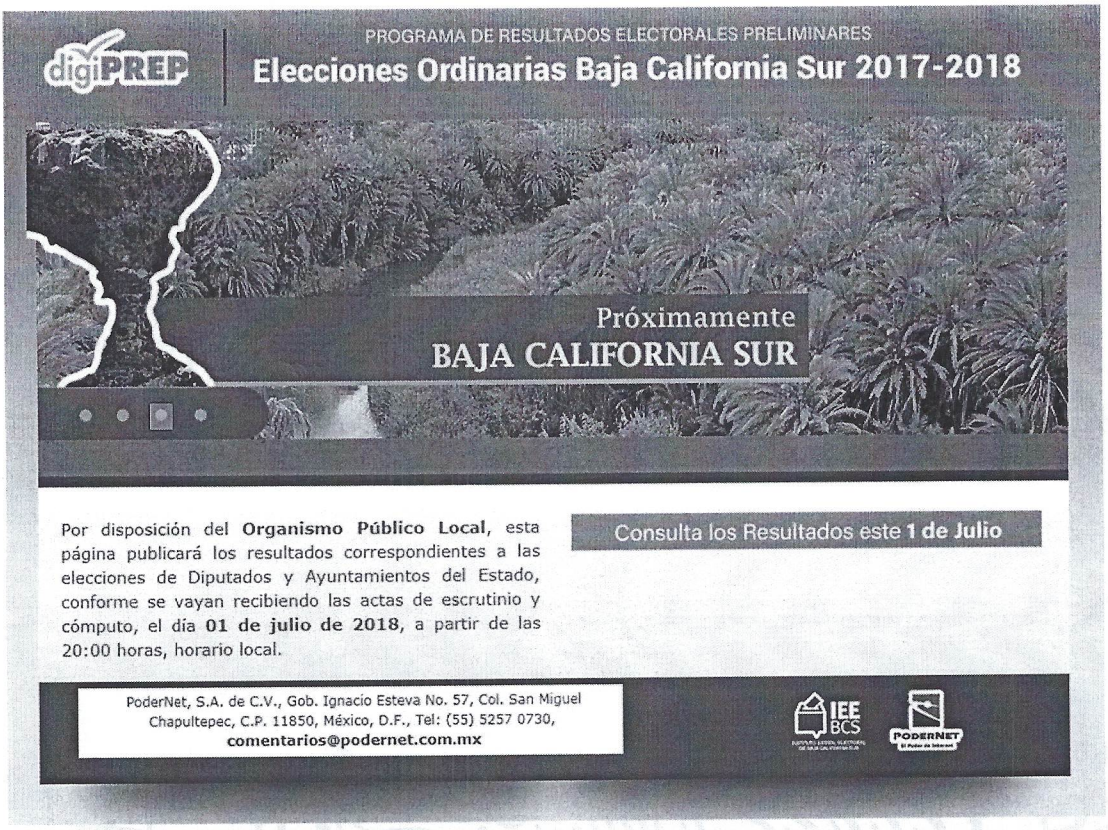
[none]

-- end --

Siendo esto, una buena medida de seguridad, ya que contar con más de un servidor DNS para identificar internacionalmente el nombre del dominio de Internet, en nuestro caso www.prep2018ieebcs.org.mx. Al contar con 4 servidores de dominio, se proporciona la redundancia necesaria mitigando cualquier riesgo de caída del sistema.

Se trabajo con celular Motorola, el cual dará servicio al PREP casilla, encontrándose este equipo con niveles fuertes de seguridad y configurado solo para el envió de datos

A partir del 27 de junio del presente, inicio su operación el servidor web con una página en formato html, con el nombre final www.prep2018ieebcs.org.mx .



Esta página tiene su código fuente a la vista, sin considerar un peligro latente.

Código fuente :

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Elecciones Ordinarias 2018 ::: Programa de Resultados Electorales Preliminares</title>

<link href="media_2016_previo/estilos_prep_slp.css" rel="stylesheet" type="text/css" />
</head>

<body>

<div id="contenedor">

<img src="media_2016_previo/img_nay/header_prox.png" border="1" />


..

..
```

Como segunda etapa del análisis de vulnerabilidades, se realizó una búsqueda de servicios disponible dentro de servidor, con un programa de búsqueda de puertos, solo se encontró disponible puerto TCP 80 y TCP 443.

Lo anterior, demuestra que se aplica una política básica en la configuración de los cortafuegos y que cambian radicalmente la filosofía fundamental de la seguridad en una organización: "Política restrictiva: Se deniega todo el tráfico excepto el que está explícitamente permitido". Lo anterior nos dice, que solo está permitido el uso de los puertos 80 y 443, habilitándose solo estos servicios para la navegación en internet.

Nmap Scan Report - Scanned at Wed Jun 27 10:47:59 2018

Scan Summary | www.prep2018ieebcs.org.mx (52.84.61.36)

Scan Summary

Nmap 7.70 was initiated at Wed Jun 27 10:47:59 2018 with these arguments:
nmap -T4 -A -v www.prep2018ieebcs.org.mx

Verbosity: 1; Debug level 0

52.84.61.36 / server-52-84-61-36.ord51.r.cloudfront.net / www.prep2018ieebcs.org.mx

Address

- 52.84.61.36 - (ipv4)

Hostnames

- www.prep2018ieebcs.org.mx (user)
- server-52-84-61-36.ord51.r.cloudfront.net (PTR)

Ports

The 998 ports scanned but not shown below are in state: **filtered**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack	Amazon CloudFront httpd		
443	tcp	open	http	syn-ack	Amazon CloudFront httpd		

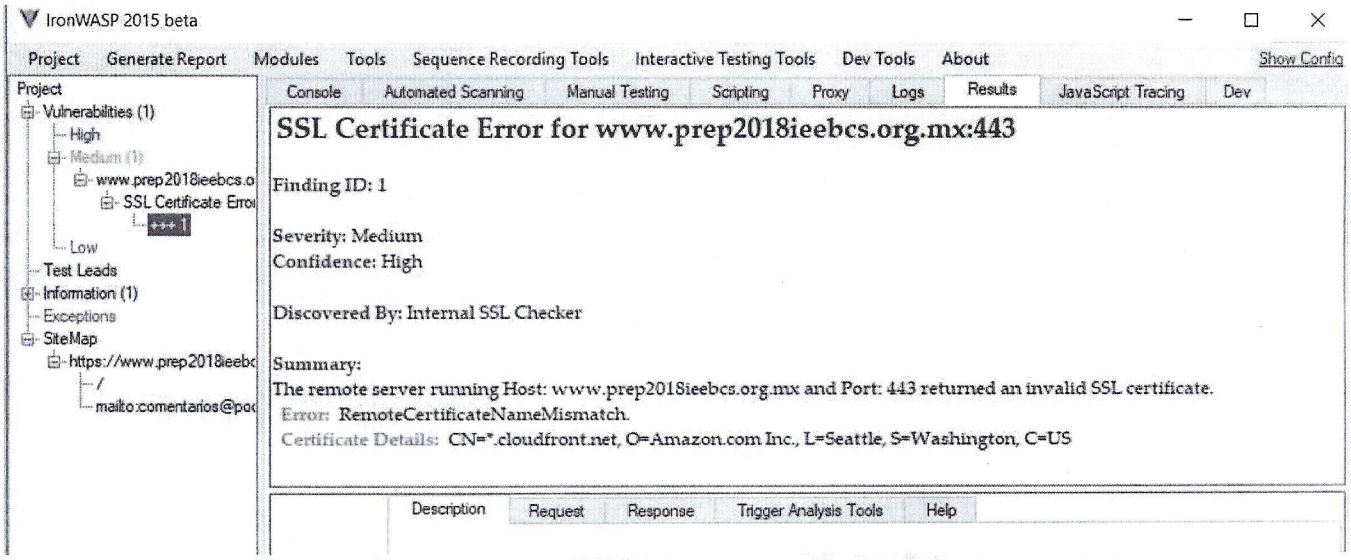
Remote Operating System Detection

- Used port: **80/tcp (open)**
- OS match: **Linux 3.2 - 4.9 (90%)**
- OS match: **Vodavi XTS-IP PBX (87%)**

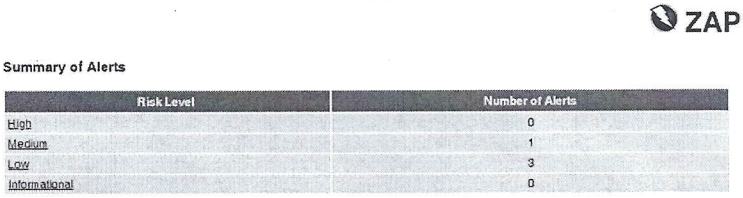
Traceroute Information (click to expand)

Misc Metrics (click to expand)

A su vez, se llevo a cabo un análisis de vulnerabilidades sobre el dominio https://www.prep2018ieebcs.org.mx haciendo uso de una herramienta especial para el caso. Este análisis nos arrojó la falta de un certificado de seguridad avalado por un organismo certificador.



Asi mismo, se corrió la aplicación ZAP de Owasp para la búsqueda de vulnerabilidades e inyección de código arrojando vulnerabilidades no consideradas como críticas que afecten el funcionamiento de los servicios web.



Hallazgos u observaciones encontradas

Con las direcciones IP se llevó a cabo un escaneo de puertos encontrándose solo los puertos 80 y 443 correspondientes a la navegación en la web.

Se identificó así mismo, que el sitio carece de un certificado de seguridad, por lo que los datos no viajan cifrados u ocultos.

No existe evidencia que se tenga instalado la herramienta modsecurity, con la cual se garantiza la seguridad ya que esta, protege contra varios tipos de ataques.

La empresa PoderNet al tener sus servicios en AMAZON, cuentan con protección suficiente mediante firewall Cisco PIX. 7.0 lo cual subsana la no aplicación de la

recomendación del Instituto Nacional Electoral de mantener sus servicios protegidos por el firewall de Owasp (modsecurity-csr).

Fase 5.

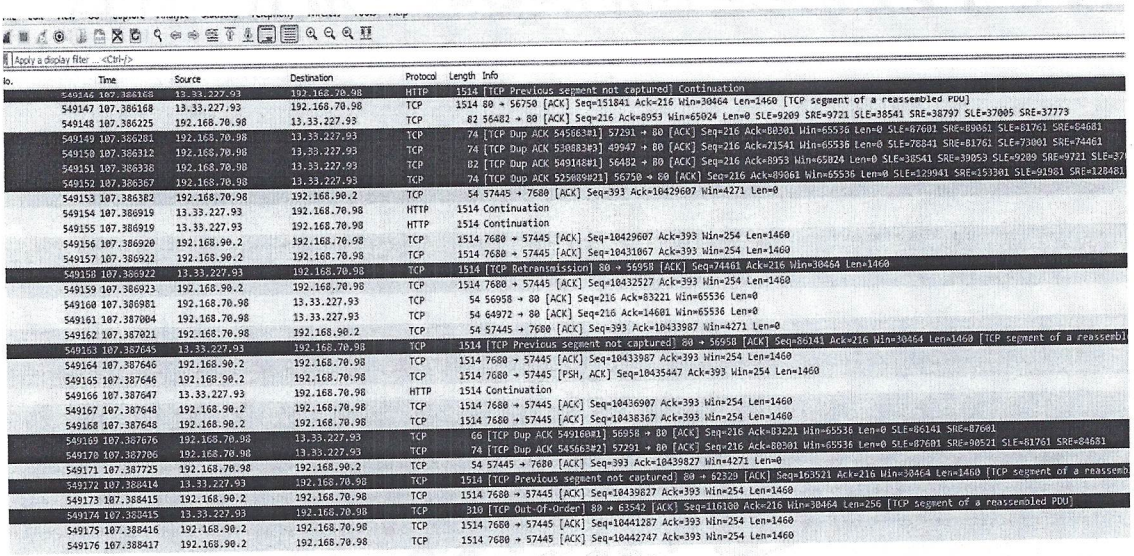
Pruebas de Denegación de Servicios al sitio web del PREP y al sitio oficial del instituto.

Se realizaron prueba de negación de servicios DoS (Deny of services) que consistieron enviar 65536 peticiones TCP simultáneas como máximo, creando conexiones con el sitio web en la siguiente liga:

http://www.prep2018ieebcs.org.mx/media_2016_previo/img_nay/slice_prox03.jpg

Esa prueba se llevó a cabo en repetidas ocasiones. Los archivos de bitácoras señalaban en promedio 500,000 paquetes enviados/recibidos. De lo anterior se generaron archivos de bitácora (log) con un tamaño de 300 Mb cada uno.

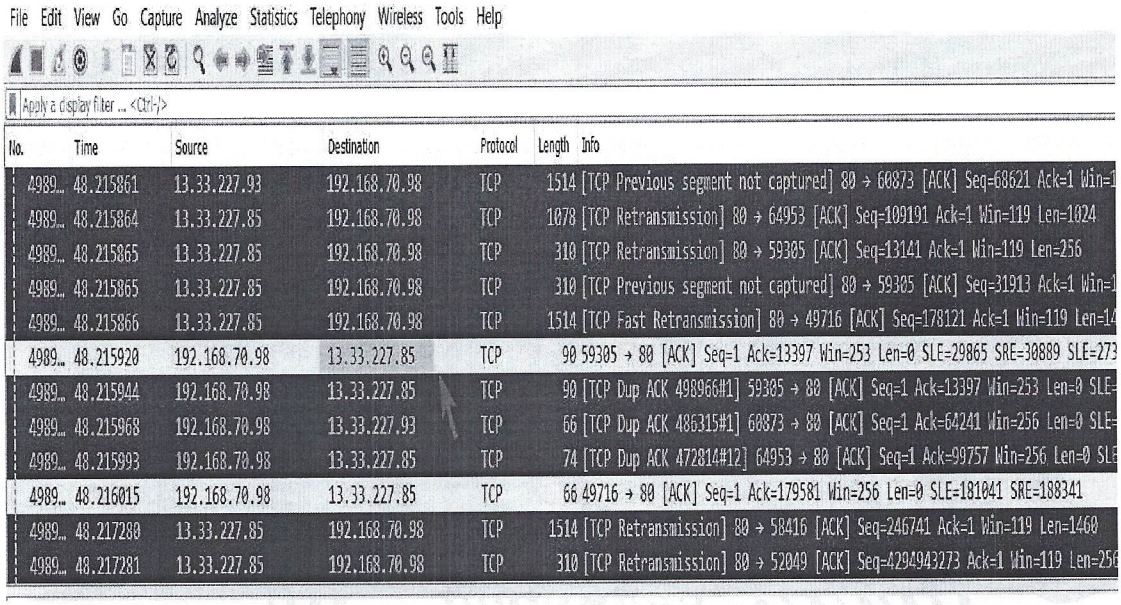
La prueba resulto exitosa ya que se puede observar que el sitio está alojado sobre una infraestructura robusta, así como lo menciona el oficio IEEEBCS/INSTACIAPREP22/2018, sin poder precisar la palabra "robusta".



No.	Time	Source	Destination	Protocol	Length	Info
549146	107.386168	13.33.227.93	192.168.70.98	HTTP	1514	[TCP Previous segment not captured] Continuation
549147	107.386168	13.33.227.93	192.168.70.98	TCP	1514	80 → 56750 [ACK] Seq=151841 Ack=216 Win=30464 Len=1460 [TCP segment of a reassembled PDU]
549148	107.386225	192.168.70.98	13.33.227.93	TCP	82	56482 → 80 [ACK] Seq=216 Ack=8953 Win=65024 Len=0 SLE=9209 SRE=9721 SLE=38541 SRE=38797 SLE=37005 SRE=37773
549149	107.386281	192.168.70.98	13.33.227.93	TCP	74	[TCP Dup ACK 545683#1] 57291 → 80 [ACK] Seq=216 Ack=80301 Win=65536 Len=0 SLE=87601 SRE=89061 SLE=81761 SRE=84681
549150	107.386312	192.168.70.98	13.33.227.93	TCP	74	[TCP Dup ACK 530883#3] 49947 → 80 [ACK] Seq=216 Ack=71541 Win=65536 Len=0 SLE=78841 SRE=81761 SLE=73001 SRE=74461
549151	107.386338	192.168.70.98	13.33.227.93	TCP	82	[TCP Dup ACK 549148#1] 56482 → 80 [ACK] Seq=216 Ack=8953 Win=65024 Len=0 SLE=38541 SRE=39053 SLE=9209 SRE=9721 SLE=37
549152	107.386367	192.168.70.98	13.33.227.93	TCP	74	[TCP Dup ACK 525089#21] 56750 → 80 [ACK] Seq=216 Ack=89061 Win=65536 Len=0 SLE=129941 SRE=153301 SLE=91981 SRE=128481
549153	107.386382	192.168.70.98	192.168.90.2	TCP	54	57445 → 7680 [ACK] Seq=393 Ack=10429607 Win=4271 Len=0
549154	107.386919	13.33.227.93	192.168.70.98	HTTP	1514	Continuation
549155	107.386919	13.33.227.93	192.168.70.98	HTTP	1514	Continuation
549156	107.386920	192.168.90.2	192.168.70.98	TCP	1514	7680 → 57445 [ACK] Seq=10429607 Ack=393 Win=254 Len=1460
549157	107.386922	192.168.90.2	192.168.70.98	TCP	1514	7680 → 57445 [ACK] Seq=10431067 Ack=393 Win=254 Len=1460
549158	107.386922	13.33.227.93	192.168.70.98	TCP	1514	[TCP Retransmission] 80 → 56958 [ACK] Seq=74461 Ack=216 Win=30464 Len=1460
549159	107.386923	192.168.90.2	192.168.70.98	TCP	1514	7680 → 57445 [ACK] Seq=10432527 Ack=393 Win=254 Len=1460
549160	107.386981	192.168.70.98	13.33.227.93	TCP	54	56958 → 80 [ACK] Seq=216 Ack=83221 Win=65536 Len=0
549161	107.387004	192.168.70.98	13.33.227.93	TCP	54	64972 → 80 [ACK] Seq=216 Ack=14601 Win=65536 Len=0
549162	107.387021	192.168.70.98	192.168.90.2	TCP	54	57445 → 7680 [ACK] Seq=393 Ack=10433987 Win=4271 Len=0
549163	107.387645	13.33.227.93	192.168.70.98	TCP	1514	[TCP Previous segment not captured] 80 → 56958 [ACK] Seq=86141 Ack=216 Win=30464 Len=1460 [TCP segment of a reassembl
549164	107.387646	192.168.90.2	192.168.70.98	TCP	1514	7680 → 57445 [ACK] Seq=10433987 Ack=393 Win=254 Len=1460
549165	107.387646	192.168.90.2	192.168.70.98	TCP	1514	7680 → 57445 [PSH, ACK] Seq=10435447 Ack=393 Win=254 Len=1460
549166	107.387647	13.33.227.93	192.168.70.98	HTTP	1514	Continuation
549167	107.387648	192.168.90.2	192.168.70.98	TCP	1514	7680 → 57445 [ACK] Seq=10436907 Ack=393 Win=254 Len=1460
549168	107.387648	192.168.90.2	192.168.70.98	TCP	1514	7680 → 57445 [ACK] Seq=10438367 Ack=393 Win=254 Len=1460
549169	107.387676	192.168.70.98	13.33.227.93	TCP	66	[TCP Dup ACK 549160#1] 56958 → 80 [ACK] Seq=216 Ack=83221 Win=65536 Len=0 SLE=86141 SRE=87601
549170	107.387706	192.168.70.98	13.33.227.93	TCP	74	[TCP Dup ACK 545683#2] 57291 → 80 [ACK] Seq=216 Ack=80301 Win=65536 Len=0 SLE=87601 SRE=90521 SLE=81761 SRE=84681
549171	107.387725	192.168.70.98	192.168.90.2	TCP	54	57445 → 7680 [ACK] Seq=393 Ack=10439827 Win=4271 Len=0
549172	107.388414	13.33.227.93	192.168.70.98	TCP	1514	[TCP Previous segment not captured] 80 → 62329 [ACK] Seq=163521 Ack=216 Win=30464 Len=1460 [TCP segment of a reassemb
549173	107.388415	192.168.90.2	192.168.70.98	TCP	1514	7680 → 57445 [ACK] Seq=10439827 Ack=393 Win=254 Len=1460
549174	107.388415	13.33.227.93	192.168.70.98	TCP	310	[TCP Out-Of-Order] 80 → 63542 [ACK] Seq=116100 Ack=216 Win=30464 Len=256 [TCP segment of a reassembled PDU]
549175	107.388416	192.168.90.2	192.168.70.98	TCP	1514	7680 → 57445 [ACK] Seq=10441287 Ack=393 Win=254 Len=1460
549176	107.388417	192.168.90.2	192.168.70.98	TCP	1514	7680 → 57445 [ACK] Seq=10442747 Ack=393 Win=254 Len=1460

Aunado a eso y tomando en cuenta los comentarios del oficio antes mencionado que "existen mayores medidas de la seguridad", se pudo observar en el análisis del

archivo de bitácoras que se generaron durante la prueba, que existe una política para ocultar la dirección real del sitio www.prep2018ieebcs.org.mx (existe más de una) y contiene un gestor que permite balancear las cargas de las peticiones o solicitudes de información y eso no lleva a que existe una redundancia en la replicación del sitio donde se alojara el PREP2018.



Se llevaron a cabo las pruebas necesarias para la Negación de servicios del sitio web del PREP así como al sitio oficial del Instituto Estatal Electoral.

Durante esta fase, se utilizaron herramientas capaces de generar tráfico suficiente y necesario para observar el comportamiento de los sitios de interés.

Hallazgos u observaciones encontradas

Los sitios web en mención soportan el envío de más de 50,000 peticiones de tamaño considerable, manteniendo su funcionalidad, por lo que se considera que son sitios seguros contra ataques de negación de servicios.

Durante la implementación del PREP los días 1 y 2 de julio, no se encontró evidencia que sugiera problema alguno en su funcionamiento. No observando falla alguna durante el procesamiento de la información.

Conclusión de la auditoria.

En base a los resultados de las diferentes actividades de auditoria aplicada se concluye que el sistema PREP se desempeña en forma íntegra en el procesamiento de la información y que la infraestructura tecnológica proporciona un ambiente estable en un marco de seguridad aceptable y que da como resultado el escenario adecuado cumpliendo con la normatividad en términos de funcionalidad, para su operación en las próximas elecciones del primero de julio del presente año.

ATENTAMENTE
EL ENTE AUDITOR

M.S.C. Javier Alberto Carmona Troyo
Auditor Líder

M.A.T.I. Luis Armando Cárdenas Florido
Auditor Auxiliar

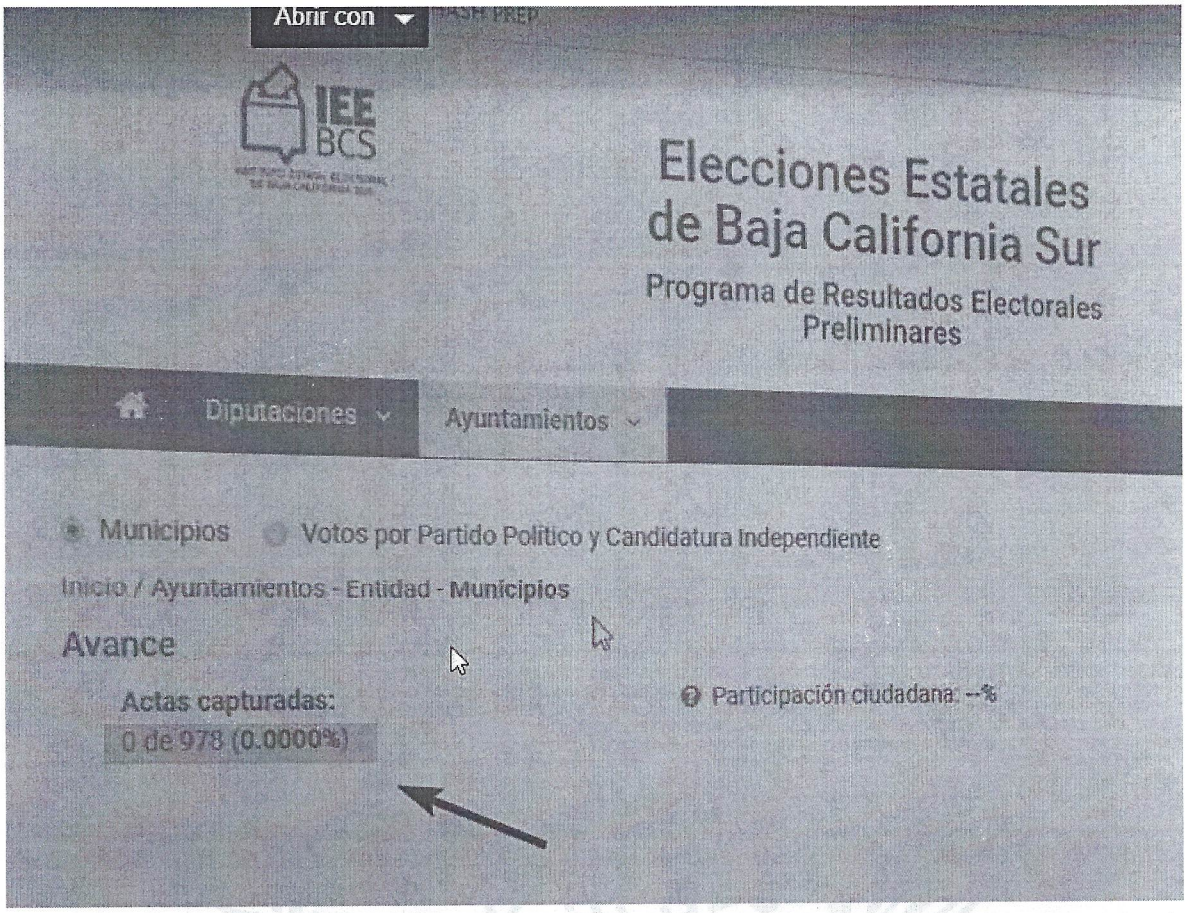
M.S.C. Ana Luz Rodríguez Sarabia
Auditor Auxiliar

M.S.C. Armando Yuen Coria
Auditor Auxiliar

Anexo

Cumplimiento al 100% de Programa de Resultados Electorales Preliminares para el estado de Baja California Sur en elecciones para diputaciones locales y ayuntamientos.

En ceros la base de datos.



100% de las actas computadas.