



**EDUCACIÓN**  
SECRETARÍA DE EDUCACIÓN PÚBLICA



TECNOLÓGICO  
NACIONAL DE MÉXICO®

Soledad de Graciano Sánchez, S.L.P, 05/junio/2021

# Informe Final de Auditoría

Servicios de auditoría al sistema informático y a la infraestructura tecnológica del PREP para el Proceso Electoral Local 2020-2021





## Tabla de contenido

Tabla de contenido .....	2
1. INTRODUCCIÓN .....	4
2. CRONOLOGÍA DEL SIMULACRO LLEVADO A CABO EL 16 DE MAYO.....	4
2.1. RECOMENDACIONES.....	10
3. CRONOLOGÍA DEL SIMULACRO LLEVADA A CABO EL 21 DE MAYO.....	10
3.1. CRONOLOGÍA DE SUCESOS EN EL CCV UBICADO EN EL CENTRO DE CENTRO DE CONVENCIONES DE SAN LUIS POTOSÍ. ....	10
3.2. CRONOLOGÍA DE SUCESOS EN EL CATD DE ARMADILLO DE LOS INFANTE. ....	11
3.3. CRONOLOGÍA DE SUCESOS EN EL CATD UBICADO EN COLONIA EL PASEO. ....	11
3.4. CRONOLOGÍA DE SUCESOS EN EL CATD UBICADO EN AV. RICARDO B ANAYA. ....	13
3.5. RECOMENDACIONES.....	15
4. CRONOLOGÍA DEL SIMULACRO LLEVADA A CABO EL 23 DE MAYO.....	15
4.1. CRONOLOGÍA DE SUCESOS EN EL CCV UBICADO EN EL CENTRO DE CENTRO DE CONVENCIONES DE SAN LUIS POTOSÍ. ....	15
4.2. CRONOLOGÍA DE SUCESOS EN EL CATD DE CERRO DE SAN PEDRO. ....	17
4.3. CRONOLOGÍA DE SUCESOS EN EL CATD UBICADO EN AV. RICARDO B ANAYA.....	19
4.4. RECOMENDACIONES.....	19
5. CRONOLOGÍA DEL SIMULACRO LLEVADA A CABO EL 27 DE MAYO.....	20
5.1. CRONOLOGÍA DE SUCESOS EN EL CCV UBICADO EN EL CENTRO DE CENTRO DE CONVENCIONES DE SAN LUIS POTOSÍ. ....	20
5.2. REVISIÓN DE SEGURIDAD DEL PUBLICADOR DE RESULTADOS DEL CEEPAC 2021. ....	23
ATAQUES DDoS .....	23
VOLUMÉTRICOS .....	24
ATAQUES LENTOS.....	24
RESULTADOS DE ATAQUES DDoS .....	24
ATAQUES AL SOFTWARE PUBLICADOR.....	25
ATAQUE A LA ENTRADA DE “RESULTADOS DE CASILLA”. ....	25
5.3. RECOMENDACIONES.....	29
6. CRONOLOGÍA DEL SIMULACRO LLEVADA A CABO EL 30 DE MAYO.....	29
6.1. CRONOLOGÍA DE SUCESOS EN EL CCV UBICADO EN EL CENTRO DE CENTRO DE CONVENCIONES DE SAN LUIS POTOSÍ. ....	30



6.2. CRONOLOGÍA DE SUCESOS EN EL CATD DE CERRO DE SAN PEDRO.....	31
6.3. CRONOLOGÍA DE SUCESOS EN EL CATD UBICADO EN AV. RICARDO B ANAYA.....	31
6.4. RECOMENDACIONES.....	33
7. CRONOLOGÍA DEL SIMULACRO LLEVADA A CABO EL 03 DE JUNIO.....	33
7.1. CRONOLOGÍA DE SUCESOS EN EL CCV UBICADO EN EL CENTRO DE CENTRO DE CONVENCIONES DE SAN LUIS POTOSÍ.....	34
7.2. CRONOLOGÍA DE SUCESOS EN EL CATD DE CERRO DE SAN PEDRO.....	34
7.3. CRONOLOGÍA DE SUCESOS EN EL CATD UBICADO EN AV. RICARDO B ANAYA.....	35
7.4. RECOMENDACIONES.....	36
8. PROCEDIMIENTO TÉCNICO CON ESQUEMA DE VALIDACIÓN DE LA BASE DE DATOS DEL SISTEMA INFORMÁTICO PREP.....	37
8.1. INICIALIZAR LA BASE DE DATOS.....	37
8.2. VALIDAR INFORMACIÓN FINAL DE LA BASE DE DATOS.....	37
9. INFORME DE PRUEBAS DE PENETRACIÓN A LA INFRAESTRUCTURA TECNOLÓGICA.....	39
RESUMEN EJECUTIVO.....	39
9.1. ALCANCE.....	39
9.2. OBTENCIÓN DE INFORMACIÓN.....	40
CDM.....	40
9.3. MODELADO DE AMENAZAS:.....	41
TASM.....	41
9.4. ANÁLISIS DE VULNERABILIDADES A LAS APLICACIONES:.....	41
9.5. ANÁLISIS DE VULNERABILIDADES A LOS DISPOSITIVOS DE RED:.....	42
EXPLOTACIÓN:.....	42
POST EXPLOTACIÓN:.....	42
REPORTE:.....	42
9.6. RESULTADOS DE LA VERIFICACIÓN.....	42
10. INFORME DE PRUEBAS DE DENEGACIÓN DE SERVICIO A LA INFRAESTRUCTURA TECNOLÓGICA.....	43
RESUMEN EJECUTIVO.....	43
10.1. ALCANCE.....	43
10.2. RESULTADOS DE LA VERIFICACIÓN.....	43



## 1. INTRODUCCIÓN

Las técnicas de pruebas de caja negra (o pruebas de comportamiento) son pruebas basadas en requisitos, donde se desconoce el trabajo interno del proceso que se está probando. Su funcionamiento se basa en proporcionar entradas al sistema y esperar que el resultado (o salida) sea aceptado de acuerdo con ciertos criterios, dependiendo de la prueba, de lo contrario la prueba será rechazada.

Las técnicas de caja negra que podemos usar son: Particiones equivalentes, análisis del valor límite, tablas de decisión y arreglos ortogonales.

En el presente informe se relata lo sucedido en los simulacros posteriores al primer simulacro. Por fallos importantes en los simulacros agendados 1 y 2, se tuvieron que repetir entre semana. En este reporte se documenta lo sucedido en los siguientes simulacros:

**[16 de mayo del 2021]** Primer simulacro.

**[21 de mayo del 2021]** Primer simulacro intermedio.

**[23 de mayo del 2021]** Segundo simulacro.

**[27 de mayo del 2021]** Segundo simulacro intermedio.



**[30 de mayo del 2021]** Tercer simulacro.

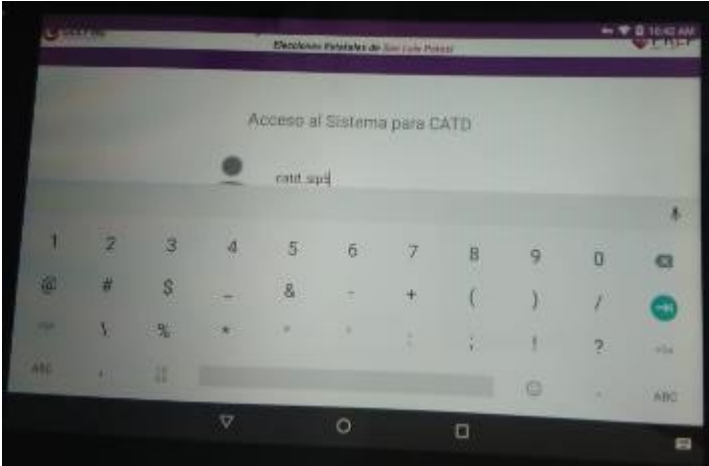
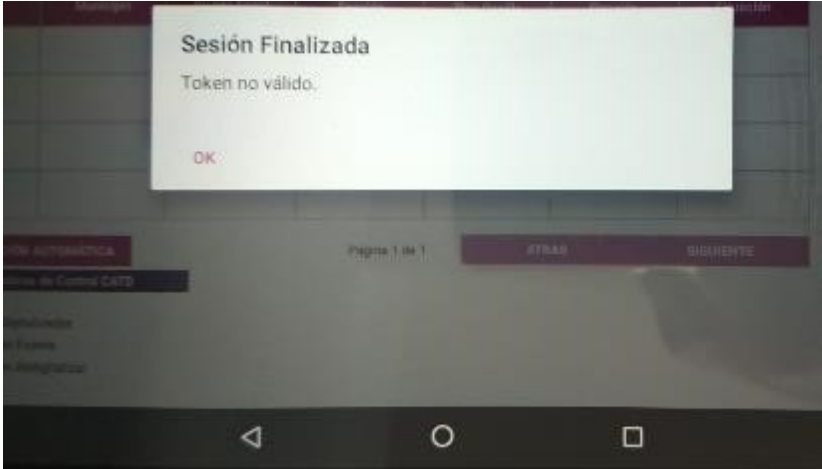
**[03 de junio del 2021]** Cuarto simulacro.

Cabe destacar que los hallazgos detectados se les dieron a conocer inmediatamente a CIATEC, con el ánimo de que los corrigieran a la brevedad posible.

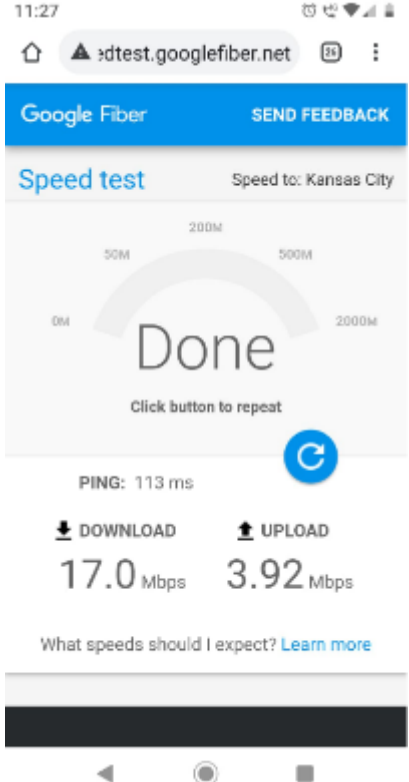
## 2. CRONOLOGÍA DEL SIMULACRO LLEVADO A CABO EL 16 DE MAYO


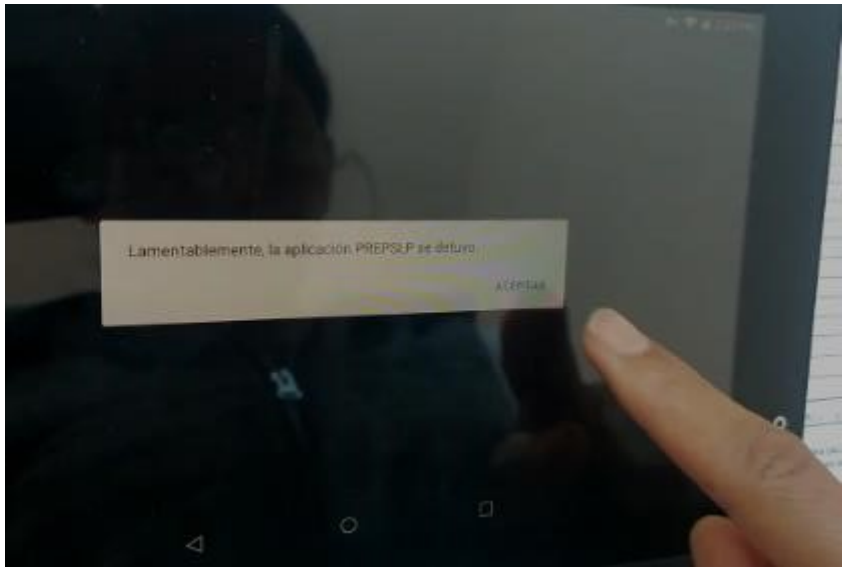
<b>Hora</b>	<b>Lugar</b>	<b>Evento</b>
9:30	Centro de convenciones	Al llegar al lugar donde se lleva a cabo la captura y verificación de actas, vimos que ya estaban aprox. El 50% de los capturistas presentes.
9:50	Cerro de San Pedro	El CATD de Cerro de San Pedro aún estaba cerrado
9:50	Oficina ubicada en B. Anaya	La oficina se encontró abierta, pero aún no llegaban las actas

10:00	Centro de convenciones	<p>El personal de CIATEC localizado en el centro de convenciones está listo para iniciar el simulacro.</p> 
10:16	Centro de convenciones	Se da inicio al simulacro. Comienza el proceso de digitalización en varios CATD del estado
11:00	Oficina ubicada en B. Anaya	Llegan las actas y se comienza el proceso de digitalización
		<p>La Tablet no cuenta con la base para la digitalización.</p> 

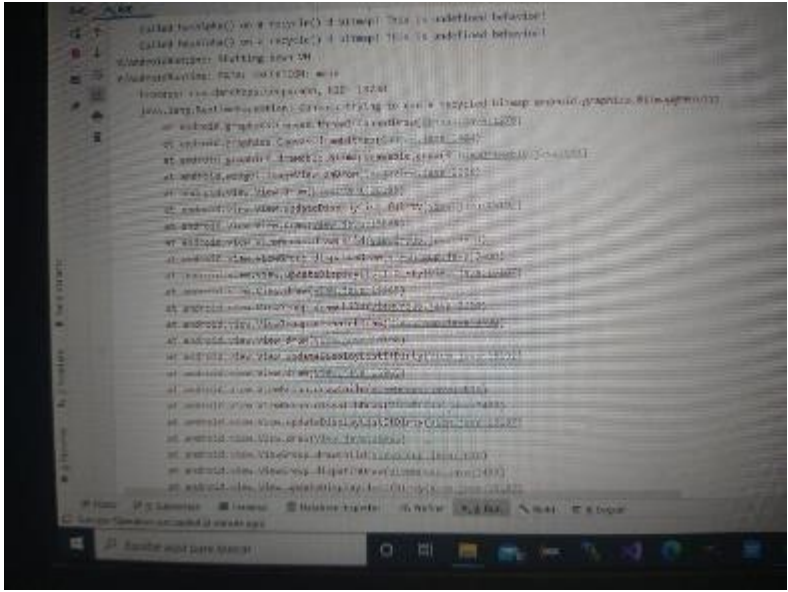

	Oficina ubicada en B. Anaya	Se obtiene un error al intentar visualizar la lista de actas: “Token no reconocido”
	Oficina ubicada en B. Anaya	Llegan las actas y se intenta comenzar la digitalización
10:43	Oficina ubicada en B. Anaya	Se presenta un error. No se pueden conectar al servidor. Se procede a configurar la VPN de la Tablet. 
10:44	Oficina ubicada en B. Anaya	Se conecta, pero obtienen el error de “token no válido” 
11:00	Centro de convenciones	Se dan cuenta que el error de “token no reconocido” se presenta en la gran mayoría de los CATD que usan Tablet para digitalizar
11:27	Oficina ubicada en B. Anaya	Se revisa la velocidad del enlace de B Anaya



		
12:05	Centro de convenciones	Se les da un descanso hasta las 14:00 horas a los capturistas en lo que se busca la causa del error.
13:20	Centro de convenciones	Se han corregido los errores de “token no reconocido”

		
14:05	Centro de convenciones	Al reiniciar la digitalización, se presenta otro error en la gran mayoría de los CATD que usan Tablet para digitalizar. Dicho error aparece al momento de cargar la imagen de un acta en la Tablet.
14:48		<p>Otro error en la digitalización, con el mensaje <b>“Lamentablemente la aplicación del prepslp se detuvo”</b> (se sugiere que el mensaje de instrucciones de como proceder):</p> 



		<p>El error surge por falta de recursos:</p> 
14:00		<p>El proceso de digitalización es muy lento, por lo cual los capturistas tienen muy poco o nada de trabajo.</p>
15:00	Cerro de San Pedro	<p>Pueden digitalizar correctamente usando “PREP casilla”</p> 
19:00		<p>Se les avisa a los capturistas que pueden retirarse. El personal de CIATEC se encarga de capturar las últimas actas.</p>
19:30		<p>Se da por terminado el proceso de captura.</p>
20:00		<p>Se hacen pruebas de la configuración del servidor.</p>
21:00		<p>Se hacen pruebas de la configuración de las tabletas: 1. Con la versión 5 funciona correctamente</p>



		<ol style="list-style-type: none"> <li>2. Se actualizan y dejan de funcionar</li> <li>3. Se recomienda hacer el “downgrade” (cambiar a una versión más antigua”</li> <li>4. Se recomienda deshabilitar la actualización automática.</li> </ol>
--	--	--

## 2.1. RECOMENDACIONES.

En base a los errores presentados, nos permitimos hacer las siguientes recomendaciones:

1. Réplica del sistema con acceso al servidor de triara
2. Contar con una tablet para efectuar las pruebas.
3. Reforzar los catd con prep-casilla
4. Que los mensajes de error sean más expresivos para el usuario y el desarrollador.
5. Que en el próximo simulacro ya se considere la toma de la huella.
6. Implementar algún mecanismo para comprobar donde hay conectividad (ping).
7. Dar una tarjeta a los usuarios con los puntos más importantes para el uso correcto del respectivo sistema

## 3. CRONOLOGÍA DEL SIMULACRO LLEVADA A CABO EL 21 DE MAYO

En este simulacro se tuvo presencia en el CATD de Cerro de San Pedro, en el CATD de Ricardo B. y en el CCV ubicado en el centro de Centro de Convenciones de San Luis Potosí. Se tenía planeado iniciar el simulacro a las 9:00 Hrs.

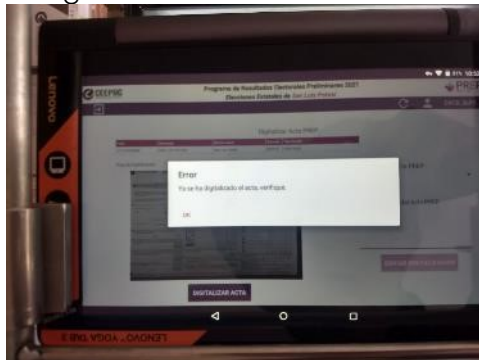
### 3.1. CRONOLOGÍA DE SUCESOS EN EL CCV UBICADO EN EL CENTRO DE CENTRO DE CONVENCIONES DE SAN LUIS POTOSÍ.


Hora	Evento
9:30	Al llegar al lugar donde se lleva a cabo la captura y verificación de actas, vimos que ya estaban aprox. El 50% de los capturistas presentes.
9:50	La oficina se encontró abierta, pero aún no llegaban las actas
10:00	El personal de CIATEC localizado en el centro de convenciones está listo para iniciar el simulacro.
10:16	Se da inicio al simulacro. Comienza el proceso de digitalización en varios CATD del estado.
14:00	El sitio del publicador está muy lento.
20:00	No coinciden algunas cantidades arrojadas en el publicador.
22:30	Se da por concluido el simulacro.


### 3.2. CRONOLOGÍA DE SUCESOS EN EL CATD DE ARMADILLO DE LOS INFANTE.

Hora	Evento
10:00	No hay conexión a internet
10:00	Ya hay conexión a internet, pero aún no se pueden conectar a la VPN
11:14	Aún no pueden iniciar la digitalización
11:16	Llega a atenderlos Karla Méndez de CIATEC
12:02	Llevaron 11 actas digitalizadas, pero faltan 22 por asignar.
12:05	Entre el envío de ellas a veces aparece "Causa genérica de que los servicios estén abajo, favor de contactar al dueño de los servicios", aunque si se envían las actas.
13:30	Se concluye la digitalización.

### 3.3. CRONOLOGÍA DE SUCESOS EN EL CATD UBICADO EN COLONIA EL PASEO.


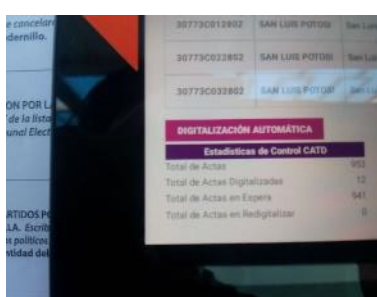
Hora	Evento
08:58	Hay un solo digitalizador al cual citaron desde las 8 y desde esa hora iban a recibir las actas.
09:49	Se reciben 953 actas a digitalizar. Se digitaliza la primera acta.
10:16	La aplicación de digitalización presentó la situación de que se muestra como vacía la tabla de actas por capturar después de 40 minutos de uso, y al recargar la interfaz ya aparecen nuevamente
10:45	Se está presentando el fallo de que, tras enviar un acta digitalizada, se muestra vacía la tabla de actas por digitalizar y se soluciona recargando la interfaz.
10:54	Los contadores ahora no muestran datos.
11:02	Tras el error <b>com.android.volley.error.servererror</b> está apareciendo el error mostrado en la fotografía. 
11:03	Se comienza a actualizar el contador de actas, pero se está incrementando de 2 en 2 y por debajo de la cantidad real.

<p>12:07</p>	<p>Se detuvo la digitalización porque ya no coinciden los números de folio de las actas con los que aparecen en la tabla de la aplicación.</p> <p>Las actas de esta foto no se encuentran físicamente aquí en el distrito 6 pero aparecen como ya digitalizadas.</p> 
<p>12:17</p>	<p>Se terminó la digitalización, más de la mitad de las actas ya no se digitalizará porque no coinciden los folios físicos en las actas, con los asignados en la aplicación.</p>
<p>12:50</p>	<p>El acta número 10773B012802 se tiene físicamente, pero no está asignado en el sistema de este catd, sin embargo, el digitalizador pudo digitalizarla y enviarla.</p> <p>De acuerdo a la capacitación que le dieron, las instrucciones son que no envíen actas que no tienen asignadas y que no les han dado la autorización de hacerlo, pero se puede hacer.</p> <p>También, en su lista de actas, le aparecen muchas en situaciones de digitalizada, enviada y publicada, pero esas actas físicamente no están aquí con él, lo cual quiere decir que alguien en otro lado tiene dicha acta e hizo el proceso.</p> <p>Sin embargo, si una de esas actas que el digitalizador tiene en su lista, aparece en la situación REDIGITALIZAR, no podría hacerlo porque físicamente no cuenta con ella y tampoco sabe quién la tiene como para comunicarse y avisar que la redigitalice.</p> <p>Se un ejemplo de actas que no están físicamente presentes en éste catd y</p>

	<p>pertenecen a la lista de actas asignadas en el sistema, pero ya están publicadas inclusive, lo cual indica que se digitalizaron en otro lado.</p> 
13:25	El digitalizador comenta que ya no está teniendo problemas de envío. El coordinador dejó instrucciones de digitalizar las actas que se tienen físicamente, pero que no están dadas de alta en el catálogo del digitalizador.
14:16	Finaliza el proceso de digitalización

### 3.4. CRONOLOGÍA DE SUCESOS EN EL CATD UBICADO EN AV. RICARDO B ANAYA.

Hora	Evento
8:00	Llegada del personal: 08:00 CATD digitalizadora, Imelda Zarazúa Cortes 08:40 Auxiliar A y B 08:45 Apertura del distrito 08 09:00 Secretaria técnica 09:55 Presidente, Jayro Morales Bernal
08:45	Se inician las actividades. La conexión wi-fi, modem ya se encontraba configurado listo para iniciar la conexión. La VPN no presentó ningún problema.
08:45	Se reciben las actas a digitalizar.
09:40	Se inicia la digitalización.
10:23	Aparece el error <b>com.Android.volley.error.ServerError</b> indicando que no se puede comunicar con el servidor.

10:38	<p>Aparte del error anteriormente mencionado existe una inconsistencia en la app según esto ya llevan digitalizada más de 25 actas, pero en el status solo aparece 12 y ya no se actualiza ese digito.</p> <p>Este error se está presentando al momento de envía un acta, y la interfaz no muestra información de si se envió o no el acta y se tiene que repetir la digitalización</p> 
12:15	<p>Se encontraron un par de posibles inconsistencias los folios que aparecen en la tabla no son los que realmente le pertenecen al CATD en cuestión y el buscador incluyendo filtros no arroja los folios esperados, pero si devuelve otros posibles folios validos</p>
12:40	<p>Primeramente, se reportó en un breve fallo en la app cuando uno escanea el código de barras, y al momento de devolver el registro con el folio aparece en blanco el registro con la leyenda "Causa genérica de que los servicios estén abajo favor de comunicarse al dueño de los servicios" lo único que se hace en ese caso es reintentar el código de barras hasta que deja continuar el proceso de digitalización. También no se actualiza el estatus(contador) de actas digitalizadas en el catd5_slp se quedó a partir del acta no 12 después ya no incremento, se intentó cerrar sesión y volver a iniciar, pero el contador solo incremento 2 de 12 a 14 (si incrementa, pero una a una velocidad baja y por debajo del número real de actas digitalizadas). Aparece un error intermitente <b>Com.Android.volley.error.ServerError</b> aproximadamente en la acta no 18.</p> 



17:00	Se finalizó el proceso de digitalización con los siguientes números: Actas transmitidas: 122, Actas legibles:121, Actas ilegibles: 1 en blanco
-------	---

### 3.5. RECOMENDACIONES.

En base a los errores presentados, nos permitimos hacer las siguientes recomendaciones:

8. Eliminar la característica de la lupa por lo pronto para que no estorbe ni canse a los capturistas
9. Verificar porque la aplicación de los capturistas pierde muy seguido la conexión.
10. En el publicador se presentan diferentes totales, en distintas partes de la página. Al revisar parece que se debe a la estrategia que usan para transferir los datos de la aplicación de captura al publicador. Lo hace usando un plug-in para implementar bases de datos federadas. Por lo cual se sugiere buscar otra estrategia para transferir los datos a publicar.
11. La respuesta del publicador es muy lenta. Se sugiere usar el CDN que les ofrece Triara. Además, las páginas resultantes son muy pesadas.


## 4. CRONOLOGÍA DEL SIMULACRO LLEVADA A CABO EL 23 DE MAYO

En este simulacro se tuvo presencia en el CATD de Cerro de San Pedro, en el CATD de Ricardo B. y en el CCV ubicado en Centro de Convenciones de San Luis Potosí.

Se tenía planeado iniciar el simulacro a las 18:00 Hrs.

### 4.1. CRONOLOGÍA DE SUCESOS EN EL CCV UBICADO EN EL CENTRO DE CENTRO DE CONVENCIONES DE SAN LUIS POTOSÍ.

Hora	Evento
17:40	Minutos antes de iniciar, ya estaba el 100% de los capturistas presentes.

18:10	Se inicia el simulacro.  
18:11	Se practicó el proceso de tomar la huella y verificar que la base de datos estuviera con los contadores de votos en ceros.
18:19	Inicia el proceso de captura de actas.
	Los capturistas se comportan con bastante respeto y dedicación. Uno de ellos tardo hasta 5 minutos en capturar un acta, pero en promedio tardan 1.7 minutos
18:40	Sucede un corte de electricidad. Arrancó la planta de energía eléctrica pero no se contaba con suficientes UPS para todos los switches, por lo cual un segmento de la red si se vió afectada. Se reiniciaron los switches quedando el 60% sin conexión a Internet, en un lapso de 15 min.  También a esta hora llovió, provocando se apreciaran un par de goteras. A las 18:50
18:50	Se generaron resultados en el portal del publicador: simulacro.prep.slp.mx
20:00	Se genera un error al usar la app "prep-casilla". Comenzaron digitalizando bien, pero después de varias actas, ya no funcionaban bien.
09:00	Se les observo que había archivos de actas antiguas y accesibles en el publicador. Mismas que en ese mismo rato lo solucionaron personal de CIA-TEC.
20:27	Error en el publicador. En la pestaña "diputaciones", al seleccionar "voto por distrito" y seleccionó "detalle por distrito" por ejemplo 01 Matehuala, seleccionó tres partidos no resulta en sumatoria, el resultado es 0%
23:00	Nos atendieron los consejeros, explicándonos información del publicado
03:00	Se deshabilitó el autoenfoco de las actas, evitando el cansacio visual prematuro de los capturistas.
06:00	Se finalizo la captura de actas. Quedando en verificación más de 600 actas



07:05		<p>La cantidad de actas capturadas y contabilizadas son iguales, lo que hace sospechar que está contando inclusive actas detectadas como "excede la lista nominal".</p>
08:00	Se termino de atender las actas en verificación	
08:20	Se reflejo en el publicador el último corte.	

#### 4.2. CRONOLOGÍA DE SUCESOS EN EL CATD DE CERRO DE SAN PEDRO.

Hora	Evento
18:15	<p>No se detectaba la red del internet inalámbrico. Desconectaron el módem y lo volvieron a conectar y ya funcionó de forma normal.</p> <p>Estuvo una patrulla desde el inicio y hasta el fin del simulacro.</p> <p>Se tuvo una Tablet para digitalizar.</p> <p>No se tuvo la caja para colocar la Tablet y poder así obtener una digitalización estandarizada.</p> <p>No hay gafetes de los participantes y los están pidiendo las personas del CATD</p> <p>La digitalizadora ya tenía las actas y la Tablet desde el simulacro anterior</p>



### 4.3. CRONOLOGÍA DE SUCESOS EN EL CATD UBICADO EN AV. RICARDO B ANAYA.

Hora	Evento																												
17:00	Se reciben las actas a digitalizar																												
17:45	Llegada del personal: 17:45 CATD digitalizadora, Perla Lucero Ortiz Guevara, móvil Xiaomi Redmi 9A 17:45 CATD digitalizadora, Imelda Zarazúa Cortes, Tablet Lenovo Yoga T 17:45 Secretaria técnica, Astrid Martínez 17:55 Presidente, Jayro Morales Bernal																												
18:00	Se inician las actividades. Se verifica la velocidad de la conexión:  <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th># ping</th> <th>PING ms</th> <th>Descarga Mbps</th> <th>Carga Mbps</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>16</td> <td>27.72</td> <td>8.78</td> </tr> <tr> <td>2</td> <td>16</td> <td>29.49</td> <td>10</td> </tr> <tr> <td>3</td> <td>16</td> <td>20.97</td> <td>9.46</td> </tr> <tr> <td>4</td> <td>16</td> <td>19.78</td> <td>8.56</td> </tr> <tr> <td>5</td> <td>16</td> <td>31.37</td> <td>9.89</td> </tr> <tr> <td colspan="2" style="text-align: center;"><b>Promedio</b></td> <td style="text-align: center;">24.04</td> <td style="text-align: center;">17.02</td> </tr> </tbody> </table>	# ping	PING ms	Descarga Mbps	Carga Mbps	1	16	27.72	8.78	2	16	29.49	10	3	16	20.97	9.46	4	16	19.78	8.56	5	16	31.37	9.89	<b>Promedio</b>		24.04	17.02
# ping	PING ms	Descarga Mbps	Carga Mbps																										
1	16	27.72	8.78																										
2	16	29.49	10																										
3	16	20.97	9.46																										
4	16	19.78	8.56																										
5	16	31.37	9.89																										
<b>Promedio</b>		24.04	17.02																										
18:00	Se inicia la digitalización. Digitalizadora Perla Lucero Ortiz Guevara																												
18:20	Se inicia la digitalización. Digitalizadora Imelda Zarazúa Cortes																												
19:30	se encontraron un par de posibles inconsistencias los folios que aparecen en la tabla no son los que realmente le pertenecen al CATD en cuestión y el buscador incluyendo filtros no arroja los folios esperados, pero si devuelve otros posibles folios validos																												
21:25	se actualiza el estatus(contador) de actas digitalizadas a un ritmo lento su-pongo que se actualiza cada vez que se refresca el acceso a los reposito-rios, solo se reportó un 2 incidente el primero es que cuando se intentó termi-nar de enviar una digitalización retorna a volver a escanear el código de ba-ras y el segundo incidente fue que un acata apareció como ya digitalizada.																												
06:00	Se finalizó el proceso de digitalización con los siguientes números: Actas transmitidas: 122, Actas legibles:121, Actas ilegibles: 1 en blanco																												

### 4.4. RECOMENDACIONES.

En base a los errores presentados, nos permitimos hacer las siguientes recomendaciones:

1. Corregir el brillo de la pantalla de los capturistas



2. La otra causa de retraso, es que varios digitalizadores toman imágenes incompletas, borrosas, oscuras o volteada. Se sugiere decirles cómo tomar imágenes de calidad.
3. Al tener todos los usuarios la misma contraseña se podría prestar a un mal uso por parte de un usuario. Crear contraseñas personalizadas tal vez sea mucho trabajo y sería más laborioso ayudar a otros capturistas que se queden atrás en números. Tal vez si se muestra un mensaje de que "Otro usuario acaba de ingresar a esta cuenta" o "Dos usuarios actualmente activos en la cuenta" ya se puede saber si es alguien que está ayudando o no tiene nada que hacer en esa cuenta.
4. La caja de texto donde se capturan los números de las actas está un poco separada de la imagen escaneada del acta, tal vez si estuviesen más juntos facilitaría y agilizaría la captura de los mismos, ya que se pueden comparar aún más rápido los números con la vista.
5. La app de digitalización funciona bien en las tabletas, pero no en los celulares. Se sugiere revisar los cambios significativos en las versiones de Android que usan los celulares y las tabletas.

## 5. CRONOLOGÍA DEL SIMULACRO LLEVADA A CABO EL 27 DE MAYO

En este simulacro se tuvo presencia solo en el CCV ubicado en el centro de Centro de Convenciones de San Luis Potosí.

Se tenía planeado iniciar el simulacro a las 10:00 Hrs.

### 5.1. CRONOLOGÍA DE SUCESOS EN EL CCV UBICADO EN EL CENTRO DE CENTRO DE CONVENCIONES DE SAN LUIS POTOSÍ.

Hora	Evento
9:27	Se da inicio el simulacro. Hay 50 capturistas. Se pretende digitalizar un total de 11250 actas y finalizar a las 21:30 Hrs.
11:38	Total de capturistas:54 Total de actas digitalizadas: 5055 Total de actas publicadas: 534 Total de actas con inconsistencias: 208
11:40	Se detecta que en programa de captura hay un tiempo muerto de aproximadamente 14 segundos entre el evento de guardar acta ver la lista de actas restantes.
14:27	Detalles encontrados en el publicador en la url simulacro.prepslp.mx, en vista para dispositivos móviles:



2:42 PM 73%

0 + 0  
0.0000% 0.0000%  
Nulos  
0  
0.0000%

**Total de votos**  
**= 0**  
100.0000%

**Detalle de votos por Casilla**

Imagen procedente de:  
Acta del proceso

Casilla	Acta digitalizada	Candidaturas registradas	Votos recibidos	Total

**Estadística de Casilla**

Participación ciudadana con base en la Lista Nominal de las A PREP Contabilizadas

Compartir

Iconos amontonados

2:46 PM 72%

simulacro.prepslp.mx

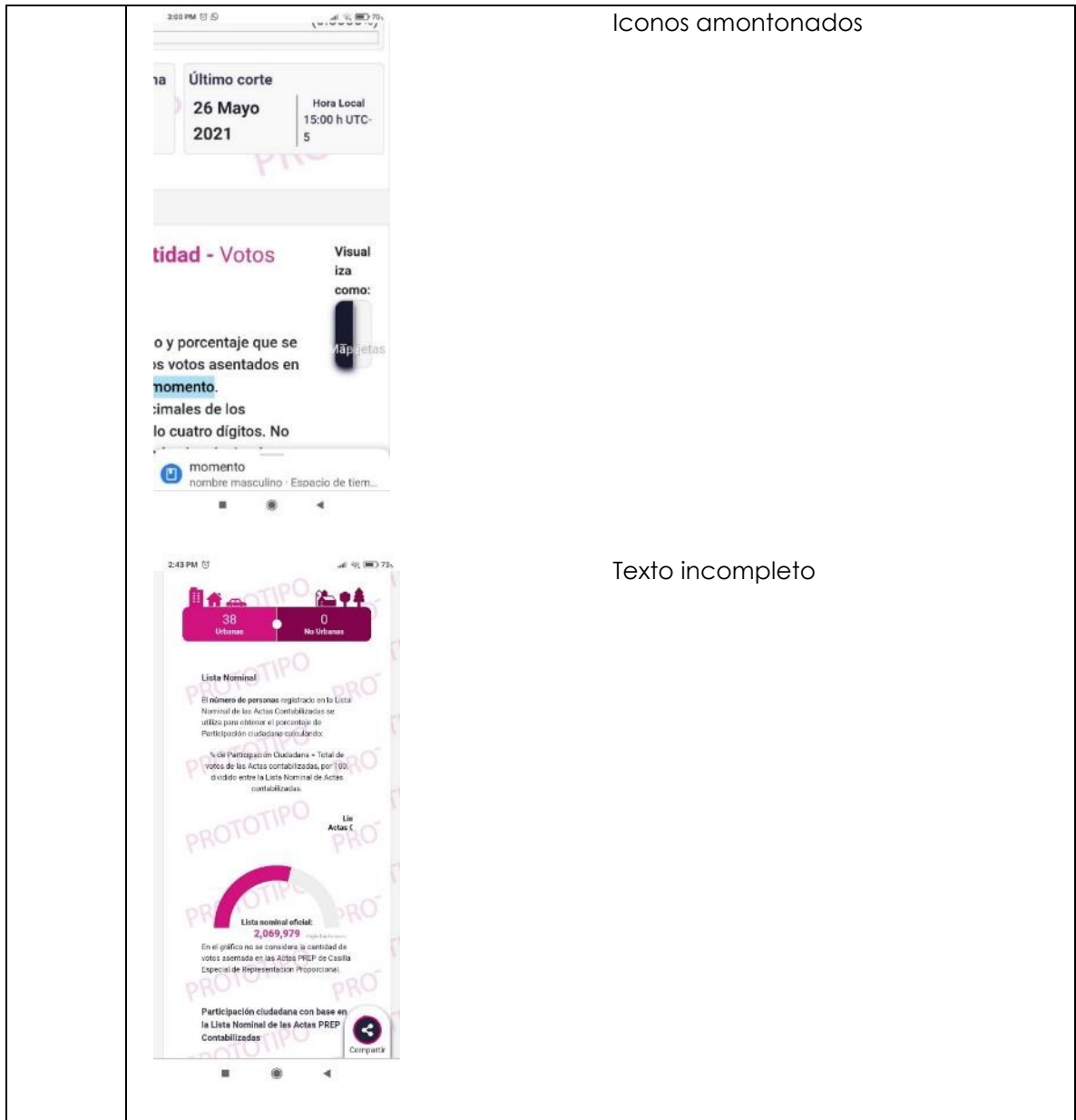
**Detalle**

Total de votos  
**10,013**

Total de votos	Porcentaje de votos	Porcentaje de distritos
10,013	100.0000%	3.2187%
323	3.23%	4.1953%
421	4.21%	1.4549%
146	1.46%	

Puedes agregar hasta tres opciones con el botón +.

Iconos amontonados



	<p>2:58 PM 4,190 1,290 1,172</p> <table border="1"> <tr> <td>Porcentaje</td> <td>18.8721%</td> <td>12.1992%</td> <td>11.0932%</td> <td>6.5333%</td> </tr> <tr> <td>En la Entidad</td> <td>2,496</td> <td>2,195</td> <td>1,996</td> <td>1,175</td> </tr> <tr> <td>En el Extranjero</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> </table> <p><b>Resumen de la votación</b></p> <p>la Entidad 17,341 96.3764%</p> <p>En el Extranjero 0 0.0000%</p> <p>Candidaturas no registradas 183 1.0171%</p> <p>Nulos 469 2.6060%</p> <p>Total de votos <b>17,99</b></p>	Porcentaje	18.8721%	12.1992%	11.0932%	6.5333%	En la Entidad	2,496	2,195	1,996	1,175	En el Extranjero	0	0	0	0	<p>Texto "En la Entidad" incompleto</p>
Porcentaje	18.8721%	12.1992%	11.0932%	6.5333%													
En la Entidad	2,496	2,195	1,996	1,175													
En el Extranjero	0	0	0	0													
<p>15:38</p>	<p>Aún se tiene acceso desde una url al directorio FILES que es donde se almacenan las imágenes de las actas.</p>																
<p>20:35</p>	<p>Total de actas digitalizadas: 10904          Total de actas publicadas: 4205          Total de actas con inconsistencias: 1034</p>																

## 5.2. REVISIÓN DE SEGURIDAD DEL PUBLICADOR DE RESULTADOS DEL CEEPAC 2021.

### ATAQUES DDoS

Los ataques de denegación de servicio intentan comprometer la continuidad del servicio, reduciendo la disponibilidad para dar respuesta a peticiones o solicitudes legítimas. De estos



ataques sobresalen dos tipos:

## VOLUMÉTRICOS

Los ataques volumétricos simplemente intentan inundar de peticiones o solicitudes el equipo servidor, el software o los canales de comunicación. La resiliencia a este tipo de ataques depende principalmente del ancho de banda del proveedor de servicios. En este caso el proveedor de servicios Triara ofrece soluciones integrales con mecanismos básicos para soportar este tipo de ataques<sup>1</sup>.

El servidor de hardware utilizado tiene especificaciones para soportar alta demanda.

## ATAQUES LENTOS

Los ataques lentos aprovechan el diseño del protocolo de comunicaciones de alto nivel (HTTP) para intentar utilizar todas las conexiones disponibles del software servidor. Los ataques más conocidos y efectivos son slowloris y slowread. Slowloris envía solicitudes incompletas, alargando la vida de las mismas lo más posible. El ataque slowread, el cliente solicita la descarga de un archivo de tamaño considerable, avisando de un tamaño de ventana pequeño para el recibimiento de la información, alargando la vida de solicitudes y tratando de acapararlas todas. En servidores web apache con configuración por defecto, solo se pueden atender hasta 250 clientes simultáneos, lo que los hace vulnerables a este tipo de ataques. Otros servidores como nginx no sufren de esta limitante.

## RESULTADOS DE ATAQUES DDoS

Triara soporto los picos de solicitudes en ataques volumétricos, tal como lo describen en sus condiciones de servicio.

Fue posible afectar la velocidad y respuesta del servidor en ataques lentos durante las primeras pruebas, antes de la configuración del servicio Sucuri<sup>2</sup>, que es un filtro y protección contra ataques DDoS, protección de malware y otros ataques web. Además, Sucuri ofrece servicio de "Content Deliver Network" o CDN para replicar el contenido del sitio en diferentes lugares y disponible a manera de cache.

Una vez configurado el servicio de Sucuri, los ataques lentos dejaron de ser exitosos y al realizar otro tipo de ataques fueron bloqueados y el servicio se vió limitado a la dirección IP que originó los ataques.

En la Figura 1 se muestra la evidencia de que el sitio web de prepslp.mx está protegido por el servicio de firewall Sucuri.

---

<sup>1</sup> <https://triara.com/certificaciones>

<sup>2</sup> <https://sucuri.net/>



```
nslookup simulacro.prepslp.mx
Server:      192.168.100.1
Address:     192.168.100.1#53

Non-authoritative answer:
simulacro.prepslp.mx  canonical name = adb66e8f8c.10032.sucurifirewall.com.
Name:   adb66e8f8c.10032.sucurifirewall.com
Address: 192.124.249.32
```

Figura 1: Servicio Sucuri configurado

## ATAQUES AL SOFTWARE PUBLICADOR

El software que publica los resultados genera contenido dinámico que se obtiene de una base de datos. Al incluir entradas de usuario, esto da oportunidad de revisar posibles ataques de inyección de código. En la Figura 2 se muestran marcadas en rojo las entradas de usuario.

## ATAQUE A LA ENTRADA DE “RESULTADOS DE CASILLA”.

Uno es una entrada de texto, que la interface limita a solo 4 caracteres, pero no realiza una validación de que sean solo dígitos. Al introducir un valor erróneo, muestra un mensaje de “No se encontró información” como lo muestra la Figura 3. Si se introducen menos caracteres, muestra un aviso de que son necesarios 4 dígitos, como lo muestra la Figura 4.

Se puede introducir cualquier valor, y el símbolo “ ’ ” genera un error en el servidor al ser parte de sentencias SQL. En este caso no muestra ningún mensaje en la interface, pero en la consola del navegador avisa que ocurrió un error 500 en el servidor, esto quiere decir que no se pudo procesar la petición, abriendo posibilidades a una inyección de SQL. La Figura 5 muestra este error.

Pareciera que el problema no es mayor, ya que la interface solo permite 4 caracteres, pero se pueden inyectar otros valores directamente a la petición.

**Se solicita que se haga una limpieza de estas variables del lado del servidor y no solo que queden limitadas del lado del cliente.**

Se intentó con diversos ataques y cuando las sentencias SQL estaban bien construidas si marcaba error y redireccionaba a la página original.

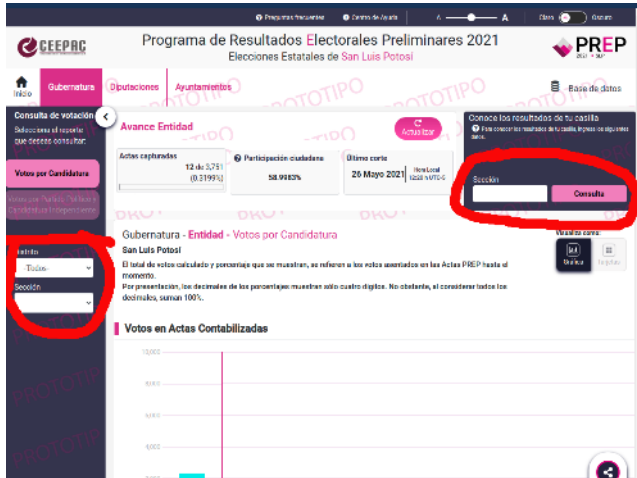


Figura 2: Portal de PREP, con entradas de usuario marcadas en rojo.

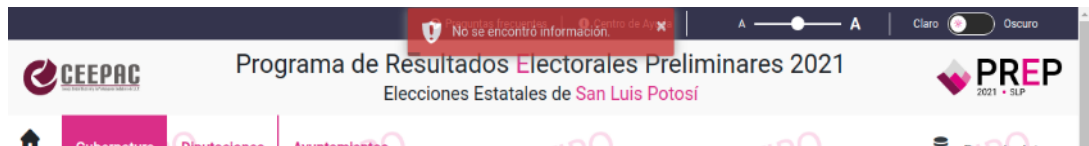


Figura 3: Mensaje de error al no existir información.

### ATAQUE A “DETALLES POR DISTRITO”.

En las diferentes pantallas, se tienen listas desplegables para seleccionar detalles, la cual activa una segunda lista desplegable y en algunos casos una tercer. Esto se realiza con una llamada tipo ajax en segundo plano.

Estos valores se modificaron usando un proxy para verificar las respuestas del servidor. En

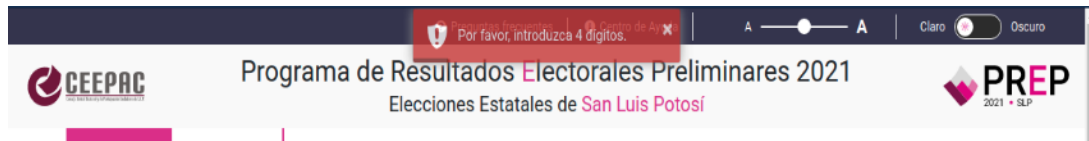


Figura 4: Error en número de dígitos:

algunos casos lo que se pudo lograr al modificar los parámetros es un error y nos manda a la página principal. Y en otros el servidor no devuelve valor alguno. Esto último se nota en dos casos:

1. Cuando el valor numérico del distrito se cambia por letras
2. Cuando se modifica o elimina alguno de los otros parámetros.

También cuando se intenta acceder por url directa, el servidor no regresa información.



Por ejemplo, la Figura 7 muestra error 500, y en la Figura 6 se muestra el contenido de esa url cuando se llega por el sistema; de la siguiente url.

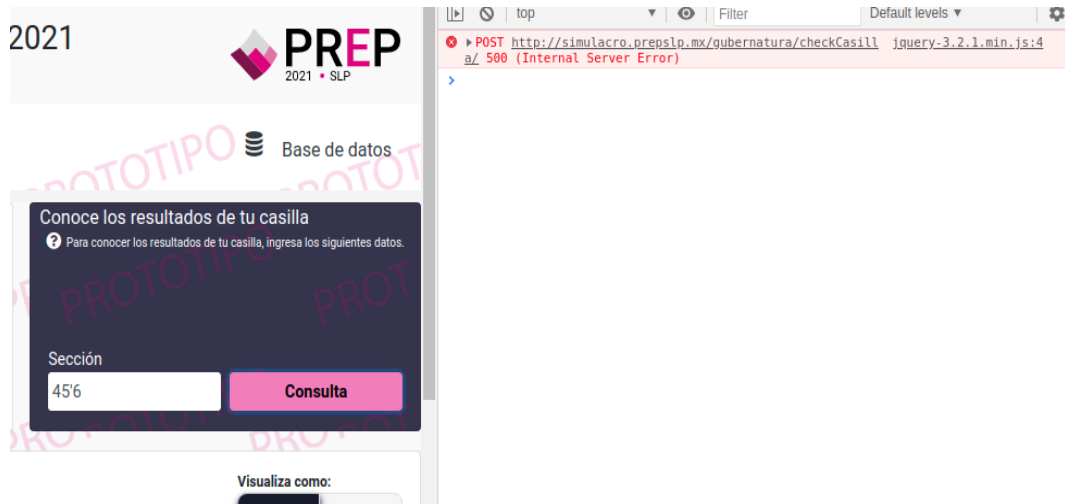


Figura 5: Error 500 al usar el carácter ' '



http://simulacro.prepslp.mx/gubernatura/distritoPpc/4

**Programa de Resultados**  
Elecciones Estadales

**CEEPAC**  
Censo Electoral y de Participación Ciudadana de S.L.P.

Inicio | **Gubernatura** | Diputaciones | Ayuntamientos

**Consulta de votación**  
Selecciona el reporte que deseas consultar:

- Votos por Candidatura
- Votos por Partido Político y Candidatura Independiente**
- Detalle por casilla

Detalle por:  
Distrito: 04.Salinas.  
Sección: SECCIÓN 0010

**Avance Entidad**

Actas capturadas	2,351 de 3,751 (62.6766%)	Participación ciudadana	66.0904%
------------------	------------------------------	-------------------------	----------

**Gubernatura - Detalle del Distrito - Votos por Partido Político y Candidatura**  
[San Luis Potosí](#) / Distrito 04. Salinas

El total de votos calculado y porcentaje que se muestran, se refieren a los votos asentados en las actas. Por presentación, los decimales de los porcentajes muestran sólo cuatro dígitos. No obstante, los cálculos se realizaron con mayor precisión.

**Votos en Actas Contabilizadas**

Partido	Votos	Porcentaje
PAN	5,253	8.8592%
PRD	5,447	9.1864%
PSD	5,200	9.1864%

Figura 6: Contenido de la URL



simulacro.prepslp.mx/gubernatura/distritoDpc/4



This page isn't working

simulacro.prepslp.mx is currently unable to handle this request.

HTTP ERROR 500

Reload

*Figura 7: Error 500 al tratar de acceder directamente a una url.*

### 5.3. RECOMENDACIONES.

En base a los errores presentados, nos permitimos hacer las siguientes recomendaciones:

1. Revisar y mejorar la logística en general.
2. Prever actividades para tiempos muertos.
3. La página del publicador aún presenta error al mostrarse en celulares y Tablet con una pantalla de 7 pulgadas o menores.
4. Aún hay detalles en las cifras mostradas por el publicador. Se recomienda revisar exhaustivamente los lineamientos respecto al conteo en general.

## 6. CRONOLOGÍA DEL SIMULACRO LLEVADA A CABO EL 30 DE MAYO

En este simulacro se tuvo presencia en el CATD de Cerro de San Pedro, en el CATD de Ricardo B. y en el CCV ubicado en el centro de Centro de Convenciones de San Luis Potosí.

Se tenía planeado iniciar el simulacro a las 10:00 Hrs.



### 6.1. CRONOLOGÍA DE SUCESOS EN EL CCV UBICADO EN EL CENTRO DE CENTRO DE CONVENCIONES DE SAN LUIS POTOSÍ.

Hora	Evento
10:15	Se da inicio el simulacro. Hay 100 capturistas. Se pretende digitalizar un total de 11251 actas y finalizar a las 22:15 Hrs.
11:15	primera digitalización.
11:30	Ya no hay retardo en la aplicación de captura.
11:35	entra primera publicación.
11:38	Se descargan los csv del publicador, se observa que está mal la fecha dentro del archivo csv.
11:40	Al dar guardar en aplicativo de capturistas a veces se queda "Freeze" y hay que volver a dar refrescar, se resolvió en 10 minutos el problema de conexión entre el servidor, Al menos durante 15 segundos se pierde la conexión.
12:00	Se incrementa la potencia del servidor de bases de datos y se soluciona el problema anterior.
12:45	Total de capturistas:100 Total de actas digitalizadas: 7027 Total de actas publicadas: 2004 Total de actas con inconsistencias: 642
14:00	San Francisco, Armadillo y Xilitla no hay internet por qué CFE hizo corte por mantenimiento, van a llevar planta de luz por parte de CIATEC, de no resolverse los llevarán al municipio Axtla de Terrazas.
17:20	El equipo de desarrollo prueba una mejora en la asignación de actas a los capturistas.  Se presenta un problema con la base de datos, reiniciaron sus aplicativos y volvieron a sus estaciones de trabajo, a partir de ese momento hubo problemas con la carga del número de actas por capturar.
18:30	Todos los capturistas han tenido problema, muchos de ellos están si poder capturar.  Se suspende temporalmente la captura y se les permite un descanso a los capturistas.
19:01	Ya no se actualizaron los archivos csv.
21:00	Se reasignan manualmente la carga de trabajo. Se inicia nuevamente la captura, aunque a un ritmo más lento.
22:10	Se retiran la mayoría de los capturistas. Se quedaron aproximadamente 20.
03:00	Se finalizó el proceso de digitalización con los siguientes números: Actas transmitidas: 11251, Actas legibles: 10580, Actas ilegibles: 671 Actas a verificación: 1850

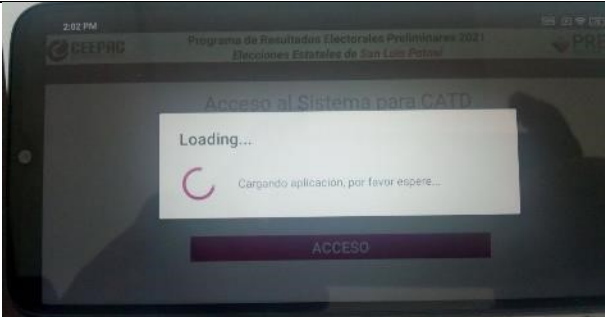


## 6.2. CRONOLOGÍA DE SUCESOS EN EL CATD DE CERRO DE SAN PEDRO.

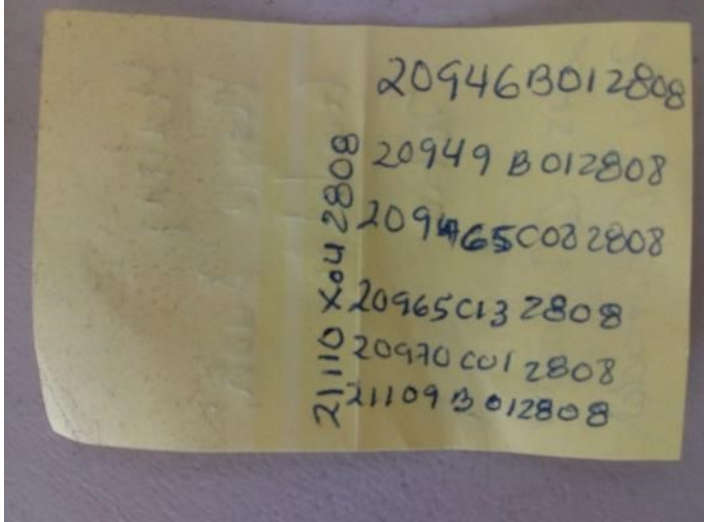
Hora	Evento
10:00	Se inicia el proceso de digitalización por parte de la digitalizadora Yadira López Mendoza.  Se tuvo un incidente con la conexión wifi pero se solucionó reiniciando el router no aparecía el ssid.
10:15	No se tuvieron problemas con la conexión vpn y el sistema funcionó de forma adecuada desde el inicio, hubo un momento que se bajó la velocidad de la conexión y al digitalizar una de las actas se observó un error de subida del archivo y en el tercer intento marcó que el acta ya estaba digitalizada.
12:00	Se finalizó el proceso de digitalización con los siguientes números: Actas transmitidas: 30, Actas legibles: 29, Actas ilegibles: 1

## 6.3. CRONOLOGÍA DE SUCESOS EN EL CATD UBICADO EN AV. RICARDO B ANAYA.

Hora	Evento
10:00	Se reciben las actas a digitalizar. Personal: CATD digitalizadora, Perla Lucero Ortiz Guevara, móvil Xiaomi Redmi 9A CATD digitalizadora, Imelda Zarazúa Cortes, Tablet Lenovo Yoga Tab 3 Presidente, Jayro Morales Bernal
10:05	La conexión wifi y el modem ya se encontraba configurado listo para iniciar la conexión.  La conexión vpn no presento ningún problema hasta que se tuvo que reiniciar el modem y un teléfono demoro un tiempo en conectarse nuevamente a la vpn.

10:18	<p>Se inician las actividades. Se verifica la velocidad de la conexión:</p> <table border="1"> <thead> <tr> <th># ping</th> <th>PING ms</th> <th>Descarga Mbps</th> <th>Carga Mbps</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>16</td> <td>23.02</td> <td>4.44</td> </tr> <tr> <td>2</td> <td>16</td> <td>29.30</td> <td>4.35</td> </tr> <tr> <td>3</td> <td>16</td> <td>23.71</td> <td>4.5</td> </tr> <tr> <td>4</td> <td>16</td> <td>20.57</td> <td>4.12</td> </tr> <tr> <td>5</td> <td>16</td> <td>29.42</td> <td>4.55</td> </tr> <tr> <td colspan="2"><b>Promedio</b></td> <td>25.20</td> <td>4.39</td> </tr> </tbody> </table>	# ping	PING ms	Descarga Mbps	Carga Mbps	1	16	23.02	4.44	2	16	29.30	4.35	3	16	23.71	4.5	4	16	20.57	4.12	5	16	29.42	4.55	<b>Promedio</b>		25.20	4.39
# ping	PING ms	Descarga Mbps	Carga Mbps																										
1	16	23.02	4.44																										
2	16	29.30	4.35																										
3	16	23.71	4.5																										
4	16	20.57	4.12																										
5	16	29.42	4.55																										
<b>Promedio</b>		25.20	4.39																										
10:20	Se inicia la digitalización con ambas digitalizadoras. Justo cuando recibieron el banderazo de inicio, las actas a digitalizar son las mismas del simulacro anterior 246 de diputaciones y 246 de gobernatura.																												
13:15	El tiempo de envío de actas digitalizadas tarda 90 segundos en enviar un acta; por ello se optó por reiniciar el modem y los dispositivos. Esta muy baja la velocidad de subida, en promedio la bajada es de 25 Mb y 4.5 Mb de subida.																												
14:00	 <p>El servidor no responde.</p>																												
15:30	<p>Surgió un pequeño inconveniente cuando un tercer digitalizador intento conectarse.</p> <p>Al parecer existió una interferencia entre un digitalizador y uno ya conectado. En este caso la interferencia fue con el digitalizador que tenía móvil.</p> <p>Se solucionó cuando el tercer digitalizador ya no intento conectarse. Al finalizar se redigitalizaron solamente 2 actas.</p>																												



16:59	<p>Se reportan los números de actas que faltaron de entregar físicamente:</p> 
18:00	<p>Se finalizó el proceso de digitalización con los siguientes números: Actas transmitidas: 122, Actas legibles: 121, Actas ilegibles: 1 en blanco</p>

#### 6.4. RECOMENDACIONES.

En base a los errores presentados, nos permitimos hacer las siguientes recomendaciones:

1. Parece que no están manejando un sistema de control de versiones en el desarrollo del código, ni una política de ramas de desarrollo y producción. Por lo cual, al realizar modificaciones en la versión de producción se pueden causar errores que comprometen gravemente la operación del sistema, y es muy complicado retomar la versión estable en corto tiempo.
2. Tener una política de respaldos de las bases de datos.

### 7. CRONOLOGÍA DEL SIMULACRO LLEVADA A CABO EL 03 DE JUNIO

En este simulacro se tuvo presencia en el CATD de Cerro de San Pedro, en el CATD de Ricardo B. y en el CCV ubicado en el centro de Centro de Convenciones de San Luis Potosí.

Se tenía planeado iniciar el simulacro a las 10:00 Hrs.



## 7.1. CRONOLOGÍA DE SUCESOS EN EL CCV UBICADO EN EL CENTRO DE CENTRO DE CONVENCIONES DE SAN LUIS POTOSÍ.

Hora	Evento
10:15	Se da inicio el simulacro. Hay 95 capturistas. Se pretende digitalizar un total de 4500 actas y finalizar a las 18:00 Hrs.  Se informa que las actas no contarán con código de barras, por lo cual se instruye a los digitalizadores a que lo usen.
14:18	Total de capturistas: 95 Total de actas digitalizadas: 2058 Total de actas publicadas: 1613 Total de actas con inconsistencias: 564  Se observa un considerable aumento en el tiempo de digitalización, lo cual es atribuible a la falta de código de barras.
17:00	Total de actas digitalizadas: 3559 Total de actas publicadas: 3330 Total de actas con inconsistencias: 952
18:00	Se finalizó el proceso de digitalización con los siguientes números: Actas transmitidas: 30, Actas legibles:29, Actas ilegibles: 1 No hubo incidentes

## 7.2. CRONOLOGÍA DE SUCESOS EN EL CATD DE CERRO DE SAN PEDRO.

Hora	Evento												
10:50	Personal y hora de llegada: 10:50 CATD digitalizador, José Alonso López  Equipos donde se lleva a cabo la digitalización: Tablet Lenovo Yoga Tab 3 ¿Cuenta con base? No												
10:50	Se inician las actividades:  Estado de la conexión wi-fi:  Estadísticas de velocidad.												
	<table border="1"> <thead> <tr> <th># ping</th> <th>PING ms</th> <th>Descarga Mbps</th> <th>Carga Mbps</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>12</td> <td>18</td> <td>4</td> </tr> <tr> <td>2</td> <td>12</td> <td>19</td> <td>4</td> </tr> </tbody> </table>	# ping	PING ms	Descarga Mbps	Carga Mbps	1	12	18	4	2	12	19	4
# ping	PING ms	Descarga Mbps	Carga Mbps										
1	12	18	4										
2	12	19	4										



	3	12	18	3
	4	12	18	3
	5	12	19	4
	<b>Promedio</b>		18.4	3.6
	La VPN no presentó ningún problema.			
10:50	Las actas ya las traía José Alonso (30 actas)			
10:50	Se inicia la digitalización			
12:14	Finaliza digitalización. No hubo incidentes			
17:00	Se finalizó el proceso de digitalización con los siguientes números: Actas transmitidas: 30, Actas legibles:29, Actas ilegibles: 1			

### 7.3. CRONOLOGÍA DE SUCESOS EN EL CATD UBICADO EN AV. RICARDO B ANAYA.

Hora	Evento																				
7:30	<p>Personal y hora de llegada: 10:18 CATD digitalizadores de Rioverde (Diana González Hernández y Silvestre Torres Briceño) 08:40 Auxiliar A y B (Daniela Alejandra Medina) 07:30 Apertura del distrito 08 07:50 Secretaria técnica (Astrid) 07:30 Presidente, Jayro Morales Bernal</p> <p>Equipos donde se lleva a cabo la digitalización: 1 Tablet (Imelda catd asignada a comisión 08) ¿Cuenta con base? No 1 Celular (Perla catd asignada a comisión 08)</p>																				
10:00	<p>Se inician las actividades:</p> <p>Estado de la conexión wi-fi:</p> <p>Estadísticas de velocidad.</p> <table border="1"> <thead> <tr> <th># ping</th> <th>PING ms</th> <th>Descarga Mbps</th> <th>Carga Mbps</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>16</td> <td>26,02</td> <td>4.98</td> </tr> <tr> <td>2</td> <td>16</td> <td>28,10</td> <td>5.3</td> </tr> <tr> <td>3</td> <td>16</td> <td>20,42</td> <td>5,5</td> </tr> <tr> <td>4</td> <td>16</td> <td>20,57</td> <td>4,91</td> </tr> </tbody> </table>	# ping	PING ms	Descarga Mbps	Carga Mbps	1	16	26,02	4.98	2	16	28,10	5.3	3	16	20,42	5,5	4	16	20,57	4,91
# ping	PING ms	Descarga Mbps	Carga Mbps																		
1	16	26,02	4.98																		
2	16	28,10	5.3																		
3	16	20,42	5,5																		
4	16	20,57	4,91																		



	<table border="1"> <tr> <td>5</td> <td>16</td> <td>25,76</td> <td>5.10</td> </tr> <tr> <td colspan="2"><b>Promedio</b></td> <td>24,17</td> <td>5,21</td> </tr> </table>	5	16	25,76	5.10	<b>Promedio</b>		24,17	5,21
5	16	25,76	5.10						
<b>Promedio</b>		24,17	5,21						
	La VPN no presentó ningún problema.								
11:00	Se reciben las actas a digitalizar (los digitalizadores de la comisión 08 no se presentaron por cuestiones laborales en su lugar fueron sustituidos por unos digitalizadores temporales de rio verde las actas a digitalizar se desconocía aproximadamente fueron 300 gobernatura y 300 diputaciones)								
11:10	Se inicia la digitalización.								
12:15	Se cronometraron varias digitalizaciones y en promedio se demora un minuto 30 segundos aproximadamente por acta a digitalizar								
12:40	Los incidentes fueron que se inició una hora después la capacitación a los nuevos digitalizadores, los digitalizadores tradicionales no tuvieron inconvenientes, pero porque estaban usando digitalización automática, en cuanto a la capacitación, se sigue teniendo el problema de los filtros de la app siguen sin funcionar correctamente, los digitalizadores pueden ver actas de otros digitalizadores y algunas que les pertenecen no las tenían asignadas aún. Al parecer existirá una nueva estrategia de asignarle de 4 a n actas a los nuevos digitalizadores los cuales se hará con un equipo celular con la vpn ya configurada con datos móviles.								
17:00	Se finalizó el proceso de digitalización con los siguientes números: Actas transmitidas: aprox. 600, Actas legibles aprox. 600								

#### 7.4. RECOMENDACIONES.

En base a los errores presentados, nos permitimos hacer las siguientes recomendaciones:

1. Documentar el proceso a seguir en caso que se tenga que usar los servidores ubicados en las instalaciones de CIATEC.
2. LA arquitectura del sistema debe considerar una reingeniería para hacer más parametrizable y configurable, para que se adapte a los datos de las elecciones y fechas sin necesidad de hacer ajustes en el código fuente.
3. Contar con manuales de usuarios de los sistemas y asegurarse que los usuarios tengan acceso a estos.



## 8. PROCEDIMIENTO TÉCNICO CON ESQUEMA DE VALIDACIÓN DE LA BASE DE DATOS DEL SISTEMA INFORMÁTICO PREP

### 8.1. INICIALIZAR LA BASE DE DATOS

Un miembro del ente auditor dirige las instrucciones a ejecutar, en colaboración con un integrante del equipo de desarrollo del PREP, para establecer que el estado inicial de la base de datos. Las siguientes sentencias inicializan la base de datos con cero registros en las tablas especificadas:

```
set foreign_key_checks = 0;  
truncate from tbl_acta_prep_situacion;  
truncate from tbl_resultados_actas;  
truncate from tbl_acta_usuario;  
truncate from tbl_acta_prep;  
truncate from cat_asignacion_catd where captura != 'D'
```

El resultado de la ejecución de las instrucciones anteriores es que la Base de Datos queda en su estado inicial previo a el arranque del PREP.

Para poder conocer las relaciones que componen la base de datos del PREP y su cantidad de registros que contiene cada una de ellas en esta etapa, se ejecuta la siguiente sentencia:

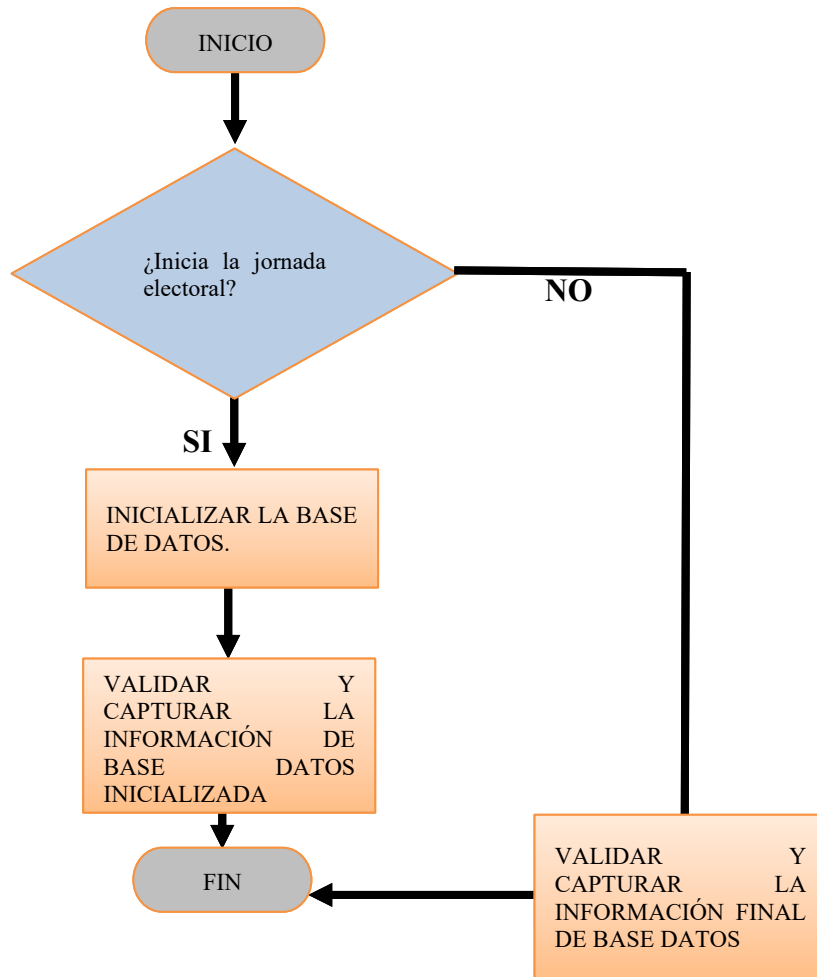
```
Select table_schema, table_name, table_rows, create_time, update_time  
from information_schema.TABLES where TABLE_SCHEMA= 'votos';
```

### 8.2. VALIDAR INFORMACIÓN FINAL DE LA BASE DE DATOS

Para poder conocer las relaciones que componen la base de datos del PREP y su cantidad de registros que contiene cada una de ellas en esta etapa, se ejecuta la siguiente sentencia:

```
Select table_schema, table_name, table_rows, create_time, update_time  
from information_schema.TABLES where TABLE_SCHEMA= 'votos';
```

NOTA: Al cabo de la jornada electoral, solo se ejecutará la sentencia que muestra la estructura de contenido de la base de datos del PREP y se guardará la información de su contenido final.





## 9. INFORME DE PRUEBAS DE PENETRACIÓN A LA INFRAESTRUCTURA TECNOLÓGICA.

### RESUMEN EJECUTIVO

Actualmente los sistemas expuestos en Internet sufren de ataques constantes, de manera automática o por atacantes que eligen como objetivo específico nuestros sistemas. En el caso de sistemas con la importancia del PREP, es indispensable realizar pruebas de seguridad para asegurarnos de su continuidad ante diferentes tipos de ataques. Una prueba ampliamente utilizada es el pentest o pruebas de penetración. Al ejecutar un pentest, se prueba de manera práctica que los sistemas no pueden ser vulnerados. Se realiza un ejercicio adversarial, donde se utilizarán herramientas y pruebas manuales para verificar la seguridad de los sistemas, basados en la metodología PTES (penetration testing execution standard) y las 10 vulnerabilidades más comunes según OWASP (OWASP Top 10).

La arquitectura de redes y seguridad desplegada por el ente desarrollador cumple los estándares y requisitos para proporcionar un nivel de seguridad alto. Los descubrimientos son menores y no tienen impacto una vez que fueron configuradas las reglas de protección del servicio de seguridad contratado.

Al ejecutar estas pruebas, se pudo comprobar que el sistema de protección que están usando (Sucuri) cumple con los requisitos de seguridad para protegerlos de ataques externos. Y las configuraciones y diseños permiten mantener la seguridad en contra de ataques internos.

### 9.1. ALCANCE

El pentest de la infraestructura tecnológica deberá realizarse con base en las etapas que se describen a continuación, adaptando la metodología PTES.

1. Obtención de información: conocer el sistema y la infraestructura, escaneo de puertos y aplicaciones. Se llena la CDM junto con el ente desarrollador.
2. Modelado de amenazas: llenar la TaSM y se valida con el ente desarrollador.
3. Análisis de vulnerabilidades: Probar las vulnerabilidades más comunes según OWASP.
4. Explotación: Usar herramientas y pruebas manuales para ganar acceso.
5. Post Explotación: medir hasta dónde se puede comprometer el sistema.
6. Reporte: Entregar hallazgos.

Las pruebas de penetración se deberán llevar a cabo tanto desde el interior como desde el exterior de la red de datos a examinar y deberán enfocarse en:



- 7. Dispositivos
- 8. Aplicaciones
- 9. Redes
- 10. Datos
- 11. Usuarios

## 9.2. OBTENCIÓN DE INFORMACIÓN

Conocer el sistema y la infraestructura, escaneo de puertos y aplicaciones. Se llena la CDM junto con el ente desarrollador.

### CDM

	<b>Identificar</b>	<b>Proteger</b>	<b>Detectar</b>	<b>Responder</b>	<b>Recuperar</b>
Dispositivos	Firewalls, servidores, switches, dispositivos móviles, terminales	Acceso	Fallos, intrusiones		
Aplicaciones	Base de datos, Captura, digitalización, Publicador	Acceso	Fallos, intrusiones, malas configuraciones		
Redes	Red interna a través de la VPN, red pública	Acceso	Fallos, intrusiones		
Datos	Actas, base de datos	Acceso, Robo	Fallos y anomalías		
Usuarios	Administrador, capturistas, digitalizadores, vpns	Credenciales	Credenciales comprometidas		

Las VPNs se utilizan con dispositivos ASA de CISCO y firewall de Palo Alto Networks. Los servidores están actualizados usando la versión estable y de soporte extendido de CentOS. Los clientes utilizan acceso a la VPN usando usuario y contraseña, además de una clave compartida y un identificador, robusteciendo el acceso. El cliente solo puede ver al servidor y no otros clientes conectados.



### 9.3. MODELADO DE AMENAZAS:

Llenar la TaSM y se valida con el ente desarrollador.

#### TASM

Amenazas	Identificar	Proteger	Detectar	Responder	Recuperar
Acceso ilegal usando ataques de fuerza bruta	Accesos, credenciales comprometidas	Credenciales, datos	Ataques fuerza bruta	Bloquear IP	
Alteración de información en publicador	Accesos ilegales, exploits	Software y código	Ataques	Bloquear IP	
Acceso a BD	Equipos intentando acceder a base de datos	Base de datos, credenciales	Accesos a BD	Bloquear IP, identificar usuario y equipo	
Ataques DoS y DDoS	Ataques de denegación de servicio	Sistema publicador	Ataques DoS	Bloquear IPs	
Ataques AIDoS	Solicitudes anómalas	Sistema publicador	Ataques slow read y slow write	Bloquear IPs	

Las amenazas principales se identificaron y se usaron para desarrollar el plan de ataque.

### 9.4. ANÁLISIS DE VULNERABILIDADES A LAS APLICACIONES:

Probar las 10 vulnerabilidades más comunes según OWASP.

1. Inyecciones. El sistema soportó inyecciones de SQL y de código. Se revisó desde la programación y el sistema publicador.
2. Autenticación rota. El sistema muestra resistencia al autenticar usuarios.
3. Exposición de datos sensibles. No se encontró.
4. Entidades externas XML(XXE). No se encontró.



5. Control de acceso roto. Se identificó un defecto leve cuando un administrador cierra sesión, otro usuario puede tener acceso a páginas administrativas por URL. Se corrigió el sistema.
6. Malas configuraciones de seguridad. No se detectaron, y el uso de sucuri redujo las superficies de ataque para esto.
7. Cross site scripting (XSS). No se encontró. El uso de sucuri redujo las superficies de ataque para esto.
8. Deserialización insegura. No se encontró.
9. Uso de componentes con vulnerabilidades conocidas. No se encontró.
10. Insuficiente registro y monitoreo. No se encontró.

## 9.5. ANÁLISIS DE VULNERABILIDADES A LOS DISPOSITIVOS DE RED:

Los dispositivos no son accesibles desde el exterior, y tampoco son accesibles desde la VPN, además, según las versiones de software reportadas, no existen vulnerabilidades públicas para ellos. Por lo que no encontramos vulnerabilidades en los dispositivos.

### EXPLOTACIÓN:

Usar herramientas y pruebas manuales para ganar acceso.

No se encontraron vulnerabilidades que explotar. Cabe mencionar que esto no significa que no existan, pero la posibilidad de encontrarlas es baja.

### POST EXPLOTACIÓN:

Medir hasta dónde se puede comprometer el sistema.

No se encontraron vulnerabilidades que explotar. Cabe mencionar que esto no significa que no existan, pero la posibilidad de encontrarlas es baja.

### REPORTE:

Entregar hallazgos.

Se reportaron los pocos hallazgos al ente desarrollador para su corrección, y fueron corregidos.

## 9.6. RESULTADOS DE LA VERIFICACIÓN

Los resultados obtenidos de esta revisión concluyen que los sistemas de software no tienen vulnerabilidades graves. Y para los equipos de comunicaciones reportados no se localizaron vulnerabilidades que afecten el funcionamiento.

Se realizaron diferentes pruebas durante los simulacros y fuera de los simulacros, resultando la prueba final aceptable en términos de seguridad, y la contratación del servicio de sucuri permite reducir las superficies de ataque al bloquear accesos sospechosos o contenido manipulado.



La revisión de los planes de respaldo y actualización no fueron entregados.

## 10. INFORME DE PRUEBAS DE DENEGACIÓN DE SERVICIO A LA INFRAESTRUCTURA TECNOLÓGICA.

### RESUMEN EJECUTIVO

Actualmente los sistemas expuestos en Internet sufren de ataques constantes, de manera automática o por atacantes que eligen como objetivo específico nuestros sistemas. En el caso de sistemas con la importancia del PREP, es indispensable realizar pruebas de seguridad para asegurarnos de su continuidad ante diferentes tipos de ataques, especialmente los ataques de denegación de servicios o bien los altos flujos de visitas que pueda tener el sistema.

El proveedor de infraestructura en sitio Triara tiene definidas las especificaciones de conectividad de manera aceptable, para poder recibir gran flujo de solicitudes. Sin embargo, el servidor (hardware y software) utilizado puede ser susceptible a ataques de solicitudes lentas. Lo cual fue confirmado en el simulacro de mediados de mayo antes de que se configurara el servicio de protección de Sucuri. En el siguiente simulacro Sucuri fue efectivo en detectar, detener y descartar el tráfico de red generado durante los ataques de denegación de servicio y denegación de servicio a nivel de aplicación o ataques de solicitudes lentas.

La configuración actual del sistema de seguridad, proveedor de infraestructura y hardware-software es suficiente para atender las solicitudes a el software publicador, y la carga de trabajo del resto de los sistemas.

### 10.1. ALCANCE

Se revisa la respuesta del sistema publicador a diferentes ataques de denegación de servicio, el firewall de Palo Alto Networks para aceptar los clientes de la VPN y la configuración de la base de datos para atender las solicitudes.

Los ataques realizados al sistema publicador, que es el que está expuesto a Internet, fueron volumétricos y ataques a la capa de aplicación o ataques lentos, por ejemplo: Slow-headers o slowloris, slow-read al descargar archivos de información del sistema.

### 10.2. RESULTADOS DE LA VERIFICACIÓN

1. La verificación del soporte para clientes de VPN fue exitosa, la configuración del sistema Palo Alto Networks está ajustada para recibir mil clientes, y no ha habido problemas directos con el acceso a través de VPN al sistema de digitalización de actas.



2. La configuración de la base de datos está ajustada para atender 1000 clientes, y que no pierda conexiones desde ninguno de los sistemas.
3. El sistema publicador es el único que está expuesto a Internet. Se ejecutan ataques volumétricos, que no afectan el funcionamiento, gracias a las especificaciones del proveedor de infraestructura. En un primer ataque en la capa de aplicación, o ataque lento al publicador, antes de usar Sucuri, fue exitoso, al afectar el rendimiento del sistema. Los detalles técnicos están en el apéndice. Una vez configurado el sistema de protección Sucuri, todos los ataques que generaron algún impacto anteriormente fueron bloqueados por el sistema.

## **ATENTAMENTE**

*Excelencia en Educación Tecnológica®  
Con tecnología y espíritu una patria forjaré®*

**Ing. Pedro García Guerrero**  
**Líder del proyecto por parte del Ente Auditor**

ccp. Archivo