Instituto Tecnológico de Durango
Departamento de Sistemas y Computación

INFORME DE AUDITORÍA AL SISTEMA INFORMÁTICO Y A LA INFRAESTRUCTURA TECNOLÓGICA DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES DEL INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DEL ESTADO DE DURANGO

INFORME FINAL

15 de junio de 2021

Av. Felipe Pescador 1830 Ote. Col. Nueva Vizcaya,
C.P. 34080, Durango, Dgo. Tel. (618) 8-29-09-00
email: dir_itdurango@tecnm.mx
tecnm.mx | itdurango.edu.mx

INFORME FINAL

El presente informe cubre lo realizado desde las pruebas de funcionalidad del sistema PREP hasta la generación y validación de Hashes al término de la jornada electoral.

PRUEBAS DE FUNCIONALIDAD DEL SISTEMA PREP DURANGO

El día 19 de abril de 2021 siendo las 10:00 horas, nos reunimos en el edificio designado para el Centro de Captura y Verificación (CCV) del PREP Durango, ubicado en la calle ubicado en calle Circuito Itrio número 109, Colonia Ciudad Industrial, con el propósito de realizar la ejecución de la prueba para verificar el correcto funcionamiento del sistema informático del PREP, que será utilizado para el proceso de elección del PREP IEPC Durango 2021.

Contándose con la presencia de:

- El consejero presidente del IEPC
- La secretaria técnica del IEPC
- Consejeros del IEPC
- La unidad técnica de cómputo
- Asesores técnicos del COTAPREP
- Ente auditor
- La empresa Informática Electoral

Se realizaron las pruebas de funcionalidad establecidos en el diseño del Proceso Técnico Operativo (PTO) aprobado:

1. Digitalización desde la casilla
2. Digitalización
3. Captura
4. Verificación
5. Publicación

La reunión inició puntualmente y la empresa Informática Electoral mostró el plan de pruebas de funcionalidad que se llevaría a cabo (figura 1).

Tomando como base este programa de acción se realizó el análisis de cada una de ellas y se procedió al llenado de la matriz de actas (tabla 1), resultado de las pruebas funcionales.

PREP 2021 • DGO

IEPC DURANGO

Cronograma para presentación de flujos

N°	Acta	Origen	N° de flujo	Flujo	Dtto / Sección / Casilla
1	1	PREP casilla	1	Flujo normal PREP Casilla (1 y 2 captura)	III / 0182 / C1
2	2	CATD celular	2	Flujo normal CATD Celular (1 y 2 captura)	VIII / 0065 / BA
3	3	Escáner	3	Flujo normal escáner (1 y 2 captura)	VI / 0030 / BA
4	4	Escáner	8	Incidencia todo ilegible capturista 1 y 2	XIV / 0084 / BA
5	5	Escáner	7	Incidencia todos sin datos capturista 1 y 2	III / 0182 / BA
6	6	PREP casilla	9	Incidencia dato ilegible capturista 1 y 2	VI / 0029 / BA
7	7	PREP casilla	10	Incidencia algún sin dato capturista 1 y 2	II / 0148 / BA
8	8	Escáner	4 24	Flujo normal escáner (1, 2, y 3 captura) Acta excede lista nominal	VIII / 0064 / BA
9	9	Escáner	6 23	Incidencia módulo de identificación de AEC Acta fuera de catálogo	ILEGIBLE PARA IDENTIFICAR
10	1	Escáner	26 11	Acta ya fue digitalizada Acta duplicada identificada en MVEVAL	III / 0182 / C1
11	-	-	25	Reinicio de base de datos	---
12	1	PREP casilla	16	Rechazo de acta PREP casilla	III / 0182 / C1
13	2	CATD celular	17	Rechazo de acta CATD celular	VIII / 0065 / BA
14	3	Escáner	18	Rechazo de acta escáner	VI / 0030 / BA
15	3	Escáner	5	Flujo normal escáner (1, 2, 3 y 4 captura)	VI / 0030 / BA
16	1	PREP casilla	14	Error en captura de votos 1, 2, 3 y 4 captura	III / 0182 / C1
17	2	CATD celular	13	Error en captura de votos 1, 2, 3 y 4 captura en coordinación	VIII / 0065 / BA

Figura 1. Plan de pruebas

Se encontró que el Sistema PREP cumple con los requerimientos funcionales que establece el IEPC para atender el proceso electoral 2021, indicando que en el sistema final se mostrara la iconografía oficial de partidos políticos y candidatos de acuerdo con lo que indique en su momento el IEPC.
Hasta ese momento, con base en las pruebas de funcionalidad, el sistema de información PREP tiene un desempeño estable y de acuerdo con lo establecido por el IEPC - INE.

Tipo de Elección	No. de Prueba	Tipo Acta PREP			Origen			Supuesto de inconsistencia							Supuestos de Captura/Verificación					
		AEC	AR	ACEF	Escaner	PREP Casilla	CATD Celular	Todos ilegibles	Todos sin dato	Algún ilegible	Algún sin dato	Excede LN	Fuera de catálogo	Sin inconsistencia	C1 = C2	C1 / C2	C1 o C2 = C3	C1 o C2 / C3	Resolución	Observación
Diputaciones	1	X				X								X	X					
	2	X					X							X	X					
	3	X			X									X	X					
	4	X			X			X							X				X	
	5	X			X				X						X					
	6	X				X				X					X					
	7	X				X					X				X					
	8	X			X							X			X				X	
	9 - NA	X			X								X						X	
	10	X			X															Se rechaza acta
	11	X					X													Se rechaza acta
	12	X				X														Se rechaza acta
	13	X					X													Se rechaza acta
	14	X			X															Se rechaza acta
	15	X			X													X		Se llega hasta el 4to capturista
	16	X				X												X		Se llega hasta el 4to capturista
	17	X					X											X		Se llega hasta el 4to capturista

Tabla 1. Matriz de actas llenada durante el proceso de pruebas funcionales

VISITA A CCV-DGO Y CATD-DGO

El día 26 de abril de 2021 siendo las 13:00 horas, nos reunimos en el edificio designado para el Centro de Captura y Verificación (CCV) del PREP Durango, ubicado en la calle ubicado en calle Circuito Itrio número 109, Colonia Ciudad Industrial, con el propósito de realizar la ejecución de las visitas para verificar el estado de los CCV-DGO y CATD DGO, que serán utilizados para el proceso de elección del PREP IEPC Durango 2021.

Se realizaron pruebas funcionales de caja negra y análisis de vulnerabilidades y seguridad de la infraestructura tecnológica.

La visita inició puntualmente y la empresa Informática Electoral recibió al equipo auditor.

Con base en los resultados obtenidos, plasmados en los anexos al presente documento, se emitieron las siguientes observaciones y recomendaciones.

VISITA A CCV-DGO.

Con relación a la auditoría de infraestructura**:**

- Se indicó que no hay una salida de emergencia en el edificio. Sin embargo, la entrada principal es lo suficientemente amplia en caso de una posible evacuación.
- Los operadores del departamento de cómputo no han sido capacitados en caso de que ocurra una emergencia ocasionada por fuego o de otra índole.
    - Nota: Esto es debido a que se sigue contratando personal.
- En el caso de la seguridad de acceso y de instalaciones físicas, el edificio cuenta con alarma y personal de vigilancia.
    - Nota: Se recomendó verificar periódicamente si las cámaras de seguridad tienen puntos ciegos.
- No se ha instruido al personal del proceso de evacuación de las instalaciones en caso de emergencia o contingencia.
    - Nota: Esto es debido a que se sigue contratando personal.
- Se cuenta con sistema UPS, indicando que se encuentra en proceso la instalación plantas de energía auxiliar.

Con relación a la auditoría de red:

- Se realizó escaneo del cableado de red. Se encontró que el enlace del nodo 26 está dañado. Se recomienda sustituir el cable o en su defecto el conector.
- Se encontró el cableado estructurado de acuerdo con los estándares del mercado.
- En el armado del panel de patcheo, se recomienda numeración visible, clara y accesible de los puntos de red.
- De momento no se cuenta con una memoria técnica de direccionamiento IP estático.
- Con relación a los enlaces de internet, se cuenta con enlaces de Megacable, Telmex Infinitum, Metro Carrier e Internet Satelital.

Con relación a la auditoría de seguridad y pruebas de caja negra:

- Se encontraron conexiones activas de TeamViewer, dichas conexiones deben ser eliminadas y bloquear en el firewall generar toda conexión a aplicaciones de control remoto, las conexiones desaparecieron durante el análisis de paquetes, sin embargo, volvieron a aparecer momentos antes del término del análisis, para este punto se recomendó el chequeo y desinstalación de cualquier programa de comunicación en los equipos de captura.
- Los equipos de cómputo que se usan para captura no están vigilados con cámaras, y si bien se tiene una bitácora interna de uso en el sistema, ésta no abarca las acciones del sistema operativo (Windows) por lo que cualquier usuario puede insertar dispositivos de almacenamiento y esto es una brecha de seguridad latente, se recomienda que los dispositivos de almacenamiento externo sean deshabilitados en cada equipo o el uso de un servidor primario con Active Directory que controle la conexión de dispositivos basado en controles de usuario.
- La comunicación que existe entre los equipos de captura y el servidor se encuentra cifrada lo cual indica una protección extra en el envío/recepción de datos.
- Se recomendó eliminar el protocolo IPV6 para tratar de optimizar el ancho de banda, si bien los paquetes que se envían a través de dicho protocolo son solo de broadcast, el desactivar dicho protocolo implica un ahorro de ancho de banda.

- Se encontraron equipos activos (Router/Switch) que tienen habilitado el protocolo CDP mismo que debe ser desactivado para evitar la extracción de datos de los dispositivos vecinos.

    - En ciertos puntos del análisis se encontraron equipos que estaban haciendo un uso excesivo del ancho de banda, los equipos fueron identificados como cámaras de videovigilancia, se recomendó que el circuito cerrado se integre en una red alterna aislada de la red de trabajo de captura, esto con la finalidad de evitar cuellos de botella en la captura por cuestiones de ancho de banda.

VISITA A CATD-DGO.

Con relación a la auditoría de infraestructura:

- No existe una salida de emergencia en el edificio. Sin embargo, la entrada principal es lo suficientemente amplia en caso de una posible evacuación.
- Los operadores del departamento de cómputo no han sido capacitados en caso de que ocurra una emergencia ocasionada por fuego o de otra índole.
    - Nota: Esto es debido a que se sigue contratando personal.
- En el caso de la seguridad de acceso y de instalaciones físicas, el edificio cuenta con alarma y personal de vigilancia.
    - Nota: Se recomendó verificar periódicamente si las cámaras de seguridad tienen puntos ciegos.
- No se ha instruido al personal del proceso de evacuación de las instalaciones en caso de emergencia o contingencia.
    - Nota: Esto es debido a que se sigue contratando personal.
- Se cuenta con sistema UPS, indicando que se encuentra en proceso la instalación plantas de energía auxiliar.
- No se cuenta con ventilación adecuada para el personal y los equipos.

Con relación a la auditoría de red:

- El cableado no está estructurado de acuerdo con los estándares del mercado.
    - Nota: Es una instalación provisional de 6 nodos. Se recomienda encinchar los cables con cinta velcro.
- Se recomendó numeración visible, clara y accesible de los puntos de red.

- De momento no se cuenta con una memoria técnica de direccionamiento IP estático.
- Con relación a los enlaces de internet, se cuenta con enlaces de Megacable, Telmex Infinitum.

Con relación a la auditoría de seguridad y pruebas de caja negra:

- Se realiza un análisis de paquetes y escaneo global de la red sin arrojar peligros potenciales.
- No se pudo llevar a cabo el proceso de captura de información ya que no se contaba con actas físicas que sirvieran como ejercicio de práctica.
    - Se hace la observación para la siguiente visita que se tengan actas suficientes en cada punto que se audite.
    - Se pidió que el servidor en donde se realicen las pruebas sea el de producción para poder verificar la seguridad y funcionamiento de este, y no servidores locales o de prueba.

Se concluyó que los CCV-DGO y CATD-DGO son funcionales para atender el proceso electoral 2021.

VISITA A CATD-GOMEZ-LERDO-CUENCAME

El día 4 de mayo de 2021 siendo las 08:00 horas, nos reunimos en el edificio del IEPC Durango, ubicado en la Ciudad Industrial, con el propósito de realizar la ejecución de las visitas para verificar el estado de los y CATD-GOMEZ, CATD-LERDO Y CATD-CUENCAME, que serán utilizados para el proceso del PREP IEPC Durango 2021.

Se realizaron pruebas funcionales de caja negra y análisis de vulnerabilidades y seguridad de la infraestructura tecnológica.

La visita inició puntualmente y la empresa Informática Electoral recibió al equipo auditor.

Con base en los resultados obtenidos, plasmados en los anexos al presente documento, se emitieron las siguientes observaciones y recomendaciones.

VISITA A CATD-GOMEZ.

Con relación a la auditoría de infraestructura:

- Los operadores del departamento de cómputo no han sido capacitados en caso de que ocurra una emergencia ocasionada por fuego o de otra índole.
  - Nota: Esto es debido a que se sigue contratando personal.
- En el caso de la seguridad de acceso y de instalaciones físicas, el edificio no cuenta con personal de vigilancia.
  - Nota: Se recomendó contratar personal de seguridad.
- No se ha instruido al personal del proceso de evacuación de las instalaciones en caso de emergencia o contingencia.
  - Nota: Esto es debido a que se sigue contratando personal.
- Se cuenta con sistema UPS, indicando que se encuentra en proceso la instalación plantas de energía auxiliar.
- El panel eléctrico no está debidamente etiquetado.
  - Nota: Se recomendó etiquetar adecuadamente dicho panel, para identificar las zonas energizadas.

Con relación a la auditoría de red:

- El cableado no está estructurado de acuerdo con los estándares del mercado.
  - Nota: Se detectaron 2 nodos con cables deficientes. Se recomienda encinchar los cables con cinta velcro, y mantenerlos a una distancia prudente del suelo.
- Se recomendó numeración visible, clara y accesible de los puntos de red.
- De momento no se cuenta con una memoria técnica de direccionamiento IP estático.
- Con relación a los enlaces de internet, se cuenta con enlaces de Megacable, Telmex Infinitum.

VISITA A CATD-LERDO.

Con relación a la auditoría de infraestructura:

- Los operadores del departamento de cómputo no han sido capacitados en caso de que ocurra una emergencia ocasionada por fuego o de otra índole.
  - Nota: Esto es debido a que se sigue contratando personal.

- En el caso de la seguridad de acceso y de instalaciones físicas, el edificio no cuenta con personal de vigilancia.
    - Nota: Se recomendó contratar personal de seguridad.
- En el caso de la ventilación de las instalaciones físicas, el edificio no cuenta con un adecuado sistema de ventilación, y por el clima del lugar será necesario.
    - Nota: Se recomendó instalar un sistema adecuado de ventilación.
- No se ha instruido al personal del proceso de evacuación de las instalaciones en caso de emergencia o contingencia.
    - Nota: Esto es debido a que se sigue contratando personal.
- Se cuenta con sistema UPS, indicando que se encuentra en proceso la instalación plantas de energía auxiliar.
- El panel eléctrico no está debidamente etiquetado.
    - Nota: Se recomendó etiquetar adecuadamente dicho panel, para identificar las zonas energizadas.

Con relación a la auditoría de red:

- El cableado no está estructurado de acuerdo con los estándares del mercado.
    - Nota: Se detectó un nodo con cables deficientes. Se recomienda encinchar los cables con cinta velcro, y mantenerlos a una distancia prudente del suelo.
- Se recomienda numeración visible, clara y accesible de los puntos de red.
- De momento no se cuenta con una memoria técnica de direccionamiento IP estático.
- Con relación a los enlaces de internet, se cuenta con enlace de Megacable.

VISITA A CATD-CUENCAME.

Con relación a la auditoría de infraestructura:

- Los operadores del departamento de cómputo no han sido capacitados en caso de que ocurra una emergencia ocasionada por fuego o de otra índole.
    - Nota: Esto es debido a que se sigue contratando personal.
- Se encontraron extintores de fuego caducados.
    - Nota: Se recomendó su revisión por parte de personal especializado a la brevedad.

- En el caso de la seguridad de acceso y de instalaciones físicas, el edificio no cuenta con personal de vigilancia.
    - Nota: Se recomendó contratar personal de seguridad.
- En el caso de la ventilación de las instalaciones físicas, el edificio no cuenta con un adecuado sistema de ventilación, y por el clima del lugar será necesario.
    - Nota: Se recomendó instalar un sistema adecuado de ventilación.
- Las instalaciones sanitarias presentan deficiencias en el suministro de agua y limpieza.
    - Nota se recomendó contratar personal de limpieza, así como realizar mantenimiento a las instalaciones sanitarias.
- No se ha instruido al personal del proceso de evacuación de las instalaciones en caso de emergencia o contingencia.
    - Nota: Esto es debido a que se sigue contratando personal.
- Se cuenta con sistema UPS, indicando que se encuentra en proceso la instalación plantas de energía auxiliar.
- El panel eléctrico no está debidamente etiquetado.
    - Nota: Se recomendó etiquetar adecuadamente dicho panel, para identificar las zonas energizadas.

Con relación a la auditoría de red:

- El cableado no está estructurado de acuerdo con los estándares del mercado.
    - Nota: no se detectaron nodos con cables deficientes. Se recomienda mantenerlos a una distancia prudente del suelo.
- Se recomendó numeración visible, clara y accesible de los puntos de red.
- De momento no se cuenta con una memoria técnica de direccionamiento IP estático.
- Con relación a los enlaces de internet, se cuenta con enlace de Telmex.

Con relación a la auditoría de seguridad y pruebas de caja negra en la segunda visita, en los tres CATD que se visitaron se encontraron las mismas incidencias:

- Se puede observar que la mayoría de las observaciones realizadas en la primera visita fueron atendidas.
- Se controló el tráfico causado por las conexiones persistentes de TeamViewer.

- Se bloquearon los puertos USB para la conexión de dispositivos de almacenamiento.
- De igual manera las conexiones a través del protocolo IPV6 fueron bloqueadas en los equipos.
- Se realiza un análisis de paquetes y escaneo global de la red arrojando peligros potenciales, los equipos de trabajo tienen instalado el XAMPP, pero con las carpetas por defecto, lo cual permite obtener información sobre el equipo en cuestión sobre los puertos 80 y 443
- El consumo de ancho de banda en la red por las cámaras de video vigilancia sigue persistiendo, existen momentos en el que el consumo de ancho de banda es considerable y esto puede ocasionar en algunos casos que el flujo de información se vea afectado.
    - Nota: Se recomendó, que las señales de video y voz hagan uso de una VLAN separada de la red de datos.
- En el caso del CAT Cuencamé, se detectó que la red inalámbrica estaba visible y aunque solicita la autenticación a través de una contraseña WPA2, el módem tiene activa la opción de autenticación WPS la cual es vulnerable a ataques externos.
    - Nota: Se recomendó desactivar la publicación del SSID de la red, así como desactivar la función WPS en el modem por su alta tasa de vulnerabilidad

Se concluyó que los CATD-GOMEZ, CATD-LERDO Y CATD-CUENCAME son funcionales para atender el proceso electoral 2021.

PRIMER PRUEBA DE DENEGACIÓN DE SERVICIO

El día 12 de mayo de 2021 siendo las 10:00 horas, nos reunimos en el edificio del CCV Durango, ubicado en la Ciudad Industrial, con el propósito de realizar la ejecución de la prueba de denegación de servicio al sistema PREP que será utilizado en el proceso del PREP IEPC Durango 2021.

La prueba dio inició a las 10:30 horas con la publicación del PREP durante la carga en el mismo de diez actas electorales por parte de la empresa Informática Electoral.

Se comenzó a las 10:30 horas la captura sin ningún problema, diez minutos después, siendo las 10:40 horas se comenzó a realizar un ataque de denegación de servicio hacia el servidor (figura 3), el ataque coordinado contó con un total de cincuenta personas, distribuidas geográficamente en distintos puntos físicos, cada persona realizó un promedio de veinticinco mil peticiones por segundo de forma simultánea hacia el servidor identificado con la URL https://prepdurango2021.mx/diputaciones.

Pasados catorce minutos, siendo las 10:54 horas, el sitio comenzó a presentar intermitencias en el servicio(figuras 4 y 5), indicativo de que el servidor estaba bajo estrés, símbolo de que el ataque estaba siendo efectivo con aproximadamente un millón doscientas cincuenta mil peticiones por segundo en total (figura 2).

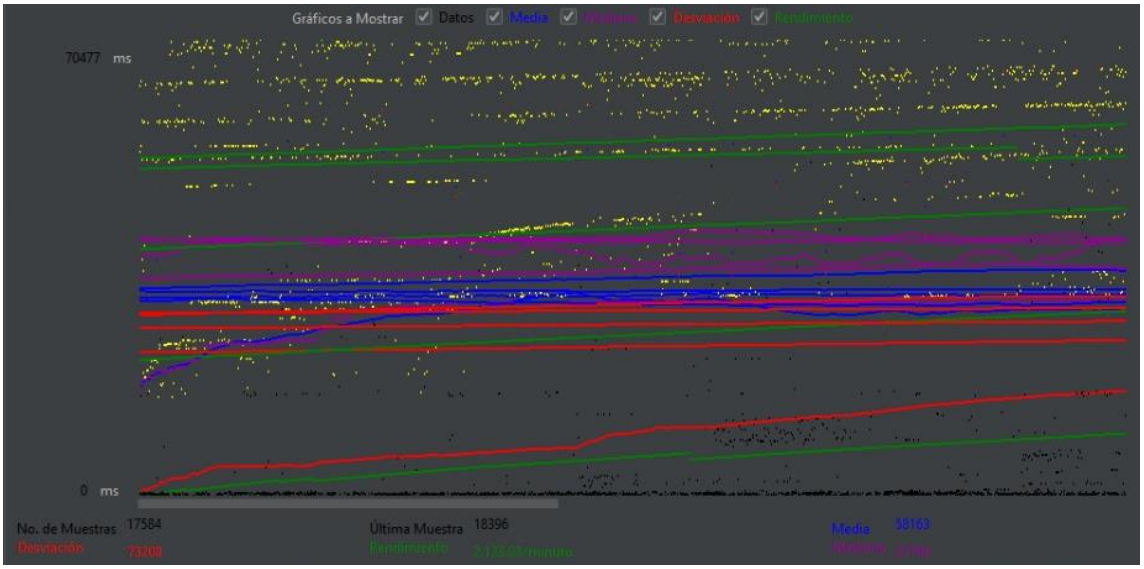


Figura 2. Gráfico de comportamiento del servidor

De acuerdo con los datos analizados, el servidor respondió a aproximadamente a un millón de peticiones simultaneas, dejando sin atención a las restantes doscientos cincuenta mil peticiones.

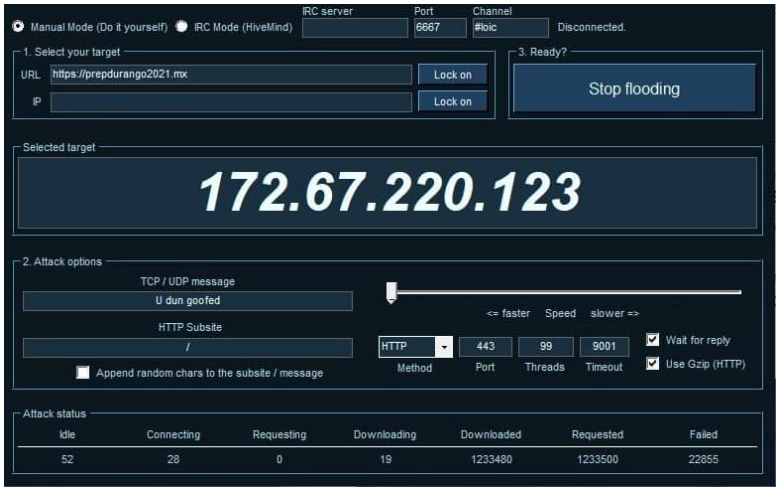
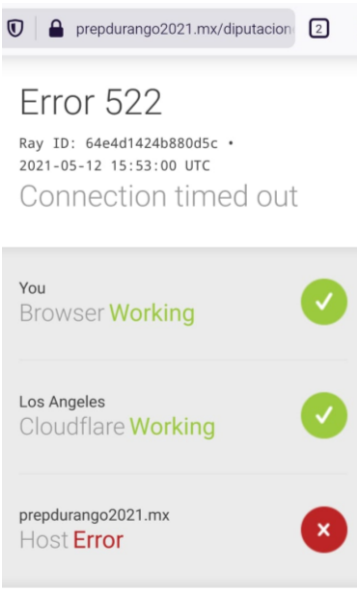


Figura 3. Aplicación de ataque con la cantidad de paquetes enviados



Figuras 4 y 5. Imagen de servidor en línea y falla de comunicación con el servidor

Una vez concluido el ataque de denegación de servicio, el servidor del PREP se reestableció casi de forma instantánea sin afectar las capturas que se habían realizado (figura 6).

Figura 6. Servidor nuevamente en línea

Posterior al ataque sobre el sitio de publicación del PREP, se realizó una prueba similar al sitio del IEPC Durango, arrojando el mismo resultado (figura 7).

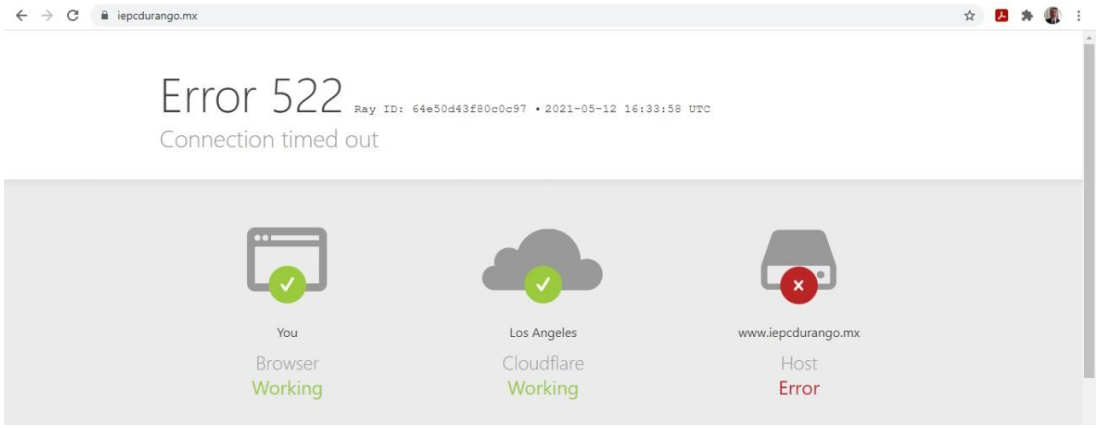


Figura 7. Sitio del IEPC sin responder

Con base a los resultados obtenidos, se recomendó que la empresa refuerce la infraestructura por medio de servidores incrementales de forma automática, de tal manera que cuando el servidor activo detecte máximo un setenta y cinco por ciento de carga se active en forma instantánea otra instancia para balancear la carga en los servidores, así mismo activar la protección contra ataque de denegación de servicio en los sistemas de seguridad perimetral instalados. Esta última recomendación es aplicable al Instituto Electoral y de Participación Ciudadana de Durango para su sitio web.

SEGUNDA PRUEBA DE DENEGACIÓN DE SERVICIO

El día 21 de mayo de 2021 siendo las 12:00 horas, nos reunimos en el edificio del CCV Durango, ubicado en la Ciudad Industrial, con el propósito de realizar la ejecución de la segunda prueba de denegación de servicio al sistema PREP que será utilizado en el proceso del PREP IEPC Durango 2021.

La prueba dio inició a las 12:00 horas con la publicación del PREP durante la carga en el mismo de diez actas electorales por parte de la empresa Informática Electoral.

Se comenzó a las 12:00 horas la captura sin presentarse ningún problema, diez minutos después, siendo las 12:10 horas se comenzó a realizar un ataque de denegación de servició hacia el servidor, el ataque coordinado contó con un total de cincuenta personas, distribuidas geográficamente en distintos puntos físicos, cada persona realizó un promedio de veinticinco mil peticiones por segundo de forma simultánea hacia el servidor identificado con la URL https://prepdurango2021.mx/diputaciones.

Pasados 30 minutos, siendo las 12:40 horas, el sitio no presento ninguna incidencia en su funcionamiento, indicativo de que el sitio cuenta con un servicio de protección contra ataques de denegación de servicio, el cual permitió que el servicio no se viera interrumpido durante el simulacro (figura 8).

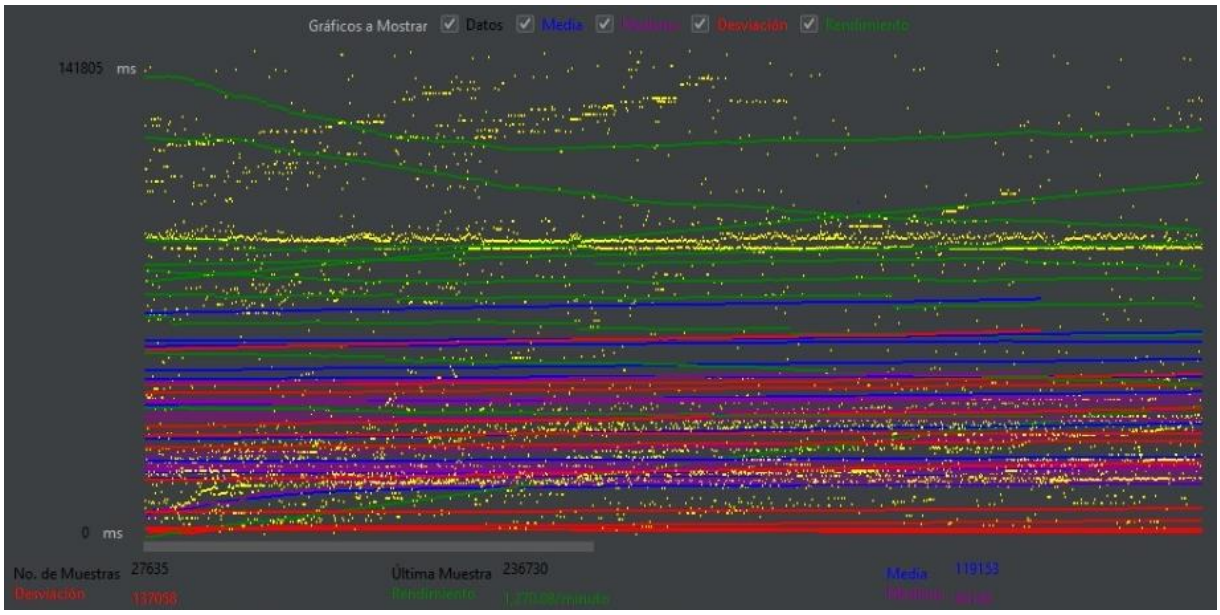


Figura 8. Gráfico de comportamiento del servidor

De acuerdo con los datos analizados, el sitio desvió tráfico para lograr balancear la solicitud de peticiones, con lo cual se logró que el servicio no presentara intermitencias en su funcionamiento (figuras 10 y 11).

```
Haciendo ping a prepdurango2021.mx [172.67.68.246] con 32 bytes de datos:
Respuesta desde 172.67.68.246: bytes=32 tiempo=850ms TTL=49
Respuesta desde 172.67.68.246: bytes=32 tiempo=354ms TTL=49
Respuesta desde 172.67.68.246: bytes=32 tiempo=466ms TTL=49
Respuesta desde 172.67.68.246: bytes=32 tiempo=240ms TTL=49

Estadísticas de ping para 172.67.68.246:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 240ms, Máximo = 850ms, Media = 477ms
```

Figura 9. Dirección IP del servidor que aloja el sitio web al comenzar el ataque (dirección IP 172.67.68.246)

```
Haciendo ping a prepdurango2021.mx [104.26.9.202] con 32 bytes de datos:
Respuesta desde 104.26.9.202: bytes=32 tiempo=91ms TTL=49
Respuesta desde 104.26.9.202: bytes=32 tiempo=86ms TTL=49
Respuesta desde 104.26.9.202: bytes=32 tiempo=89ms TTL=49

Estadísticas de ping para 104.26.9.202:
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 86ms, Máximo = 91ms, Media = 88ms
```

Figura 10. Dirección IP del servidor que aloja el sitio web al después de 30 minutos de comenzado el ataque (dirección IP 104.26.9.202)

Una vez concluido el ataque de denegación de servicio, el servidor que aloja el sitio del PREP mostro casi de forma instantánea la dirección IP 172.67.68.246, lo cual es un indicativo de que atendieron las recomendaciones derivadas del primer ataque de denegación de servicio (figura 9).

.

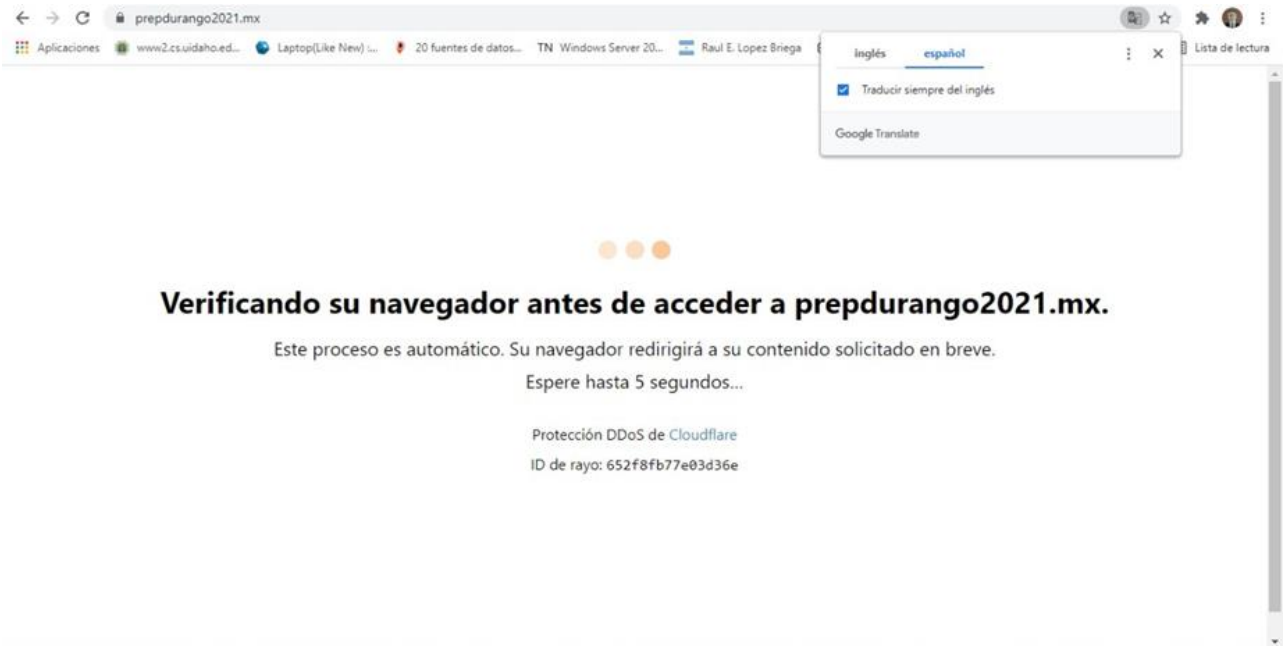


Figura 11. Servicio de protección contra ataques de denegación de servicio en funcionamiento.

La empresa proporciono la información técnica que indica que son cuatro servidores que se activan de forma progresiva y automática al llegar al 70 por ciento de su carga nominal de solicitudes, con lo que se cuenta con la capacidad de atender las solicitudes de los visitantes durante la jornada electoral.

Posteriormente se realizó el mismo procedimiento con el sitio web del Instituto Electoral y de Participación Ciudadana del Estado de Durango, detectando que se encuentra habilitada la protección contra ataques de denegación de servicio, de igual forma se detecta el cambio de direcciones IP al momento de realizar el ataque, y el sitio web de igual forma no presentó intermitencias en su funcionamiento (figuras 12 y 13).

```
Haciendo ping a iepcdurango.mx [104.26.5.8] con 32 bytes de datos:
Respuesta desde 104.26.5.8: bytes=32 tiempo=61ms TTL=57
Respuesta desde 104.26.5.8: bytes=32 tiempo=64ms TTL=57
Respuesta desde 104.26.5.8: bytes=32 tiempo=66ms TTL=57
Respuesta desde 104.26.5.8: bytes=32 tiempo=59ms TTL=57

Estadísticas de ping para 104.26.5.8:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 59ms, Máximo = 66ms, Media = 62ms
```

Figura 12. Dirección IP del servidor que aloja el sitio web al comenzar el ataque (dirección IP 104.26.5.8)

```
Haciendo ping a iepcdurango.mx [172.67.181.15] con 32 bytes de datos:
Respuesta desde 172.67.181.15: bytes=32 tiempo=86ms TTL=49
Respuesta desde 172.67.181.15: bytes=32 tiempo=88ms TTL=49
Respuesta desde 172.67.181.15: bytes=32 tiempo=75ms TTL=49
Respuesta desde 172.67.181.15: bytes=32 tiempo=67ms TTL=49

Estadísticas de ping para 172.67.181.15:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 67ms, Máximo = 88ms, Media = 79ms
```

Figura 13. Dirección IP del servidor que aloja el sitio web al después de 30 minutos de comenzado el ataque (dirección IP 172.67.181.15)

Con base a los resultados obtenidos, se observó que se atendieron las recomendaciones mostrándose que la empresa Informática Electoral reforzó la infraestructura y activó la protección contra ataque de denegación de servicio. Así mismo el Instituto Electoral y de Participación Ciudadana del Estado de Durango reforzó a su vez la protección de su sitio web, estas acciones encaminadas a estar listos para la jornada electoral y que los servicios no presenten intermitencias, dándole certeza a la ciudadanía de los resultados mostrados por el Programa De Resultados Electorales Preliminares.

INFORME DEL TERCER SIMULACRO Y CREACIÓN DEL HASH

El día 30 de mayo la jornada inicio las 09:00 horas con las actividades propias del simulacro programado. A las 14:00 horas, el ente auditor fue convocado por el Ing. Jorge Galo Solano a las instalaciones del CCV del PREP en las personas del Ing. José Roberto López Quiñones y el M.C.C. Salvador Ramos Collins como responsables de las funciones de auditor de seguridad y auditor de caja negra respectivamente.

La empresa Informática Electoral, nombró al Ing. Juan de Jesús Rubio Pinto para llevar a cabo por su parte el procedimiento de generación de hash de los archivos del código del sistema del PREP, así como de la estructura de la base de datos.

Se acordó llevar a cabo el procedimiento para la generación de los archivos hash, con el siguiente procedimiento: generar dos hashes, uno que represente a los archivos de código del sistema PREP y otro que represente a la estructura de la base de datos.

Para obtener el primero de los hashes, el que representa los archivos de código del sistema es necesario obtener de manera individual un hash de cada archivo y posteriormente un hash global del conjunto de archivos hash. Para ello se inició con un sorteo ascendente de todos los archivos componentes del código en la carpeta de almacenamiento del sistema del PREP, para posteriormente generar un archivo individualmente de hash para cada uno de los archivos integrantes en la carpeta en donde éstos se encuentran almacenados. Posteriormente un tercer paso que consistió en generar un archivo de hash global del conjunto de todos los archivos de hash individuales generados de los archivos códigos del sistema

del PREP, esto último con la finalidad de asegurar que sí se hiciera posteriormente un cambio en cualquiera de los archivos originales del código del sistema PREP se detectaría, primero un cambio en el hash global y posteriormente en él, o los, archivos del sistema. Posteriormente a través de un análisis comparativo archivo por archivo de hash se encontraría cual sería el archivo que habría sido alterado hasta en la más mínima parte de su código (figura 14).

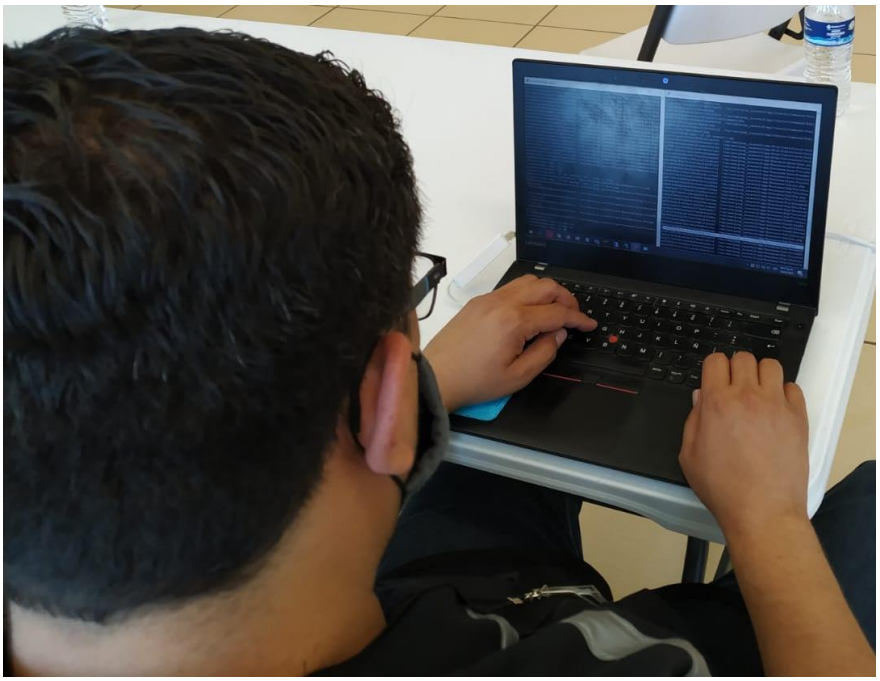


Figura 14. Creación de los hashes del sistema PREP

Así mismo se acordó que el notario público incluyera una frase adyacente a los hashes para así evidenciar que se generaron en el momento que él estuviera presente y dando fe de los hechos.

Antes de las 16:30horas, como se completó el 100% de capturas de actas en el simulacro programado para este día se procede al traslado al edificio que alberga el CCV para dar inicio al proceso de generación de los hashes.

Siendo las 16:30 horas, se reunieron en al CCV los consejeros electorales Mtra. Ma. Cristina Campos Zavala y Lic. Laura Fabiola Bringas Sánchez, así como sus asesores, y el notario público Lic. Vicente Guerrero Romero quien dio fe de la creación de los hashes, los miembros del COTAPREP Mtro. José Luis Bautista, Dr. Martín Gallardo y Dra. Alejandra Arreola, así como personal del IEPC de su unidad técnica de cómputo, encabezada por el Ing. Jorge Galo Solano, así como el L.I. Roberto Mendoza Ponce representante del INE, y personal de Informática Electoral, entre ellos el Ing. Juan de Jesús Rubio Pinto, y ente auditor en presencia de el Ing. José Roberto López Quiñones y el M.C.C. Salvador Ramos Collins (figura 15).

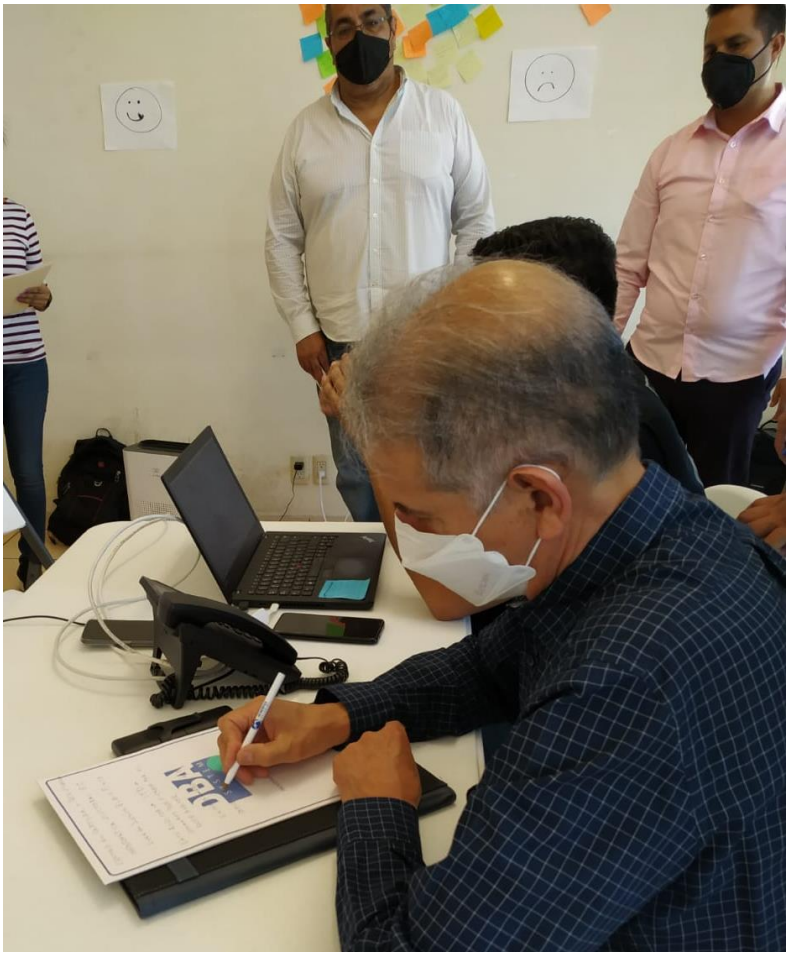


Figura 15. Fe de hechos por el notario público de la creación de los hashes

Una vez que se llevó a cabo la obtención de los dos hashes bajo el procedimiento acordado (figura 16).

Archivos del código del sistema del PREP
8976e45478ab18c417de15abee6f6e23 ordenados4.txt
Estructura de la base de datos
3e962d6086414d417bfc630bc34ea159 basededatos3.sql

Quedaron a resguardo en una memoria USB en posesión del notario público Lic. Vicente Guerrero Romero, para su comprobación al momento previo y final de la contabilización de actas en el sistema PREP el día de la jornada electoral.

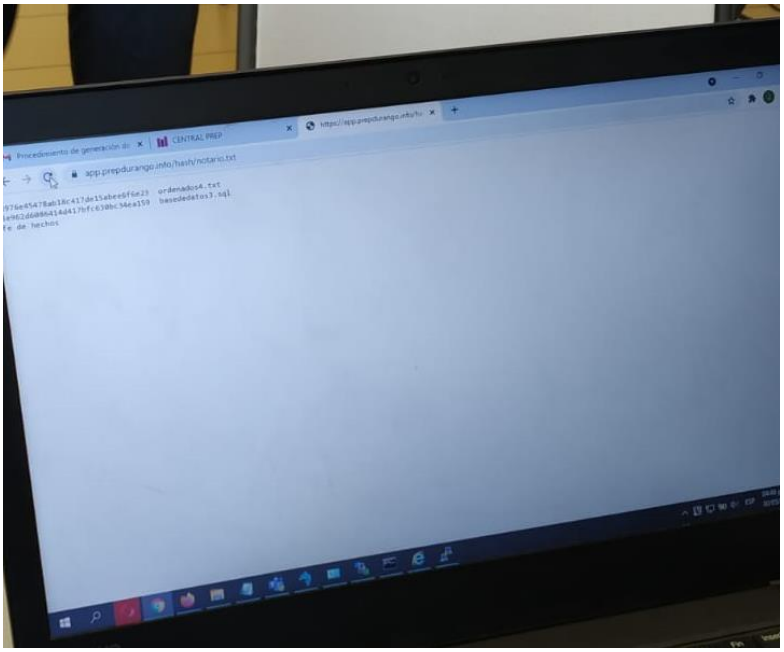


Figura 16. Captura de los hashes generados

Concluyendo las actividades del simulacro y la generación de los hashes a las 17:00 horas.

El día 5 de junio de 2021 atendiendo requerimientos del INE se procedió a realizar ajustes a la imagen del sistema PREP por lo que se tuvieron que generar los

hashes nuevamente ante notario, mismos que sustituyen a los anteriores y deberán ser validados con los del inicio y cierre de la jornada electoral.

Archivos del código del sistema del PREP
8447ed205a4d238eceaa79d46edb20c8 ordenados2021-06-05.txt
Estructura de la base de datos
18bc1191595ab164f23897fb4d0c648e basededatos2021-06-05.sql

INFORME DE LA JORNADA DE FUNCIONAMIENTO DEL SISTEMA PREP

El día 06 de mayo previo a la jornada del sistema PREP, siendo las 19:00 horas el ente auditor fue convocado por el Ing. Jorge Galo Solano a las instalaciones del CCV del PREP.

La empresa Informática Electoral, nombró al Ing. Juan de Jesús Rubio Pinto para llevar a cabo por su parte el procedimiento de generación de hash de los archivos del código del sistema del PREP, así como de la estructura de la base de datos.

Se siguió el mismo procedimiento para la generación de los archivos hash y generar dos hashes, uno que represente a los archivos de código del sistema PREP y otro que represente a la estructura de la base de datos.

Ante el notario público Lic. Vicente Guerrero Romero, se obtuvieron los dos hashes, quedando a resguardo de éste para ser validados con los hashes previamente obtenidos, así como con los que se obtendrán al cierre del funcionamiento del sistema PREP, una vez realizado lo anterior se dio inicio al sistema PREP siendo las 20:00 horas.

Archivos del código del sistema del PREP
8447ed205a4d238eceaa79d46edb20c8 ordenados2021-06-06.txt
Estructura de la base de datos
18bc1191595ab164f23897fb4d0c648e basededatos2021-06-06.sql

Siendo las 19:30 horas del día 7 de junio, el ente auditor fue convocado nuevamente por el Ing. Jorge Galo Solano a las instalaciones del CCV del PREP.

Ante el notario público Lic. Vicente Guerrero Romero, a las 20:00 horas se dio cierre al sistema PREP, una vez realizado el cierre, con base al procedimiento previamente realizado al inicio del sistema PREP, se obtuvieron nuevamente los dos hashes.

Archivos del código del sistema del PREP
8447ed205a4d238eceaa79d46edb20c8 ordenados2021-06-07.txt
Estructura de la base de datos
18bc1191595ab164f23897fb4d0c648e basededatos2021-06-07.sql

Una vez realizado lo anterior se procedió a la validación de estos hashes del cierre con los hashes previamente obtenidos, todo esto ante el notario público.

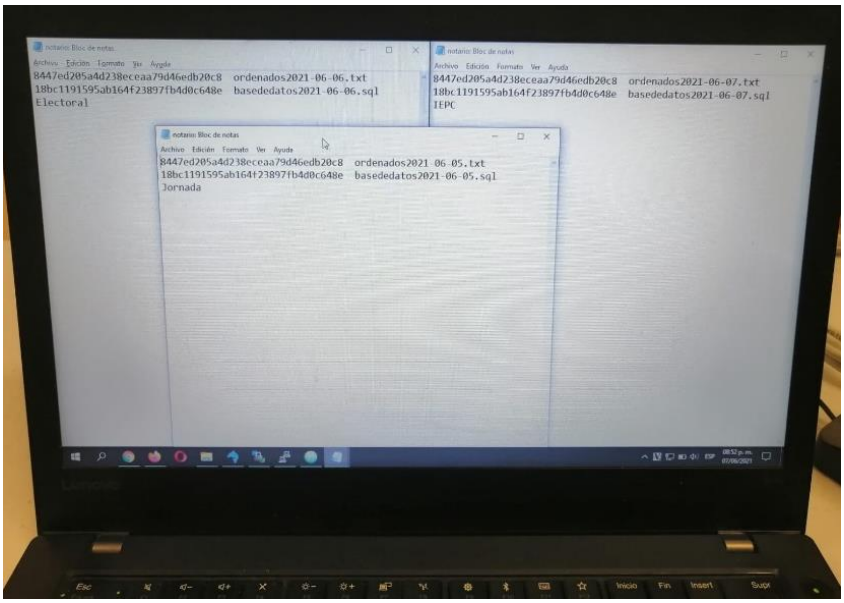


Figura 17. Validación de los hashes obtenidos previo, al inicio y al cierre del sistema PREP

Para la validación se procedió primero a la revisión visual y posteriormente por medio de una hoja de cálculo en Excel, lo anterior para tener una certeza de que

los tres pares de Hashes sean iguales, y con base en esto se valide el sistema PREP que se utilizó para mostrar los resultados preliminares de la jornada electoral del día 6 de junio de 2021 (figuras 17 y 18).

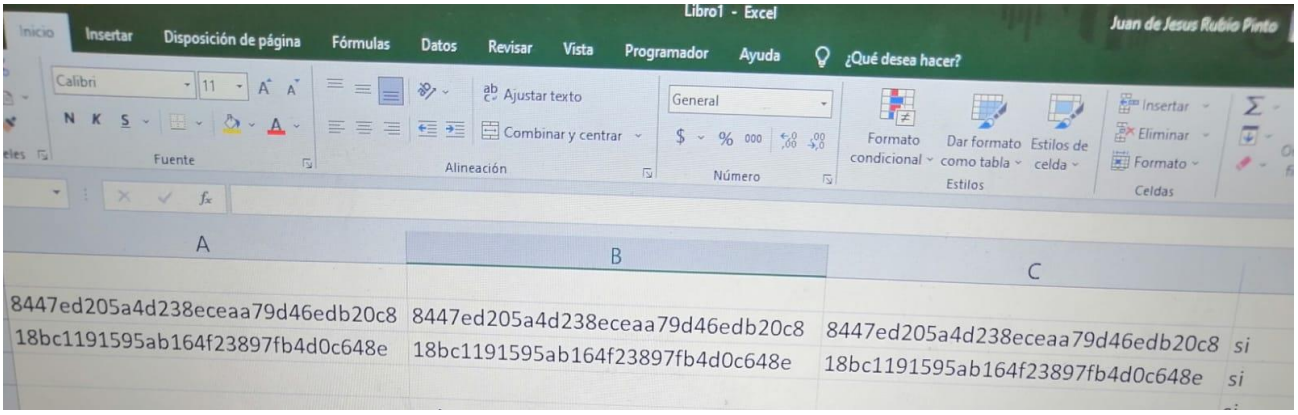


Figura 18. Validación de los hashes obtenidos previo, al inicio y al cierre del sistema PREP en Excel

Una vez que se llevó a cabo la validación de los tres pares de hashes ante el notario público, consejeros electorales, representantes de partidos, integrantes COTAPREP y personal del IEPC, se procedió a levantar el acta correspondiente por el notario público Lic. Vicente Guerrero Romero, dándose por concluido el proceso siendo las 21:00 horas del día 7 de junio de 2021.