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 DE AUDITORÍA

Mayo de 2024

INFORME FINAL

El presente informe cubre lo realizado desde las pruebas de funcionalidad del sistema PREP hasta el simulacro previo al día de la jornada electoral.

REPORTE DE PRUEBAS FUNCIONALES DE CAJA NEGRA

Los días jueves 11 y lunes 15 de abril de 2024 se llevaron a cabo las pruebas para verificar el correcto funcionamiento del sistema informático del PREP, proporcionado por la empresa Informática Electoral S.C.

Cabe mencionar que los coordinadores de las actividades de ejecución de las pruebas estuvieron, por parte de la empresa, a cargo de la Ing. Lidia Lorena Padilla Gómez y por parte de la Instancia Interna el Ing. Jorge Galo Solano García.

¿QUÉ SON LAS PRUEBAS FUNCIONALES DE CAJA NEGRA?

Como Ente Auditor tenemos la responsabilidad de garantizar el sistema de información para el PREP, utilizado en el próximo proceso electoral del 2 de junio de este año, cumpla con todos los posibles escenarios que se puedan presentar durante la jornada electoral. Para poder llevar a cabo el proceso de evaluación es que se llevan a cabo las pruebas funcionales de caja negra que consisten en probar su funcionamiento sin tener un conocimiento previo de su funcionamiento interno. Esto es, que sin conocer el código fuente del sistema, la documentación sobre el análisis y diseño del mismos, así como respetando los derechos de autor, se pueda conocer si dicho sistema cumple con los requisitos funcionales establecidos por el INE y el IEPC, al momento de contratar los servicios de la empresa Informática Electoral S.C.

Dicho lo anterior, se estableció un plan de pruebas en donde pudimos validar todos los posibles flujos que se podrían presentar durante el proceso electoral. En este plan se ven de manera integral, como proceso, los sistemas de información, vistas del sistema, aplicaciones móviles que intervienen en el proceso, así como equipo utilizado para garantizar el correcto funcionamiento del PREP. Las pruebas se limitan a dar entrada a los datos, imágenes requeridas para alimentar al sistema y se recibe como salida un resultado esperado a partir de las entradas.

Bajo una metodología de pruebas funcionales de caja negra, el Ente Auditor es un órgano que viene a coadyuvar con el IEPC como los responsables de realizar las pruebas y será la empresa Informática Electoral S.C. quien facilite el acceso a su sistema para llevar a cabo el proceso, de tal manera que se crea una separación entre ambos equipos.

PLAN DE PRUEBAS FUNCIONALES DE CAJA NEGRA

El plan de pruebas funcionales se basó en 13 flujos:

1. Sin incidencias
2. Algún dato ilegible
3. Todos ilegibles / Algún sin dato
4. Todos sin datos
5. Algún Ilegible / Excede lista nominal
6. Algún ilegible / Algún sin datos
7. Algún ilegible
8. Sin acta por paquete no entregado
9. Sin acta por casilla no instalada
10. Sin acta por paquete entregado sin bolsa
11. Acta fuera de catálogo
12. Datos de identificación iguales a los de otra
13. Acta de voto anticipado

Los perfiles de usuario que intervienen durante el proceso son:

PERFIL DE USUARIO DEL SISTEMA	DESCRIPCIÓN
API PREP Casilla	Usuario que tiene acceso al sistema a través de la app PREPCasilla y se va a encontrar ubicado en el CATD
MCADI	Usuario cuya función es identificar que las actas que llegan al CCV provenientes del CATD llegues en condiciones para ser procesada
MCADF	Usuario Foliador, es quien identifica los datos que contiene el acta
CVPREP	Usuario Capturista, este perfil tiene acceso únicamente a las actas que de manera aleatoria le van a llegar para el registro de los votos plasmados en el acta.

MRI	Usuario que estará en la Mesa de Resolución de Incidencias
Sitio web público	Este no es propiamente un perfil, pero es la aplicación web para la publicación de las actas computadas.

Los servidores que se encuentran integrados en el proceso para el ambiente de auditoría son los siguientes:

Activo	Dirección IP	Propósito
server-auditapp	10.2.0.232	Servicios necesarios para aplicativos CORE (front-end, back-end, BD).
server-auditapc	10.2.0.233	Servicios necesarios para aplicativos PREP Casilla
server-auditweb	10.2.0.234	Servicios necesarios para aplicativos webs públicos (sitio web público)

Los servidores que se encuentran integrados en el proceso para el ambiente de pruebas son los siguientes:

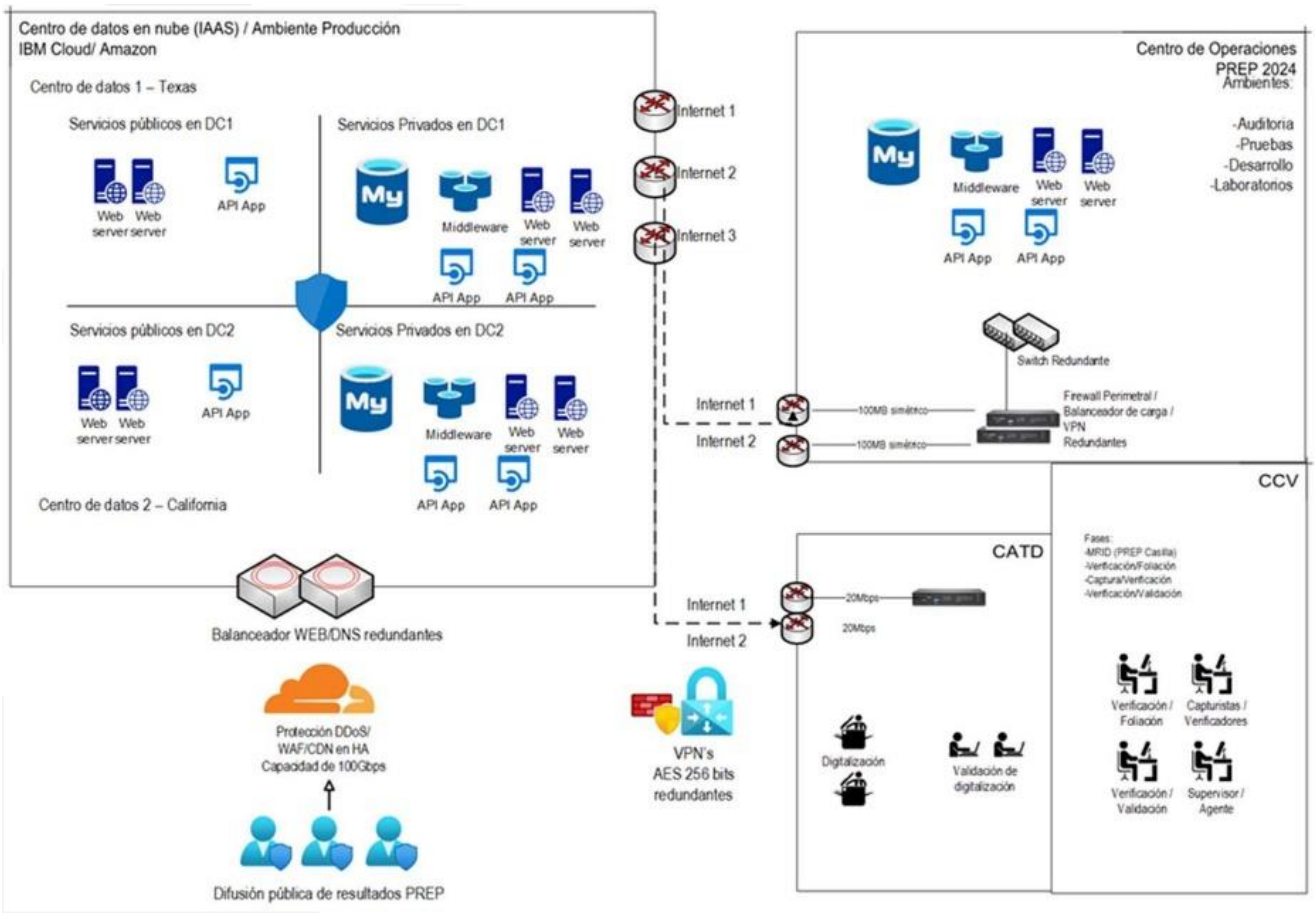
Activo	Dirección IP	Propósito
server-app	10.2.0.222	Servicios necesarios para aplicativos CORE (front-end, back-end, BD)
server-pc	10.2.0.223	Servicios necesarios para aplicativos PREP Casilla
server-web	10.2.0.224	Servicios necesarios para aplicativos webs públicos (sitio web público)

Otros equipos activos integrados para el proceso:

Activo	Dirección IP	Propósito
NVR1	10.2.0.20	Concentrar la grabación del circuito cerrado de cámaras IP
NVR2	10.2.0.21	Concentrar la grabación del circuito cerrado de cámaras IP
NVR3	10.2.0.22	Concentrar la grabación del circuito cerrado de cámaras IP
PBX-IP	10.2.0.50	Administras las líneas telefónicas IP internas
ESX8a	10.2.0.201	Servidor que administra máquinas virtuales (nodo primario)
ESX8b	10.2.0.202	Servidor que administra máquinas virtuales (nodo secundario)

ESX8a_admin	10.2.0.211	Administración de servidor físico 1
ESX8b_admin	10.2.0.212	Administración de servidor físico 2
Firewall	10.2.0.254	Firewall perimetral

DIAGRAMA DE INTERCONEXIÓN DE EQUIPO Y SEGURIDAD DE RED



EVALUACIÓN SOBRE PRUEBAS FUNCIONALES

Una vez concluido el plan de pruebas funcionales podemos determinar que el sistema de información para el programa de resultados preliminares PREP concluyó satisfactoriamente cada una de las 13 pruebas tipo, con las cuales muestra la funcionalidad para llevar a cabo este proceso.

Algunas observaciones que se realizaron durante las pruebas y que es importante anotar:
Se tomó el tiempo por cada una de las pruebas contabilizando 86.03 min en el total de las pruebas y un tiempo promedio por prueba de 7.02 min.

El sistema una vez que una AEC ha pasado por el proceso de identificación y foliación pasa a la captura en donde de manera aleatoria esa acta es asignada para su captura, pudiendo pasar por este proceso de 2 o hasta 4 veces, dependiendo de la inconsistencia entre los capturistas. En el peor de los casos, si los 4 capturistas cometen algún error de captura entonces esa acta pasa a la Mesa de Resolución de Incidencias (MRI) para su correcto registro. Cada capturista tiene hasta 3 min para capturar los datos de una AEC, de exceder el tiempo automáticamente pasará a otro capturista. La MRI tiene un minuto para la revisión del acta y 3 más para la captura de sus datos.

La anotación de lo anteriormente expuesto es para establecer que un AEC puede tener un tiempo máximo para su procesamiento de aproximadamente 20 min., si tuviera que pasar por todas las etapas. Sin embargo, durante las pruebas funcionales en cada uno de los diferentes escenarios evaluados se dio una explicación de lo que iba ocurriendo bajo el acompañamiento de los participantes en el evento, lo cual nos indica que el tiempo promedio de 7.02 min, puede ser reducido de manera importante durante la jornada electoral.

El IEPC tiene consideradas un total de 2,626 AEC para el proceso de elección a Diputaciones Locales en el estado, de tal manera que considerar el tiempo para promedio registrado en el procesamiento de un AEC nos llevaría 307.24 horas o 12.8 días, lo cual nos habla de que estos tiempos son producto de las pruebas de funcionalidad y de que se evalúa un flujo, no de la operación en sí. Al momento de la jornada electoral se contará con 60 capturistas que agilizarán el proceso reduciendo drásticamente los tiempos de procesamiento de un AEC.
Otra anotación importante es que el sistema presenta diferentes vistas de este, dependiendo del usuario y el rol que juega dentro del proceso, es decir, que sólo tiene acceso para llevar a cabo su tarea, sin poder realizar algo diferente de su perfil de usuario.

PREPCasilla es la aplicación móvil que permite digitalizar mediante la cámara de un teléfono celular, que es asignado por Informática Electoral S.C. a los responsables del proceso de digitalización en los CATD, cada una de las AEC. Si bien pudimos comprobar que funciona de manera correcta para el proceso de digitalización, aun no tenemos una respuesta por parte de la empresa de como garantiza la seguridad de acceso al sistema de información.

Por otro lado, además de los usuarios que participan en el proceso de registro de un AEC, hasta su publicación debemos tener otros usuarios para el proceso de administración del sistema, administración de la base de datos los cuales pudimos evaluar durante esta etapa de pruebas funcionales. Sería muy recomendable que el IEPC si cuente con esta información y nos garantice temas como seguridad de la información, control de inconsistencias en las bases de datos, licenciamientos de aplicaciones de terceros, etc.

Como Ente Auditor, podemos concluir que el sistema de información de la empresa Informática Electoral S.C. evaluado para llevar a cabo el PREP, cumple con los requisitos de funcionalidad, desempeño y comunicación que se esperaba.

PRUEBAS Y ANÁLISIS DE VULNERABILIDADES, SEGURIDAD FÍSICAS Y LÓGICAS A LA INFRAESTRUCTURA TECNOLÓGICA DEL CCV-DURANGO

En conjunto con las pruebas funcionales se realizaron pruebas y análisis de vulnerabilidades, seguridad físicas y lógicas a la infraestructura tecnológica del CCV.

INFRAESTRUCTURA LÓGICA

Se comenzó con un proceso de verificación del estado de la red informática consistente en un escaneo detallado de la red 10.2.101.0/24 utilizando la herramienta Nmap. El objetivo del escaneo fue identificar los dispositivos activos, mapear la topología de red y las posibles formas de acceso a los diferentes equipos que estarán trabajando durante el ejercicio de captura de actas del sistema PREP durante la jornada electoral.

Se debe tener en cuenta que el escaneo se llevó a cabo siguiendo buenas prácticas éticas de acuerdo con las primeras 3 fases de la metodología Certified Ethical Hacker y respetando las políticas de seguridad establecidas.

A través de este análisis, se busca brindar una comprensión clara de la situación actual de la red y ofrecer sugerencias concretas para fortalecer su seguridad y confiabilidad.

METODOLOGÍA

El escaneo de la red 10.2.101.0/24 se llevó a cabo utilizando la herramienta Nmap con la finalidad de obtener información detallada sobre los dispositivos y servicios disponibles en la red.

A continuación, se detallan los pasos y parámetros utilizados durante el escaneo:

Selección de la red objetivo: La red objetivo fue identificada como 10.2.101.0/24, lo que indica que se escanearon todas las direcciones IP en el rango de 10.2.101.1 a 10.2.101.254.

Se utilizó el siguiente comando para realizar el escaneo:

sudo nmap -A -sS 10.2.101.0/24

-A: Este parámetro activa la detección de sistemas operativos, detección de versiones de servicios y detección de scripts de Nmap. Proporciona una recopilación exhaustiva de información sobre los hosts escaneados.

-sS: Especifica el tipo de escaneo a realizar, en este caso, un escaneo de tipo SYN. Este tipo de escaneo envía un paquete SYN al puerto destino y espera una respuesta SYN/ACK. Si recibe esta respuesta, indica que el puerto está abierto.

Una vez completado el escaneo, se analizaron los resultados obtenidos para identificar los dispositivos activos, los puertos abiertos, los sistemas operativos detectados y cualquier posible vulnerabilidad o riesgo de seguridad en la red.

OBSERVACIONES Y RECOMENDACIONES

Cabe hacer mención que al momento de realizar el escaneo algunos dispositivos se encontraban en modo suspendido por lo cual no fue posible llevar a cabo el análisis sobre todos y cada uno de ellos, de igual forma se encontraban conectados algunos dispositivos dentro de la red que fueron analizados y llama la atención la apertura de ciertos puertos disponibles que no deberían estar para los equipos de trabajo normal el informe detallado de los equipos que se pudieron escanear se encuentra dentro de la sección de anexos del presente documento.

Para los equipos que se pudieron analizar y que se detectaron como parte del conjunto de computadoras que van a ser usadas durante la jornada electoral se puede observar lo siguiente:
El puerto 6646 se encuentra abierto, pero ha sido redireccionado de forma interna, la " huella digital" del sistema operativo que es una versión modificada de Linux, aunque visualmente pudimos constatar era Windows.

Se encontró un servidor web disponible que proporciona información sobre el puerto 80 y el puerto 443 de forma abierta además de un listado de 24 puertos disponibles que se encuentran filtrados, de acuerdo con la huella digital del sistema operativo se identifica como una impresora Epson misma que debería de configurarse su acceso por medio de credenciales.

Para el análisis de comunicación de red se ejecutó un comando para obtener las diferentes redes comunes a las cuales los equipos tienen conexión, satisfactoriamente se encontró que la red en la que se encuentran los equipos que van a ser usados para la jornada electoral, exclusivamente tienen comunicación vía el firewall y en su momento hacia la aplicación que va a estar hospedada en la nube, sin afectar esto el rendimiento de los otros equipos que se encuentran en redes diferentes dentro de las propias instalaciones.

Se recomendó realizar las pruebas nuevamente en un entorno de trabajo lo más similar al que habrá durante la jornada electoral, así como en los otros sitios a visitar.

INFRAESTRUCTURA FÍSICA

Con relación a la auditoría de infraestructura y seguridad física, en la cual se revisó la totalidad del edificio que alberga al CCV se observó lo siguiente:

- El site de telecomunicaciones se encuentra en la planta alta.
- Se recomienda realizar la nomenclatura adecuada en cada nodo y switch.
- Se cuenta con cableado estructurado.
- En el área de la planta baja todos los nodos y conexiones de red funcionan correctamente. Solo un punto no pasó la prueba, mismo que fue solventado de inmediato al detectarse el incidente.
- En el Site en planta alta todas las conexiones funcionan adecuadamente y se cuenta con todo lo necesario para el óptimo funcionamiento.
- En cuestión de infraestructura, se cuenta con todo lo necesario como extintores, cámaras, aire acondicionado para el enfriamiento de los equipos, dispositivos de acceso biométrico, UPS y plantas para el proceso del PREP.
- Se cuenta con sistema de Fail Over y enlaces redundantes con diferentes ISP.
- Se cuenta con control de acceso al site y las instalaciones en general.
- Se realizaron cortes de energía y los equipos de respaldo funcionaron adecuadamente.
- El site cuenta con sistema de refrigeración adecuado. Sin embargo, se sugiere que en las áreas de captura exista ventilación adecuada ya que el calor se acumula demasiado.
- El edificio cuenta con la señalización adecuada.

OBSERVACIONES Y RECOMENDACIONES

En general se observó que toda la infraestructura se encontraba con un funcionamiento óptimo, cumpliendo con los estándares requeridos. Se sugirió realizar las correcciones pertinentes en la nomenclatura e identificación de los puntos de red, así mismo se recomendó implementar los mecanismos necesarios para la adecuada ventilación de las áreas de captura, para garantizar el bienestar del personal, y el correcto funcionamiento de los equipos, que se encuentra en los mismos.

INFORME DE VISITAS CATD-GÓMEZ PALACIO, CATD-LERDO y CATD-MAPIMÍ

El día 25 de abril de 2024 se realizaron las visitas para la verificación del estado de los CATD-GOMEZ, CATD-LERDO y CATD-MAPIMÍ.

Se realizaron pruebas y análisis de vulnerabilidades, así como de seguridad física y de infraestructura tecnológica.

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

REVISIÓN DE SEGURIDAD FÍSICA E INFRAESTRUCTURA TECNOLÓGICA.

CATD-GÓMEZ PALACIO

Observaciones:

- Se realizó la revisión de infraestructura del área cómputo.
- Se cuenta con cableado estructurado.
- En el área de cómputo todos los nodos y conexiones de red funcionan correctamente.
- Cuentan con dos proveedores de enlace (ISP), un enlace de Telmex y un enlace de Megacable.
- En cuestión de infraestructura, se cuenta con todo lo necesario como extintores, cámaras, aire acondicionado para el enfriamiento de los equipos, UPS y plantas para el proceso del PREP.
- Se cuenta con sistema de Fail Over y enlaces redundantes con diferentes ISP.
- Se realizaron cortes de energía y los equipos de respaldo funcionaron adecuadamente.
- El site cuenta con sistema de refrigeración adecuado.
- El edificio cuenta con la señalización adecuada.

Recomendaciones:

- En general, toda la infraestructura se encuentra en funcionamiento adecuado y óptimo, cumpliendo con los estándares requeridos.

- Se recomendó realizar las correcciones pertinentes señaladas en las observaciones.
- Se recomendó proteger las cajas de los interruptores eléctricos.
- Se recomendó implementar los mecanismos necesarios para la adecuada vigilancia de las áreas de captura.

CATD-LERDO

Observaciones:

- Se realizó la revisión de infraestructura del área cómputo.
- Se cuenta con cableado organizado.
- En el área de cómputo todos los nodos y conexiones de red funcionan correctamente.
- Cuentan con dos proveedores de enlace (ISP), un enlace de Telmex y un enlace de Megacable.
- En cuestión de infraestructura, se cuenta con todo lo necesario como extintores, cámaras, aire acondicionado para el enfriamiento de los equipos, dispositivos de acceso biométrico, UPS y plantas para el proceso del PREP.
- Se cuenta con sistema de Fail Over y enlaces redundantes con diferentes ISP.
- Se realizaron cortes de energía y los equipos de respaldo funcionaron adecuadamente.
- El edificio cuenta con la señalización adecuada.

Recomendaciones:

- En general, toda la infraestructura se encuentra en funcionamiento adecuado y óptimo, cumpliendo con los estándares requeridos.
- Se recomendó realizar las correcciones pertinentes señaladas en las observaciones.
- Se recomienda tener vigilancia permanente para cuidar el acceso al centro de captura.
- Se recomendó implementar los mecanismos necesarios para la adecuada vigilancia de las áreas de captura.

CATD-MAPIMÍ

Observaciones:

- Se realizó la revisión de infraestructura del área cómputo.
- Se cuenta con cableado organizado.
- En el área de cómputo todos los nodos y conexiones de red funcionan correctamente.
- Cuentan con dos proveedores de enlace (ISP), un enlace de Telmex y un enlace de satelital.
- En cuestión de infraestructura, se cuenta con todo lo necesario como extintores, cámaras, aire acondicionado para el enfriamiento de los equipos, UPS y plantas para el proceso del PREP.
- Se cuenta con sistema de Fail Over y enlaces redundantes con diferentes ISP.
- Se realizaron cortes de energía y los equipos de respaldo funcionaron adecuadamente.
- El edificio cuenta con la señalización adecuada.

Recomendaciones:

- En general, toda la infraestructura se encuentra en funcionamiento adecuado y óptimo, cumpliendo con los estándares requeridos.

REVISIÓN DE SEGURIDAD LÓGICA Y ANÁLISIS DE VULNERABILIDADES.

Redes analizadas:

10.2.5.0/24 – CATD-Gómez Palacio
10.2.6.0/24 – CATD-Lerdo
10.2.4.0/24 – CATD-Mapimí

ACTIVIDADES

En los tres CATDs se identificaron los dispositivos activos, se mapeó la topología de la red y se detectaron las posibles vulnerabilidades de seguridad.

El análisis abarcó la totalidad de cada una de las redes especificadas al inicio. Se debe tener en cuenta que el escaneo se llevó a cabo siguiendo buenas prácticas

éticas de acuerdo con las primeras tres fases de la metodología Certified Ethical Hacker y respetando las políticas de seguridad establecidas.

Se proporciono una descripción detallada de los resultados del análisis, incluyendo la lista de hosts encontrados, los puertos abiertos, las posibles vulnerabilidades identificadas y las recomendaciones para mejorar la seguridad de la red.

A través de este análisis, se buscó brindar una comprensión clara de la situación actual de la red y ofrecer sugerencias concretas para fortalecer su seguridad y confiabilidad.

METODOLOGÍA

El análisis de las redes se llevó a cabo utilizando la herramienta Nmap con la finalidad de obtener información detallada sobre los dispositivos y servicios disponibles en la red.

Selección de la red objetivo:

- La red objetivo para CATD-Gómez Palacio fue identificada como 10.2.5.0/24, lo que indica que se escanearon todas las direcciones IP en el rango de 10.2.5.1 a 10.2.5.254.
- La red objetivo para CATD-Lerdo fue identificada como 10.2.6.0/24, lo que indica que se escanearon todas las direcciones IP en el rango de 10.2.6.1 a 10.2.6.254.
- La red objetivo para CATD-Mapimí fue identificada como 10.2.4.0/24, lo que indica que se escanearon todas las direcciones IP en el rango de 10.2.4.1 a 10.2.4.254.

Se utilizó el siguiente comando para realizar el escaneo:

```
sudo nmap -A -sS 10.2.5.0/24
sudo nmap -A -sS 10.2.6.0/24
sudo nmap -A -sS 10.2.4.0/24
```

-A: Este parámetro activa la detección de sistemas operativos, detección de versiones de servicios y detección de scripts de Nmap. Proporciona una recopilación exhaustiva de información sobre los hosts escaneados.

-sS: Especifica el tipo de escaneo a realizar, en este caso, un escaneo de tipo SYN. Este tipo de escaneo envía un paquete SYN al puerto destino y espera una respuesta SYN/ACK. Si recibe esta respuesta, indica que el puerto está abierto.

ANÁLISIS DE LOS RESULTADOS

Una vez completado el escaneo, se analizaron los resultados obtenidos para identificar los dispositivos activos, los puertos abiertos, los sistemas operativos detectados y cualquier posible vulnerabilidad o riesgo de seguridad en la red.

En los tres lugares que se visitaron se pudieron encontrar el mismo tipo de servicios y segmentación de la red de forma independiente, teniendo identificados los servicios de telefonía, videovigilancia, acceso remoto y servicios propios de los equipos en funcionamiento.

Se encontraron algunos servicios web propios de edad telefonía y videovigilancia que al ser accedidos desde el navegador fue posible que contestaran la petición solicitando la información de acceso para la configuración el equipo de análisis procedió a realizar pruebas simples de intrusión utilizando las credenciales por default de los equipos y observando que a todas las peticiones las credenciales fueron rechazadas, lo que indica que dentro de la configuración base de dichos dispositivos se encuentran personalizadas y con una gran seguridad las credenciales de acceso para dichos dispositivos.

Por otro lado, es importante recalcar que durante los análisis en cada uno de los sitios se intentó acceder a sitios genéricos de internet mismos que fueron bloqueados y no fue posible realizar la navegación lo que indica que el control de firewall se encuentra funcionando sin problemas.

RECOMENDACIONES

Los proveedores de internet que se tienen contratados en cada uno de los sitios dejaron un módem con acceso inalámbrico a manera de ruteador, si bien las redes inalámbricas que se pudieron observar están protegidas por contraseña se recomendó que la difusión del nombre de la red sea ocultada para evitar posibles ataques por Fuerza bruta para intentar descifrar las contraseñas.

INFORME DE VISITAS CATD-DURANGO y CATD-GUADALUPE VICTORIA

El día 2 de mayo de 2024 se realizaron las visitas para la verificación del estado de los CATD-DURANGO y CATD-GUADALUPE VICTORIA.
Se realizaron pruebas y análisis de vulnerabilidades, así como de seguridad física y de infraestructura tecnológica.

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

REVISIÓN DE SEGURIDAD FÍSICA E INFRAESTRUCTURA TECNOLÓGICA.

CATD-DURANGO

Observaciones:

- Se realizó la revisión de infraestructura del área cómputo.
- Se cuenta con cableado organizado.
- En el área de cómputo todos los nodos (5) y conexiones de red funcionan correctamente.
- Cuentan con dos proveedores de enlace (ISP), un enlace de Telmex y un enlace de Megacable.
- En cuestión de infraestructura, se cuenta con todo lo necesario como extintores, cámaras, UPS y plantas para el proceso del PREP.
- Se cuenta con sistema de Fail Over y enlaces redundantes con diferentes ISP.
- Se realizaron cortes de energía y los equipos de respaldo funcionaron adecuadamente.
- El edificio cuenta con la señalización adecuada.

Recomendaciones:

- El área de captura no cuenta con ventilación. Se recomendó tomar medidas al respecto.
- Se recomendó adecuar las tomas eléctricas que se pusieron con extensión.
- En general, toda la infraestructura se encuentra en funcionamiento adecuado y óptimo, cumpliendo con los estándares requeridos.

CATD-GUADALUPE VICTORIA

Observaciones:

- Se realizó la revisión de infraestructura del área cómputo.
- Se cuenta con cableado organizado.
- En el área de cómputo todos los nodos (3) y conexiones de red funcionan correctamente.
- Cuentan con dos proveedores de enlace (ISP), un enlace de Telmex y un enlace de Cosmocable.
- En cuestión de infraestructura, se cuenta con todo lo necesario como extintores, cámaras, aire acondicionado para el enfriamiento de los equipos, UPS y plantas para el proceso del PREP.
- Se cuenta con sistema de Fail Over y enlaces redundantes con diferentes ISP.
- Se realizaron cortes de energía y los equipos de respaldo funcionaron adecuadamente.
- El edificio cuenta con la señalización adecuada.

Recomendaciones:

- Uno de los puntos de red no pasó la prueba del Pentascanner. Sin embargo, se sustituyó en el momento.
- En general, toda la infraestructura se encuentra en funcionamiento adecuado y óptimo, cumpliendo con los estándares requeridos.

REVISIÓN DE SEGURIDAD LÓGICA Y ANÁLISIS DE VULNERABILIDADES.

Redes analizadas:

10.2.1.0/24 – CATD-DURANGO
10.2.3.0/24 – CATD-GUADALUPE VICTORIA

ACTIVIDADES

En los dos CATDs se identificaron los dispositivos activos, se mapeó la topología de la red y se detectaron las posibles vulnerabilidades de seguridad.

El análisis abarcó la totalidad de cada una de las redes especificadas al inicio. Se debe tener en cuenta que el escaneo se llevó a cabo siguiendo buenas prácticas éticas de acuerdo con las primeras tres fases de la metodología Certified Ethical Hacker y respetando las políticas de seguridad establecidas.

Se proporciono una descripción detallada de los resultados del análisis, incluyendo la lista de hosts encontrados, los puertos abiertos, las posibles vulnerabilidades identificadas y las recomendaciones para mejorar la seguridad de la red.

A través de este análisis, se buscó brindar una comprensión clara de la situación actual de la red y ofrecer sugerencias concretas para fortalecer su seguridad y confiabilidad.

METODOLOGÍA

El análisis de las redes se llevó a cabo utilizando la herramienta Nmap con la finalidad de obtener información detallada sobre los dispositivos y servicios disponibles en la red.

Selección de la red objetivo:

- La red objetivo para CATD-DURANGO fue identificada como 10.2.1.0/24, lo que indica que se escanearon todas las direcciones IP en el rango de 10.2.1.1 a 10.2.1.254.

- La red objetivo para CATD-GUADALUPE VICTORIA fue identificada como 10.2.3.0/24, lo que indica que se escanearon todas las direcciones IP en el rango de 10.2.3.1 a 10.2.3.254.

Se utilizó el siguiente comando para realizar el escaneo:

sudo nmap -A -sS 10.2.1.0/24
sudo nmap -A -sS 10.2.3.0/24

-A: Este parámetro activa la detección de sistemas operativos, detección de versiones de servicios y detección de scripts de Nmap. Proporciona una recopilación exhaustiva de información sobre los hosts escaneados.

-sS: Especifica el tipo de escaneo a realizar, en este caso, un escaneo de tipo SYN. Este tipo de escaneo envía un paquete SYN al puerto destino y espera una respuesta SYN/ACK. Si recibe esta respuesta, indica que el puerto está abierto.

ANÁLISIS DE LOS RESULTADOS

Una vez completado el escaneo, se analizaron los resultados obtenidos para identificar los dispositivos activos, los puertos abiertos, los sistemas operativos detectados y cualquier posible vulnerabilidad o riesgo de seguridad en la red.

En los dos lugares que se visitaron se pudieron encontrar el mismo tipo de servicios y segmentación de la red de forma independiente, teniendo identificados los servicios de telefonía, videovigilancia, acceso remoto y servicios propios de los equipos en funcionamiento. Sin embargo, en el CATD-GUADALUPE VICTORIA uno de los switches no estaba en funcionamiento por lo que no se pudieron hacer las pruebas completas sobre todos los dispositivos principalmente las cámaras ya que en ese switch es donde se encontraban conectadas las mismas.

Se encontraron algunos servicios web propios de edad telefonía y videovigilancia que al ser accedidos desde el navegador fue posible que contestaran la petición solicitando la información de acceso para la configuración el equipo de análisis procedió a realizar pruebas simples de intrusión utilizando las credenciales por

default de los equipos y observando que a todas las peticiones las credenciales fueron rechazadas, lo que indica que dentro de la configuración base de dichos dispositivos se encuentran personalizadas y con una gran seguridad las credenciales de acceso para dichos dispositivos.

Por otro lado, es importante recalcar que durante los análisis en cada uno de los sitios se intentó acceder a sitios genéricos de internet mismos que fueron bloqueados y no fue posible realizar la navegación lo que indica que el control de firewall se encuentra funcionando sin problemas.

Al momento de realizar las pruebas se intentó acceder a los servicios propios del sistema operativo y en estos casos sí fue posible acceder a la consola de comandos.

RECOMENDACIONES

Los proveedores de internet que se tienen contratados en cada uno de los sitios dejaron un módem con acceso inalámbrico a manera de ruteador, si bien las redes inalámbricas que se pudieron observar están protegidas por contraseña se recomendó que la difusión del nombre de la red sea ocultada para evitar posibles ataques por Fuerza bruta para intentar descifrar las contraseñas.

Se recomendó un barrido a todos y cada uno de los equipos para garantizar que los servicios del sistema estén bloqueados, que no puedan ser accedidos de ninguna manera por parte de los usuarios, si bien se nos indicó que estas acciones eran debido a una actualización de controladores, el que los equipos se encuentren en este estado supone un problema de seguridad, de igual manera el reemplazo del switch en el CATD-GUADALUPE VICTORIA es necesario.

INFORME DE EJERCICIO DDoS

El día 7 de mayo de 2024 se llevó a cabo un ataque de denegación de servicio distribuido (DDoS) al sitio web del Programa de Resultados Electorales Preliminares (PREP) y al sitio web del Instituto Electoral y de Participación Ciudadana del estado de Durango, este proceso se realizó utilizando herramientas de código libre que permiten a un solo usuario simular múltiples

conexiones simultáneas al mismo lugar causando un “estrés” al servidor lo que permite saber el comportamiento del mismo con una carga mucho mayor a la esperada durante el ejercicio electoral.

El ejercicio contó con la participación de 45 personas distribuidas en diferentes partes de la República Mexicana. Cada participante simuló una carga de 6000 solicitudes por segundo. El objetivo principal fue evaluar la resistencia y capacidad de respuesta de los servidores de publicación ante un ataque DDoS.

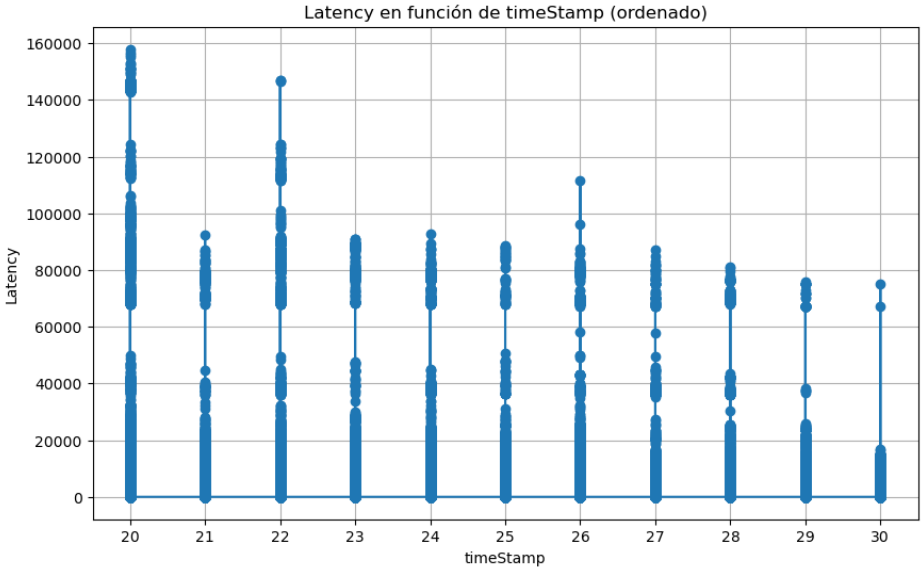
METODOLOGÍA

Cada participante simuló una carga de 6000 solicitudes por segundo hacia los servidores de la publicación durante 10 minutos, tras el paso de 1 minuto cada participante incrementó a 7000 solicitudes por segundo durante 2 minutos, al término de ese tiempo se regresaron a las 6000 solicitudes por segundo originales, este mismo proceso se llevó a cabo al minuto 6 del ejercicio. Se usó la herramienta Apache Jmeter (https://jmeter.apache.org/) configurada previamente para simular el tráfico https hacia el sitio de publicación y permitiendo así recuperar estadísticas de la simulación.

RESULTADOS

Durante el ejercicio, se observó un aumento significativo en el tráfico hacia los servidores. Este aumento fue consistente con un ataque DDoS coordinado. Los sistemas de monitoreo detectaron el incremento en el tráfico y se activaron los protocolos de respuesta ante incidentes deteniendo la mayor parte del tráfico "malicioso" y solo observándose un incremento en los tiempos de respuesta por parte del sistema, sin embargo, no se produjo una interrupción completa del servicio.

INCREMENTO DE LATENCIA DURANTE EL EJERCICIO



Esta gráfica muestra cómo varió el tiempo de conexión (Con) en función del tiempo (tS) durante la ejecución del ejercicio HTTP. La marca de tiempo indica cuándo se realizó cada solicitud, y la conexión representa el tiempo transcurrido entre el envío de la solicitud y la recepción de la respuesta.

Interpretación: Si la gráfica tiene picos o fluctuaciones significativas, podría indicar momentos de congestión en el servidor o variaciones en la velocidad de la red.

Los valores de tS mostrados en la gráfica corresponden al minuto específico del ejercicio. Por ejemplo 20, corresponde a las 10:20 am del 7 de mayo de 2024

CONCLUSIONES

Se puedo observar que el nivel de protección con los que cuentan los servidores puede soportar una cantidad considerable de solicitudes sin perder conexión, pero reduciendo tiempos de respuesta. Para este ejercicio se llevaron a cabo un total aproximado de 172,800,000 solicitudes en un lapso de 10 minutos de las cuales, la gran mayoría fueron rechazadas por los servicios de seguridad.

RECOMENDACIONES

Al observar y analizar los resultados anteriores se puede tener un gran nivel de certeza en que la protección se encuentra activa, sin embargo, se recomendó tener monitores que supervisen durante la jornada electoral, y que se encuentren valorando las posibles amenazas, y en determinado momento, de ser necesario, poder llevar a cabo un bloqueo directo de los atacantes en forma manual para salvaguardar la disponibilidad del sitio web del PREP.

PRIMER SIMULACRO OFICIAL

El día 12 de mayo de 2024 se llevó a cabo el primer simulacro del Programa de Resultados Electorales Preliminares (PREP).

OBJETIVOS DEL DÍA

- Supervisar y mantener la publicación de actas digitalizadas y capturadas
- Visualizar como se resuelven las posibles contingencias que pueden ocurrir durante la jornada.
- Asegurar la digitalización y publicación del 100% de las actas esperadas.

CONTINGENCIAS PLANIFICADAS Y RESOLUCIÓN

Durante la jornada, se planificaron y ejecutaron tres contingencias críticas para evaluar la capacidad de respuesta del equipo y la resiliencia del sistema.

Falla completa de scanner en Gómez Palacio
Resultado: La contingencia se resolvió eficazmente, manteniendo la continuidad de las operaciones.

Corte de señal del proveedor principal de internet en El Salto
Resultado: La contingencia se manejó con éxito, sin interrupciones significativas en las operaciones.

Falla completa de equipo en Durango
Resultado: La contingencia se gestionó sin inconvenientes, asegurando la operatividad continua.

RESULTADOS Y LOGROS

- Todas las actividades planificadas se llevaron a cabo exitosamente.
- Las contingencias se gestionaron conforme a los protocolos establecidos, demostrando la capacidad de respuesta y la resiliencia del sistema.
- Se logró la digitalización y publicación del 100% de las actas a las 16:15 horas.

DESAFÍOS Y PROBLEMAS

- No se presentaron desafíos o problemas fuera de las contingencias planificadas.
- La coordinación y comunicación entre los equipos fue efectiva.
- Posterior a la digitalización y publicación del 100% de las actas se procedió a dar por terminado el simulacro.

CONCLUSIONES DEL PRIMER SIMULACRO

Se pudo observar que trascurrió sin incidentes que reportar, y se capturo el 100 por ciento de las actas computadas.

SEGUNDO SIMULACRO OFICIAL

El día 19 de mayo de 2024 se llevó a cabo el segundo simulacro del Programa de Resultados Electorales Preliminares (PREP).

OBJETIVOS DEL DÍA

- Supervisar y mantener la publicación de actas digitalizadas y capturadas
- Visualizar como se resuelven las posibles contingencias que pueden ocurrir durante la jornada.
- Asegurar la digitalización y publicación del 100% de las actas esperadas.
- Presentación y demostración de la aplicación PREPCasilla.
- Ejercicio de toma de Hashes en preparación al tercer simulacro.

CONTINGENCIAS PLANIFICADAS Y RESOLUCIÓN

Durante la jornada, se planificaron y ejecutaron tres contingencias críticas para evaluar la capacidad de respuesta del equipo y la resiliencia del sistema.

Pérdida de energía eléctrica en Guadalupe Victoria
Resultado: Durante esta simulación, el equipo practicó los protocolos establecidos para restablecer el funcionamiento utilizando generadores portátiles y otros recursos de respaldo.

Cabe hacer mención que durante este proceso se observó que algunos equipos no se encontraban protegidos por los UPS temporales, por lo que el proceso se vio interrumpido por un par de minutos en lo que el equipo de soporte encendía la planta eléctrica y realizaba el puente eléctrico usando las extensiones con las que contaba previamente.

Pérdida del enlace principal de internet en Guadalupe Victoria
Resultado: Los asistentes practicaron los procedimientos de conmutación a enlaces de respaldo y la utilización de conexiones alternativas para asegurar la continuidad en la transmisión de datos.

Pérdida de comunicación con un servidor de publicación
Resultado: Esta situación fue manejada sin repercusiones en el proceso, ya que los sistemas de "respaldo" o clúster funcionaron adecuadamente y los capturistas no tuvieron ningún impacto.

Pérdida del enlace principal de internet
Resultado: Los sistemas de respaldo se activaron de manera eficaz, y la continuidad del proceso se mantuvo sin problemas para los capturistas.

Pérdida del firewall primario
Resultado: Este escenario también fue manejado exitosamente con los sistemas de respaldo, garantizando que el proceso continuara de forma transparente para los capturistas.

CONTINGENCIAS CRÍTICAS NO PLANEADAS

Fallo en la aplicación PREPCasilla en Guadalupe Victoria
Algunos usuarios envían actas mal digitalizadas lo cual experimentaron fallos en la captura.

Fallo en el servicio Docker en Guadalupe Victoria
Durante el transcurso de la visita, se detectó que no se distribuyeron las digitalizaciones de actas hacia los capturistas, la empresa Informática Electoral informó que fue debido a que un servicio Docker no fue activado de forma automática antes del simulacro. El equipo de informática electoral detectó el problema y lo solucionó. Según informó el equipo, se tomaron medidas para que el inicio de los servicios sea de forma automática y esta contingencia no vuelva a ocurrir.

PRESENTACIÓN Y DEMOSTRACIÓN DE LA APLICACIÓN PREPCasilla
Dentro de las actividades de este día se llevó a cabo una presentación detallada sobre el uso de la aplicación PREPCasilla. Se mostraron las características principales de la aplicación, destacando su interfaz intuitiva y los pasos a seguir para capturar las actas correctamente.

OBSERVACIÓN DEL PROCESO DE PUBLICACIÓN EN EL IEPC
Durante el simulacro se observó que el proceso de publicación de actas capturadas no tenía la fluidez esperada. Se procedió a preguntar a la encargada de la empresa de informática electoral las razones detrás de este problema, surgiendo varias contingencias no planeadas en Mapimí.

PROBLEMAS IDENTIFICADOS
Manejo Incorrecto del Escáner
Se detectó que el manejo del escáner no era el correcto por parte de los digitalizadores, lo cual afectaba la calidad y velocidad de la digitalización de actas.

Conexión a Internet Inadecuada
La conexión a internet en Mapimí no era la adecuada, lo que dificultaba la transmisión rápida y efectiva de los datos digitalizados.

Comunicación Deficiente entre Personal Técnico y Operativo
La comunicación entre el personal técnico y el personal operativo no era eficiente, lo que causaba retrasos y errores en el proceso.

Monitoreo Insuficiente por Parte de la Empresa
Se observó que el monitoreo por parte de la empresa hacia cada uno de los CATD no era adecuado, lo que impedía una respuesta rápida a los problemas que surgían.

OBSERVACIONES ADICIONALES

Se observó que la infraestructura técnica que ofrece la empresa de informática electoral ha sido probada y verificada, pero los procesos de índole humano necesitan ser verificados y documentados adecuadamente para evitar problemas el día de la jornada electoral. Se recomendó que se realicen simulaciones adicionales y se proporcionen capacitaciones específicas para asegurar que todos los involucrados comprendan y manejen correctamente sus tareas.

PUBLICACIÓN DE ACTAS

Después de identificar el problema de comunicación y la velocidad de internet en Mapimí, se observó que el proceso de publicación de actas fue considerablemente afectado en términos de tiempo, con un promedio de 10 actas publicadas en cada corte. A pesar de estos retrasos, el proceso concluyó exitosamente con el 100% de las actas capturadas y .

CONCLUSIONES Y RECOMENDACIONES DEL SEGUNDO SIMULACRO

RECOMENDACIONES

Implementación de una lista de verificación
Se recomendó la implementación de una lista de verificación durante los simulacros, y durante la jornada electoral, para revisar cada uno de los procesos críticos que puedan afectar los procesos y la publicación de resultados. Esta lista de verificación deberá incluir la validación y verificación de servicios como Docker, enlaces de Internet, y suministro eléctrico, entre otros.

Capacitación Adicional para Digitalizadores
Recomendación: Proporcionar capacitación adicional a los digitalizadores en el manejo correcto del escáner para mejorar la eficiencia y calidad de la digitalización de actas.

Mejorar la Infraestructura de Internet
Recomendación: Asegurar que las conexiones a internet en todos los CATD, especialmente en Mapimí, sean adecuadas y estables.

Fortalecer la Comunicación
Recomendación: Mejorar la comunicación entre el personal técnico y operativo para asegurar que los problemas sean identificados y resueltos rápidamente.
Monitoreo Proactivo
Recomendación: Implementar un sistema de monitoreo más proactivo y efectivo por parte de la empresa de informática electoral para cada uno de los CATD.

Documentación de Procesos Humanos
Recomendación: Verificar y documentar adecuadamente todos los procesos de índole humano para prevenir errores y mejorar la eficiencia operativa el día de la jornada electoral.

CONCLUSIONES

Si bien se observaron incidentes reportados se logró la captura del 100 por ciento de las actas computadas. Con base en las observaciones y recomendaciones emitidas se esperó que no se presenten los incidentes anteriores en el tercer simulacro.

TERCER SIMULACRO OFICIAL

El día 26 de mayo de 2024 se llevó a cabo el tercer simulacro del Programa de Resultados Electorales Preliminares (PREP).

OBJETIVOS DEL DÍA

- Supervisar y mantener la publicación de actas digitalizadas y capturadas

- Visualizar como se resuelven las posibles contingencias que pueden ocurrir durante la jornada.
- Verificar que no se presenten las incidencias de los simulacros anteriores.
- Asegurar la digitalización y publicación del 100% de las actas esperadas.

CONTINGENCIAS PLANIFICADAS Y RESOLUCIÓN

Durante la jornada, se planificaron y ejecutaron cinco contingencias críticas para evaluar la capacidad de respuesta del equipo y la resiliencia del sistema.

Comunicación Vía Telefónica con CATDs

Resultado: La contingencia se resolvió eficazmente, se realizaron una serie de llamadas telefónicas a distintos CATD para asegurar que la comunicación entre el CCV Principal y estos centros es fluida y sin interrupciones. Durante estas llamadas, se verificó que el personal estuviera informado sobre los procedimientos a seguir y que contaran con los recursos necesarios para la transmisión de datos. Esta actividad es crucial para garantizar que, en caso de cualquier incidente o emergencia, la comunicación no se vea comprometida.

Verificación del Personal Técnico en los CATDs

Resultado: La contingencia se manejó con éxito, se realizó una verificación del personal técnico en los CATD para confirmar que el personal técnico asignado estuvieran presentes y listos para responder ante cualquier eventualidad. Esta verificación es esencial para garantizar que haya suficiente personal capacitado para manejar cualquier problema técnico que pueda surgir durante la jornada electoral.

Simulacro de Incendio en los CATDs

Resultado: La contingencia se gestionó sin inconvenientes, asegurando la operatividad continua. Se llevó a cabo un simulacro de incendio en los CATD para evaluar la capacidad de respuesta del personal ante una situación de emergencia. Este simulacro incluyó la activación de alarmas contra incendios, la evacuación ordenada del personal y el pase de lista de todos los integrantes fuera de las instalaciones, para retornar posteriormente a las actividades normales.

Simulacro de Falla en la Red Eléctrica en CCV Principal
Resultado: La contingencia se resolvió eficazmente. Se simuló una falla en la red eléctrica para evaluar la respuesta del sistema y del personal técnico. Se verificó el correcto funcionamiento de la planta eléctrica de respaldo, asegurándose de que se activará automáticamente dentro de los tiempos especificados para proporcionar energía que mantenga las operaciones sin interrupciones.

En esta contingencia se detectó que tres equipos de captura que se apagaron durante la interrupción eléctrica lo que indica que las baterías de las laptops están fallando o dañadas, pero después que se restableció la energía eléctrica por medio de la planta eléctrica de respaldo pueden continuar con la captura.

Simulacro de Incendio en el CCV Principal
Resultado: La contingencia se gestionó sin inconvenientes, asegurando la operatividad continua. Se llevó a cabo un simulacro de incendio, similar al realizado en los CATDs, en las instalaciones del CCV Principal. Este ejercicio incluyó la activación del sistema de alarma, la evacuación ordenada del edificio y el pase de lista de todos los integrantes fuera de las instalaciones, para retornar posteriormente a las actividades normales, adicionalmente se revisaron también las rutas de evacuación y puntos de reunión. El objetivo fue evaluar la rapidez y eficacia de la respuesta del personal.

RESULTADOS Y LOGROS

- Todas las actividades planificadas se llevaron a cabo exitosamente.
- Las contingencias se gestionaron conforme a los protocolos establecidos, demostrando la capacidad de respuesta y la resiliencia del sistema.
- Se logró la digitalización y publicación del 100% de las actas.

DESAFÍOS Y PROBLEMAS

- No se presentaron desafíos o problemas fuera de las contingencias planificadas.
- La coordinación y comunicación entre los equipos fue efectiva.
- Posterior a la digitalización y publicación del 100% de las actas se procedió a dar por terminado el simulacro.

PRIMER TOMA DE HASH

Dentro de las actividades realizadas en el tercer simulacro se tomó la primera serie de hash del sistema PREP, esta actividad se realizo en presencia del notario público Lic. Sergio Eduardo Gutiérrez Maldonado. En colaboración entre el ente auditor y el personal técnico de la empresa Informática Electoral, se explicó detalladamente a los presentes el procedimiento de generación e importancia de los hashes. Los archivos que contienen los hashes del sistema PREP generados en esta actividad se almacenaron en una memoria USB, misma que queda a resguardo del Lic. Gutiérrez Maldonado.

Estos hashes se compararán con los que se tomarán en los siguientes dos momentos, mismos que al final se compararán y deberán coincidir.

Hash del sistema PREP obtenido el día 26 de mayo de 2024:
bb7e727bb54c9f08908f6391e7f5c9d81dfca6f718df8ea885bc1abf0176c93d

CONCLUSIONES DEL TERCER SIMULACRO

Se pudo observar que transcurrió sin incidentes que reportar, haciendo mención especial de que se atendieron las observaciones y recomendaciones de los simulacros anteriores, y se capturó el 100 por ciento de las actas computadas dentro de los tiempos planeados. Y se llevo exitosamente la toma de hashes al sistema PREP.

CONCLUSIONES GENERALES.

El proceso de auditoria se realizó exitosamente, todas las fases y compromisos se cumplieron con base en lo estipulado en el convenio y en las reuniones de trabajo, lo que permite garantizar que las condiciones técnicas y de seguridad del sistema PREP, permitirán un proceso con la transparencia y buen funcionamiento de índole técnico, haciendo especial mención por el apoyo brindado por el IEPC de Durango para poder llevar a cabo exitosamente la presente auditoria.