UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MORELOS

COORDINACIÓN GENERAL DE PLANEACIÓN Y ADMINISTRACIÓN

DIRECCIÓN DE DESARROLLO DE TECNOLOGÍAS

INFORME DE FINAL DE AUDITORIA AL SISTEMA INFORMÁTICO E INFRAESTRUCTURA TECNOLÓGICA DEL PREP-MORELOS 2018

29 de junio 2018

impepac
Instituto Morelense
de Procesos Electorales
y Participación Ciudadana

Tabla de contenido

GLOSARIO

Acopiador: El personal que se disponga para recibir el Sobre PREP, en los Consejos Municipales Electorales.

Acta-PREP: primera copia del acta de escrutinio y cómputo destinada para el PREP o, en ausencia de ésta, cualquier otra copia del acta escrutinio y cómputo.

AEC: Acta de Escrutinio y Cómputo de casilla.

Asistente Electoral Municipal: Ciudadanos que designe el Consejo Estatal Electoral de EL IMPEPAC, y cuyas funciones serán entre otras, apoyar a los Consejos Municipales Electorales en actividades relacionadas con el proceso electoral, y en específico con el PREP.

Base de Datos: Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

BOTS: Bot es la palabra robot acortada. Se refiere a un tipo de programa informático autónomo que es capaz de llevar a cabo tareas concretas e imitar el comportamiento humano.

CAE: (Capacitador Asistente-Electoral Local) Ciudadano que designe el Consejo General de EL IMPEPAC, y cuyas funciones serán, entre otras, tomar la imagen del Acta de Escrutinio y Cómputo en la casilla (PREP-Casilla) y enviarla para su procesamiento en el CATD.

Capturista: El personal que, una vez acopiada y digitalizada una Acta-PREP, se disponga para realizar la captura de los datos plasmados el acta por medio del sistema informático creado para tal fin.

CATD: Centro de Acopio y Transmisión de Datos.

CCTV: Circuito Cerrado de Televisión.

CCV: Centro de Captura y Verificación.

CLOUDFLARE: Es una empresa estadounidense que proporciona una red de entrega de contenido, servicios de seguridad de internet y servicios de servidores de nombres de dominio distribuidos, localizados entre el visitante y el proveedor de alojamiento del usuario de Cloudflare, y que actúan como proxy inverso para sitios web.

Código QR: Estampado bidimensional que almacena de forma codificada la información que permite identificar, a través de medios electrónicos, la casilla a la que está asociada el Acta-PREP.

Control de Acceso Biométrico: Es un sistema de identificación basado en cualidades biológicas (huella dactilar, facial, ocular, etc.).

COPREP: Centro de Operaciones del Programa de Resultados Electorales Preliminares.

DDOS: Ataque de Denegación de Servicio.

Digitalizado: El personal que se disponga para realizar la digitalización de la imagen del Acta-PREP en el CATD y la incorpore al sistema informático.

DNS: Servidor de Nombres de Dominio (DNS).

DVR: Digital Video Recorder.

Ethernet: Es la tecnología de red de área local más ampliamente instalada.

Firewall: Es un programa informático que controla el acceso de una computadora o dispositivo a la red y de elementos de la red a la computadora, por motivos de seguridad.

Hosting Alojamiento Web: Es el servicio que provee a los usuarios de internet un sistema para poder almacenar información, imágenes, vídeo o cualquier contenido accesible vía web.

HTTP: Hypertext Transfer Protocol.

ICMP: Por sus siglas en inglés Internet Control Message Protocol, Protocolo de Mensajes de Control de Internet y notificación de errores del protocolo de internet (IP).

ICMP FLOOD: El Protocolo de mensajes de control de Internet (ICMP) es un protocolo sin conexión utilizado para operaciones IP, diagnósticos y errores. Un ataque Flood ICMP

Identificador SHA: Identificador único asociado al archivo de cada Acta-PREP digitalizada, que consta de una cadena de caracteres que representa de manera única a cada imagen y que es generado mediante el estándar criptográfico denominado “SHA256”.

IMPEPAC: Instituto Morelense de Procesos Electorales y Participación Ciudadana.

INE: Instituto Nacional Electoral.

Inicialización: Proceso informático mediante el cual se asegura que NO existan datos en la base de sistema informático del PREP.

IP: Es un protocolo de comunicación de datos digitales clasificado funcionalmente en la capa de red según el modelo internacional OSI.

ISP: Proveedor de Servicios de Internet.

LAN: Red de Área Local.

Load testing: Las pruebas de carga generalmente se refieren a la práctica de modelar el uso esperado de un programa de software simulando múltiples usuarios que acceden al programa al mismo tiempo y se suele medir en términos de tiempos de respuesta. SLA.

Mac Adress: También conocida como Dirección Física, es un identificador de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red.

Mbps: Es la sigla con la cual popularmente se designa el concepto de Megabit por segundo.

NOC: Centro de Operaciones de Red.

PDU: Unidad de Distribución de Energía para redes y centros de datos.

PREP: Programa de Resultados Electorales Preliminares.

PREP-Casilla: Mecanismo que tiene como propósito sacar una imagen del Acta-PREP dentro de la casilla y enviarla al CATD mediante una aplicación de software que opere en un celular (aplicación móvil), para que se proceda y agilice la captura, verificación y publicación de los resultados.

PROVEEDOR: Tercero que se haya contratado para la implementación del PREP-Morelos.

Servidor: Es un equipo de cómputo dedicado con una aplicación en ejecución capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

SIP: Session Initiation Protocol.

SLA: (Service Level Aggrement) Medida usada para cuantificar el rendimiento del sistema probado en términos de tiempos de respuesta promedio.

SLOWLORIS ATTACK: Desarrollado por Robert " RSnake " Hansen, Slowloris es un software de ataque DDoS que permite que una sola computadora derribe un servidor web. Debido a la naturaleza simple pero elegante de este ataque, requiere un ancho de banda mínimo para implementar y afecta solo al servidor web del servidor de destino, sin casi efectos secundarios en otros servicios y puertos.

SNMP: Protocolo Simple de Administración de Red, es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

Sobre-PREP: Sobre diseñado especialmente para cada proceso electoral en el que se guarda la copia del AEC de la casilla, y se coloca por fuera del paquete electoral.

SOC: Centro de Operaciones de Seguridad.

SSL: Secure Sockets Layer.

ST: Sello que se imprimirá en el Acta-PREP con la información de Fecha y Hora de acopio.

Supervisor/Coordinador: El personal que se designe para asegurar la operación correcta del CATD.

Switch: Es un dispositivo de interconexión utilizado para conectar equipos en red formando una red LAN y resolver problemas de rendimiento en la red.

SYN FLOOD: Una inundación SYN (SYN flooding) es un método que el usuario de un programa cliente hostil puede utilizar para llevar a cabo un ataque de denegación de servicio (DoS) en un servidor informático. El cliente hostil envía repetidamente paquetes SYN (sincronización) a cada puerto en el servidor, usando direcciones IP falsas.

TCP: Protocolo de Control de Transmisión.

Througput: Es la capacidad efectiva de transferencia de datos sobre el enlace.

TIER: Nivel de certificación.

UAEM: Universidad Autónoma del Estado de Morelos.

UDP: User Datagram Protocol.

Verificador/Publicador: El personal que tendrá como objetivo validar los datos capturados en el sistema informático, incluidos los de identificación del Acta-PREP, y confirmar que coincidan con la información plasmada en el Acta digitalizada. Una vez realizada la verificación, podrá llevar a cabo la publicación.

VPN: Red Privada Virtual, permite una extensión segura de la LAN sobre una red pública o no controlada como internet.

WAF: Web Application Firewall.

KEYLOGGER: Un keylogger es un software o hardware que puede interceptar y guardar las pulsaciones realizadas en el teclado de un equipo que haya sido infectado.

ROOTKIT: Rootkit es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema.

LOGS: Registros de actividad de un sistema.

ANTECEDENTES

UAEM

El 25 de diciembre de 1938 se fundó el Instituto de Estudios Superiores del Estado de Morelos, para transformarse el 7 de abril de 1953 en la Universidad del Estado de Morelos, adoptando el lema "Por una humanidad culta".

La UAEM es un organismo público autónomo del Estado de Morelos con plenas facultades de gestión y control presupuestal, personalidad jurídica y patrimonio propios cuyos fines son la prestación de servicios públicos de educación de los tipos medio superior y superior, de investigación, de difusión de la cultura y extensión de los servicios. Para lo cual la Dirección de Desarrollo de Tecnologías es el área encargada de evaluar, diseñar, implementar y mantener disponibles y funcionales los sistemas, así como los servicios de tecnologías de la información y comunicación en la Institución.

IMPEPAC

En febrero de 2014 inició la reforma política más reciente en México que contempla la creación de una nueva estructura electoral nacional; que dé mayor certidumbre, transparencia y estabilidad a la competencia en las votaciones de las consultas populares.
De acuerdo con el compromiso 89 del Pacto por México, está transformación dará más homogeneidad a los estándares de calidad y eficiencia con que se realizan los procesos electorales del país.
Por primera vez, después de concretar la transformación del órgano nacional denominado ahora Instituto Nacional Electoral (INE), se lanzó la convocatoria abierta en los Estados que tendrían elecciones concurrentes en 2015 para elegir consejeros electorales de órganos locales que se integraron para organizar los procesos de votación en cada Entidad del País.
Así, surgió el nuevo Instituto Morelense de Procesos Electorales y Participación Ciudadana (IMPEPEAC); en sustitución del Instituto Estatal Electoral (IEE) que en Morelos condujo los procesos electorales durante 17 años.

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

Así mismo, como lo establece el Reglamento de Elecciones y su Anexo 13, el Sistema que se utilizará para la operación del PREP tendrá que ser auditado. Para ello, EL IMPEPAC celebro el durante el mes de mayo del 2018 un instrumento legal con la Universidad Autónoma del Estado de Morelos - UAEM como ente auditor con el propósito de desarrollar un proyecto de Auditoría en materia de Tecnologías de Información y Comunicaciones al PREP.

ALCANCE

El presente documento aplica para el PREP (Programa de Resultados Electorales Preliminares) del IMPEPAC (Instituto Morelense de Procesos Electorales y Participación Ciudadana) para el informe final de auditoría externa de su Sistema Informático e Infraestructura Tecnológica en sus módulos de: digitalización, captura, verificación y publicación de resultados.

Es importante mencionar que el presente informe de auditoría es realizado conforme los lineamientos del anexo técnico para la contratación de servicios de auditoría al sistema informático y a la infraestructura tecnológica del Programa de Resultados Electorales Preliminares del Instituto Morelense de Procesos Electorales y Participación Ciudadana (IMPEPAC).

OBJETIVO GENERAL

El objetivo de la auditoría realizada es evaluar la integridad en el procesamiento de la información y la generación de resultados. El presente reporte auditoría incluye las pruebas realizadas durante los simulacros realizados los **días 8, 10, 15, 17, 22 y 24 de junio** del 2018, incluyendo los sistemas, bases de datos y la infraestructura informática (eléctrico, telecomunicaciones, servidores y computo) que se utiliza en el desarrollo del PREP. Esta actividad se desarrolló en los sitios COPREP/CCV y los descritos en la tabla inferior:

Consejo Municipal/CATD	
0	Cuernavaca
1	Amacuzac
2	Atlatlahucan
3	Axochiapan
4	Ayala
5	Coatlán del Río
6	Cuautla
7	Cuernavaca
8	Emiliano Zapata
9	Huitzilac
10	Jantetelco
11	Jiutepec
12	Jojutla
13	Jonacatepec
14	Mazatepec
15	Miacatlán
16	Ocuituco
17	Puente de Ixtla
18	Temixco
19	Tepalcingo
20	Tepoztlán
21	Tetecala
22	Tetela del Volcán
23	Tlalnepantla
24	Tlaltizapán
25	Tlaquiltenango
26	Tlayacapan
27	Totolapan
28	Xochitepec
29	Yautepec
30	Yecapixtla
31	Zacatepec
32	Zacualpan
33	Temoac

OBJETIVOS ESPECIFICOS Y LÍNEAS DE TRABAJO PARA LA PRESENTE AUDITORIA SE LISTAN EN LA PARTE INFERIOR:

1. Pruebas funcionales de caja negra al sistema informático del PREP-Morelos 2018.
2. Validación del sistema informático del PREP y de sus bases de datos.
3. Análisis de vulnerabilidades a la infraestructura tecnológica.
4. Pruebas de negación de servicio al sitio Web de publicación del PREP y a la página de EL IMPEPAC, ya sea en su propia infraestructura o en la que provea un tercero que lo apoye en la implementación del PREP.

Debido a lo antes mencionado se hace del conocimiento del IMPEPAC el informe final de auditoría al sistema informático e infraestructura tecnológica del PREP – Morelos 2018, lo anterior con el objetivo de su análisis, evaluación de la factibilidad de atención y se determinen las acciones para seguimiento de las observaciones presentadas.

Derivado del presente reporte la empresa Informática electoral y el IMPEPAC deberán analizar y evaluar la factibilidad de atención de las observaciones y hallazgos reportados en el presente documento.

Se anexa al presente documento los cronogramas de avance de actividades actualizados al 28 de junio del 2018 (ver anexos 1, 2, 3, 4 y 5).

METODOLOGIA

La presente metodología está desarrollada bajo los criterios y normatividad listada:

PCI Security Standards Council.

NIST - Instituto Nacional de Estándares y Tecnología.

Norma ISO/IEC 27001 Seguridad informática y seguridad de la información.

Norma mexica de Centro de Datos NMX- C -J - I- 489 - ONNCCE - ANCE - NYCE- 2013.

NMX-I-248-NYCE-2008, (Especificaciones de Desempeño de Transmisión para Cableado – Norma Mexicana).

IEEE std 1028-2008 “IEEE Standar for Software Reviews and Audits”.

OSSTM – ISECOM (Manual de la Metodología Abierta de Testeo de Seguridad).

ISO/IEC 11801 – Estándar Internacional de Cableado genérico.

ANSI/TIA/EIA-568-C.2 (Especificaciones de Desempeño de Transmisión para Cableado UTP Categoría 6).

ANSI/TIA/EIA-569-B (Espacios y Canalizaciones de Telecomunicaciones).

ANSI/TIA/EIA-606-A (Norma de Administración para Telecomunicaciones/Infraestructuras).

ICREA-Std-131-2007 (Norma Internacional para la construcción de centros de procesamiento de datos, clima, UPS, Tierra física, etc).

NOM001-SEDE-2012, (Instalaciones Eléctricas (utilización) – Norma Oficial Mexicana).

ANSI-J-STD-607-A (Requisitos para telecomunicaciones de puesta a tierra).

NMX-J-549-ANCE-2005. Protección contra tormentas eléctricas

OWASP Top 10 es un documento de los diez riesgos de seguridad más importantes en aplicaciones web según la organización OWASP (en inglés Open Web Application Security Project, en español Proyecto Abierto de Seguridad de Aplicaciones Web). Esta lista se publica y actualiza cada tres años por dicha organización.

RESULTADOS DE LA AUDITORIA

Al ser este documento de naturaleza pública, se omiten datos específicos como pantallas del sistema, pruebas particulares realizadas, direcciones de internet (IP), versiones de software, listado de hardware, listas de verificación, imágenes, fotografías y cualquier otro dato técnico que pudiese comprometer la seguridad y la integridad los sistemas de información, infraestructura de telecomunicaciones, servidores, bases de datos y aplicaciones del PREP Morelos 2018.

Los detalles técnicos se describen en los reportes parciales de auditoria proporcionados al IMPEPAC en fechas descritas en la parte inferior:

1. Primer informe de auditoría – 12 de junio del 2018.
2. Segundo informe de auditoría - 19 de junio del 2018.
3. Tercer informe de auditoría - 26 de junio del 2018.

Las pruebas realizadas en la presente auditoria se realizaron previo, durante y posterior a las fechas de simulacros estatales y nacionales.

Durante las fechas de realización de la presente auditoria, el equipo de auditor se abstuvo de:

- Instalar cualquier tipo de puerta trasera o aplicación que permita acceso remoto encubierto.
- Instalar cualquier tipo de software malicioso como boot, keylogger rootkit, o tecnología similar.
- Software que pudiera comprometer la seguridad e integridad del PREP.
- Borrar, alterar o apagar el uso de bitácoras (logs) en cualquier dispositivo, estación de trabajo o servidor.
- Modificar la configuración de servidores, estaciones de trabajo y equipo de telecomunicaciones.

Durante las fechas de realización de la presente auditoria, el equipo de cómputo del ente auditor conectado a la infraestructura del PREP Morelos 2018, estuvo protegido y actualizado contra código malicioso, virus, troyanos, gusanos, etc. La conexión del equipo auditor a la infraestructura del PREP fue autorizada y supervisada en todo momento por el personal de la empresa informática electoral mediante el Director de Proyecto – Lic. Jasiel Gerardo Espinoza Vidaca y los coordinadores de los CATD, lo anterior alineado al calendario de recorridos proporcionado previo a las visitas físicas a personal del IMPEPAC y empresa encargada de la operación del PREP.

Es importante mencionar que una vez concluida la presente auditoria y entregado el tercer informe de trabajo, el equipo auditor no realizó ninguna modificación, instalación de software, hardware o cualquier otro elemento técnico que pudiera comprometer la seguridad e integridad del PREP, por lo que es total y absoluta responsabilidad de la empresa informática electoral e IMPEAC garantizar la seguridad, integridad, así como la continuidad de la infraestructura y operación del PREP Morelos 2018 y la página principal del OPLE previo, durante y posterior a la jornada electoral del 1 de julio del 2018.

1.0 CAJA NEGRA

Los resultados mostrados durante las pruebas incluidas en los anexos 11,12, 13 y 14 del tercer informe de auditoría muestran una depuración en el sistema y no presenta algún problema grave que ponga en riesgo o afecte los resultados del PREP Morelos.

Se realizó la inspección en el SIPREP, archivos descargables y base de datos mediante consultas teniendo como resultado que son consistentes con las actas contabilizadas.

Si bien se encontró un caso donde no coincidían los totales capturados, pero fue por razones de prueba en la captura que el total de votos capturada en letra y número no hacían la sumatoria de los votos plasmados en el acta, pero el sistema al contabilizar los votos hizo de forma correcta el ajuste, es decir fue un caso poco probable en donde los encargados de la casilla llenaron incorrectamente la suma de votos sin embargo el sistema lo realizo de manera correcta y no se vio afectado.

Con el resultado de las pruebas en anexos 11,12, 13 y 14 realizados el día 24 de junio del 2018 se puede determinar que el software no contiene defectos que afecten su desempeño, y por lo tanto está cumpliendo con los requerimientos que solicito IMPEPAC.

Se finaliza con éxito el tercer simulacro nacional el día 24 de junio del 2018 con el 100% de actas capturadas de la cual se muestra evidencia de portal web en sitio público.

Imagen de portal web público.

Resultados de pruebas de carga a los módulos del sistema PREP Morelos 2018:
Las pruebas fueron realizadas con una carga estimada de 200 usuarios en ráfagas de 50 ciclos, dando un total de 10,000 usuarios utilizando el sistema, los tiempos de respuesta encontrados fueron satisfactorios ya que no excedían de los 3 segundos para responder al usuario.

2.0 VALIDACIÓN DEL SISTEMA INFORMÁTICO DEL PREP Y DE SUS BASES DE DATOS.

Se verifico la base de datos del PREP Morelos y se mostró con solo contenido de datos de catálogos previo al inicio del simulacro.

El día lunes 25 de junio del 2018, se realiza la primera huella criptográfica la cual es preliminar y en espera que el IMPEPAC y empresa informática electoral definan la fecha de generación de versión final de huellas criptográficas del PREP Morelos 2018.

Se programan las siguientes actividades a realizar del 27 junio al 2 de julio del 2018:

1. El día 27 de junio la empresa informática electoral deberá proporcionar el procedimiento documentado y puntos a considerar (ver sección 2.7) para la realización de constancia de hechos a IMPEPAC para la definición y conocimiento del instrumento jurídico. (Informática electoral – IMPEPAC –Notario publico).
2. El día 28 de junio se realizará el procedimiento mencionado en el apartado 2.4 para generar la versión final de huellas criptográficas las cuales serán utilizadas para validar la utilización del sistema PREP auditado por la UAEM (UAEM – Informática electoral).
3. El día 29 de junio se realizará el procedimiento mencionado en el apartado 2.4 del tercer informe de auditoría para generar, validar y comparar el software en producción como ensayo previo a la jornada electoral.
4. El día 1 y 2 de julio se realizará el procedimiento mencionado en el apartado 2.4 del tercer informe de auditoría para generar, validar y comparar el software en producción previo y posterior a la jornada electoral.
5. El día 29 de junio se recibe la última huella criptográfica generada por la empresa Informática Electoral, indicando que ser la versión final del PREP, y por lo cual debe ser la huella a tomar en cuenta previo y posterior a la jornada electoral del 1 de Julio del 2018, se anexa el hash generado:
   [root@web1 auditoria]# cat 28-jun/sha256_sistemas_prep.txt
   0f6865446324cb283cf4ec3aea06fbeeda319d9dfb27f518f51f43826546fcb2 sistemas_prep.tar
   [root@web1 auditoria]# cat 29-jun/sha256_sistemas_prep_29jun.txt
   0f6865446324cb283cf4ec3aea06fbeeda319d9dfb27f518f51f43826546fcb2 sistemas_prep_29jun.tar
   [root@web1 auditoria]# cat sha256_sistemas_prep_29jun_2.txt
   0f6865446324cb283cf4ec3aea06fbeeda319d9dfb27f518f51f43826546fcb2 sistemas_prep_29jun_2.tar

3.0 ANÁLISIS DE VULNERABILIDADES A LA INFRAESTRUCTURA TECNOLÓGICA.

3.1 PRUEBAS DE PENETRACIÓN (PENTEST)

Se realizó un Pentest de caja negra previo durante y posterior a simulacros directamente hacia el portal previo del PREP Morelos, en el cual se siguió la metodología OWASP para revisión del top 10 de vulnerabilidades mundiales, teniendo en cuenta la actualización de la metodología del 2017.

Fueron encontradas las siguientes vulnerabilidades al realizar el análisis de vulnerabilidades pertinente:
- *10 de tipo bajas.*
-- *4 de tipo medias.*
- *0 críticas*

Se reporta por parte de la empresa informática electoral la atención a las recomendaciones realizada por ente auditor del primer informe de auditoría el día 29 de junio del 2018. Se solicitó a la empresa informática electoral evidencia de las acciones realizadas para las vulnerabilidades de la sección 3.1 del tercer informe de auditoría lo anterior con el objetivo de garantizar la integridad del sistema PREP Morelos 2018, la empresa desarrolladora del PREP cumple con un 85 % de atención con evidencia de lo solicitado dejando una modificación pendiente de tipo "baja".

Se recomienda se continúe asegurando la correcta implementación y administración de Cloudflare como medida anti DDOS, así como el Firewall de aplicaciones Web del PREP Morelos 2018 hasta al menos 5 días posteriores al final de jornada electoral.

3.2.1 REVISIÓN DE CONFIGURACIONES

Se utiliza actualmente el certificado genérico de Cloudflare, que, si bien cuenta con mecanismos criptográficos robustos, se recomienda:

La adquisición de certificado digital específico URL de página final del PREP - certificado standard SSL, 2048-bit.

Se corrobora una correcta configuración de DNS, misma que es gestionada por Cloudflare, garantizando que se mantenga la confidencialidad de la aplicación.

En relación a aplicación de PREP Casilla se recomienda que los dispositivos móviles cuenten con la capacidad de software y hardware para el sistema PREP Morelos 2018, se cuente con las visiones de sistema operativo actualizados, se implemente un correcto sistema de autenticación que garantice la seguridad de la información, que permita el uso exclusivo de la aplicación, asegure trafico encriptado e integridad de los datos, se asegure que en los sitios a implementar se cuente con la cobertura de proveedor de servicios suficiente para correcta transmisión de la digitalización de actas, realice la capacitación al personal que realizara la digitalización mediante este procedimiento y se cuente con el soporte técnico oportuno para lo antes mencionado.

3.2.2 REVISIÓN DE CONFIGURACIONES (INFRAESTRUCTURA Y COMPUTO)

Se cuenta parcialmente con condiciones para la correcta operación del PREP en relación a infraestructura eléctrica, de telecomunicaciones, alta disponibilidad de servidores y enlaces de internet en CATD's.

En la actualidad el sistema PREP Morelos 2018 es funcional como lo demuestra el resultado de 100% de actas capturadas del tercer simulacro nacional realizado el 24 de junio del 2018 sin embargo, ponemos a consideración del IMPEPAC la atención de los hallazgos de las secciones 3.2.2 del tercer informe de auditoría y evidencias fotográficas para disminuir situaciones de riesgo en caso de contingencias en el proceso de digitalización, captura, verificación y flujo del PREP.

RESUMEN FORTALEZAS, HALLAZGOS Y RECOMENDACIONES A SITIOS COPREP Y CCV.

RESPECTO AL CENTRO DE DATOS

Fortalezas

Se tiene redundancia activo - activo en firewall y servidor de VPN en sitio CCV/COPREP.
Se cuenta con redundancia activo – activo de servidores físicos en dos centros de datos diferentes y como tercera opción nodo COPREP/CCV.
Se tiene plan de continuidad y recuperación de desastres el cual se aplica para atención de contingencias.
Se tiene NOC/SOC con panel o tablero visible en sitio central.
Se cuenta con sistema de video vigilancia el cual vigila y guarda video del CCV/COPREP y CATDs.
Se cuenta con redundancia en enlaces de internet.
Se observa la correcta implementación de alta disponibilidad en bases de datos, sitios Web, firewalls y servidor de VPN.

Hallazgos.

No se monitorea el desempeño de la velocidad de subida y bajada de los enlaces principales, secundarios e interfaces de firewall, así como switches.
Se cuenta con limitantes en acondicionamiento ambiental en CCV/COPREP actualmente no funciona correctamente.

Recomendaciones
Contar con evidencia de niveles de disponibilidad y certificado Tier que ofrecen los centros de datos donde se hospedan los servidores.
Monitorear desempeño de las interfaces de entrada /salida con objetivo de tener la certeza de usar las interfaces más adecuadas en cuestión de velocidad.
Realizar mantenimiento correctivo a sistema de aire acondicionado de espacio CCV/COPREP.

RESPECTO A LA INSTALACIÓN DE ENERGÍA Y SEGURIDAD FÍSICA.

Fortalezas
Se cuenta con control de acceso biométrico para acceso a COPREP y CCV.
Se cuenta con sistema CCTV.
Se cuenta con seguridad en puerta de acceso principal.
Se cuenta dos UPS en área de rack de telecomunicaciones.
Se cuenta con planta generadora de energía eléctrica.

Hallazgos
No se tiene instalación eléctrica adecuada y normalizada.
No se cuenta con sistema de puesta a tierra física.
No se cuenta con sistema de protección contra tormentas eléctricas.
No se cuenta con supresores de picos clase A, B, C.
Inadecuada instalación eléctrica de alimentación de UPS de servidores y equipo de telecomunicaciones.
No se tiene una correcta administración del cableado eléctrico.
No se cuenta con redundancia en DVR o respaldo en la nube.

Recomendaciones
Se recomienda se realice la instalación eléctrica apegada a la norma NOM-001-SEDE 2012.
Considerar la redundancia de la planta de energía.
Considerar PDU con doble cable de alimentación para aquellos dispositivos que cuentan con una sola fuente y poder conectarlos a los dos UPS existentes.
Mejorar la administración de cableado eléctrico en área rack y centro de cómputo que evite se ponga en riesgo la desconexión de algún elemento de misión crítica.
DVR no se instale en la misma localidad, deber contar con redundancia y se tenga respaldo en la nube.

RESPECTO A LOS PUNTOS CONECTIVIDAD

Fortalezas

Se cuenta con redundancia activa en relación al acceso a internet.
Si falla completamente la conexión a internet del sitio COPREP se cuenta con capturistas y verificadores distribuidos en diferentes CATD's.
Se cuenta con mesa de ayuda mediante conmutador de voz privado, línea comercial y telefonía móvil.
Se cuenta con velocidades de 88.5 descarga y 17.33 de carga enlace principal de internet.
Se cuenta con velocidades de 42.61 descarga y 2.46 de carga enlaces de respaldo de internet.
La conexión entre equipos de capturistas y verificadores contra los servidores de aplicación se realiza mediante VPN Site to Site entre Firewalls.
Seguridad en la red LAN basada por MAC Address e IP fija.
Puertos de módems ISP bloqueados.

Hallazgos

No se tiene una correcta administración de cableado horizontal.
No se cuenta con puntos de sujeción ni canalización del cableado horizontal (entre el rack y el equipo de cómputo), se cuenta con instalación expuesta directamente en piso.

Recomendaciones

Administrar de manera adecuada el cableado horizontal de la red LAN de COPREP/CCV.
Realizar una correcta sujeción del cableado horizontal del cableado de la red LAN COPREP/CCV sobre muro a una altura mínima de 40 cm. (NMX-I-248-NYCE-2008 y ANSI/TIA/EIA-569-B).

RESPECTO AL EQUIPO DE COMPUTO

Fortalezas:

Se cumple con los requerimientos de hardware y software especificado en el anexo técnico del IMPEPAC para el PREP.
Se cuenta con acceso seguro de los dispositivos a la red del sistema PREP al contar con red local basada en sistema de VPN y direccionamiento IP privado.
Se cuentan en la gran mayoría de los equipos de cómputo con software firewall y antivirus activado y actualizado.
Se cuenta con equipos con respaldo de batería interno y externo mediante el uso de UPS.
Se cuenta con seguridad de acceso al sistema operativo y a su vez del sistema PREP.
Versiones de sistema operativo adecuadas.
Bloqueadas aplicaciones innecesarias por PREP. Únicamente acceso a navegador para uso de módulos PREP.
Se detecta que las conexiones de red inalámbricas de equipos de cómputo portátil se encuentran desactivadas.

Hallazgos:

Se tiene una cantidad mínima de equipos con firewall desactivado, conexión activa wifi concurrente a la red alambrada y se observa una computadora con acceso a internet simultáneamente con acceso a PREP.

Recomendaciones:

Activar en su totalidad de los equipos de cómputo firewall y antivirus actualizados, desactivar conexión activa wifi concurrente a la red alambrada y restringir acceso a internet simultáneamente con acceso a PREP a la totalidad de los equipos de cómputo.

RESUMEN FORTALEZAS, HALLAZGOS Y RECOMENDACIONES A 33 SITIOS CATD

RESPECTO A EQUIPO DE COMPUTO

Fortalezas

Se cumple con los requerimientos de hardware y software especificado en el anexo técnico del IMPEPAC para el PREP.
Se cuenta con acceso seguro de los dispositivos a la red del sistema PREP al contar con red local basada en sistema de VPN y direccionamiento IP privado.
Los equipos de cómputo cuentan con respaldo de energía mediante UPS.
Se cuenta con seguridad de acceso al sistema operativo y a su vez del sistema PREP.
Versiones de sistema operativo adecuadas
Bloqueadas aplicaciones innecesarias por PREP. Únicamente acceso a navegador para uso de módulos PREP.
Se detecta que las conexiones de red inalámbricas de los equipos de cómputo portátil se encuentran desactivadas.

Hallazgos

Se detectó en la mayoría de los equipos de cómputo portátil de los CATD's, con el firewall de Windows desactivado y el programa antivirus Kaspersky Free no cuenta con el modulo por ser una versión básica.
Se detectó en la mayoría de los equipos de cómputo portátil de los CATD's, no tienen actualizada la base antivirus del programa Kaspersky Free.

Recomendaciones

Se recomienda activar el firewall de Windows en todos los equipos CATD's.
Actualizar la base antivirus y mejorar la versión del programa antivirus Kaspersky free.

RESPECTO A LA INSTALACIÓN DE ENERGÍA Y SEGURIDAD

Fortalezas

Se cuenta con sistema CCTV.
Se cuenta con seguridad municipal con una bitácora en la puerta de acceso principal.
Se cuenta con dos UPS, el primero para el equipo de telecomunicaciones y el segundo para el equipo de digitalización.
Se cuenta con el uso de gafete con código QR para la identificación por medio de la aplicación COORD en la cuál se puede comprobar la identidad del personal del CATD.
Se cuenta con planta generadora de energía para CATD.

Hallazgos y seguridad física

No se tiene instalación eléctrica adecuada y normalizada.
No se cuenta con sistema de puesta a tierra física.
No se cuenta con sistema de protección contra tormentas eléctricas.
No se cuenta con sistema o elementos contra incendios.
No se tiene una correcta administración del cableado eléctrico.
Se cuenta con UPS, sin embargo existen CATD's con dispositivos de misión crítica como firewalls y módems, que se encuentran conectados a las salidas de protección y no respaldo de energía.

Recomendaciones

Se recomienda se realice la instalación eléctrica apegada a la norma NOM-001-SEDE 2012.
Contar con sistema o elementos contra incendios.
Mejorar la administración de cableado eléctrico del CATD que evite se ponga en riesgo la desconexión de algún elemento de misión crítica, corto circuito o accidente.

RESPECTO A LA CONECTIVIDAD

Fortalezas

Se cuenta con mesa de ayuda mediante conmutador de voz privado, Whatsapp y telefonía móvil.
La conexión entre equipos de capturistas y verificadores contra los servidores de aplicación se realiza mediante VPN Site to Site entre Firewalls.
Seguridad en la red LAN basada por MAC Address e IP fija.
Puertos ethernet de módems ISP bloqueados en la mayoría de los CATD's.
Únicamente soporte técnico tiene acceso a las configuraciones de los equipos de telecomunicaciones.
Atención vía remota para la atención y solución de contingencias en equipos de cómputo portátil, digitalizadores y/o equipos de telecomunicaciones por parte de soporte técnico.

Hallazgos

No se tiene una correcta administración de cableado horizontal, no hay puntos de sujeción ni canalización del cableado estructurado (entre el equipo de telecomunicaciones y el equipo de cómputo), se cuenta con instalación expuesta directamente en piso.
El acceso inalámbrico de los módems ISP de algunos CATD's se encontraron encendidos, se pudo accesar a la red inalámbrica, aunque no a las configuraciones de modem ISP.
En algunos CATD,s no se ha realizado cambio en la contraseña que muestra la etiqueta pegada al módem ISP, en la cual se puede acceder tanto a la red inalámbrica como a las configuraciones del mismo modem.
Se han detectado los puertos Ethernet del modem ISP habilitados, además del que está en uso para la Red.
En la mayoría de los CATD no cuentan con enlaces de respaldo de internet tipo ISP.
Las velocidades de carga encontradas en algunos CATD's son menores a 0.5 Mbps.
Las velocidades de descarga encontradas en algunos CATD's son menores a 10 Mbps.
Inicio de sesión en el sistema en algunos CATD,s han tomado hasta 40 min.
Lentitud al digitalizar, llega a tardar hasta más de 30 segundos para enviar el acta del digitalizador al sistema.
En la captura de datos del acta, el sistema presenta fallas de conexión, al finalizar de capturar por segunda vez los datos del acta, se queda cargando el sistema y después de 3 minutos muestra el mensaje de "Tiempo excedido". El capturista debe actualizar la página y en ocasiones cerrar el navegador, volverlo abrir e iniciar sesión.
Falla detectada en el sistema al cargar el acta para realizar la captura de datos por segunda ocasión (en ocasiones en la primera captura), se queda en negro la parte de la página donde muestra la imagen del acta y el capturista debe actualizar la página para cargar una nueva acta.

Recomendaciones

Administrar de manera adecuada el cableado horizontal de la red LAN y realizar una correcta sujeción del cableado horizontal del cableado de la red LAN CATD sobre muro a una altura mínima de 40 cm. (NMX-I-248-NYCE-2008 y ANSI/TIA/EIA-569-B).

Se recomienda apagar el acceso inalámbrico de los módems ISP desde configuración interna y cambiar la contraseña de la etiqueta pegada al modem ISP, esto provoca que los equipos conectados de manera inalámbrica puedan realizar cambios en la configuración y consumo de ancho de banda.

Deshabilitar los puertos Ethernet del modem ISP, dejar únicamente habilitado el puerto Ethernet que será utilizado para la Red.

Verificar con los ISP se garanticen mejores velocidades de carga y descarga.

Contar con enlace de internet de respaldo de diferentes ISP's.

Se realicen pruebas de contingencia de fallo en equipos de seguridad y comunicaciones que garanticen el proceso de plan de continuidad y recuperación de desastres.

4.0 ANÁLISIS DE VULNERABILIDADES A LA INFRAESTRUCTURA TECNOLÓGICA.

Se generó tráfico malicioso desde 50 mil bots simulando tráfico real, distribuidos alrededor del mundo, así como desconexiones constantes hacia el sistema PREP sin tener éxito.
Con respecto a la inundación de usuarios no se pudo concretar la inundación de usuarios, los cuales simulan tráfico real de la aplicación, así como recorridos por las rutas de la aplicación.
Se ejecutó un ataque con paquetes previamente pre configurados, los cuales al llegar al destino NO impactaron en el rendimiento de la aplicación. No se identificó degradación alguna al servicio de PREP, siendo el ataque contenido correctamente.
Se lanzaron más de 300 mil paquetes malformados, los cuales contenían un encabezado de 32 bytes para amplificarlo a 65535, y en los cuales NO se tuvo éxito en el ataque.
Se efectuó un ataque de tipo SYN Flood, alcanzando 1.5 GB por segundo y el cual **NO** fue exitoso debido a la configuración actual de Cloudflare. Se observa que Cloudflare se encuentra correctamente instalado.
Se enviaron masivamente, durante 3 horas, paquetes tipo SYN para probar protecciones anti-DDOS, así como ataque secuencial tipo SYN a la aplicación sin tener éxito de impactar a aplicación, se observa Cloudflare se encuentra correctamente instalado.
Se realizaron pruebas de tipo UDP hacia el sistema PREP, donde NO se tuvo éxito. se identifica una correcta implementación del WAF, así como las reglas configuradas.
Se realizó un ataque tipo ICMP (Ping flood), en la cual se utilizó la herramienta HULK, en el cual NO hubo degradación alguna al servidor, sin embargo, hubo mensajes de error de tipo 500 desde Cloudflare.
Se realizó un ataque con la herramienta LOIC, dentro de la LAN de IMPEPAC, en el cual se simularon 10 millones de peticiones sintéticas, emulando la actividad el día de la elección. Se detectó una degradación mínima en el sistema, por la protección de Cloudflare. Cloudflare actúa como barrera en este tipo de paquetes (ICMP) por lo que fueron desviados en su totalidad.
Se realizó un ataque vía TCP con alrededor de 26 mil paquetes, empezando desde las 2:30 pm el domingo 17 de enero, generando tráfico malintencionado, a su vez, se mencionó lentitud en los sistemas informáticos de conteo posiblemente por este ataque.
Se envió un envenenamiento vía Slowloris al DNS principal de PREP Morelos, sin tener éxito en alentar el sistema.

Se recomiendo atender los puntos con respecto a la configuración de banderas de seguridad en los encabezados http para garantizar sesiones seguras.
Se recomiendo verificar la conexión TCP con banderas SYN.
Las pruebas realizadas durante la tercera jornada de simulacros muestran que no existen anormalidades o riesgos de seguridad en el sistema PREP Morelos 2018 al 25 de junio del presente año.
Se recomiendo se realicen los escenarios de prueba para confirmar la efectividad de plan de continuidad y recuperación de desastres que contemple al menos las contingencias del nivel “a” y “m” en relación a servidores de aplicaciones web.
Con respecto a la configuración del WAF el cual protege al PREP Morelos se encuentra correctamente implementado, y en el cual se encuentra protegido a su vez el DNS principal de PREP Morelos.
A la fecha no se pudo concretar la inundación de usuarios, los cuales simulan tráfico real de la aplicación, así como recorridos por las rutas de la aplicación.
A la fecha se identifica una correcta implementación del WAF, así como las reglas de seguridad configuradas.
Se tiene a la fecha Cloudflare correctamente instalado y configurado para ataques DDOS.
Cloudflare actúa como barrera en este tipo de paquetes (ICMP) por lo que fueron desviados en su totalidad.
Se recomienda se continúe asegurando la correcta implementación y administración de Cloudflare como medida anti DDOS, así como el Firewall de aplicaciones web del PREP Morelos 2018 hasta al menos 5 dias posteriores al final de jornada electoral.
Se recomendó para URL de la página principal del IMPEPAC implementar con carácter de urgente Cloudflare como medida anti DDOS, así como activar la protección en consola de denegaciones de servicio. lo anterior como resultado de pruebas exitosas a ataques de denegación de servicio.
Se recomendó para URL de la página principal del IMPEPAC verificar con carácter de urgente que el wordpress (cms) instalado cuente con las actualizaciones más recientes.
Se recomendó para URL de la página principal del IMPEPAC se adquiera e implemente certificado digital SSL para sitio web.

Anexos

1. **PRIMER INFORME DE AUDITORIA**
2. **SEGUNDO INFORME DE AUDITORIA**
3. **TERCER INFORME DE AUDITORIA**
4. **REPORTE FOTOGRAFICO EVIDENCIAS DE HALLAZGOS EN CCV/COPREP Y CATD'S.**
5. **CRONOGRAMAS DE ACTIVIDADES**
6. **LISTAS DE VERIFICICACION DE INFRAESTRUCTURA CCV/COPREP/CATD**
7. **PLAN DE PRUEBAS FUNCIONALES DE CAJA NEGRA DEL SISTEMA INFORMATICO.**

EQUIPO AUDITOR

L.I. Ignacio Sánchez Zamudio

MTI. Miguel A. Córdova Serrano

Lic. Aldo Ivaan Valdez Mota

Lic. Alfonso Ruiz Palacios