UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MORELOS

COORDINACIÓN GENERAL DE PLANEACIÓN Y ADMINISTRACIÓN

DIRECCIÓN GENERAL DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

INFORME FINAL

SERVICIOS DE AUDITORÍA AL SISTEMA INFORMÁTICO E INFRAESTRUCTURA Y/O SERVICIOS RELACIONADOS CON TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DONDE SE IMPLEMENTE EL PREP

31 DE MAYO DEL 2024.

Universidad Autónoma del Estado de Morelos | UAEM Rectoría 2023-2029 | Coordinación General de Planeación y Desarrollo Sustentable | DGTIC Dirección General de Tecnologías de Información y Comunicación | impepac Instituto Morelense de Procesos Electorales y Participación Ciudadana

TABLA DE CONTENIDO

INFORME FINAL DE LOS SERVICIOS DE AUDITORÍA AL SISTEMA INFORMÁTICO E INFRAESTRUCTURA Y/O SERVICIOS RELACIONADOS CON TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DONDE SE IMPLEMENTE EL PREP 4

GLOSARIO 5

ANTECEDENTES 8

UAEM 8

IMPEPAC 8

ALCANCE 9

OBJETIVO GENERAL 9

OBJETIVOS ESPECIFICOS Y LÍNEAS DE TRABAJO PARA LA PRESENTE AUDITORIA SE LISTAN EN LA PARTE INFERIOR: 10

METODOLOGIA 11

RESULTADOS DE LA AUDITORÍA 12

INFORME FINAL DE LAS PRUEBAS FUNCIONALES DE CAJA NEGRA DEL SISTEMA INFORMÁTICO Y/O SERVICIOS RELACIONADOS CON TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES 13

/OBJETIVO 14

/ALCANCE 14

/CAJA NEGRA 14

/ VALIDACIÓN DEL SISTEMA INFORMÁTICO DEL PREP Y/O SERVICIOS RELACIONADOS CON TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES, ASÍ COMO DE SUS BASES DE DATOS. 15

INFORME FINAL DE LAS PRUEBAS DE PENETRACIÓN A LA INFRAESTRUCTURA Y/O SERVICIOS RELACIONADOS CON TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DONDE SE IMPLEMENTE EL PREP 16

/ Introducción 17

/ Objetivo 17

/ Alcance 17

/ Resumen ejecutivo 19

/ Observaciones 21

/ Recomendaciones generales 21

INFORME FINAL DE LA REVISIÓN DE CONFIGURACIONES DE LA INFRAESTRUCTURA Y/O SERVICIOS RELACIONADOS CON TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DONDE SE IMPLEMENTE EL PREP 22

/ Introducción 23

/ Objetivo 23

/ Alcance 23

/ Resumen ejecutivo 23

/ Conclusiones 25

INFORME FINAL DE LA REVISIÓN DE CONFIGURACIONES DE LA INFRAESTRUCTURA Y/O SERVICIOS RELACIONADOS CON TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DONDE SE IMPLEMENTE EL PREP 26

/ Introducción 27

/ Objetivo general 27

/ Objetivos específicos 27

/ Alcance 28

/ Resumen ejecutivo 30

REPORTE FINAL DE LAS VISITAS A LOS SITIOS CATD 31

/ Introducción 32

/ Objetivo general 32

/ Objetivos específicos 32

/ Alcance 33

/ Resumen ejecutivo 33

/ Conclusiones 33

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MORELOS

INFORME FINAL DE LOS SERVICIOS DE AUDITORÍA AL SISTEMA INFORMÁTICO E INFRAESTRUCTURA Y/O SERVICIOS RELACIONADOS CON TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DONDE SE IMPLEMENTE EL PREP

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.

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: centros de acopio y transmisión de datos.

CCV: Centro de Captura y Verificación.

COTAPREP: Comité Asesor del PREP.

CVPREP: Módulo de Captura y Verificación PREP.

MCAD: Módulo de Captura, Acopio y Digitalización.

MRI: Mesa de Resolución de Incidencias.

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.

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

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.

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

INE: Instituto Nacional Electoral.

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.

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.

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.

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.

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

TCP: Protocolo de Control de Transmisión

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

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.

UDP: User Datagram Protocol.

DNS: Servidor de nombres de dominio (DNS).

ICMP: Por sus siglas en inglés Internet Control Message Protocol, Protocolo de mensajes de control de Internet.

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: el envío de un número anormalmente grande de paquetes ICMP de cualquier tipo (especialmente paquetes "ping" de prueba de latencia de red) puede abrumar a un servidor objetivo que intenta procesar cada solicitud ICMP entrante, y esto puede dar como resultado una denegación condición de servicio para el servidor de destino.

HTTP: Hypertext Transfer Protocol

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.

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.

TIER: Nivel de certificación.

NOC: Centro de Operaciones de Red.

SOC: Centro de Operaciones de Seguridad.

DVR: Digital Video Recorder.

WAF: Web Application Firewall.

SIP: Session Initiation Protocol.

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.

SSL: Secure Sockets Layer.

UAEM: Universidad Autónoma del Estado de Morelos.

DDOS: Ataque de denegación de servicio.

SLA - service level aggrement - Medida usada para cuantificar el rendimiento del sistema probado en términos de tiempos de respuesta promedio.

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.

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 General de Tecnologías de información y comunicación 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 el diseño, implementación y operación del Programa de Resultados Electorales Preliminares (PREP) para el Proceso Electoral Concurrente 2023-2024 en el estado de Morelos, se requiere que se lleve a cabo una auditoría al sistema informático e infraestructura tecnológica del PREP, de conformidad con lo dispuesto en el Libro Tercero. Proceso Electoral, Título III. Actos posteriores a la elección, Capítulo II. PREP, Sección Cuarta. Sistema informático y su auditoría, artículos 346 y 347 del Reglamento de Elecciones del Instituto Nacional Electoral (INE); así como con lo dispuesto en el Título II. De la Implementación, Capítulo III. De la Auditoría al Sistema Informático, del Anexo 13 del citado Reglamento, relativo a los Lineamientos del 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.

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 12, 17, 19 y 26 de mayo del 2024, 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:

ID CATD	Municipio	ID CATD	Municipio
CCV	Cuernavaca	24	Tetecala
1	Amacuzac	25	Tetela del volcán
2	Atlatlahucan	26	Tlalnepantla
3	Axochiapan	27	Tlaltizapán
4	Ayala	28	Tlaquiltenango
5	Coatetelco	29	Tlayacapan
6	Coatlán del Rio	30	Totolapan
7	CUAUTLA	31	Xochitepec
8	Cuernavaca	32	Xoxocotla
9	Emiliano Zapata	33	Yautepec
10	Hueyapan	34	Yecapixtla
11	Huitzilac	35	Zacatepec
12	Jantetelco	36	Zacualpan de Amilpas
13	Jiutepec		
14	Jojutla		
15	Jonacatepec		
16	Mazatepec		
17	Miacatlán		
18	Ocuituco		
19	Puente de Ixtla		
20	Temixco		
21	Temoac		
22	Tepalcingo		
23	Tepoztlán		

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 y a la aplicación que se utilizarán para operar el mecanismo de digitalización de las Actas desde las casillas, para evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares.
2. Análisis de vulnerabilidades, considerando al menos pruebas de penetración y revisión de configuraciones a la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP.
3. Pruebas de negación de servicio al sitio de publicación del PREP y al sitio principal del IMPEPAC.
4. Validación del sistema informático del PREP y de sus bases de datos, ante un tercero con fe pública.

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 2024, 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.

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 AUDITORÍA

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 2024.

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

1. Recomendaciones de Seguridad y Reporte de Vulnerabilidades - DGTIC / 97 / 24 del 27 de Marzo del 2024
2. Resultado de la primera visita de auditoría la sitio COPREP - DGTIC/ 114 /24 – 16 de abril del 2024.
3. Pruebas funcionales al sistema PREP - DGTIC / 118 / 24 del 18 de abril del 2024
4. Oficio de Información de Resultados y Acuerdos - DGTIC/ 133 /24 del 26 de abril del 2024.
5. Entrega de informes preliminares de pruebas funcionales de caja negra, pruebas de penetración a la infraestructura y revisión de configuraciones de la infraestructura. DGTIC/ 145/24 del 7 de mayo del 2024.
6. Resumen del Primer Simulacro del Programa de Resultados Electorales Preliminares del Proceso Electoral Ordinario Local 2023-2024 – DGTIC/ 148 24/ del 13 de mayo del 2024.
7. Reporte fotográfico de las visitas a los sitios CATD - DGTIC/ 160 /24 del 25 de mayo de 2024.
8. Presentación de Informes Finales del Programa de Resultados Electorales Preliminares (PREP) en el estado de Morelos - DGTIC / 164 / 24 del 29 de mayo de 2024.

Se anexa al listado antes mencionado los siguientes informes.

1. Informe 4to Simulacro Auditoría PREP 2024 (Nombre del archivo: Informe4toSimulacroAuditoriaPREP2024.pdf)
2. Análisis final de vulnerabilidades al sitio de IMPEPAC (Nombre del archivo: AFDV-187.216.223.230-Final.pdf)

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 2024, estuvo protegido y actualizado contra código malicioso, virus, troyanos, gusanos, etc.

Es importante mencionar que una vez concluida la presente auditoria y entregado el informe final 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 2024 y la página principal del OPLE previo, durante y posterior a la jornada electoral del 2 de junio del 2024.

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MORELOS

INFORME FINAL DE LAS PRUEBAS FUNCIONALES DE CAJA NEGRA DEL SISTEMA INFORMÁTICO Y/O SERVICIOS RELACIONADOS CON TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

| OBJETIVO

Analizar el sistema informático del PREP, mediante la ejecución de pruebas funcionales de caja negra, para evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares, conforme a lo establecido en el artículo 347, numeral 1, inciso a) del Reglamento de Elecciones.

| ALCANCE

Las pruebas de caja negra deberán ejecutarse en términos de funcionalidad del sistema informático del PREP, y deberán considerar, al menos, los siguientes aspectos:

- Analizar el funcionamiento del sistema informático del PREP, en relación con las fases del PTO, considerando al menos, la **digitalización, captura de datos, verificación y publicación de resultados**, mediante flujos completos e interacción entre los diversos módulos.

- Analizar el funcionamiento del aplicativo desarrollado para la digitalización de las Actas desde las casillas, y, en su caso, la captura de datos desde las casillas. Dicho análisis se hará mediante flujos completos e interacción entre los diversos módulos y fases del PTO.

- Se debe verificar la correspondencia de la captura de los datos plasmados en las Actas PREP con los presentados en la publicación, mediante los distintos tipos de reportes desplegados por el PREP, considerando datos, imágenes y bases de datos.

| CAJA NEGRA

Los resultados mostrados durante las pruebas incluidas en los anexos a este informe final de auditoría muestran las pruebas realizadas, desde la presentación de la demo funcional y los simulacros llevados a cabo.

Se realizo la validación de diferentes actas donde los datos capturados se presentan en la base de datos, siendo así un correcto registro.

Se valido el módulo de digitalización, captura de datos y verificación, cumpliendo con el alcance esperado, sin embargo, no se pudieron concluir pruebas con la digitación a través del **aplicativo PREP CASILLA**:

- Obtención de la imagen digital del Acta PREP, considerando en este apartado el mecanismo que permita la digitalización y, en su caso, la captura de datos, de las Actas desde las casillas.

    - **OBSERVACIÓN** : No fue posible la obtención de actas digitales por medio de la aplicación PREP CASILLA, no se llevó a cabo con éxito la validación dando incumplimiento al alcance esperado por PREP CASILLA.

- Captura de la información contenida en las Actas PREP.

    - Validación exitosa de datos registrados.

- Verificación de la información capturada.
    - Validación exitosa de datos registrados.
- Revisión de la obtención de los resultados, así como de la emisión de reportes y su despliegue, de acuerdo con la documentación técnica y la normatividad aplicable.
    - Se detecta variación en porcentajes, se sugiere verificar si esta diferencia corresponde a un error, y de ser asi aplicar su corrección.

| VALIDACIÓN DEL SISTEMA INFORMÁTICO DEL PREP Y/O SERVICIOS RELACIONADOS CON TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES, ASÍ COMO DE SUS BASES DE DATOS.

Durante los simulacros llevados a cabo, en el primer simulacro no se llevó a cabo la validación de base de datos, los posteriores se cumplió con la verificación y se mostró la base de datos sin información previa.

Se menciona que se utilizará un nuevo mecanismo, realizando una consulta directa a la base de datos para asegurar que esta se encuentre vacía antes del inicio del PREP. Al 31 de mayo de 2024, no se cuenta con el procedimiento documentado.

En relación con la generación, obtención y validación de huellas criptográficas en SHA-256 del PREP auditado, solo se ha llevado a cabo una validación de hash durante un simulacro. Hasta la fecha de este informe, no se ha presentado de forma oficial la huella criptográfica de la versión final del sistema.

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MORELOS

INFORME FINAL DE LAS PRUEBAS DE PENETRACIÓN A LA INFRAESTRUCTURA Y/O SERVICIOS RELACIONADOS CON TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DONDE SE IMPLEMENTE EL PREP

| INTRODUCCIÓN

Esta sección del documento presenta el resumen del Informe final de las pruebas de penetración a la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP, con el objetivo de presentar el estado de seguridad de dichos componentes, así como las recomendaciones de mitigación y mejora, así como documentar los resultados de las pruebas realizadas.

| OBJETIVO

El objetivo fue evaluar el nivel de seguridad de los aplicativos que conforman el sistema informático del PREP en el IMPEPAC, mediante la ejecución de pruebas de seguridad para identificar y minimizar los riesgos de seguridad.

Estas pruebas de seguridad tienen como objetivo identificar defectos, desviaciones de buenas prácticas de seguridad y debilidades o vulnerabilidades relacionados con los aplicativos e infraestructura desarrollados e implementados por el IMPEPAC y por terceros y que forman parte del sistema PREP de 2024.

El presente informe incluye el estatus de los hallazgos posterior a la remediación de los mismos por parte del IMPEPAC y los proveedores externos relacionados con dichas vulnerabilidades.

| ALCANCE

Activos relacionados con los módulos y aplicaciones del PREP:

Activo	Dirección IP	Propósito
server-auditapp	X.X.X.X	Servicios necesarios para aplicativos CORE (front-end, back-end, BD)
server-auditpc	X.X.X.X	Servicios necesarios para aplicativos PREP Casilla
server-auditweb	X.X.X.X	Servicios necesarios para aplicativos web públicos (sitio web público)

URL’s relacionadas con los módulos y aplicaciones del PREP:

Sistema	URL
API PREP Casilla	https://pcaudit.prepmorelos.info/
MCAD	https://appaudit.prepmorelos.info/mcad/

CVPREP	https://appaudit.prepmorelos.info/cvprep/
MRI	https://appaudit.prepmorelos.info/mri/
Sitio web público	https://wwwaudit.prepmorelos.info/

Otros activos relacionados con el PREP:

Activo	Dirección IP	Propósito
NVR1	X.X.X.X	Concentrar la grabación del circuito cerrado de cámaras IP
PBX-IP	X.X.X.X	Administras las líneas telefónicas IP internas
ESX8a	X.X.X.X	Servidor que administra máquinas virtuales (nodo primario)
ESX8b	X.X.X.X	Servidor que administra máquinas virtuales (nodo secundario)
ESX8a_admin	X.X.X.X	Administración de servidor físico 1
ESX8b_admin	X.X.X.X	Administración de servidor físico 2
Firewall	X.X.X.X	Firewall perimetral

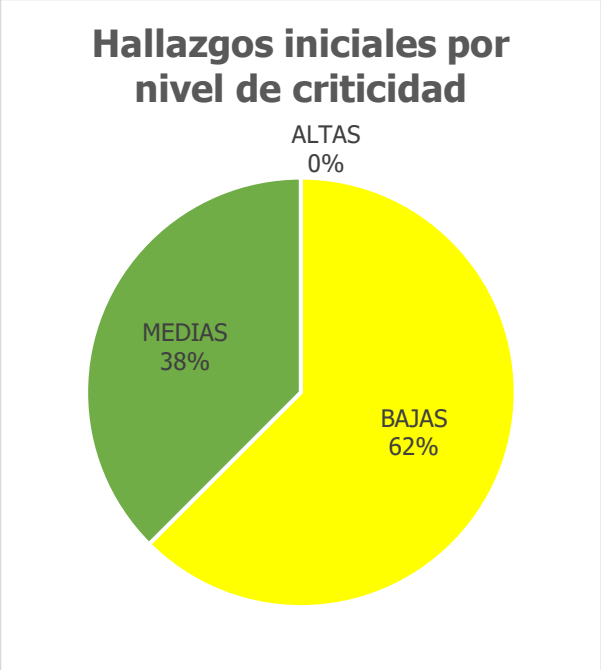
Elementos productivos (CLOUD):

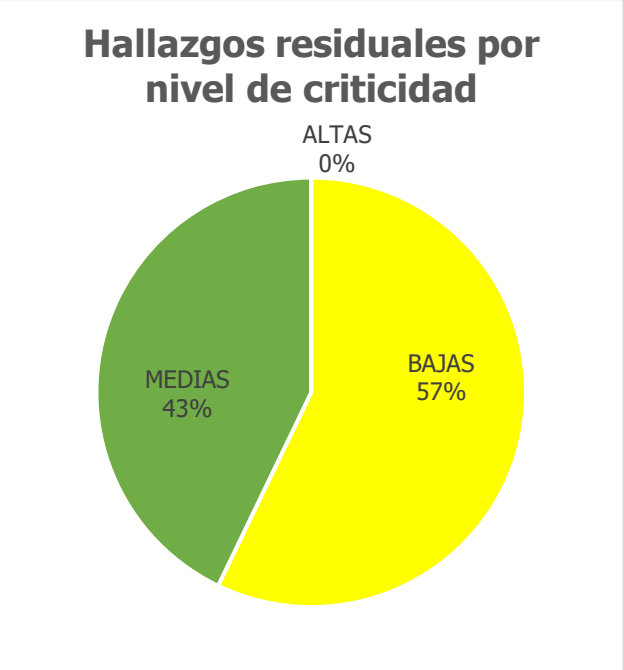
Activo	URL
Direccionamiento VPN	X.X.X.X
Servicios en internet	prep2024mor.mx

| RESUMEN EJECUTIVO

Como resultado del ejercicio de las pruebas de penetración ejecutadas fue posible identificar un total de 8 hallazgos con los siguientes niveles de criticidad:

ID	Vulnerabilidad	Referencia OWASP	Criticidad	Estado
1	**Uso de credenciales por defecto en Grandstream**	**A07-2021**	**3.3**	**Remediado**
2	**Envío de credenciales en claro**	**A07-2021**	**4.4**	**Sin Remediar**
3	**Reutilización de tokens por ausencia de inhabilitación**	**A01-2021**	**2.9**	**Sin Remediar**
4	**Acceso no autorizado a BD de MCAD**	**A04-2021**	**6.8**	**Sin Remediar**
5	**Ausencia de cabeceras de seguridad**	**A05-2021**	**3.6**	**Sin Remediar**
6	**Control de tiempo delegado al front end**	**A05-2021**	**3.3**	**Sin Remediar**
7	**Inadecuado manejo de errores**	**A05-2021**	**1.9**	**Sin Remediar**
8	**Validación de longitud de datos ingresados**	**A04-2021**	**4.0**	**Sin Remediar**


Hallazgos iniciales por nivel de criticidad
ALTAS 0%
MEDIAS 38%
BAJAS 62%


Hallazgos residuales por nivel de criticidad
ALTAS 0%
MEDIAS 43%
BAJAS 57%

| OBSERVACIONES

Con respecto a las recomendaciones emitidas, el IMPEPAC y los proveedores externos relacionados con los hallazgos detectados emitieron la siguiente respuesta (RESPUESTA A OFICIO DGTIC/ 114 /24 Y DGTIC/145/24"):

Hallazgo	Observación
Uso de credenciales por defecto en Grandstream	Se subsanó.
Acceso no autorizado a BD de MCAD	Se subsanó.
Envío de credenciales en claro:	De acuerdo con la evaluación de riesgos realizada por Informática Electoral, estos hallazgos no representan una vulnerabilidad real dado que se encuentran dentro de una red VPN. Sin embargo, si son monitoreados durante la duración del proyecto para evitar que se conviertan en riesgos reales.
Reutilización de tokens por ausencia de inhabilitación:	
Ausencia de cabeceras de seguridad	
Control de tiempo delegado al front end	
Validación de longitud de datos ingresados	
Inadecuado manejo de errores	

De lo anterior, el umbral de los hallazgos residuales, se mantiene en el nivel de riesgo bajo, por lo que se recomienda la implementación de medidas compensatorias de monitoreo y prevención de accesos no autorizados para evitar que estas sean explotadas por una persona malintencionada.

Es importante enfatizar que el hallazgo "Acceso no autorizado a BD de MCAD" fue reportado como subsanado, sin embargo, durante la revisión se identificó que la vulnerabilidad prevalece (Ver hallazgo ID PREP_PT_04)

Es importante mencionar que se generado el día 31 de mayo el análisis de vulnerabilidades al sitio https://impepac.mx/ cual se anexa los resultados el archivo adjunto.

| RECOMENDACIONES GENERALES

El riesgo general identificado para la arquitectura general como resultado de la prueba de penetración se considera en el umbral bajo, sin embargo, recomendamos ampliamente mejorar y disminuir riesgos mediante la aplicación de las recomendaciones plasmadas en los reportes emitidos por el ente auditor encaminadas a la remediación de los hallazgos detectados.

INFORME FINAL DE LA REVISIÓN DE CONFIGURACIONES DE LA INFRAESTRUCTURA Y/O SERVICIOS RELACIONADOS CON TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DONDE SE IMPLEMENTE EL PREP

| INTRODUCCIÓN

Esta sección del documento presenta el resumen del Informe final de la Revisión de configuraciones a la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP, con el objetivo de presentar el estado de seguridad de dichos componentes, así como las recomendaciones de mejora en configuración, así como documentar los resultados de las revisiones.

| OBJETIVO

El objetivo es evaluar el nivel de seguridad de los activos que conforman el sistema informático del PREP en el IMPEPAC, mediante la revisión de configuraciones para su comparación contra mejores prácticas y recomendaciones de marcos de seguridad.

Estas revisiones tienen como objetivo identificar desviaciones de buenas prácticas de seguridad y debilidades o vulnerabilidades relacionados con los activos implementados por el IMPEPAC y por terceros y que forman parte del sistema PREP de 2024.

| ALCANCE

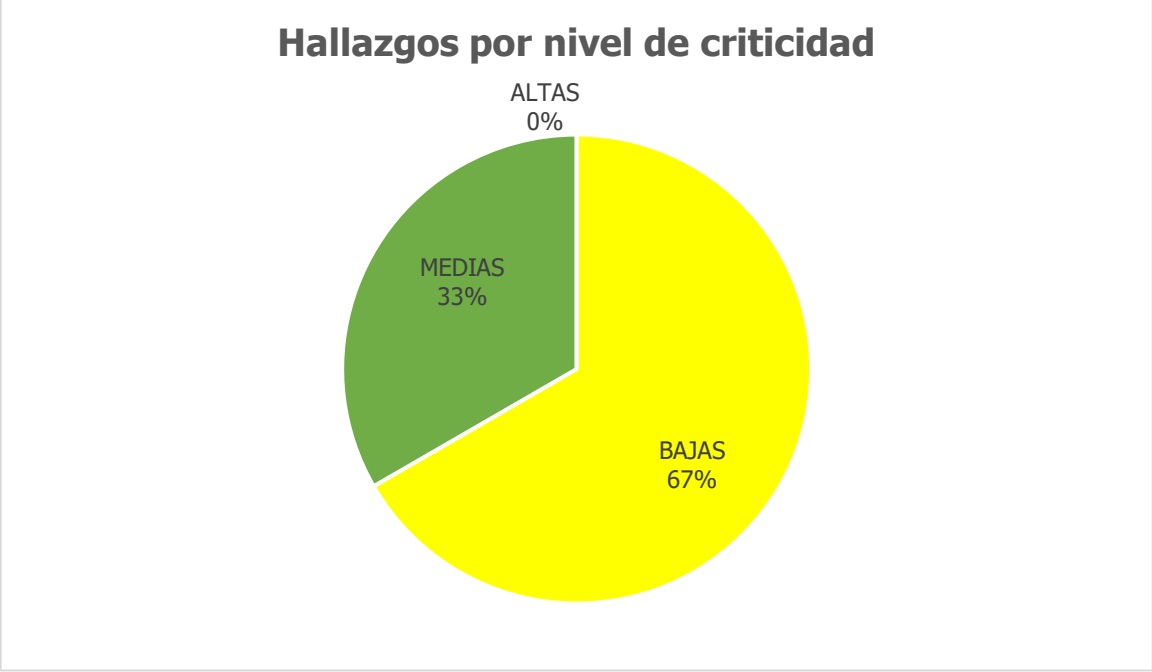
Activos relacionados con los módulos y aplicaciones del PREP:

Activo	Tecnología	Propósito	Estatus
IBM Cloud	N/A	Cuenta donde se albergan los servicios productivos del PREP	Completado
5 Instancias de servidores	Ubuntu Server 22.04	Servicios necesarios para aplicativos CORE (front-end, back-end, BD)	Completado
Servidor de base de datos	MariaDB 10.4	Base de datos de persistencia de información del PREP	Evidencia no entregada por parte de la empresa informática electoral.
Servidor web	Nginx	Exposición de aplicaciones y servicios	Evidencia no entregada por parte de la empresa informática electoral.

| RESUMEN EJECUTIVO

Como resultado de las pruebas de penetración ejecutadas fue posible identificar un total de 2 hallazgos con los siguientes niveles de criticidad:

ID	Vulnerabilidad	Marco de Buena Práctica	Criticidad	Estado
1	Ausencia de cifrado en discos de instancias de cómputo	CIS IBM Cloud Foundations Benchmark	3.8	Sin remediar
2	Ausencia de configuraciones de herramientas de monitoreo de seguridad	CIS IBM Cloud Foundations Benchmark	4.1	Sin remediar
3	Configuraciones inseguras de sistema operativo	CIS Ubuntu Linux 22.04 LTS Benchmark v2.0.0	3.3	Sin remediar



| CONCLUSIONES

Se han identificado configuraciones que suponen un riesgo para la confidencialidad, integridad y disponibilidad de la información del PREP. el umbral de dichos hallazgos se mantiene en el nivel de riesgo bajo y medio, lo que supone un esfuerzo de bajo a moderado en la aplicación de las recomendaciones sugeridas para elevar la postura de ciberseguridad durante las jornadas del PREP. Recomendamos ampliamente mejorar y disminuir riesgos mediante la aplicación de las recomendaciones plasmadas en los reportes emitidos por el ente auditor encaminadas a la remediación de los hallazgos detectados.

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MORELOS

INFORME FINAL DE LA REVISIÓN DE CONFIGURACIONES DE LA INFRAESTRUCTURA Y/O SERVICIOS RELACIONADOS CON TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DONDE SE IMPLEMENTE EL PREP

| INTRODUCCIÓN

Este documento presenta el Informe de las pruebas de negación de servicio al sitio de publicación del PREP, con el objetivo de presentar el estado de seguridad de los componentes que lo soportan, así como las recomendaciones de mitigación y mejora, así como documentar los resultados de las pruebas realizadas.

| OBJETIVO GENERAL

El objetivo es evaluar el nivel de seguridad de los componentes que conforman el sistema informático del PREP en el IMPEPAC, mediante la ejecución de pruebas de negación de servicio para identificar y minimizar los riesgos de seguridad ante ataques reales.

Estas pruebas tienen como objetivo identificar defectos, desviaciones de buenas prácticas de seguridad y debilidades o vulnerabilidades relacionados con los componentes y controles de red y anti-DoS implementados por el IMPEPAC y por terceros y que forman parte del sistema PREP de 2024.

| OBJETIVOS ESPECÍFICOS

- Medir el impacto sobre la infraestructura derivado de un ataque DDoS.
- Confirmar que la solución de mitigación de Cloudflare es capaz de detectar automáticamente cada vector de ataque.
- Confirmar que la solución de mitigación de Cloudflare es capaz de alertar automáticamente sobre cada vector de ataque.
- Confirmar que la solución de mitigación de Cloudflare es capaz de mitigar automáticamente cada vector de ataque.
- Confirmar que la solución de mitigación de Cloudflare no causa degradación al tráfico legítimo.

| ALCANCE

Activos relacionados con el sitio de publicación:

Fecha de prueba	URL	Detalles
2024.05.14 12:00 EDT - 2024.05.14 13:25 EDT	https://www.prep2024mor.mx/	• Inundación de ancho de banda TCP ACK (volumétrica) ◦ Volumen de solicitud objetivo 5,0 Gbps ◦ Incremento gradual ▪ 0-11 minutos 1,0 Gbps ▪ 11-21 minutos 2,0 Gbps ▪ 21-31 minutos 3,0 Gbps ▪ 31-41 minutos 4,0 Gbps ▪ 41-60 minutos 5,0 Gbps ◦ Duración: 60 minutos • Inundación de ancho de banda UDP (volumétrico) ◦ Volumen de solicitud objetivo 5,0 Gbps ◦ Incremento gradual ▪ 0-11 minutos 1,0 Gbps ▪ 11-21 minutos 2,0 Gbps ▪ 21-31 minutos 3,0 Gbps ▪ 31-41 minutos 4,0 Gbps ▪ 41-60 minutos 5,0 Gbps ◦ Duración: 60 minutos

2024.05.19 12:00 EDT - 2024.05.19 13:40 EDT	https://simulacro510642.prep2024mor.mx/	• Inundación de banda SYN tsunami (volumétrica) ◦ Volumen de solicitud objetivo 5,0 Gbps ◦ Incremento gradual ▪ 0-11 minutos 1,0 Gbps ▪ 11-20 minutos 2,0 Gbps ▪ 20-30 minutos 3,0 Gbps ▪ 30-40 minutos 4,0 Gbps ▪ 40-50 minutos 5,0 Gbps ◦ Duración: 60 minutos • Protocolo IP 50 inundación de ancho de banda (volumétrico) ◦ Volumen de solicitud objetivo 5,0 Gbps ◦ Incremento gradual ▪ 0-11 minutos 1,0 Gbps ▪ 11-20 minutos 2,0 Gbps ▪ 20-30 minutos 3,0 Gbps ▪ 30-40 minutos 4,0 Gbps ▪ 40-50 minutos 5,0 Gbps ◦ Duración: 60 minutos

| RESUMEN EJECUTIVO

Se llevaron a cabo pruebas de negación de servicio tipo DDoS el 14 de mayo y 19 de mayo. Durante las pruebas, se lanzaron 4 vectores de ataque DDoS alcanzando 20 Gbps distribuidos en los ejercicios contra los puntos finales que están protegidos por el servicio proxy de Cloudflare. Los ataques DDoS fueron mitigados con éxito sin ningún impacto en el entorno de destino.

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MORELOS

REPORTE FINAL DE LAS VISITAS A LOS SITIOS CATD

| INTRODUCCIÓN

Esta sección del documento presenta resultado de visita a los sitios CATD CATD Amacuzac, Atlatlahucan, Jojutla, Tepoztlán, Tlaltizapán, Tlalnepantla, Tlaquiltenango, Tlayacapan, Totolapan, Zacatepec, Yautepec, Tetecala, Ocuituco, Tetela del volcán CATD Temoac, Yecapixtla, Cuernavaca, Jonacatepec, Jonacatepec, Zacualpan de Amilpas, Jantetelco, Jiutepec, Mazatepec, Coatlán de Río, Coatetelco, Cuautla, Temixco, Miacatlán, Puente de Ixtla y Hueyapan con el objetivo de verificar el estado de la infraestructura de los componentes que soportan los sitios antes mencionados e identificar oportunidades de mejora.

| OBJETIVO GENERAL

El objetivo es evaluar el nivel de cumplimiento de los componentes que conforman el sistema informático del PREP los CATD.

Estas pruebas tienen como objetivo identificar defectos, desviaciones de buenas prácticas de seguridad y debilidades relacionados con los componentes implementados por el IMPEPAC y por terceros que forman parte del sistema PREP de 2024.

| OBJETIVOS ESPECÍFICOS

- Verificar la seguridad física del sitio.
- Verificar la seguridad lógica de acceso a la red.
- Verificar las condiciones de instalación de red cableada, equipos de comunicaciones y enlaces a internet.
- Verificar los métodos para resolución de problemas de hardware y software.

| ALCANCE

Activos relacionados a los sitios CATD Amacuzac, Atlatlahucan, Jojutla, Tepoztlán, Tlaltizapán, Tlalnepantla, Tlaquiltenango, Tlayacapan, **Totolapan**, Zacatepec, Yautepec, Tetecala, Ocuituco, Tetela del volcán CATD Temoac, Yecapixtla, Cuernavaca, Jonacatepec, Jonacatepec, Zacualpan de Amilpas, Jantetelco, Jiutepec, Mazatepec, Coatlán de Río, Coatetelco, Cuautla, Temixco, Miacatlán, Puente de Ixtla y Hueyapan

| RESUMEN EJECUTIVO

Durante las visitas se identificaron oportunidades de mejora las cuales fueron emitidas por el ente auditor para consideración del IMEPEPAC y de la empresa informática electoral para su resolución.

| CONCLUSIONES

Se recomienda:

- La correcta instalación de la red física de cableado estructurado, evitando cables expuestos en el piso y mal enrutados.
- La correcta administración de cableado eléctrico de datos, equipo de comunicaciones y etiquetado.
- Se realicen las pruebas de alta disponibilidad de enlaces de internet.
- El correcto monitoreo de las direcciones IP públicas de los dos enlaces de internet.
- Se cuente con equipo de seguridad contra incendios.
- Se verifique el correcto funcionamiento de la planta de emergencia en conjunto con la instalación existente.
- Se verifique el cumplimiento de las velocidades de cada uno de los enlaces de internet.
- Se limite el libre acceso a la red alámbrica e inalámbrica a dispositivos ajenos al proceso.
- Se realice la correcta organización física de los dispositivos de comunicaciones como firewall, módems, UPS y teléfono IP que permita disminuir los riesgos de la interrupción de la continuidad de la operación de los servicios.
- Se verifique la seguridad de los dispositivos finales en general incluyendo equipos de telefonía celular.

Universidad Autónoma del Estado de Morelos

UAEM
RECTORÍA
2023-2029

Coordinación
General de Planeación y
Desarrollo Sustentable

DGTIC
Dirección General de Tecnologías
de Información y Comunicación

impepac
Instituto Morelense
de Procesos Electorales
y Participación Ciudadana

UAEM | *Por una humanidad culta*

© 2024 · Dirección General de Tecnologías de Información y Comunicación · www.uaem.mx