INFORME FINAL

"SERVICIO DE AUDITORÍA AL SISTEMA INFORMÁTICO Y A LA INFRAESTRUCTURA TECNOLÓGICA DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES DEL INSTITUTO ELECTORAL DEL ESTADO DE MÉXICO 2021"

INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

UNIDAD CULHUACAN

SECCIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN

AV. SANTA ANA NO. 1000 COL. CULHUACÁN CTM SECCIÓN V C.P. 04440, DELEGACIÓN COYOACÁN, CIUDAD DE MÉXICO.

ID	APREP.E04
VERSIÓN	2.0
REVISIÓN	1.0
FECHA	15 DE JUNIO DE 2021

IEEM Instituto Electoral del Estado de México	ING. JOSÉ PABLO CARMONA VILLENA DIRECTOR DEL PROYECTO IEEM	M.S.I. DARÍO MEDINA RAMÍREZ RESPONSABLE DEL PROYECTO SEPI ESIME CULHUACAN	IPN

Tabla de contenido

1. Aviso de propiedad

Restricciones de uso y divulgación del contenido.

El **INSTITUTO POLITÉCNICO NACIONAL** traslada a quien recibe, el resguardo y buen uso de la información total o parcial del presente documento, siendo el **INSTITUTO ELECTORAL DEL ESTADO DE MÉXICO** quien tiene los derechos de uso y divulgación de esta información, utilizando las cláusulas previstas en el convenio de colaboración y su anexo técnico entre ambas instituciones firmado el 3 de marzo de 2021.

2. Alcance del Documento

De acuerdo con el Plan de Trabajo de Auditoría del **"Servicio de Auditoría al Sistema Informático y a la Infraestructura Tecnológica del Programa de Resultados Preliminares del Instituto Electoral del Estado de México 2021"**, en el presente documento se presenta el Informe Final de las actividades desarrolladas durante el servicio.

3. Introducción

En el marco de las actividades para la implementación y operación del Programa de Resultados Electorales Preliminares (PREP) para el Proceso Electoral Local 2021 en el Estado de México, se requirió llevar 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.

El Instituto Politécnico Nacional a través de la Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán fue seleccionado como Ente Auditor para prestar el "Servicio de Auditoría al Sistema Informático y a la Infraestructura Tecnológica del Programa de Resultados Electorales Preliminares del Instituto Electoral del Estado de México 2021" en las seis líneas de trabajo requeridas que permitiera fortalecer el esfuerzo emprendido por el Instituto Electoral del Estado de México (IEEM) para lograr que la Jornada Electoral que se llevará a cabo el 6 de junio de 2021 cumpla con los principios de certeza, legalidad, independencia, imparcialidad, máxima publicidad y objetividad que la sociedad mexiquense exige, aportando la experiencia, conocimientos, responsabilidad y compromiso que caracterizan al Equipo de Trabajo del IPN designado para dar atención a este importante proyecto de alcance estatal.

El objetivo del servicio de auditoría es realizar la revisión del sistema informático del PREP desde una perspectiva de caja negra, así como realizar pruebas de seguridad a la infraestructura tecnológica y emitir una opinión objetiva e imparcial si es confiable y realiza las operaciones y funciones para las cuales fue diseñado de acuerdo con el Proceso Técnico Operativo (PTO).

4. Alcance de Auditoría

El alcance del servicio de auditoría al sistema informático y a la infraestructura tecnológica del Programa de Resultados Electorales Preliminares del Instituto Electoral del Estado de México 2021 contempla las siguientes líneas de trabajo:

- Pruebas funcionales de caja negra al sistema informático del PREP 2021 y a la aplicación móvil que se utilizará para operar el mecanismo de digitalización de las Actas desde la casilla.
- Validación del sistema informático del PREP y de sus bases de datos, ante un tercero con fe pública.
- Análisis de vulnerabilidades a la infraestructura tecnológica.
- Pruebas de negación de servicio al sitio de publicación del PREP y al sitio principal del IEEM.
- Análisis al Código Fuente en materia de Seguridad.
- Revisión de las pantallas de publicación del PREP, verificando el apego a las pantallas base de la interfaz proporcionadas por el Instituto.

5. Actividades Realizadas

Dentro de las actividades realizadas del Servicio de Auditoría se destacan las siguientes actividades:

5.1 Reuniones de Trabajo

Se llevaron a cabo 43 reuniones de trabajo en modalidad virtual y presencial para capacitación, solicitud de requerimientos, aclaración de dudas de requerimientos, revisión de requerimientos y seguimiento de actividades, entre otras, de las cuales se generó su minuta respectiva.

5.2 Recopilación y Análisis Documental

Se tienen registradas 31 fechas en las que se realizaron entregas documentales para las diferentes líneas de trabajo por parte del IEEM cada una analizada por el equipo auditor del IPN.

5.3 Análisis de Requerimientos

El Equipo Auditor del IPN realizó diferentes Análisis de Requerimientos Iniciales con la Información e insumos proporcionados por el IEEM. (Se anexa versión 4 de Análisis de Requerimientos de Sistemas de fecha 2 de junio de 2021).

5.4 Acompañamiento en Pruebas Funcionales y Simulacros del sistema PREP

El Equipo Auditor del IPN estuvo presente en 2 Pruebas Funcionales, 3 Simulacros y 1 Prueba Técnica del sistema PREP llevadas a cabo en las instalaciones del Instituto Electoral del Estado de México.

6. Ejecución de Auditoría

De acuerdo con el Plan de Trabajo de Auditoría v1.1 autorizado, el avance que tuvieron las actividades de las diferentes líneas de trabajo, algunas de ellas afectadas por la falta de entrega de requerimientos de tipo documental y entornos adecuados para la ejecución de las pruebas respectivas, se presenta en los siguientes apartados:

6.1 Pruebas funcionales de caja negra al sistema informático del PREP 2021 y a la aplicación móvil que se utilizará para operar el mecanismo de digitalización de las Actas desde la casilla

#	Actividad	Avance Esperado a la fecha	Avance Real a la Fecha
27	Diseño de Pruebas Funcionales	100%	80%
28	Ejecución de Pruebas en Ambiente Preliminar	100%	0%
29	Ejecución de Pruebas en Ambiente Final	100%	0%
31	Atención de Hallazgos (IEEM)	100%	0%
32	Segunda Vuelta de Pruebas Funcionales (Validación de hallazgos)	100%	0%

6.2 Validación del sistema informático del PREP y de sus bases de datos, ante un tercero con fe pública

#	Actividad	Avance Esperado a la fecha	Avance Real a la Fecha
36	Sesiones Técnicas sobre la infraestructura	100%	20%
38	Diseño del Procedimiento técnico de extracción y validación de huellas y de las bases de datos	80%	75%
39	Ejecución de pruebas del procedimiento de validación	100%	0%
40	Ejecución del procedimiento de extracción de huellas	100%	0%

6.3 Análisis de vulnerabilidades a la infraestructura tecnológica y Revisión de Configuraciones

#	Actividad	Avance Esperado a la fecha	Avance Real a la Fecha
46	Preparación de entornos y equipos de trabajo	100%	100%
47	Ejecución de Análisis de vulnerabilidades	100%	100%
48	Revisión de configuraciones de la plataforma en la materia de seguridad	100%	100%
49	Ejecución de pruebas de penetración	100%	100%
52	Atención de Hallazgos (IEEM)	100%	55%
53	Pruebas de seguimiento (Validación de hallazgos)	100%	0%

6.4 Pruebas de negación de servicio al sitio de publicación del PREP y al sitio principal del IEEM

#	Actividad	Avance Esperado a la fecha	Avance Real a la Fecha
59	Preparación de entornos y equipos de trabajo	100%	100%
61	Ejecución de Pruebas de Negación de Servicio	100%	100%
63	Atención de Hallazgos (IEEM)	100%	100%
64	Pruebas de seguimiento (Validación de hallazgos)	100%	100%

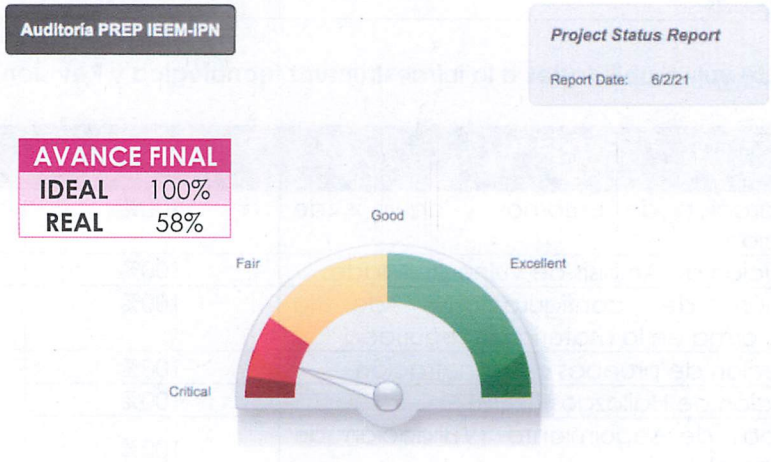
6.5 Análisis al Código Fuente en materia de Seguridad

#	Actividad	Avance Esperado a la fecha	Avance Real a la Fecha
67	Preparación de entornos y equipos de trabajo	100%	100%
68	Ejecución de Pruebas al Código Fuente	100%	95%
71	Atención de Hallazgos (IEEM)	100%	0%
72	Pruebas de seguimiento (Validación de hallazgos)	100%	0%

6.6 Revisión de las pantallas de publicación del PREP.

#	Actividad	Avance Esperado a la fecha	Avance Real a la Fecha
75	Ejecución de las validaciones	100%	0%
77	Segunda Vuelta de Pruebas Funcionales (Validación de hallazgos)	100%	0%

El estado a la fecha de avance general de las actividades de auditoría se presenta en el siguiente gráfico.



Nota: Los atrasos en las actividades presentados a lo largo del servicio de auditoría no son imputables al ente auditor, estás se debieron principalmente a los retrasos de entrega de información y requerimientos por parte del IEEM, especialmente por la falta de disponibilidad de un entorno de uso exclusivo para pruebas funcionales.

7. Entregables generados

A continuación, se presenta el estado del listado de entregables comprometidos del servicio de auditoría.

Servicio de Auditoría al Sistema Informático y a la Infraestructura Tecnológica del Programa de Resultados Preliminares del Instituto Electoral del Estado de México 2021			
ID	**Documento**	**Estado**	**Fecha de Entrega**
Auditoría General			
APREP.E01	**Plan de Trabajo de Auditoría**	Entregado	25/marzo/2021
APREP.E02	**Informe de Avance de Auditoría**	Entregado	5/abril/2021 5/mayo/2021
APREP.E03	**Minuta de Cierre de Auditoría**	Entregado	2/jun/2021
APREP.E04	**Informe Final de Auditoría y Acta de Cierre de Auditoría**	Entregado	3/jun/2021
Pruebas funcionales de caja negra al sistema informático del PREP 2021 y a la aplicación móvil que se utilizará para operar el mecanismo de digitalización de las Actas desde la casilla			
PFCN.E01	**Plan de pruebas funcionales de caja negra del sistema informático**	Entregado	26/marzo/2021
PFCN.E02	**Informe preliminar de las pruebas funcionales de caja negra del sistema informático**	Entregado	30/abril/2021
PFCN.E03	**Informe final de las pruebas funcionales de caja negra del sistema informático**	No generado por falta de entorno de uso exclusivo para pruebas funcionales	Oficio SEPI/0363/2021 31/mayo/2021
PFCN.E04	**Informe de desempeño de la operación del sistema informático**	No generado por falta de entorno de uso exclusivo para pruebas funcionales	Oficio SEPI/0363/2021 31/mayo/2021

Servicio de Auditoría al Sistema Informático y a la Infraestructura Tecnológica del Programa de Resultados Preliminares del Instituto Electoral del Estado de México 2021			
ID	**Documento**	**Estado**	**Fecha de Entrega**
Validación del sistema informático del PREP 2021 y de sus Bases de Datos, ante un tercero con fe pública			
VSBD.E01	**Plan de trabajo de Validación del sistema informático**	No generado por falta de información y entorno de uso exclusivo para pruebas	Oficio SEPI/0364/2021 31/mayo/2021
VSBD.E02	**Procedimiento técnico con el esquema de validación de los programas y de la base de datos**	No generado por falta de información y entorno de uso exclusivo para pruebas	Oficio SEPI/0364/2021 31/mayo/2021
VSBD.E03	**Constancia de hechos de la validación de los programas y de la base de datos**	El ente auditor al no estar en posibilidad de generar un procedimiento técnico, no puede presentar una constancia de hechos ante un tercero de fe pública	Oficio SEPI/0364/2021 31/mayo/2021
Análisis de vulnerabilidades a la infraestructura tecnológica			
AVIT.E01	**Plan de pruebas de penetración a la infraestructura tecnológica**	Entregado	26/marzo/2021
AVIT.E02	**Informe preliminar de las pruebas de penetración a la infraestructura tecnológica**	Entregado	6/mayo/2021
AVIT.E03	**Informe de verificación de la aplicación de recomendaciones resultado de las pruebas de penetración a la infraestructura tecnológica**	Entregado	31/mayo/2021
AVIT.E04	**Plan de revisión de configuraciones de la infraestructura**	Entregado	26/marzo/2021
AVIT.E05	**Informe preliminar de revisión de configuraciones de la infraestructura tecnológica**	Entregado	6/mayo/2021
AVIT.E06	**Informe de la aplicación de recomendaciones de la revisión de configuraciones de la infraestructura**	Entregado	31/mayo/2021

Servicio de Auditoría al Sistema Informático y a la Infraestructura Tecnológica del Programa de Resultados Preliminares del Instituto Electoral del Estado de México 2021			
ID	**Documento**	**Estado**	**Fecha de Entrega**
AVIT.E07	**Informe final del análisis de vulnerabilidades a la infraestructura tecnológica.**	Entregado	31/mayo/2021
AVIT.E08	**Informe de Desempeño de la operación del sistema informático**	No generado por falta de acceso al sistema e infraestructura en última versión y en producción	Oficio SEPI/0365/2021 31/mayo/2021
Pruebas de Negación de Servicio a sitios web del PREP y al sitio principal del IEEM			
PNSW.E01	**Plan de trabajo detallado**	Entregado	26/marzo/2021
PNSW.E02	**Plan de ataque de negación de servicio**	Entregado	15/abril/2021
PNSW.E03	**Informe de resultados Estadísticas del tráfico de red generado**	Entregado	31/mayo/2021
Auditoría al Código Fuente en materia de seguridad			
ACFS.E01	**Reportes de hallazgos identificados**	Entregado	26/abril/2021
ACFS.E02	**Reportes preliminares de las pruebas (Web y Móvil)**	Entregado	31/mayo/2021
ACFS.E03	**Informes Finales de Pruebas (uno por cada tipo WEB y Móvil)**	Entregado	2/junio/2021
Revisión de pantallas de publicación del PREP, verificando el apego a las pantallas base de la interfaz proporcionada por el Instituto			
RPPP.E01	**Reporte Final**	No generado por falta de entorno de uso exclusivo para pruebas funcionales	Oficio SEPI/0363/2021 31/mayo/2021
RPPP.E02	**Informe Ejecutivo**	No generado por falta de entorno de uso exclusivo para pruebas funcionales	Oficio SEPI/0363/2021 31/mayo/2021

8. Resultados y Recomendaciones

A continuación se presentan los resultados y recomendaciones que emite el ente auditor por cada línea de trabajo establecida en el alcance del **"Servicio de Auditoría al Sistema Informático y a la Infraestructura Tecnológica del Programa de Resultados Preliminares del Instituto Electoral del Estado de México 2021"**.

8.1 Pruebas funcionales de caja negra al sistema informático del PREP 2021 y a la aplicación móvil que se utilizará para operar el mecanismo de digitalización de las Actas desde la casilla.

8.1.1 Pruebas Realizadas

No se pudieron ejecutar pruebas de la línea de pruebas funcionales por falta del cumplimiento al requerimiento PFCN.R03 sobre la entrega de un entorno de uso exclusivo ni en ambiente preliminar, ni en ambiente final por parte del IEEM en las fechas o espacio de tiempo para la realización de las actividades.

8.1.2 Hallazgos

El equipo auditor del Instituto Politécnico Nacional no pudo reportar hallazgos en el sistema de bug tracking Mantis debido a la falta del cumplimiento al requerimiento PFCN.R03 sobre la entrega de un entorno de uso exclusivo por parte del IEEM.

Impacto de Hallazgos		
Bajo	Medio	Alto
0	0	0

8.1.3 Conclusiones y recomendaciones de Pruebas Funcionales

El equipo auditor del Instituto Politécnico Nacional no se encuentra en posibilidad de determinar una conclusión y/o recomendación, debido a que no se pudieron ejecutar los ciclos de prueba previstos para la línea de trabajo, situación causada por falta del cumplimiento al requerimiento PFCN.R03 sobre la entrega de un entorno de uso exclusivo por parte del IEEM.

8.2 Validación del sistema informático del PREP y de sus bases de datos, ante un tercero con fe pública.

8.2.1 Actividades Realizadas

Los scripts desarrollados por el equipo auditor del Instituto Politécnico Nacional, encargados de la validación del sistema informático y de sus bases de datos, no pudieron ser completados debido a la falta de precisión en la información correspondiente a la definición, roles, responsables y configuraciones de los artefactos involucrados en el sistema PREP, además del

incumplimiento en la entrega del entorno de uso exclusivo para la revisión de Pruebas Funcionales de Caja Negra previa a la validación.

8.2.2 Hallazgos

Debido al incumplimiento por parte del IEEM de los requerimientos solicitados por el IPN para la generación de un proceso de validación, no se pudo concluir el diseño y ejecución de la validación del sistema informático del PREP y de sus bases de datos, sin embargo es de informarse que, con base a la información proporcionada por el IEEM, el equipo técnico auditor identificó un cambio completo del código base de la aplicación para la digitalización de actas con la integración de un desarrollo externo de un tercero, agregando con ello artefactos adicionales a los ya contemplados en la etapa de análisis de documentación de la auditoría.

Impacto de Hallazgos		
Bajo	Medio	Alto
0	0	0

8.2.3 Conclusiones y recomendaciones de Validación del Sistema y sus Bases de Datos

El equipo auditor del Instituto Politécnico Nacional no se encuentra en posibilidad de determinar una conclusión referente a la validación del sistema informático del PREP y de sus bases de datos, debido a que no se pudieron ejecutar los ciclos de prueba planeados en pruebas funcionales y simulacros situación causada por la falta de cumplimiento a los requerimientos establecidos para la validación del sistema.

Se recomienda ampliamente al IEEM que haga uso de un proceso de desarrollo de software de inicio a fin contemplando planeación, roles, responsables, definición de etapas, tiempos estimados, entornos, pruebas unitarias y pruebas de integración, con un análisis previo bien definido para evitar cambios significativos no programados en la codificación del sistema, artefactos y/o arquitectura.

8.3 Análisis de vulnerabilidades a la infraestructura tecnológica y Revisión de Configuraciones.

8.3.1 Pruebas Realizadas

Se desarrolló un conjunto de revisión con una batería de pruebas y herramientas técnicas de caja negra, desde el interior y desde el exterior de la red de datos, para la identificación de vulnerabilidades y/o debilidades en la configuración de la infraestructura tecnológica puesta a disposición del ente auditor por el IEEM y que dan soporte al sistema PREP (servidores, equipos de telecomunicaciones, estaciones de trabajo designadas como muestra por el IEEM que se usarán en: CATD, CCV y CESCO, dispositivos móviles, servidores de dase de datos, firewalls y sistema de gestión de móviles MDM). Las pruebas se limitaron en términos de análisis de vulnerabilidades y pruebas con herramientas tecnológicas y técnica de revisión por pares

y de Penetration Testing (pentest), las cuales, tuvieron como marco los siguientes estándares y buenas prácticas: OSSTMM 3 (Open Source Security Testing Methodology Manual versión 3), Guías de Fortalecimiento de seguridad RedHat, Guía de Cloud Controls Matrix V4 y Consensus Assessment Initiative Questionnaire (CAIQ) de Cloud Security Alliance (CSA), Guía de Configuraciones de Seguridad de Sistemas Knox Samsung, y Guías de seguridad disponibles en los sitios oficiales de proveedores (RedHat y Fortinet).

El ente auditado en solicitud documentada puso a disposición del ente auditor para realizar actividades de evaluación, una infraestructura a título de "producción", misma que en la fecha de cierre del presente informe, no tuvo integrada la última versión de los artefactos y aplicativos que soportan el sistema PREP.

8.3.2 Hallazgos

Se detectaron 32 hallazgos identificados (análisis de vulnerabilidades y revisión de configuraciones) por el equipo auditor del Instituto Politécnico Nacional durante el diseño y ejecución de pruebas, que fueron registrados y clasificados en el sistema Mantis del Instituto Electoral del Estado de México con evidencia de soporte. De los cuales pudo verificarse a la fecha, que fueron atendidos y remediados 3 hallazgos de impacto alto por el IEEM.

	Impacto de Hallazgos		
Situación	Bajo	Medio	Alto
Atendidos	0	0	3
No atendidos	1	11	17

8.3.3 Conclusiones y recomendaciones de Análisis de vulnerabilidades a la infraestructura tecnológica y Revisión de Configuraciones

En conclusión, con solo tres hallazgos atendidos de un total de treinta y dos, y las circunstancias concurrentes anteriormente citadas y con el más alto sentido ético: "... a este ente auditor, no le es posible emitir criterio en sentido positivo respecto a que exista un nivel de riesgo de seguridad adecuado, como resultado del análisis de vulnerabilidades y revisión de configuraciones de la Infraestructura Tecnológica que soporta la operación del sistema PREP".

Por lo anterior se permite recomendar lo siguiente:

1. El ente auditado deberá gestionar a través del sistema de bug tracking Mantis, la atención de las remediaciones a las áreas de oportunidad y mejora emitidas por el ente auditor. En su caso, revisar los tickets que no han sido atendidos en razón de su nivel de impacto y prioridad para solicitar que se cierren por no estar en posibilidades de atenderlos o tratarse de infraestructura ajena que no participará en la jornada.
2. El ente auditado deberá identificar bajo un análisis de costo-beneficio la conveniencia y factibilidad de implementar los controles de seguridad recomendados por el ente auditor incorporándolas en un ciclo de mejora continua.

3. Como área de mejora se identifica que la infraestructura tecnológica que emplea de forma interna el IEEM, debería de contar con mecanismos de monitoreo interior con herramientas de detección y contención de código malicioso a nivel de red, específicamente para el repositorio de archivos digitales de actas y en los firewalls de frontera.

8.4 Pruebas de negación de servicio al sitio de publicación del PREP y al sitio principal del IEEM

8.4.1 Pruebas Realizadas

Se realizó la evaluación de seguridad de la disponibilidad a través de la técnica de ataques de negación de servicio y pruebas de disponibilidad con tráfico recurrente a los sitios de dominio prep.ieem.org.mx y www.ieem.org.mx.

El conjunto de pruebas se efectuaron bajo el principio de caja gris y considerando los siguientes ataques y protocolos:

- Pruebas a nivel de aplicación. Web fuzzer, http smuggling, http injection, inundación por HTTP-Request, HTTP Slowloris.
- Pruebas a nivel de capa de transporte. NTP, SNMP, CLDAP, LDAP, ACK, DNS, SQLPING, SSYN, TCP-SYN.
- Pruebas a nivel de capa de red. Mensajes ICMP.

8.4.2 Hallazgos

Se detectaron 4 hallazgos identificados por el equipo auditor del Instituto Politécnico Nacional durante el diseño y ejecución de pruebas, que fueron registrados y clasificados en el sistema de bug tracking Mantis del Instituto Electoral del Estado de México con evidencia de soporte asimismo fueron atendidos por el IEEM y disminuyó el nivel de riesgo.

Impacto de Hallazgos		
Bajo	Medio	Alto
4	0	0

8.4.3 Conclusiones y recomendaciones de Pruebas de Negación de Servicio Web

El ente auditor se permite concluir respecto a la disponibilidad del sistema revisado, lo siguiente: "...que habiendo identificado que la infraestructura que aloja los dominios www.ieem.org.mx y prep.ieem.org.mx (mismos que se encuentran alojados y redireccionados respectivamente en la infraestructura de AWS que cuenta con servicios de WAF), mostró un esquema robusto de direcciones IP's redundantes y configuraciones, que conforme a las pruebas de seguridad y de volumen de tráfico realizadas, permiten mantener la disponibilidad del servicio para la publicación de resultados".

Por lo anterior se permite recomendar lo siguiente:

1. El IEEM deberá fortalecer el conocimiento o contar con personal capacitado para la gestión e identificación de ataques del tipo de negación de servicio, a fin de detectar de manera oportuna algún incidente relacionado, recomendándose dominar a nivel de análisis los módulos: VPC Traffic Mirroring y herramientas Packer Analyzer del proveedor de nube que fue evaluado.
2. El IEEM deberá considerar si la configuración en el sitio prep.ieem.org.mx para atender solamente peticiones de direcciones IP registradas desde México y E.U.A. es la decisión más adecuada, en virtud de que al realizar consultas al sitio desde el extranjero y que como resultado presenten un error de falta de disponibilidad debido a las políticas de restricción, esto se podría interpretar por usuarios sin conocimientos informáticos que el sitio se encuentra fuera de servicio.
3. El ente auditado deberá gestionar a través del sistema de bug tracking Mantis, la atención de las remediaciones a las áreas de oportunidad y mejora emitidas por el ente auditor al observar que persisten los tickets de atención abiertos.

8.5 Análisis al Código Fuente en materia de Seguridad.

8.5.1 Pruebas Realizadas

Pruebas de caja negra y de caja blanca, con la técnica de análisis estático y dinámico, ejecutando una batería de pruebas para auditoría de seguridad al código fuente del servidor web del PREP y de la aplicación móvil del sistema informático e infraestructura del PREP, basadas en metodologías de verificación de seguridad del proyecto OWASP, revisión de usuarios con privilegios, validación de diferentes roles de usuario, revisión y análisis de la fuerza de los algoritmos de cifrado empleados en los artefactos y aplicaciones, interacciones con las plataformas donde fueron instalados y verificación de la seguridad de la comunicación entre los componentes del sistema PREP.

8.5.2 Hallazgos

Se detectaron 28 hallazgos identificados por el equipo auditor del Instituto Politécnico Nacional durante el diseño y ejecución de pruebas, que fueron registrados y clasificados en el sistema Mantis del Instituto Electoral del Estado de México con evidencia de soporte. La mayoría de los hallazgos son atribuibles a cambios significativos recientes en el código por una reingeniería de los artefactos y aplicación móvil que componen el sistema.

Impacto de Hallazgos		
Bajo	Medio	Alto
1	3	24

8.5.3 Conclusiones y recomendaciones de Análisis al Código Fuente en Materia de Seguridad

Al encontrarse cercana la fecha de realización de la jornada electoral y circunstancias, no atribuibles al ente auditor, ocasionados por los retrasos mostrados por el equipo de desarrollo del IEEM respecto de la entrega de los códigos a revisar del sistema PREP y aplicación móvil,

al ente auditor "NO" le fue posible verificar si el ente auditado realizó acciones para la atención de las vulnerabilidades o fallas reportadas, por lo que no le es posible emitir conclusión en sentido positiva respecto al nivel de riesgo de seguridad, como resultado de la Auditoría al código fuente de los artefactos y App móvil que soportan la operación del sistema PREP.

Por lo anterior se permite emitir las siguientes recomendaciones:

1. Considerar a mediano plazo, contar con personal con conocimientos de seguridad informática para el diseño e implementación de controles de seguridad en proyectos posteriores, a fin de incorporar los requerimientos de seguridad desde el inicio y estar en posibilidad de ejecutar un proceso de revisión o auditoría en esta materia.
2. Considerar como área de oportunidad, fortalecer a su personal con conocimientos de gestión de proyectos de desarrollo de sistemas, a fin de dimensionar los requerimientos humanos, financieros y materiales, para realizar sus entregas en tiempo y forma.
3. Se recomienda que los hallazgos identificados durante la presente auditoría no sean descartados y se incorporen como parte de los requisitos de diseño en la programación de versiones posteriores, estableciendo un ciclo de mejora continua.

8.6 Revisión de las pantallas de publicación del PREP.

8.6.1 Pruebas Realizadas

No se pudieron ejecutar pruebas de la línea de pruebas funcionales por falta del cumplimiento al requerimiento PFCN.R03 sobre la entrega de un entorno de uso exclusivo ni en ambiente preliminar, ni en ambiente final por parte del IEEM en las fechas o espacio de tiempo para la realización de las actividades.

8.6.2 Hallazgos

El equipo auditor del Instituto Politécnico Nacional no pudo reportar hallazgos en el sistema de bug tracking Mantis debido a la falta del cumplimiento al requerimiento PFCN.R03 sobre la entrega de un entorno de uso exclusivo por parte del IEEM.

Impacto de Hallazgos		
Bajo	Medio	Alto
0	0	0

8.6.3 Conclusiones y recomendaciones de Revisión de las pantallas de publicación del PREP

El equipo auditor del Instituto Politécnico Nacional no se encuentra en posibilidad de determinar una conclusión y/o recomendación, debido a que no se pudieron ejecutar los ciclos de prueba previstos para la línea de trabajo, situación causada por falta del cumplimiento al requerimiento PFCN.R03 sobre la entrega de un entorno de uso exclusivo por parte del IEEM.

9. Conclusiones Generales

Como resultado del análisis de los trabajos realizados en las diferentes líneas motivo del alcance del **"Servicio de auditoría al Sistema Informático y a la Infraestructura Tecnológica del Programa de Resultados Preliminares del Instituto Electoral del Estado de México 2021"**, el ente auditor concluye lo siguiente:

- En cuanto a los servicios de nube contratados con el proveedor Amazon Web Services (AWS) para la publicación de los resultados del PREP, a los que este ente auditor realizó pruebas de carga y negación de servicio conforme a las características solicitadas por el IEEM, este ente auditor dictamina que "resultaron satisfactorias para mantener la disponibilidad del servicio".
- Respecto a las pruebas funcionales de caja negra, validación del sistema y sus bases de datos y revisión de las pantallas de publicación del PREP, y derivado del incumplimiento por parte del IEEM en la entrega de información, de los requerimientos solicitados por el IPN y la inviabilidad de ejecución de este tipo de pruebas en tiempos menores a 3 semanas, este ente auditor "No puede emitir un dictamen en ningún sentido acerca del funcionamiento del sistema PREP para los procesos de digitalización, captura, procesamiento, publicación y difusión de los resultados preliminares", a razón de que no han sido validados con base en la metodología de auditoría acordada entre el ente auditor y el IEEM u otro ente imparcial para dar certeza del cumplimiento a la normativa aplicable y requerimientos funcionales.
- Finalmente, el nivel de impacto de los hallazgos de seguridad identificados en la infraestructura tecnológica que soporta el sistema PREP, la falta de entrega de las versiones definitivas de todos los componentes del sistema PREP y la inviabilidad para verificar que se hayan ejecutado acciones de remediación para atender los hallazgos en el tiempo menor a 72 horas, el equipo auditor del IPN concluye que "existe un alto nivel de riesgo para la operación del sistema PREP y su aplicación móvil, dejando la decisión final de su puesta en operación el día de la jornada electoral a la Unidad de Informática y Estadística del IEEM".

10. Firmas de Aceptación

Por medio del presente, se firma de conformidad este documento.

POR EL INSTITUTO POLITÉCNICO NACIONAL	POR EL INSTITUTO ELECTORAL DEL ESTADO DE MÉXICO
M.S.I. Darío Medina Ramírez	Ing. José Pablo Carmona Villena
	Mtro. Aldo Idulio Hernández Cuevas