Anexo 1

Especificaciones técnicas para la contratación de servicios de **auditoría** al sistema informático y a la infraestructura tecnológica del **Programa de Resultados Electorales Preliminares**

PEL 2017-2018

Contenido

Glosario

PREP: Programa de Resultados Electorales Preliminares.

IEPC: Instituto Electoral y de Participación Ciudadana del Estado de Durango.

Reglamento de elecciones: Reglamento de Elecciones emitido por el Instituto Nacional Electoral.

INE: Instituto Nacional Electoral.

.

SERVICIOS DE AUDITORÍA AL SISTEMA INFORMÁTICO Y A LA INFRAESTRUCTURA TECNOLÓGICA DEL PREP

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 Durango, 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.

Para tal efecto, en el presente documento se describe el alcance que el proveedor de servicios deberá cumplir, en caso de ser seleccionado como ente auditor. Asimismo, se detallan los requerimientos de cada línea de trabajo que deberán considerarse en la propuesta técnico-económica que se presente ante el Instituto Electoral y de Participación Ciudadana del Estado de Durango. Las líneas de trabajo a considerar son:

1.1. Pruebas funcionales de caja negra al sistema informático del PREP 2018.
1.2. Validación del sistema informático del PREP y de sus bases de datos.
1.3. Análisis de vulnerabilidades a la infraestructura tecnológica.
1.4. Pruebas de negación de servicio al sitio web del PREP y al sitio principal del **IEPC**.

1.1 Pruebas funcionales de caja negra al sistema informático del PREP

a. Objetivo

El ente auditor deberá analizar el sistema informático del PREP, mediante la realización 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.

b. Alcance

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

- Se debe analizar el funcionamiento de la aplicación en relación con las fases del proceso técnico operativo, considerando al menos, la **digitalización, captura y publicación de resultados,** mediante flujos completos e interacción entre los diversos módulos.
- Se debe verificar el cumplimiento de las especificaciones funcionales y requerimientos contenidos en la documentación técnica y normatividad aplicable que será proporcionada por el **IEPC**.
- 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.

El alcance de las pruebas funcionales de caja negra deberá incluir los siguientes módulos del sistema informático del PREP:

I. Módulo de Digitalización, Captura y Validación
   - Obtención de la imagen digital del acta.
   - Captura de la información contenida en las Actas PREP.
   - Validación de la información capturada.

II. Módulo de Publicación de Resultados
   - 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.

Para realizar las pruebas, el **IEPC** deberá proporcionar los insumos de información necesarios, entre los que se encuentran, de manera enunciativa más no limitativa, los señalados en el apartado 1.6 del presente Anexo.

c. Entregables

El ente auditor deberá entregar los siguientes documentos derivados de los trabajos realizados:

Entregable	Descripción y Contenido	Criterios de Aceptación
Plan de pruebas funcionales de caja negra del sistema informático	Describe los elementos generales que deben considerarse para la realización de las pruebas funcionales de caja negra: • Introducción • Objetivo • Alcance • Pruebas a aplicar • Planeación de las pruebas • Necesidades de ambiente • Casos de prueba • Datos de prueba • Criterios de pruebas • Administración de riesgos • Entregables	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.
Informe preliminar de las pruebas funcionales de caja negra del sistema informático	Documento que contiene el detalle de cada una de las observaciones identificadas en la revisión y pruebas del sistema y que incluya, al menos: • Introducción • Metodología • Criterios utilizados para la auditoria • Metodología para clasificar los hallazgos • Observaciones y recomendaciones • Conclusiones	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.
Informe final de las pruebas funcionales de caja negra del sistema informático	Documento que contiene el resultado final de las pruebas del sistema: • Introducción • Metodología • Criterios utilizados para la auditoría • Resumen ejecutivo • Resultados	Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.

d. Calendario de trabajo.

El calendario de actividades para esta línea de trabajo deberá establecer, de forma clara, los periodos para la ejecución de cada actividad y los avances esperados en cada periodo de trabajo.

1.2 Validación del sistema informático del PREP y de sus bases de datos

a. Objetivo

Validar que el sistema informático del PREP que operará el día de la Jornada Electoral, corresponda al software auditado, así como que la base de datos se encuentre sin registros adicionales a los necesarios para que el sistema opere. La validación respecto a la correspondencia del software auditado y el utilizado en la operación del PREP, se tendrá que realizar al inicio, durante y al final de la operación del sistema informático del PREP.

b. Alcance

Especialistas del ente auditor deberán llevar a cabo un procedimiento técnico para verificar que los programas auditados se encuentren operando desde el inicio y hasta el cierre de operación del sistema informático del PREP, así como que la base de datos

se encuentre debidamente inicializada. Dicho procedimiento deberá ser validado por el personal que el **IEPC** designe para tal efecto, contemplando los siguientes aspectos como mínimo:

- El procedimiento deberá contar con un diagrama de flujo.
- El procedimiento deberá incluir los roles y responsabilidades de los involucrados.
- El procedimiento deberá documentar como mínimo, las siguientes etapas:
    - Generación, obtención y validación de huellas criptográficas en SHA-256 del software PREP auditado.
    - Generación, obtención y validación de huellas criptográficas en SHA-256 del software PREP instalado en el ambiente productivo que operará el día de la Jornada Electoral.
    - Validación de la información inicial y final de la base de datos del PREP.
    - Constancia de hechos.

El procedimiento deberá realizarse el domingo 1° de julio de 2018 en las instalaciones del **IEPC**, concluyendo el 2 de julio y deberá ser atestiguado preferentemente por un tercero con fe pública designado por el **IEPC**, conforme se señala en el inciso I del numeral 23, Capítulo I, Título III del Anexo 13 del Reglamento de Elecciones.

c. Entregables

Los productos para entregar, por parte del ente auditor, deberán incluir:

- Plan de trabajo detallado que cuente, como mínimo, con: el desglose de actividades, entregables, duración, fecha inicio, fecha fin y responsables de las actividades.

- Procedimiento técnico con el esquema de validación de los programas y de la base de datos del sistema informático previamente auditado del PREP, junto con las etapas de validación, generación de diagramas y descripciones correspondiente que se acuerden conjuntamente entre el **IEPC** y el ente auditor.

- Constancia de hechos de la generación de huellas criptográficas de los programas probados del sistema informático del PREP. Esta constancia deberá describir el protocolo de la actividad, fecha y lugar, hora de inicio y término, objetivo, actividades realizadas, resultados obtenidos y las firmas autógrafas del personal participante por parte del **IEPC** y del ente auditor.

- Constancias de hechos de la validación de los programas y de la base de datos del sistema informático del PREP. Estas validaciones se deberán realizar previo al inicio, durante y posterior al cierre de operaciones del PREP y deberán describir el protocolo de validación en el ambiente de producción del sistema informático del PREP. Además, deberán incluir la fecha y lugar, hora de inicio y término, objetivo, actividades realizadas, resultados y las firmas autógrafas del personal participante por parte del **IEPC** y el ente auditor.

d. Calendario de trabajo

El calendario de actividades para esta línea de trabajo deberá considerar que esta validación se lleva a cabo el día de la Jornada Electoral y al concluir la operación del PREP.

1.3 Análisis de vulnerabilidades a la infraestructura tecnológica

a. Objetivos

- Identificar debilidades de seguridad en la infraestructura tecnológica mediante la ejecución de pruebas de penetración y revisión de configuraciones de seguridad.

- Clasificar el impacto y documentar las vulnerabilidades identificadas con el propósito de recomendar al **IEPC** las posibles medidas para la mitigación de las vulnerabilidades que previamente fueron identificadas y documentadas.

- Verificar que las medidas implementadas por el **IEPC** hayan atendido adecuadamente las vulnerabilidades reportadas.

b. Alcance

El análisis de vulnerabilidades de la infraestructura tecnológica deberá realizarse con base en las etapas que se describen a continuación.

I. **Junta de inicio.** Se convocará al personal involucrado en la realización de la auditoría con el objetivo de presentar las actividades consideradas como parte de la auditoría, definir los roles y responsabilidades de las partes, establecer las metodologías y estándares con las que se realizará la auditoría, así como los tiempos generales de ejecución.

- El **IEPC** pondrá a consideración del ente Auditor una lista de activos durante la junta de inicio.
- El **IEPC** proporcionará espacios de trabajo a los integrantes del ente auditor para que realicen el análisis de vulnerabilidades a la infraestructura tecnológica del sistema.
- El **IEPC** otorgará los accesos correspondientes y las ventanas de tiempo necesarias para la ejecución de la auditoría.

II. **Plan de trabajo detallado.** Con base en la información obtenida y analizada, el ente auditor deberá elaborar el plan de trabajo en el que se incluyan los detalles del proyecto de auditoría de seguridad a la infraestructura tecnológica del PREP. Este documento integrará la información necesaria durante y después del proceso de auditoría e incluirá, como mínimo, lo siguiente:

- Pruebas de penetración (*pentest*)
- Revisión de configuraciones de seguridad

c. Pruebas de penetración (pentest).

Las pruebas de penetración se deberán llevarán a cabo tanto desde el interior como desde el exterior de la red de datos a examinar y deberán enfocarse en:

- Servidores
- Aplicaciones web
- Equipos de telecomunicaciones
- Estaciones de trabajo

I. Presentación de hallazgos. El ente auditor deberá presentar un informe preliminar con los hallazgos encontrados, así como la recomendación para atender los mismos.

Para la presentación de hallazgos se utilizará un registro de datos en el que, de forma conjunta el ente auditor y el **IEPC**, puedan dar seguimiento a los mismos.

II. Validación de reporte de hallazgos. El **IEPC** presentará al ente auditor la retroalimentación acerca de los hallazgos encontrados con el fin de descartar falsos positivos (hallazgos que indican incorrectamente sobre la presencia de una vulnerabilidad) y homologar criterios de interpretación de dichos hallazgos.

III. Atención de hallazgos. Una vez validados los hallazgos, el **IEPC** aplicará los diferentes controles necesarios para mitigarlos y atenderlos. Cabe señalar que el ente auditor deberá considerar dentro de su plan de trabajo, otorgar al menos 10 días hábiles para que el **IEPC** pueda atender los hallazgos.

IV. Validación de la atención de los hallazgos. El ente auditor validará que el **IEPC** haya aplicado los controles necesarios para atender a los hallazgos reportados.

V. Entregables

El ente auditor deberá entregar los siguientes documentos derivados de la realización de pruebas de penetración (*pentest*):

Entregable	Descripción y Contenido	Criterios de Aceptación
Plan de pruebas de penetración a la infraestructura tecnológica	Describe los elementos generales de planeación que deben considerarse para el desarrollo de las pruebas de penetración. • Alcance	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.

Entregable	Descripción y Contenido	Criterios de Aceptación
	• Calendario de trabajo • Responsables técnicos	
Informe preliminar de las pruebas de penetración a la infraestructura tecnológica	Documento que contiene el resultado de las pruebas realizadas sobre los activos: • Resumen ejecutivo • Alcance • Resultado de las pruebas • Recomendaciones generales	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.
Informe de la aplicación de recomendaciones de las pruebas de penetración a la infraestructura tecnológica	Documento que describe el estado de seguridad de la infraestructura una vez que fueron aplicadas las recomendaciones por parte del ente auditor. • Resumen ejecutivo • Alcance • Resultado de la verificación	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.

d. Revisión de configuraciones.

El objetivo es analizar las configuraciones de los dispositivos que conforman la infraestructura tecnológica con base en mejores prácticas de seguridad informática para identificar oportunidades y emitir recomendaciones orientadas al fortalecimiento de esta.

e. Entregables

Derivado de la revisión de configuraciones, el ente auditor deberá proporcionar al **IEPC** los siguientes documentos:

Entregable	Descripción y Contenido	Criterios de Aceptación
Plan de revisión de configuraciones de la infraestructura	Describe los elementos generales de planeación que deben considerarse para el desarrollo de la revisión: • Alcance • Calendario de trabajo • Responsables técnicos	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.
Informe preliminar de la revisión de configuraciones de la infraestructura	Documento que contiene el detalle de cada hallazgo identificado en la revisión de configuraciones. • Resumen ejecutivo • Objetivos • Alcance	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.

Entregable	Descripción y Contenido	Criterios de Aceptación
	• Hallazgos y recomendaciones	
Informe de la aplicación de recomendaciones de la revisión de configuraciones de la infraestructura	Documento que contiene el resultado final de la revisión de configuraciones: • Resumen ejecutivo • Objetivos • Alcance	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.

f. Informe final de análisis de vulnerabilidades a la infraestructura tecnológica.

Al concluir las pruebas de penetración y revisión de configuraciones, el ente auditor deberá elaborar un informe final con el resultado del análisis de vulnerabilidades a la infraestructura tecnológica, de acuerdo con lo siguiente:

Producto	Descripción y Contenido	Criterios de Aceptación
Informe final del análisis de vulnerabilidades a la infraestructura tecnológica	Documento que contiene el resultado final del análisis de vulnerabilidades: • Introducción • Resultados Generales	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.

g. Calendario de trabajo.

El calendario de actividades para esta línea de trabajo deberá establecer de forma clara los periodos de actividades, las fechas límite y los avances esperados.

1.4 Pruebas de negación de servicio a sitios web del PREP y al sitio principal del IEPC

a. Objetivo

Realizar ataques de negación de servicio que permitan identificar, evaluar y aplicar las medidas necesarias para asegurar la correcta y continua disponibilidad del servicio Web de los sitios de publicación de resultados del PREP y del sitio principal del **IEPC**, durante el periodo de operación del PREP.

Documentar los hallazgos detectados durante la realización de las pruebas.

b. Alcance

Generar tráfico de red desde la infraestructura del ente auditor, o en su caso la que éste determine, hacia los servicios web que se publican dentro del dominio del **IEPC**, ya sea en su propia infraestructura o en la que provea un tercero.

Las pruebas de negación de servicio deberán considerar dos apartados:

- Tráfico no malintencionado que consiste en transacciones sintéticas que simulen el tráfico legítimo que se espera el día de la jornada.
- Tráfico de red malintencionado, consistente en paquetes de red malformados.

Las pruebas mencionadas anteriormente deberán realizarse de manera concurrente. Los ataques de negación de servicio deben contemplar, al menos, tráfico de red malintencionado con las siguientes características:

- Ataques volumétricos por protocolo TCP

- Al menos de 400 Mbps de throughput
- Al menos realizar SYN FLOOD

- Ataques volumétricos por protocolo UDP
  - Al menos de 400 Mbps de throughput
  - Al menos realizar DNS AMPLIFICATION

- Ataques volumétricos por protocolo ICMP
  - Al menos de 400 Mbps de throughput
  - Al menos realizar ICMP FLOOD

- Ataques en la capa de aplicación (HTTP)
  - Al menos realizar SLOWRIS ATACK

Las pruebas mencionadas anteriormente deberán realizarse de manera concurrente; considerando la generación de tráfico malintencionado (SYN FLOOD, DNS AMPLIFICATION, ICMP FLOOD, SLOWRIS ATACK) en un volumen que represente las condiciones de un ataque.

Durante las pruebas, cada simulación de ataque deberá apegarse a las condiciones de un ataque para hacer que el sitio web que se esté probando quede fuera de línea (no disponible) por, al menos 2 minutos, previo a que el **IEPC** efectué la contramedida para la mitigación.

c. Entregables

- Plan de trabajo detallado que cuente como mínimo con el desglose de actividades, entregables, duración, fecha inicio, fecha fin y responsables de las actividades.
- Plan de ataques de negación de servicio.
- Informe de resultados.
- Estadísticas del tráfico de red generado.

d. Calendario de trabajo.

El calendario de actividades para esta línea de trabajo deberá establecer de forma clara, los periodos de actividades, las fechas límite y los avances esperados.

CONDICIONES GENERALES

1.5 Por parte del ente auditor.

Para la realización de la auditoría, el ente auditor deberá presentar la siguiente documentación:

- Protocolos y metodologías de trabajo para llevar a cabo las actividades de cada auditoría definidas en los planes detallados de trabajo.
- Comprobar la experiencia de participación en proyectos similares, particularmente en las líneas de trabajo que forman parte de la presente auditoría.
- Presentar ejemplos de esquemas de validación de software, ejecutados en proyectos similares llevados a cabo anteriormente.
- El ente auditor deberá presentar ejemplos comprobables de informes relacionados con los resultados obtenidos en proyectos similares que haya realizado durante los tres últimos años.
- En su caso, carta de la máxima autoridad del ente auditor seleccionado, donde se acepte la colaboración con el **IEPC** para este proyecto.

Dentro del marco de normatividad aplicable para cada IEPC, la información que sea entregada por el ente auditor debe resguardarse con los mecanismos y procedimientos necesarios para evitar su divulgación a terceros.

1.6 Por parte del IEPC.

Para la realización de las pruebas, el **IEPC** deberá proporcionar los siguientes insumos de información necesarios para la realización de las pruebas:

- Normatividad aplicable y vigente.
- Documentación técnica del sistema informático sobre la arquitectura tecnológica implementada (tanto de software como de hardware) y el proceso que se automatiza.
- Relación de los partidos políticos, coaliciones y candidatos independientes que participarán en la elección y su correspondencia con la geografía electoral aplicable a la elección.
- Ejemplares muestra de las actas de escrutinio y cómputo que se utilizarán en la elección.
- Base de datos con las casillas electorales aplicables a la elección.
- Capacitación inicial y apoyo técnico necesario.
- Usuarios y contraseñas respectivas para realizar las pruebas.
- Un ambiente de auditoría que permita controlar las versiones del Sistema Informático que se audite.

Durante el periodo de trabajo, el **IEPC** proporcionará al ente auditor, el espacio físico, equipo de cómputo y periféricos para instalar una maqueta con la infraestructura tecnológica necesaria para la realización de las pruebas funcionales de caja negra, así como los accesos a los servidores centrales del **IEPC** en donde se encuentre instalado el sistema informático, además de brindar la capacitación inicial y apoyo técnico necesario para habilitar la operación de esta.

REQUERIMIENTOS ADICIONALES

1.7 Formalización

La propuesta técnica deberá incluir el tipo de instrumento jurídico que se celebrará entre las partes para el otorgamiento del servicio descrito en este anexo técnico, así como los nombres y puestos de responsables y administradores del proyecto.

1.8 Marco de trabajo

En el marco de trabajo se deberá considerar lo siguiente:

- Términos de confidencialidad y divulgación de la información para la celebración del instrumento jurídico entre las partes.
- Pautas de interacción entre las partes para el control y seguimiento de las actividades desarrolladas durante la ejecución del proyecto.
- Criterios para la aceptación de las entregas establecidas en el instrumento jurídico.
- Nombres y puestos de las personas responsables de cada línea de trabajo con las que se establecerá contacto para el seguimiento del proyecto.
- Plan de comunicación por cada línea de trabajo, en el que se establezcan los mecanismos de comunicación, nombres, roles y responsabilidades en la comunicación.
- Calendario y monto de las aportaciones de las entregas que se mencionen en la propuesta técnico-económica, ajustándose a las condiciones establecidas en el convenio y a entera satisfacción del **IEPC**.

1.9 Comunicación Social Conjunta

En el marco de trabajo se deberá considerar lo siguiente:

- Sesiones formales con periodicidad mensual para informar los avances de la auditoría y sesiones extraordinarias para atender cualquier situación de contingencia o riesgo.
- Comunicado público para informar la colaboración entre el ente auditor y el **IEPC**.
- Comunicado público para informar los resultados de la auditoría.

1.10 Estructura de la propuesta

La propuesta que presente el ente auditor deberá estructurarse de la siguiente manera y deberá incluir, como mínimo, los siguientes aspectos.

I. Propuesta técnica, respuesta a los rubros del documento anexo técnico.
II. Propuesta económica.
III. Plan de trabajo.
IV. Cronograma de actividades.
V. Presentación de metodología propuesta.
VI. Currículum del ente auditor.
VII. Currículum del personal a asignar por parte del ente auditor.
VIII. Cartas de referencia y certificados.