ANEXO 1.

ANEXO TÉCNICO PARA AUDITORÍA DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES (PREP)

Índice

1. Antecedentes

En el Proceso Electoral Estatal Ordinario 2017-2018, se contará con el Programa de Resultados Electorales Preliminares (PREP), el cual está sujeto a los Lineamientos del Programa de Resultados Electorales Preliminares, emitidos por Consejo General del Instituto Nacional Electoral. En el diseño, instalación e implementación del PREP se deberá de cumplir con los principios de certeza, legalidad, independencia, imparcialidad, máxima publicidad y objetividad, en el ejercicio de la función electoral.

De acuerdo a lo que establecen los Lineamientos, la auditoría de verificación y análisis del sistema informático que será utilizado en la implementación y operación del PREP, se deberá realizar con la finalidad de evaluar la integridad, disponibilidad y seguridad en el procesamiento de la información y la generación de los resultados conforme a la normativa aplicable y vigente. Así mismo se deberán incorporar en el desarrollo de su sistema informático, la función requerida para la generación y el almacenamiento de bitácoras que faciliten los procedimientos de verificación, análisis y auditoría del sistema.

Las disposiciones generales que se establecen en los **requisitos mínimos para la elaboración del anexo técnico para la contratación de servicios de auditoría al sistema informático y a la infraestructura tecnológica del Programa de Resultados Electorales Preliminares**, señalan que se deben considerar al menos las siguientes líneas de trabajo:

- Pruebas Funcionales de Caja Negra
- Validación del sistema informático del PREP y de sus bases de datos
- Análisis de Vulnerabilidades a la Infraestructura tecnológica
- Pruebas de Negación de servicio al sitio web del PREP y al sitio principal del IEEC.

Para tal efecto y dar cumplimiento a lo establecido en el punto 7 relativo a la preparación de los Servicios de Auditoría de la Minuta de Trabajo de la reunión extraordinaria del día 9 de Febrero de 2018 del Comité Técnico Asesor, el Comité Técnico Asesor, ha elaborado este **Anexo Técnico** para la Contratación de Servicios de Auditoría al Sistema Informático y a la Infraestructura Tecnológica del Programa de Resultados Electorales Preliminares de acuerdo a los Lineamientos del Programa de Resultados Electorales Preliminares.

2. Generalidades

En primer lugar es importante definir el término de Auditoría, ya que el mismo se ha usado principalmente para referirse a una revisión cuyo único fin es detectar errores, fraudes, señalar fallas y como consecuencia recomendar el despido o remoción del personal, no obstante, la Auditoría es un concepto mucho más amplio que The American Accounting Association lo define claramente como "El proceso sistemático para evaluar y obtener de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados". El fin del proceso consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como determinar si dichos informes se han elaborado observando los principios establecidos para el caso". Podemos decir que toda auditoría y cualquier tipo de auditoría "es una actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas."

Hasta hace poco tiempo, la comprobación de la gestión y control de la actividad económica y financiera de las organizaciones, se hacía solamente por medio de la Auditoría Financiera, sin embargo, por el grado de informatización de las empresas, la misma no era suficiente y se hizo necesario conocer qué ocurría dentro de los sistemas de información, ya que la Auditoría Financiera podía llegar a conocer la información de entrada al sistema y el resultado obtenido, pero no podía determinar lo que sucedía entre el momento de entrada de la información y los resultados o salida de la misma, es decir se conocían los "inputs" y los "outputs" pero no desconocía cómo se habían generado estos últimos y si habían sido objeto o no de alguna manipulación. El examen de lo que acontece realmente en los Sistemas de Información, se puede realizar gracias a la Auditoría Informática.

¿Cómo se define a la Auditoría Informática? No existen definiciones oficiales sobre la misma, y algunas de las que aparecen en libros o se dan en cursos y seminarios tienen la influencia y criterio personal de su autor, no obstante, a continuación mencionamos las que consideramos más importantes:

Una primera definición podría ser la siguiente: "Se entiende por Auditoría Informática una serie de exámenes periódicos o esporádicos de un sistema informático cuya finalidad es analizar y evaluar la planificación, el control, la eficacia, la seguridad y la adecuación de la infraestructura informática de la organización".

Otros autores proponen la siguiente definición: "La Auditoría Informática comprende la revisión y la evaluación independiente y objetiva, por parte de personas independientes y teóricamente competentes del entorno informático de una entidad, abarcando todo o algunas de sus áreas, los estándares y procedimientos en vigor, su idoneidad y el cumplimiento de éstos, de los objetivos fijados, los contratos y las normas legales aplicables, el grado de satisfacción de usuarios y directivos, los controles existentes y el análisis de riesgos".

Finalmente se tomará la definición que determina el Artículo 5 de los Lineamientos del Programa de Resultados Electorales Preliminares, que dice: "La auditoría de verificación y análisis del sistema informático que será utilizado en la implementación y operación del PREP, se deberá realizar con la finalidad de evaluar la integridad, disponibilidad y seguridad en el procesamiento de la información y la generación de los resultados conforme a la normativa aplicable y vigente".

3. Objetivo

El objetivo de este documento, es cumplir con lo establecido en el punto 7 relativo a la preparación de los Servicios de Auditoría de la Minuta de Trabajo de la reunión extraordinaria del día 9 de febrero de 2018 del Comité Técnico Asesor para la elaboración del Anexo Técnico para la contratación de servicios de auditoría al sistema informático y a la infraestructura tecnológica del Programa de Resultados Electorales Preliminares.

4. Propuesta de Procedimiento de Auditoría al sistema informático y a la infraestructura tecnológica del Programa de Resultados Electorales Preliminares

4.1. Planificación de la Auditoría

En el procedimiento de Auditoría Informática, la Planificación de la Auditoría resulta fundamental, para asegurar que dicha Auditoría, cumpla el propósito para la cuál es establecida. En la Planificación de la Auditoría de los Sistemas Informáticos del PREP, se establecerá el Alcance así como los Recursos Materiales y Técnicos, con que se cuenta a fin de establecer los mejores mecanismos, para llevar a cabo

la Auditoría. En la etapa de Planeación, se revisa la documentación (técnica y normativa), del PREP, que permita comprender la arquitectura y características del sistema informático, y de esta forma contar con los elementos suficientes de información que permitan generar un plan de trabajo específico, donde se detalle los elementos que señalan los Lineamientos del PREP, como son la metodología y criterios a seguir en la revisión del código fuente del Sistema Informático, así como la preparación de los datos, casos, escenarios, ejercicios y simulacros necesarios, para cumplir con el objetivo de la Auditoría de los Sistemas Informáticos que se llevará a cabo.

4.1.1. Propuesta de Fecha de Entrega de la Auditoría Informática

De acuerdo a lo establecido en el artículo 9 de los Lineamientos, la auditoría deberá de ejecutarse sobre todos los módulos del sistema informático previo al inicio de los simulacros, por lo tanto sólo se podrá llevar a cabo la auditoria cuando el sistema informático alcance el 100% de avance en su desarrollo. Considerando que los Lineamientos del PREP, establecen que los ejercicios y simulacros se lleven a cabo durante el mes previo a la Jornada Electoral que será el domingo 1 de julio del 2018, la auditoría al Sistema Informático deberá entregarse a más tardar el **15 de Mayo de 2018**. Si de las pruebas y simulacros resultara necesario realizar ajustes al sistema, esto deberá hacerse del conocimiento del ente auditor para contar con un margen de tiempo que permita aplicar las medidas que resulten necesarias y se garantice que el sistema auditado sea el que opere para el PREP.

4.1.2. Alcance

En lo relativo al alcance, se estará salvaguardando en todo momento los derechos de la propiedad intelectual y se deberán de contemplar que lleven a cabo al menos las siguientes actividades:

- Prueba Funcionales de Caja Negra al Sistema Informático (incluyendo revisión del Código Fuente). Estas pruebas funcionales tienen como objetivo evaluar la integridad en el procesamiento de información y la generación de resultados preliminares, conforme a lo establecido en el artículo 347, numeral 1, inciso a) del Reglamento de Elecciones. Además se deberá incluir la revisión del código fuente, línea por línea, a fin de verificar que no se haya incorporado elemento o algoritmo alguno que pudiera alterar el funcionamiento del PREP en los términos que establecen los Lineamientos del PREP. Los aspectos que se deberán de considerar:
    - 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 el módulo de digitalización, captura y validación (obtención de imagen digital del acta, captura de la información contenida en las actas PREP, validación de la información capturada) y el módulo de Publicación de Resultados incluyendo la revisión de la obtención de los resultados, así como la emisión de reportes y su despliegue, de acuerdo con la documentación técnica y la normatividad aplicable.
    - Verificar el cumplimiento de las especificaciones funcionales y requerimientos contenidos en la documentación técnica y normativa aplicable por el IEEC.
    - Verificar la correspondencia de la captura de los datos plasmados en las actas PREP con los presentados en la publicación, mediante los distintos reportes desplegados por el PREP, considerando datos, imágenes y bases de datos.

- Validación del Sistema Informático del PREP y de sus bases de datos. El auditor deberá 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. Los aspectos mínimos que se deberán de considerar son:
    - El procedimiento deberá de 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: a) generación, obtención y validación de huellas criptográficas en SHA-256 del software PREP auditado; b) 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; c) validación de la información inicial y final de la base de datos del PREP y; d) constancia de hechos.
- Análisis de Vulnerabilidades en la Infraestructura Tecnológica del PREP, se deberá realizar con base en las etapas que se describen a continuación:
    - Junta de Inicio, donde se convoca al personal del área técnica del IEEC así como al personal del ente auditor y se presentan las actividades a realizar como parte de la auditoria, se definen roles, y se proporcionan la lista de activos, análisis de puntos vulnerables en la infraestructura tecnológica del sistema, y se otorgan los accesos correspondientes así como las ventanas de tiempo necesarias para la ejecución de las auditorias.
    - Plan de Trabajo Detallado. Con base a la información obtenida en la Junta de Inicio, y una vez analizada, el ente auditor deberá elaborar el plan de trabajo en el que se incluyan detalles del proyecto de auditoria de seguridad a la infraestructura tecnológica del PREP. Deberá de incluir al menos: a) pruebas de penetración (pentest); b) revisión de configuraciones de seguridad
- Pruebas de negación del servicio al sitio web del PREP y al sitio principal del IEEC. Se deberá de generar tráfico desde el la infraestructura del ente auditor o en su caso la que éste determine, hacia los servicios web que se publican dentro del dominio del IEEC, ya sea en su propia infraestructura o en la que se provea por un tercero. Las pruebas de negación de servicio deberán de considerar dos apartados: a) el tráfico no malintencionado que consiste en transacciones sintéticas que simulen el tráfico legítimo que se espera el día de la jornada y; b) el tráfico de red malintencionado, consistente en paquetes de red malformados.

4.1.3. Recursos Materiales

En lo relativo a los recursos materiales con que se cuenta en el Instituto Electoral del Estado de Campeche, no se cuentan con los Recursos Materiales, que puedan ser usados para llevar a cabo o apoyar las actividades relacionadas con la Auditoría. Por lo anterior, se deberá de considerar que el Instituto Electoral del Estado de Campeche, pueda disponer de los Recursos Materiales, ya sea por medio de adquisición o por contratación a efectos de considerar los recursos materiales que se requerirán para hacer la Auditoria.

4.1.4. Recursos Técnicos

En lo relativo a los recursos técnicos con que se cuenta en el Instituto Electoral del Estado de Campeche, no se cuentan con los Recursos Técnicos suficientes para llevar a cabo o apoyar las actividades relacionadas con la Auditoría por medios propios. Por lo anterior, se deberá de considerar que el Instituto Electoral del Estado de Campeche, deberá de contratar los servicios de auditoría con alguna institución académica, de investigación o una empresa privada con reconocimiento nacional o internacional, y que disponga de la experiencia en auditoría de sistemas. También se considera que la organización responsable de llevar a cabo la Auditoría de los sistemas informáticos, cuenten con los Recursos Técnicos (también se podrá considerar que tenga los recursos materiales) que se requerirán para hacer la Auditoria.

4.2. Metodología de la Auditoría

Metodología es una secuencia de pasos lógica y ordenada de proceder para llegar a un resultado. Para el caso de la Metodología de la Auditoría de Sistemas Informáticos, consiste en verificar el funcionamiento de un sistema de información, aplicando una serie de conocimientos, técnicas y métodos con el propósito de examinar la funcionalidad del sistema. En el caso que nos ocupa, se propone llevar a cabo dos tipos de auditorías: la primera será del Tipo Auditoría Informática de Producción, también conocida como de Operación, que se ocupa de revisar todo lo que se refiere con producir resultados informáticos, listados impresos, archivos soportados magnéticamente, ordenes automatizadas para lanzar o modificar procesos, etc., el segundo tipo de Auditoría será la de Auditoría de Seguridad Informática, que abarca los conceptos de seguridad física y lógica. La seguridad física se refiere a la protección del hardware y los soportes de datos, así como la seguridad de los edificios e instalaciones que los albergan. El auditor informático debe contemplar situaciones de incendios, inundaciones, sabotajes, robos, catástrofes naturales, etc. Por su parte, la seguridad lógica se refiere a la seguridad en el uso de softwares, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información. El auditar la seguridad de los sistemas, también implica que se debe tener cuidado que no existan copias piratas, o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión de virus. Como parte de este tipo de auditoría también se enfoca en verificar los aspectos, tales como: Evaluación de los riesgos de internet (operativos, tecnológicos y financieros) y así como su probabilidad de ocurrencia; Evaluación de vulnerabilidades y la arquitectura de seguridad implementada; Verificar la confidencialidad de las aplicaciones y la publicidad negativa como consecuencia de ataques exitosos por parte de hackers.

4.2.1. Procedimiento y Enfoque. El procedimiento para llevar a cabo la Auditoría del Sistema Informático, deberá comprender los puntos que serán mencionados a continuación y deberán de tener un enfoque al Sistema Informático del PREP, así como a las Vulnerabilidades de la Infraestructura Tecnológica:

- Planeación y Preparación de la Auditoría.
- Metodología de la Auditoria.
- Revisión del código fuente.
- Pruebas Funcionales de caja negra.
- Validación del sistema informático del PREP y de sus bases de datos.
- Análisis de Vulnerabilidades a la Infraestructura Tecnológica.
- Pruebas de negación del servicio al sitio web del PREP y al sitio principal del IEEC.

- Informes de Auditoría, tanto informes parciales, informe final así como el informe de evaluación de la operación.

4.2.2. Formato y Contenido de los Reportes. El formato y contenido de los reportes que se generarán como parte de la Auditoría, podrá usarse un formato libre, sin embargo, deberá de contener con al menos la siguiente información:

- Nombre de la institución que elabora la Auditoría.
- Nombre del Responsable directo de la Auditoría por parte de la Institución encarga de la Auditoria.
- Antecedentes.
- Objetivos de la Auditoría.
- Metodología de la Auditoria.
- Alcances de la Auditoria.
- Informe Parcial de la Auditoria, que incluya los resultados emitidos durante el proceso de auditoría, los cuales tendrán calidad de reservados en términos de las disposiciones aplicables en materia de transparencia y acceso a la información. Deberá incluir: a) los criterios utilizados para la auditoría; b) el método para clasificar los hallazgos que permitan priorizar su atención; c) los hallazgos identificados y clasificados, y; d) las posibles recomendaciones que permitan al IEEC atenderlos.
- Informe Final de la Auditoria, que incluya los resultados finales de la auditoría, que considere el cierre de operaciones del PREP, así como también la etapa de evaluación del mismo. Dicho informe deberá publicarse en el portal oficial del IEEC, a más tardar un día antes de la Jornada Electoral.
- Informe de evaluación de la operación: considera el cierre de operaciones del PREP, así como la etapa de evaluación del mismo.

4.3. Revisión del Sistema Informático (Revisión de Código Fuente)

La revisión del sistema informático, consiste en la revisión visual (análisis estático) del código fuente (programas de cómputo), que integrará cada uno de los módulos del sistema informático del PREP, mismo que estará conformado por líneas de texto plano, para verificar que las instrucciones de cada uno de los programas implementen la funcionalidad indicada en la documentación técnica del sistema informático del PREP, y que el procesamiento de la información de los resultados electorales preliminares sea integro.

Se tiene la finalidad de evaluar la lógica de los programas relacionados con el tratamiento de la información, desde su captura hasta su despliegue en pantalla (publicación), así como los cálculos efectuados para la emisión de los resultados electorales preliminares, con el fin de determinar si el tratamiento de la información es adecuado y conforme con las especificaciones técnicas y Lineamientos del PREP. Con dicha revisión también se podrá evaluar las prácticas de programación utilizadas por los desarrolladores del sistema informático del PREP.

El análisis del código fuente el desarrollador del sistema informático deberá de entregar los archivos fuente y la documentación técnica modular en formato electrónico, misma que estará bajo resguardo del IEEC, y sólo servirá para hacer el análisis del código fuente respectivo, y NO podrá ser usada con algún otro fin. Para la inspección visual del código fuente se podrá contar con las ayudas de herramientas de análisis, de tal forma que se pueda verificar que las instrucciones de los métodos y funciones, así como

las variables contenidas en cada uno de los programas, harán la función indicada en la documentación técnica, y que el procedimiento de la información sea integro.

Se deberá de revisar adicionalmente, la no existencia de vulnerabilidades de seguridad, que tampoco existan códigos redundantes o en desuso, o empleo ineficiente de recursos de cómputo, así como que el código fuente deberá de cumplir los estándares de codificación y documentación generalmente aceptados en el desarrollo de software.

4.4. Prueba Funcionales de Caja Negra al Sistema Informático del PREP

a) Objetivo: en lo relativo a la Prueba Funcionales de Caja Negra al Sistema Informático del PREP, éstas tienen como objetivo evaluar la integridad en el procesamiento de 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: como parte del alcance de las pruebas funcionales de caja negra, se deben de considerar aquellas etapas que fueron definidas en el Procedimiento Técnico Operativo que incluyen el uso del sistema informático. Las pruebas de caja negra, deberán realizarse en términos de funcionalidad del sistema informático del PREP, y deberán de considerar los siguientes aspectos:
   - 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 el módulo de digitalización, captura y validación (obtención de imagen digital del acta, captura de la información contenida en las actas PREP, validación de la información capturada) y el módulo de Publicación de Resultados incluyendo la revisión de la obtención de los resultados, así como la emisión de reportes y su despliegue, de acuerdo con la documentación técnica y la normatividad aplicable.
   - Verificar el cumplimiento de las especificaciones funcionales y requerimientos contenidos en la documentación técnica y normativa aplicable por el IEEC.
   - Verificar la correspondencia de la captura de los datos plasmados en las actas PREP con los presentados en la publicación, mediante los distintos reportes desplegados por el PREP, considerando datos, imágenes y bases de datos.

c) Entregables: el ente auditor deberá de 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	Descripción de elementos generales que deben considerarse para la realización de las pruebas funcionales de caja negra: • Introducción • Objetivo • Alcance • Pruebas a aplicar • Planeación de pruebas • Necesidades de ambiente • Casos de prueba • Datos de prueba • Criterios de prueba • Administración de riesgos	En formato electrónico Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido

	• Entregables	
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 lo siguiente: • Introducción • Metodología • Criterios utilizados para la auditoria • Metodología para clasificar los hallazgos • Observaciones y recomendaciones • Conclusiones NOTA: como parte del control de incidencias y a fin de dar un puntual seguimiento a la atención de las mismas, el ente Auditor deberá de proporcionar una herramienta de Help-Desk que permita la gestión de cada incidencia, para saber el estatus de que incidencias se han abierto, cuales se han atendido, cuales se han cerrado, y cuales están con el estatus de pendientes. Así mismo se deberá de llevar un control de versión del sistema informático auditado	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 auditoria • Resumen ejecutivo • Resultados	Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido

d) Calendario de Trabajo: El calendario de trabajo para realizar las Pruebas Funcionales de Caja Negra, deberá de establecer claramente, los periodos para ejecutar cada una de las actividades y los avances esperados en cada período de trabajo.

e) Consideraciones adicionales: se deberá de llevar a cabo pruebas funcionales de caja negra en un entorno tecnológico con las características similares (de preferencia exactamente las mismas características) al ambiente de operación de la jornada electoral, con la finalidad de comprobar que los resultados de la operación del PREP sean consistentes con la funcionalidad que deben de cubrir, desde la captura de datos en el sistema, hasta el despliegue de los resultados preliminares en Internet. Se debe verificar la integridad en el procesamiento de información y la generación de resultados preliminares del sistema informático, bajo diversos escenarios y casos de prueba, conforme a lo indicado en los Lineamientos del PREP. Las pruebas funcionales de caja negra, se deberán de llevar a cabo en las instalaciones que el IEEC defina que ocuparan el Recinto Central, en el ambiente tecnológico de operación de la jornada electoral. Se deberán de definir por parte del Auditor la definición de los escenarios y datos de prueba, con la finalidad de verificar el funcionamiento y comportamiento del sistema en diferentes situaciones, así como la integridad y precisión de los datos ingresados desde su captura en el sistema informático hasta su publicación en internet. **Se deberá de realizar al menos tres ciclos de prueba y una verificación final.**

4.5. 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. Esta validación de la correspondencia del software auditado y el utilizado en la operación del PREP, se tendrá que realizar al inicio, durante y la final de la operación del sistema informático del PREP.

b) Alcance: El personal técnico que designe el ente auditor deberá llevar a cabo el proceso técnico para verificar que los programas auditados, así como la base de datos se encuentre debidamente inicializada. Este procedimiento será validado por los miembros del Comité Técnico Asesor del PREP, así como por las personas que designe el IEEC. Los aspectos mínimos que se deberán incluir en la validación del sistema informático y de sus bases de datos son los siguientes:

- El procedimiento deberá de 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:
  - a) generación, obtención y validación de huellas criptográficas en SHA-256 del software PREP auditado;
  - b) 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;
  - c) validación de la información inicial y final de la base de datos del PREP y;
  - d) constancia de hechos.

Este procedimiento se llevará a cabo el domingo 1 de julio de 2018, a las 9:00 AM en las instalaciones que ocupe el Recinto Central, concluyendo el 2 de julio de 2018, y será atestiguado por la fe de un notario público que haya designado el IEEC, conforme a lo señalado en el inciso I del numeral 23, Capítulo I, Título III del Anexo 13 del Reglamento de Elecciones.

c) Entregables: Los productos que deberá de entregar el Ente Auditor, deberán incluir:

- Plan de Trabajo detallado que cuente como mínimo con: el desglose de actividades, entregables, duración, fecha de 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 correspondientes que se acuerden conjuntamente entre el IEEC y el Ente Auditor.
- Constancia de Hechos de la generación de huellas criptográficas de los programas probados del sistema informático. Esta constancia deberá describir el protocolo de la actividad, fecha y lugar, hora de inicio y hora de término, objetivo, actividades realizadas, resultados obtenidos y las firmas autógrafas del personal participante por parte del IEEC 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 hora de término, objetivo, actividades realizadas, resultados y las firmas autógrafas del personal participante por parte del IEEC y del Ente Auditor.

d) Calendario de Trabajo: El calendario de actividades para esta línea de trabajo deberá de considerar que la Validación se lleve a cabo el día de la Jornada Electoral y al concluir la operación del PREP.

e) Consideraciones Adicionales: La validación del software auditado consiste en la compilación y firma de los programas auditados para validar que el software que será instalado y utilizado en la jornada electoral, es el mismo que fue auditado por el Auditor. Como resultado de esta validación, se emitirán constancias de hechos que describen las actividades realizadas. El protocolo del proceso de validación que se propone es el siguiente:
   - Compilación de los programas.
   - Obtención de firmas criptográficas.
   - Al finalizar la obtención de firmas criptográficas, el Auditor generará tres copias en disco compacto (disco externo USB, disco duro externo) donde se contenga el resultado de dichas firmas, las cuales serán distribuidas al IEEC, al Auditor, y al Notario Público. Además se proporcionará al Notario Público un listado con las firmas criptográficas resultantes para que dé fe de las actividades realizadas.
   - Recolección de los archivos y programas del Recinto Central en la víspera de la jornada electoral, que consistirá en la recolección en medios de almacenamiento portátil, los archivos y programas binarios del sistema informático del PREP instalados en cada uno de los servidores en las consolas del ambiente de producción del Recinto Central y del Centro de Cómputo, tanto en los equipos primarios de producción como en los equipos secundarios (los equipos de respaldo en caso de contingencias). El personal técnico del IEEC (o en su caso del personal técnico del Proveedor del PREP), en presencia del personal técnico del Auditor, obtendrá una copia de los archivos binarios que conformarán el sistema informático del PREP, los cuáles cuales serán copiados a un dispositivo portátil nuevo, que será resguardado en un sobre cerrado y firmado por ambas partes, ante notario.
   - Validación de la inicialización de la base de datos. El día de la jornada electoral se constatará que la base de datos se encuentre debidamente inicializada, es decir, que las tablas contengan sólo la información que deben de tener y que no exista evidencia de actas con resultados. Para esto, el personal técnico del IEEC (o en su caso el personal técnico del Proveedor del PREP), en presencia del Auditor, del IEEC, y de un notario público, ejecutarán un script (programa con una secuencia de comandos validados), que contiene las consultas necesarias para verificar el contenido de las tablas que conforman la base de datos del sistema informático del PREP. Los resultados obtenidos, deberán de ser comparados contra un listado de resultados esperados. El script que se correrá deberá de estar previamente validado por el Auditor.
   - Validación final de las firmas criptográficas de los programas el día de la jornada electoral. El día de la jornada electoral en presencia de autoridades del IEEC, del Auditor y de notario público, se realizará la comparación de las firmas criptográficas de los programas recolectados en el Recinto Central, contra las firmas criptográficas de los programas compilados a partir del código fuente auditado por el personal técnico del Auditor.

4.6. Análisis de Vulnerabilidades a la Infraestructura Tecnológica

a) Objetivos: El Análisis de Vulnerabilidades en la Infraestructura Tecnológica del PREP, tiene como objetivos:
   - Identificar debilidades de la Seguridad en la infraestructura tecnológica mediante la ejecución de pruebas de penetración y revisión de configuraciones de seguridad

- Clasificar el impacto y documentar las debilidades identificadas con el propósito de recomendar al IEEC las posibles medidas para la mitigación de las vulnerabilidades que previamente fueron identificadas y documentadas.
- Verificar que las medidas implementadas por el IEEC hayan atendido adecuadamente las vulnerabilidades reportadas.

b) Alcance:
   - El análisis de Vulnerabilidades de la infraestructura tecnológica deberá realizar con base en las etapas que se describen a continuación:
     - Junta de Inicio, donde se convoca al personal del área técnica del IEEC así como al personal del ente auditor y se presentan las actividades a realizar como parte de la auditoria, se definen roles, y se proporcionan la lista de activos, análisis de puntos vulnerables en la infraestructura tecnológica del sistema, y se otorgan los accesos correspondientes así como las ventanas de tiempo necesarias para la ejecución de las auditorias.
     - Plan de Trabajo Detallado. Con base a la información obtenida en la Junta de Inicio, y una vez analizada, el ente auditor deberá elaborar el plan de trabajo en el que se incluyan detalles del proyecto de auditoría de seguridad a la infraestructura tecnológica del PREP. Deberá de incluir al menos: a) pruebas de penetración (pentest); b) revisión de configuraciones de seguridad

c) Pruebas de penetración (pentest): Las pruebas de penetración se deberán llevar a cabo tanto desde el interior como desde el exterior de la red de datos a examinar y se deberán enfocar en los siguientes elementos:

- 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 entre el auditor y el IEEC, puedan dar seguimiento a los mismos.

ii. Validación de reporte de hallazgos: El IEEC 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 vulnerabilidad) y homologar criterios de interpretación de dichos hallazgos.

iii. Atención de hallazgos: Una vez validados los hallazgos, el IEEC aplicará los diferentes controles necesarios para mitigarlos y atenderlos. El ente auditor deberá de considerar dentro de su Plan de Trabajo, otorgar al menos 10 días hábiles para el IEEC pueda atender los hallazgos.

iv. Validación de atención a hallazgos: el ente auditor validará que el IEEC 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 las pruebas de penetración (pentest).

Entregable	Descripción y Contenido	Criterios de Aceptación

Plan de Pruebas Funcionales de penetración a la infraestructura tecnológica	Descripción de elementos generales de planeación que deben considerarse para el desarrollo de las pruebas de penetración: • 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 las pruebas de penetración a la infraestructura tecnológica	Documento que contiene el resultado de las pruebas de penetración realizada sobre los activos: • Resumen Ejecutivo • Alcance • Resultado de las pruebas • Recomendaciones generales NOTA: como parte del control de incidencias que pudiera reportar el ente auditor y a fin de dar un puntual seguimiento a la atención de las mismas, el ente Auditor deberá de proporcionar una herramienta de Help-Desk que permita la gestión de cada incidencia, para saber el estatus de que incidencias se han abierto, cuales se han atendido, cuales se han cerrado, y cuales están con el estatus de pendientes. Así mismo se deberá de llevar un control de versión de la revisión que está efectuando y cada versión deberá de tener los incidentes encontrados	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 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 las mejores prácticas de seguridad informática para identificar oportunidades y emitir recomendaciones orientadas al fortalecimiento de esta.

e) Entregables: Derivado de la revisión de las configuraciones, el ente auditor deberá proporcionar al IEEC los siguientes documentos:

Entregable	Descripción y Contenido	Criterios de Aceptación
Plan de revisión de configuraciones de la infraestructura.	Descripción de 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 tecnológica	Documento que contiene el detalle de cada hallazgo identificado en la revisión de configuraciones: • Resumen Ejecutivo • Objetivo • Alcance • Hallazgos y Recomendaciones	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido

	NOTA: como parte del control de incidencias que pudiera reportar el ente auditor y a fin de dar un puntual seguimiento a la atención de las mismas, el ente Auditor deberá de proporcionar una herramienta de Help-Desk que permita la gestión de cada incidencia, para saber el estatus de que incidencias se han abierto, cuales se han atendido, cuales se han cerrado, y cuales están con el estatus de pendientes. Así mismo se deberá de llevar un control de versión de la revisión que está efectuando y cada versión deberá de tener los incidentes encontrados	
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 • Resultado de la revisión	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 de elaborar un informe final con el resultado del análisis de vulnerabilidades a la infraestructura tecnológica, de acuerdo a 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	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 límites y los avances esperados.

4.7. Pruebas de Negación del servicio al sitio web del PREP y al sitio principal del IEEC

a) Objetivo: Realizar ataques de negación del servicio que permitan identificar, evaluar y aplicar las medidas necesarias, para asegurar la correcta y continua disponibilidad del servicio web www.prepcampeche2018.org.mx así como del sitio principal del IEEC www.ieec.org.mx, durante el período de operaciones del PREP.

b) Alcance: Se deberá de generar tráfico desde el la infraestructura del ente auditor o en su caso la que éste determine, hacia los servicios web que se publican dentro del dominio del IEEC, ya sea en su propia infraestructura o en la que se provea por un tercero. Las pruebas de negación de servicio deberán de considerar dos apartados:

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

Estas pruebas 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 de apegarse a las condiciones de un ataque para hacer que los sitios web que se están probando (www.prepcampeche2018.org.mx, www.ieec.org.mx) queden fueran de línea (no disponible) por al menos 2 minutos, previo a que el IEEC efectué la contramedida para la mitigación.

c) Entregables: los entregables para esta línea de trabajo serán los siguientes:
   - 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 límites y los avances esperados.

4.8. Mención de las Características del Informe de Resultados y Recomendaciones de la Auditoría

Los informes del ente Auditor deberán de considerar tres modelos básicos, tal como lo señalan los Lineamientos:

- Informe Parcial de la Auditoria, que incluya los resultados emitidos durante el proceso de auditoría, los cuales tendrán calidad de reservados en términos de las disposiciones aplicables en materia de transparencia y acceso a la información. Deberá incluir: a) los criterios utilizados para la auditoría; b) el método para clasificar los hallazgos que permitan priorizar su atención; c) los

hallazgos identificados y clasificados, y; d) las posibles recomendaciones que permitan al IEEC atenderlos.

- Informe Final de la Auditoria, que incluya los resultados finales de la auditoría, que considere el cierre de operaciones del PREP, así como también la etapa de evaluación del mismo. Dicho informe deberá publicarse en el portal oficial del IEEC, a más tardar un día antes de la Jornada Electoral.
- Informe de evaluación de la operación: considera el cierre de operaciones del PREP, así como la etapa de evaluación del mismo.

4.9. Responsables de llevar a Cabo la Auditoría

Tal como lo señala el Artículo 7 de los Lineamientos del PREP, los responsables de llevar a cabo la auditoría deberán de contar con experiencia en auditoría a sistemas informáticos. El mismo artículo señala que se deberá dar preferencia a instituciones académicas o de investigación, con reconocimiento nacional o internacional. Debido a lo anterior, y haciendo un análisis de aquellas instituciones que cuentan con personal con experiencia o áreas de investigación relacionadas con las tecnologías de información, así como con la conveniencia de la ubicación física de dichas instituciones que nos permitan abaratar costos de traslados, estancias, transportación de personal y equipos tecnológicos.

Con fundamento en el Capítulo II, Titulo III del Reglamento de Elecciones, en su artículo 339 de los acuerdos a emitir, y en relación al **Título IV Del Seguimiento a la Implementación y Operación del PREP de las Elecciones Locales del Anexo 13 del Programa de Resultados Electorales Preliminares, en relación con los** fines de seguimiento, los OPL deberán remitir al Instituto, **en los plazos especificados y** por el medio establecido en el Reglamento, los siguientes documentos:

No	Documento/Informe	Fecha de entrega del Proyecto por parte del OPL	Fecha de entrega del documento aprobado o final por parte del OPL
8	**El o los candidatos a entes auditores, así como la síntesis de su experiencia en materia de auditorías.**	No aplica	**El documento final deberá ser emitido, al menos, 5 (cinco) meses antes del día de la jornada electoral y remitido dentro de los 5 (cinco) días posteriores.**

CANDIDATO A DESIGNAR EN MATERIA DE AUDITORÍAS:

INSTITUTO TECNOLÓGICO DE ESTUDIOS SUPERIORES DE CALKINI, CAMPECHE "ITESCAM"

1. De **"EL ITESCAM":**

1.1. Que es un Organismo Público Descentralizado de la Administración Pública Estatal, con personalidad jurídica, patrimonio propio, que ejerce las funciones de docencia, investigación y extensión, de conformidad con lo establecido en el artículo 1 del acuerdo de creación del Ejecutivo del Estado de Campeche publicado el día 12 de octubre de 2001, en el Periódico Oficial del Gobierno del Estado de Campeche, y del acuerdo de modificación al acuerdo anterior publicado en el mismo periódico el día 14 de marzo de 2002.

1.2. Que Conforme al mismo acuerdo, en su artículo 3 tiene por objeto la formación de profesionales con estudios de licenciatura y de postgrado, actualizar y desarrollar a los cuadros profesionales insertos en el aparato productivo regional de bienes y servicios, realizar investigaciones científicas y tecnológicas, desarrollar estudios y proyectos, prestar servicios de carácter científico y tecnológico, y promover la cultura nacional y universal.

1.3. Que en términos del acuerdo de creación del Ejecutivo Estatal, puede realizar toda clase de actos jurídicos necesarios para el logro de su objetivo y el cumplimiento de sus atribuciones; así como expedir las disposiciones necesarias a fin de hacer efectivas las facultades que le fueron otorgadas para el cumplimiento de su objeto..

1.4. Que con base el artículo 16 del Acuerdo de Creación del Ejecutivo Estatal, el Director General es la autoridad institucional a la que compete administrar y representar legalmente al organismo, con las facultades de apoderado general para pleitos y cobranzas, y actos de administración.

1.5. Que el XXXXXX, acredita su carácter del Director General, mediante nombramiento de fecha xx/xx/xxxx acordado por la junta directiva del ITESCAM y notificado por el Gobernador Constitucional del Estado Libre y Soberano de Campeche

1.6. Que para los efectos del presente convenio señala como su domicilio el ubicado en la Avenida Ah-Canul SN por Carretera Federal, S/Colonia, en el Municipio de Calkini, Estado de Campeche, CP. 24900.

OBJETO BASES DEL CONVENIO BASE DE SU EXPERIENCIA EN EL INSTITUTO ELECTORAL DEL ESTADO DE CAMPECHE:

a) Auditoría de software al Sistema del Programa de Resultados Electorales Preliminares 2015, en adelante "PREP 2015", que en lo sucesivo se denominará "Auditoría de Software".

b) Auditoría en materia de seguridad informática a la infraestructura de la Red del INSTITUTO ELECTORAL DEL ESTADO DE CAMPECHE "IEEC" y del "PREP 2015", así como monitoreo y respuesta a incidentes durante la jornada electoral del 7 de junio de 2015, que en lo sucesivo se denominará "Auditoría de Seguridad Informática"

EXPERIENCIA EN MATERIA ELECTORAL EN MATERIA DE AUDITORIAS DE SOFTWARE Y SEGURIDAD INFORMÁTICA.

a) INSTITUTO ELECTORAL DEL ESTADO DE CAMPECHE, 2015.

b) INSTITUTO ELECTORAL DE QUINTANA ROO, 2015.

c) INSTITUTO DE ELECCIONES Y PARTICIPACIÓN CIUDADANA DEL ESTADO DE CHIAPAS, 2016.

5. Designación

5.1. Designación

Como lo establece el objetivo de esta Propuesta de Procedimiento de Auditoría de los sistemas informáticos que serán utilizados para la implementación del PREP, se han detallado todos los puntos que señala el Capítulo III relativo a la Auditoría en los Sistemas Informáticos. Uno de los principales puntos, a señalar es que se requieren establecer la comunicación con las Instituciones Educativas señaladas en el punto 4.10 para determinar cuál de ellas cuenta con los recursos materiales y técnicos, y está en condiciones de poder llevar a cabo la Auditoría Informático a los Sistemas del PREP. Es importante que los acuerdos se lleven a cabo a más tardar a mediados del mes de marzo del 2018, para dar tiempo a la Institución que fungirá como Auditor a preparar y organizar las actividades de la Auditoría en los términos señalados en esta Propuesta de Procedimiento de Auditoría.

Por tanto, hago de su conocimiento que **el candidato a ente auditor, así como la síntesis de su experiencia en materia de auditorías** será el INSTITUTO TECNOLOGICO DE ESTUDIOS SUPERIORES DE CALKINI, CAMPECHE "ITESCAM" para que por su conducto se haga llegar a la Unidad Técnica de Vinculación con los OPL al Ing. Jorge Humberto Torres Antuñano, Coordinador General de la Unidad de Servicios de Informática del INE, para su trámite y efectos administrativos a que haya lugar.

Sirva igualmente este considerando, para darlo a conocer al Consejo General del Instituto Electoral del Estado de Campeche, que con fundamento en este Anexo Técnico, el Comité Técnico Asesor del Programa de Resultados Electorales Preliminares, recomienda la designación del INSTITUTO TECNOLÓGICO SUPERIOR DE CALKINI EN EL ESTADO DE CAMPECHE "ITESCAM", para que funja como Auditor del Programa de Resultados Electorales Preliminares durante el Proceso Electoral Estatal Ordinario 2017-2018.

Que en esta consideración, el Comité Técnico Asesor del Programa de Resultados Electorales de Cómputo en las Elecciones Locales PRECEL, podrá igualmente utilizar la misma propuesta técnica del PREP en los mismos términos.