Instituto Electoral del Estado de Sinaloa

COMITÉ DE ADQUISICIONES, ARRENDAMIENTOS, SERVICIOS Y ADMINISTRACIÓN DE BIENES MUEBLES DEL INSTITUTO ELECTORAL DEL ESTADO DE SINALOA

Presidencia del Comité
Oficio N°: IEES-CAASABM/009/2021.

Culiacán, Sinaloa, a 03 de febrero de 2021.

Instituto Tecnológico y de Estudios
Superiores de Monterrey
Av. Eugenio Garza Sada Sur #2501
Col. Tecnológico, Monterrey, Nuevo León, C.P. 64849
P r e s e n t e . –

El Instituto Electoral del Estado de Sinaloa, a través de su Comité de Adquisiciones, Arrendamientos, Servicios y Administración de Bienes Muebles, con fundamento en el artículo 21 Fracción IX y XIII del Reglamento para las Adquisiciones, Arrendamientos, Servicios y Administración de Bienes Muebles del Instituto Electoral del Estado de Sinaloa y demás relativos de la Ley de Adquisiciones, Arrendamientos, Servicios y Administración de Bienes Muebles para el Estado de Sinaloa, lo invita a participar en el "Procedimiento de concurso por invitación restringida de por lo menos tres proveedores", para la contratación del servicio de **"AUDITORÍA DE VERIFICACÓN Y ANÁLISIS DEL SISTEMA INFORMÁTICO QUE SERÁ UTILIZADO EN LA IMPLEMENTACIÓN Y OPERACIÓN DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES (PREP) PARA EL PROCESO ELECTORAL LOCAL 2020-2021"**; cuyas especificaciones y demás condiciones se detallan en el Anexo Técnico adjunto a la presente.

Las propuestas técnicas y económicas se recibirán en sobre cerrado en las oficinas de la Coordinación de Administración de este Instituto ubicadas en Paseo Niños Héroes #352 Int. 2, Col. Centro, Culiacán, Sinaloa, del día 04 al 09 de febrero del presente año, en horario de lunes a viernes de 9:00 a 17:00 horas y sábados de 9:00 a 13:00 horas.

La apertura se llevará a cabo el día 10 de febrero del presente año a las 10:00 horas, en la cual ustedes podrán presenciar los trabajos del Comité, bajo la condición de registrar su asistencia y abstenerse de intervenir en los trabajos del mismo, el fallo se dará a conocer el mismo día en junta pública a las 16:00 horas, dichas acciones se llevarán a cabo en las instalaciones del IEES.

Sin otro particular, reciba un cordial saludo.

ATENTAMENTE

Lic. Arturo Fajardo Mejía
Presidente del Comité y Secretario Ejecutivo

C.C.P. Archivo

Anexo Técnico

Ente Auditor del Programa de Resultados Electorales Preliminares (PREP)

Proceso Electoral Local 2020-2021

ÍNDICE

1. Descripción general 3
1.1 Fundamento normativo 3
1.2 Requerimiento general de los servicios 3
1.3 Aspectos Generales. 4
2. Servicios de auditoría al sistema informático e infraestructura tecnológica del PREP 4
2.1 Pruebas funcionales de caja negra al sistema informático del PREP. 4
a. Objetivo 4
b. Alcance 4
c. Entregables 5
d. Calendario de entregables 7
2.2 Validación del sistema informático del PREP y de sus bases de datos, ante un tercero con fe pública. 7
a. Objetivo 7
b. Alcance 7
c. Entregables 8
d. Calendario de trabajo 9
2.3 Análisis de vulnerabilidades a la infraestructura tecnológica del PREP 9
a. Objetivos 9
b. Alcance 9
c. Pruebas de penetración (pentest) 10
d. Entregables 12
e. Informe final de análisis de vulnerabilidades a la infraestructura tecnológica 13
f. Calendario de trabajo 14
2.4 Pruebas de denegación de servicio al sitio de publicación del PREP y al sitio principal del **IEES** 14
a. Objetivo 14
b. Alcance 14
c. Entregables 15
d. Calendario de trabajo. 15
3. Condiciones Generales 16
3.1 Por parte del ente auditor. 16
3.2 Por parte del **IEES**. 17
3.3 Revisión de las pantallas de publicación del PREP, verificando el apego a las plantillas base de la interfaz proporcionadas por el INE. 17
3.4 Marco de trabajo 18
3.5 Comunicación Social Conjunta 19
3.6 Estructura de la propuesta 20

1. Descripción general

1.1 Fundamento normativo

En el marco de las actividades para la implementación y operación del Programa de Resultados Electorales Preliminares (PREP) para el Proceso Electoral Local 2020-2021 en el estado de Sinaloa, se requiere que se lleve a cabo una auditoría al sistema informático e infraestructura tecnológica del PREP, de conformidad con lo dispuesto en el Libro Tercero. Proceso Electoral, Título III. Actos posteriores a la elección, Capítulo II. PREP, Sección Cuarta. Sistema informático y su auditoría, artículos 346 y 347 del Reglamento de Elecciones del Instituto Nacional Electoral (INE); así como con lo dispuesto en el Título II. De la Implementación, Capítulo III. De la Auditoría al Sistema Informático, del Anexo 13 del citado Reglamento, relativo a los Lineamientos del PREP.

1.2 Requerimiento general de los servicios

En el presente documento se describe el alcance que el proveedor de servicios deberá cumplir, en caso de ser seleccionado como ente auditor. Es importante señalar que se debe contar con manuales de los sistemas, historiales de usuarios y demás materiales que faciliten la ejecución de la auditoría, así como aquella documentación legal que señale la forma en la que el sistema informático debe operar. 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 del Estado de Sinaloa (IEES)**.

Las líneas de trabajo a considerar son:

1. Pruebas funcionales de caja negra al sistema informático del PREP y a la aplicación móvil que se utilizarán para operar el mecanismo de digitalización de las Actas desde las casillas.

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

3. Análisis de vulnerabilidades a la infraestructura tecnológica del PREP.

4. Pruebas de denegación de servicio al sitio de publicación del PREP y al sitio principal del OPL.

1.3 Aspectos Generales.

1. El ente Auditor deberá nombrar un Auditor o Auditora líder dentro de su equipo de trabajo, quien tendrá la responsabilidad de presentar los planes e informes señalados en el presente Anexo, así como ser el medio de comunicación del ente Auditor con la Instancia Interna para la coordinación del PREP del IEES.

2. A todo entregable señalado en las líneas de trabajo del presente documento, se deberá especificar la Fecha de entrega en el Plan de Trabajo que el ente auditor deberá entregar al inicio de sus trabajos.

3. En lo que respecta a la entrega de los planes e informes, se deberán remitir de manera electrónica al correo prep2021@ieesinaloa.mx. A la par de lo anterior, los informes finales deberán ser entregados de manera impresa a la Instancia Interna de coordinación del PREP del IEES en las oficinas ubicadas en Paseo Niños Héroes #352 Ote. Int 2, Col. Centro C.P.80000, Culiacán, Sinaloa.

2. **Servicios de auditoría al sistema informático e infraestructura tecnológica del PREP**

2.1 Pruebas funcionales de caja negra al sistema informático del PREP.

a. Objetivo

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

b. Alcance

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

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

- Se debe analizar el funcionamiento de la aplicación móvil desarrollada para la digitalización de las Actas desde las casillas, y, en su caso, la captura de datos desde las casillas. Dicho análisis se hará mediante flujos completos e interacción entre los diversos módulos y fases del proceso técnico operativo.

- Se debe verificar el cumplimiento de las especificaciones funcionales y los requerimientos

contenidos en la documentación técnica y normatividad aplicable que será proporcionada por **el IEES**.

- 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 de Datos y Verificación

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

   b. Captura de la información contenida en las Actas PREP.

   c. Verificación de la información capturada.

II. Módulo de Publicación de Resultados

   a. 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 ejecutar las pruebas, el **OPL** 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 documentos derivados de los trabajos hechos que se detallan en la tabla 1.

Tabla 1. Entregables derivados de las pruebas funcionales de caja negra

Nombre del documento	Contenido mínimo del documento	Responsable de la entrega	Forma de entrega
Plan de pruebas funcionales de caja negra del sistema informático	Describe los elementos generales que deben considerarse para la ejecución de las pruebas funcionales de caja negra: • Introducción • Objetivo • Alcance • Pruebas por aplicar • Planeación de las pruebas • Necesidades de ambiente • Casos de prueba • Datos de prueba • Criterios de pruebas • Administración de riesgos • Entregables	**El ente auditor**	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 auditoría • Metodología para clasificar los hallazgos • Observaciones y recomendaciones • Conclusiones	**El ente auditor**	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	**El ente auditor**	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.

Nombre del documento	Contenido mínimo del documento	Responsable de la entrega	Forma de entrega
Informe de desempeño de la operación del sistema informático	Documento que contiene el resultado de la operación del sistema: • Introducción • Metodología • Criterios utilizados para la auditoría • Resumen ejecutivo • Resultados • Observaciones y recomendaciones	**El ente auditor**	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.

d. Calendario de entregables

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.

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

a. Objetivo

Validar que el sistema informático del PREP que operará al término de la Jornada Electoral, corresponda al software auditado. Asimismo, verificar que el sitio de publicación del PREP y las bases de datos, no cuenten con información referente a los resultados electorales preliminares antes de su puesta en operación del Programa, previendo que, al momento de hacer esta validación, el sitio de publicación del PREP no se encuentre disponible para la ciudadanía en general, si no únicamente para el personal involucrado en la tarea de validación de la información. Cabe señalar que, los campos de las bases de datos cuyo contenido corresponda a la información sobre los datos de identificación de las actas que pertenecen al catálogo de actas esperadas de casillas aprobadas, la información relativa a la lista nominal, a representantes de partidos políticos y candidaturas independientes que se acrediten ante mesa directiva de casilla, así como los mecanismos de traslado que se utilizarán, podrán contener datos por tratarse de información que es de previo conocimiento al día de la operación del PREP. La validación respecto a la correspondencia del software auditado y el utilizado en la operación del PREP se tendrá que ejecutar al inicio, durante y al final de la operación del PREP.

b. Alcance

Los 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 PREP y que las bases de datos se encuentren debidamente inicializadas. Dicho procedimiento deberá ser

validado por el personal que el **IEES** designe para tal efecto, el procedimiento deberá, como mínimo contemplar los siguientes aspectos:

- Contar con un diagrama de flujo.
- Incluir los roles y responsabilidades de los involucrados.
- Documentar como mínimo, las siguientes etapas:
    - Generación, obtención y validación de huellas criptográficas en SHA-256 de la versión del final software PREP auditado.
    - Generación, obtención y validación de huellas criptográficas en SHA-256 del software PREP instalado en el ambiente productivo que operará al término de la Jornada Electoral.
    - Validación de la información de las bases de datos del PREP previo al inicio de la operación del Programa y al cierre de la publicación.
    - Constancia de hechos.

El procedimiento deberá ejecutarse el día de la Jornada Electoral, y deberá ser atestiguado y validado por un tercero con fe pública designado por el **IEES**, quien deberá dejar constancia de lo anterior, conforme lo señalan los numerales 14 y 23, fracción I, del Anexo 13, del Reglamento de Elecciones relativo a los Lineamientos del PREP.

Por otra parte, durante la implementación del PREP se deberán incorporar los procedimientos y componentes requeridos para la generación y el almacenamiento de bitácoras del sistema informático, y de ser posible, también la infraestructura tecnológica, que faciliten los procedimientos de auditoría.

c. Entregables

Los productos que el ente auditor deberá entregar deberán incluir lo siguiente:

- **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 las bases de datos** del sistema informático del PREP previamente auditado, junto con las etapas de validación, generación de diagramas y descripciones correspondientes, que se acuerden conjuntamente entre el **IEES** 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 llevadas a cabo, resultados obtenidos y las firmas autógrafas del personal participante por parte del **IEES** y del ente auditor.

- **Constancias de hechos de la validación de los programas y de las bases de datos** del sistema informático del PREP. Estas validaciones se deberán ejecutar 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 llevadas a cabo, resultados y las firmas autógrafas del personal participante por parte del **IEES** y el ente auditor.

d. Calendario de trabajo

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

2.3 Análisis de vulnerabilidades a la infraestructura tecnológica del PREP

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 **IEES** las posibles medidas para la mitigación de las vulnerabilidades que previamente fueron identificadas y documentadas.

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

b. Alcance

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

I. **Junta de inicio.** Se convocará al personal involucrado en ejecutar 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 los que se llevará a cabo la auditoría, así como los tiempos generales de ejecución.

   - El **IEES** pondrá a consideración del ente auditor una lista de activos durante la junta de inicio.

   - El **IEES** proporcionará espacios de trabajo a los integrantes del ente auditor para que ejecuten el análisis de vulnerabilidades a la infraestructura tecnológica del sistema.

   - El **IEES** 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)

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

Las pruebas de penetración se deberán llevar a cabo tanto desde el interior como desde el exterior de la red relacionada con la operación del PREP, particularmente:

- 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 formato de registro de datos en el que, de forma conjunta el ente auditor y el **IEES**, puedan dar seguimiento a los mismos.

II. **Validación de reporte de hallazgos.** El **IEES** 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 **IEES** 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 **IEES** pueda atender los hallazgos.

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

V. **Entregables.** El ente auditor deberá elaborar y entregar derivado de la ejecución de pruebas de penetración (pentest), los documentos referidos en la Tabla 2.

Tabla 2. Entregables derivados de las pruebas de penetración

Nombre del documento	Contenido mínimo del documento	Responsable de la entrega	Forma de entrega
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 • Calendario de trabajo • Responsables técnicos	**El ente auditor**	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 ejecutadas sobre los activos: • Resumen ejecutivo • Alcance • Resultado de las pruebas • Recomendaciones generales	**El ente auditor**	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	**El ente auditor**	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.

d. Entregables

Derivado de la revisión de las configuraciones, el ente auditor deberá proporcionar al **OPL** los documentos referidos en la Tabla 3:

Tabla 3. Entregables derivados del análisis de las vulnerabilidades a la infraestructura tecnológica del PREP

Nombre del documento	Contenido mínimo del documento	Responsable de la entrega	Forma de entrega
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	**El ente auditor**	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 • Hallazgos y recomendaciones	**El ente auditor**	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.

Nombre del documento	Contenido mínimo del documento	Responsable de la entrega	Forma de entrega
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	**El ente auditor**	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.

e. 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 establecido en la Tabla 4.

Tabla 4. Entregables finales

Nombre del documento	Contenido mínimo del documento	Responsable de la entrega	Forma de entrega
Informe final del análisis de vulnerabilidades a la infraestructura tecnológica	Documento que contiene el resultado final del análisis de vulnerabilidades: • Introducción • Resultados Generales • Observaciones y recomendaciones	**El ente auditor**	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.

Nombre del documento	Contenido mínimo del documento	Responsable de la entrega	Forma de entrega
Informe de desempeño de la operación del sistema informático	Documento que contiene el resultado de la operación del sistema: • Introducción • Resultados • Observaciones y recomendaciones	**El ente auditor**	En formato electrónico. Contenido de acuerdo con los puntos señalados en la sección de descripción y contenido.

f. 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.

2.4 Pruebas de denegación de servicio al sitio de publicación del PREP y al sitio principal del **IEES**

a. Objetivo

Llevar a cabo ataques de denegación de servicio que permitan identificar, evaluar y aplicar las medidas necesarias para asegurar **la correcta y continua disponibilidad del servicio Web, así como de los sitios de publicación de resultados del PREP y del sitio principal del IEES, durante el periodo de operación del PREP.**

Documentar los hallazgos detectados durante la ejecución 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 **IEES**, ya sea en su propia infraestructura o en la que provea un tercero.

Las pruebas de denegación 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 Electoral.
- Tráfico de red malintencionado, consistente en paquetes de red malformados.

Las pruebas mencionadas anteriormente deberán ejecutarse de manera concurrente. Los ataques de denegación 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 ejecutar SYN FLOOD.

- Ataques volumétricos por protocolo UDP:
  - Al menos de 400 Mbps de throughput.
  - Al menos ejecutar DNS AMPLIFICATION.

- Ataques volumétricos por protocolo ICMP:
  - Al menos de 400 Mbps de throughput.
  - Al menos ejecutar ICMP FLOOD.

- Ataques en la capa de aplicación (HTTP):
  - Al menos ejecutar SLOWRIS ATACK.

Las pruebas mencionadas anteriormente, deberán ejecutarse 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 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 **IEES** 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 denegación 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.

3. Condiciones Generales

3.1 Por parte del ente auditor.

Para la ejecución 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 definida 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 ejecutado durante los tres últimos años.
- En su caso, carta de la máxima autoridad del ente auditor seleccionado, donde se acepte la colaboración con el **IEES** para este proyecto.

En la Tabla 5, se presentan algunas metodologías de seguridad como referencia para su consideración:

Tabla 5. Metodologías para llevar a cabo las auditorías

METODOLOGÍA	DIRECCIÓN WEB
OWASP Testing Guide	https://www.owasp.org/index.php/OWASP_Testing_Project
Penetration Testing Framework	www.vulnerabilityassessment.co.uk/Penetration%20Test.html
Penetration Testing Execution Standard	http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
Information Systems Security Assessment Framework (ISSAF)	http://www.oissg.org/issaf
Technical Guide to Information Security Testing and Assessment	https://csrc.nist.gov/publications/detail/sp/800-115/final

Entro del Marco de normatividad aplicable en el IEES, la información que sea entregada por el ente auditor debe resguardarse con los mecanismos y procedimientos necesarios para evitar su divulgación a terceros.

De conformidad con el numeral 8, párrafo segundo, inciso IV del Anexo 13 del Reglamento de Elecciones, se debe establecer un apartado que haga referencia, a la necesidad de salvaguardar en todo momento los derechos de propiedad intelectual, respecto de la información que el **IEES** pone a disposición del ente Auditor.

Es importante que el ente auditor brinde las facilidades necesarias a las representaciones de los Partidos Políticos y, en su caso, de las Candidaturas Independientes, así como a los integrantes del Comité Técnico Asesor del PREP, para que asistan y lleven a cabo un seguimiento al desarrollo de los procesos de auditoría.

3.2 Por parte del **IEES**.

Para la ejecución de las pruebas, el **IEES** deberá proporcionar los siguientes insumos de información necesarios:

- 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, candidaturas comunes, 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 ejecutar las pruebas.
- Un ambiente de auditoría que permita controlar las versiones del sistema informático que se audite.

3.3 Revisión de las pantallas de publicación del PREP, verificando el apego a las plantillas base de la interfaz proporcionadas por el INE

Adicional a los alcances establecidos en las disposiciones normativas respecto a la ejecución de la auditoría, se considera de gran relevancia que el ente auditor verifique que el sitio de publicación del PREP se ajuste al diseño definido por el INE para la versión web y la versión móvil, tanto en la interfaz como en la usabilidad, a fin de lograr un mayor nivel de homologación de la información.

Se sugiere que la revisión que se haga al sitio de publicación del PREP incluya los siguientes elementos:

- Los niveles de agregación de la información de acuerdo con el tipo de elección que se trate, esto conforme a lo establecido en el numeral 30 del Anexo 13 del Reglamento de Elecciones.
- Los datos mínimos por publicar de acuerdo con lo establecido en el numeral 30, fracciones I a la X del Anexo 13 del Reglamento de Elecciones.
- La distribución de los elementos dentro de la interfaz de usuario conforme a las plantillas base proporcionadas por el INE, tanto para la versión web como para la versión móvil.
- La funcionalidad de los elementos gráficos.
- Los cálculos presentados en las tablas y gráficas y su correspondencia con los datos contenidos en las bases de datos.
- Los elementos emergentes.
- El contenido del Centro de Ayuda.

Asimismo, se sugiere que el ente auditor informe al **IEES**, de los hallazgos derivados de la revisión del sitio de publicación, al menos, 3 meses antes del día de la Jornada Electoral, para que estos puedan ser presentados a los integrantes del Comité Técnico Asesor del PREP.

3.4 Marco de trabajo

En el marco de trabajo se deberá considerar lo siguiente:

- Para la elaboración del Plan de Trabajo, el ente auditor se coordinará con la Instancia interna para la coordinación del PREP del Instituto, para efectos de establecer en dicho plan las actividades, fechas, responsabilidades, así como los recursos necesarios para llevar a cabo la auditoría.
- El ente auditor tendrá la obligación de coadyuvar al Instituto, otorgando la información que requiera para la ejecución de sus actividades.
- El Instituto deberá indicar el formato, medios de almacenamiento y fechas de entrega para cada producto de trabajo o entregable establecidos en el Plan de Trabajo.
- Acordar la obligación del ente auditor de brindar las facilidades necesarias para el seguimiento y supervisión que haga tanto el Instituto como el Comité Técnico Asesor del PREP (COTAPREP).
- Se deberá contemplar dentro del Plan de Trabajo, reuniones de trabajo conjuntas entre el ente auditor, el Instituto y el COTAPREP.

- El ente auditor podrá coadyuvar al Instituto para la elaboración de los planes de seguridad y continuidad del PREP.

- Se deberá establecer la vigencia del instrumento jurídico establecido entre el ente auditor y el Instituto.

- Convenir la posibilidad de que el instrumento jurídico pueda modificarse, siempre y cuando las partes estén de acuerdo y manifiesten su consentimiento por escrito conforme a la normatividad aplicable.

- Acordar las causales de rescisión del instrumento jurídico, así como las penas convencionales a que las partes se sujetarán.

- 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 **IEES**.

3.5 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, se sugiere que estas reuniones se lleven a cabo en conjunto con el tercero que, en su caso, auxilie en la implementación y operación del PREP, así como con el Comité Técnico Asesor del PREP.

- Comunicado público para informar la colaboración entre el ente auditor y el **IEES**, a través del sitio web del IEES.

- Comunicado público para informar los resultados de la auditoría, a través del sitio web del IEES.

3.6 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. Manifestación bajo protesta de decir verdad, de que cuenta con la capacidad técnica, financiera y operativa para la ejecución de la auditoría.

IX. Cartas de referencia y certificados.