Anexo Técnico

para la contratación de servicios de auditoría al sistema informático y a la infraestructura tecnológica del Programa de Resultados Electorales Preliminares 2021

Contenido

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 Oaxaca, 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.

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 Estatal Electoral y de Participación Ciudadana de Oaxaca (IEEPCO).

Las líneas de trabajo a considerar son:

1.1. 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.

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

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

1.4. En caso de que el IEEPCO, determine llevar a cabo la auditoría al código fuente, dicha previsión deberá ser incorporada tanto en el instrumento jurídico celebrado con el ente auditor como, en su caso, con el tercero que auxilie en la implementación y operación del PREP.

1.5. Pruebas de volumetría sobre el sitio de publicación del PREP y al sitio principal del IEEPCO, para validar saturación, bloqueo de cuentas y caída sobre sus sistemas.

1.3 Recomendaciones generales para el instrumento jurídico que sea celebrado con el ente auditor.

Además del requerimiento general de los servicios, se deben tomar en consideración en el instrumento jurídico celebrado con el ente auditor los siguientes aspectos:

1. Acordar la elaboración de un plan de trabajo en coordinación con el **IEEPCO**, a través de su instancia interna, con la finalidad de definir las actividades, fechas, responsabilidades, así como los recursos necesarios, metodologías, herramientas y entregables para llevar a cabo la auditoría.

2. Indicar los alcances de la auditoría al sistema PREP con el objetivo de establecer con claridad las responsabilidades de las partes.

3. Estipular la **obligación del IEEPCO y, en su caso, del tercero de facilitar al Auditor**, la información que

requiera para la ejecución de sus actividades. En caso de que **EL IEEPCO** determine llevar a cabo la auditoría al código fuente, en su caso, dicha previsión también debe ser incorporada en el instrumento jurídico firmado con el tercero.

4. **El IEEPCO** debe indicar el formato, los medios de almacenamiento y las fechas de entrega para cada producto de trabajo o entregable, las cuales quedarán establecidas en el plan de trabajo. En ese sentido, el ente auditor debe entregar dichos productos de trabajo en las oficinas del **IEEPCO** ubicadas en ubicadas en Heroica Escuela Naval Militar 1212, colonia Reforma, Oaxaca de Juárez, Oaxaca, junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la cuenta que EL IEEPCO determine y que queden asentadas en dicho documento.

5. Acordar la obligación del ente auditor de brindar las facilidades necesarias para el seguimiento y supervisión que haga el IEEPCO, y en su caso, el Instituto.

6. Acordar la obligación del ente auditor de brindar las facilidades necesarias para el seguimiento y supervisión que lleve a cabo COTAPREP.

7. Establecer que el ente auditor y su personal designado para ejecutar las auditorías al sistema PREP no tengan relación directa o indirecta con el tercero que auxilie al IEEPCO en la implementación y operación del PREP que pudiese generar un posible conflicto de interés.

8. Convenir reuniones de trabajo conjuntas con **EL IEEPCO**, el COTAPREP que haya integrado **EL IEEPCO**, en su caso, con el tercero y el Instituto.

9. Coadyuvar con **EL IEEPCO**, en la elaboración de los planes de seguridad y de continuidad.

10. Establecer la vigencia de dicho instrumento jurídico.

11. 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.

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

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 2020-2021 en el estado de *Oaxaca*, 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 Estatal Electoral y de Participación Ciudadana de Oaxaca (IEEPCO). Las líneas de trabajo a considerar son:

1.1. Pruebas funcionales de caja negra al sistema informático del PREP 2021.
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 IEEPCO.

1.1. Pruebas funcionales de caja negra al sistema informático del PREP 2021.

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 IEEPCO**.
- 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 IEEPCO** 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:

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

Nombre del documento	Contenido mínimo del documento	Fecha límite de la entrega	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 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	Conforme al plan de trabajo elaborado en coordinación con el IEEPCO, referido en el numeral 1 del punto 1.3 de este documento (**Recomendaciones generales para el instrumento jurídico que sea**	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEPCO ubicadas en Heroica Escuela Naval Militar 1212, colonia Reforma, Oaxaca de Juárez, Oaxaca, junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la cuenta que EL IEEPCO determine y que

Nombre del documento	Contenido mínimo del documento	Fecha límite de la entrega	Responsable de la entrega	Forma de entrega
	• Criterios de pruebas • Administración de riesgos • Entregables	**celebrado con el ente auditor)**		queden asentadas en dicho documento.
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	Conforme al plan de trabajo elaborado en coordinación con el IEEPCO, referido en el numeral 1 del punto 1.3 de este documento (**Recomendaciones generales para el instrumento jurídico que sea celebrado con el ente auditor)**	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEPCO ubicadas en Heroica Escuela Naval Militar 1212, colonia Reforma, Oaxaca de Juárez, Oaxaca, junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la cuenta que EL IEEPCO determine y que queden asentadas en dicho documento.
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	Conforme al plan de trabajo elaborado en coordinación con el IEEPCO, referido en el numeral 1 del punto 1.3 de este documento (**Recomendaciones generales para el instrumento jurídico que sea celebrado con el ente auditor)**	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEPCO ubicadas en Heroica Escuela Naval Militar 1212, colonia Reforma, Oaxaca de Juárez, Oaxaca, junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la cuenta que EL IEEPCO determine y que queden asentadas en dicho documento.
Informe de desempeño de operación del sistema informático	Documento que contiene el resultado final de las pruebas del sistema: • Introducción • Metodología • Criterios utilizados para la auditoría • Resumen ejecutivo • Resultados • Observaciones y recomendaciones	Conforme al plan de trabajo elaborado en coordinación con el IEEPCO, referido en el numeral 1 del punto 1.3 de este documento (**Recomendaciones generales para el instrumento jurídico que sea celebrado con el ente auditor)**	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEPCO ubicadas en Heroica Escuela Naval Militar 1212, colonia Reforma, Oaxaca de Juárez, Oaxaca, junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la cuenta que EL IEEPCO determine y que queden asentadas en dicho documento.

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.

1.2. 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 sistema informático del PREP, así como que la base de datos se encuentre debidamente inicializadas. Dicho procedimiento deberá ser validado por el personal que el IEEPCO designe para tal efecto, contemplando los siguientes aspectos como mínimo, el procedimiento deberá:

- 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 final del 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 realizarse el día de la Jornada Electoral, el domingo 6 de junio de 2021, y deberá ser atestiguado y validado por un tercero con fe pública designado por el IEEPCO, 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.

c. Entregables

Los productos que el ente auditor, deberá entregar se deben 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 del PREP previamente auditado, junto con las etapas de validación, generación de diagramas y descripciones correspondiente que se acuerden conjuntamente entre el Proveedor del PREP 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 IEEPCO 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 IEEPCO 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 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 Proveedor del PREP las posibles medidas para la mitigación de las vulnerabilidades que previamente fueron identificadas y documentadas.

- Verificar que las medidas implementadas por el Proveedor del PREP 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 Proveedor del PREP pondrá a consideración del ente Auditor una lista de activos durante la junta de inicio.
- El Proveedor del PREP proporcionará espacios de trabajo a los integrantes del ente auditor para que realicen el análisis de vulnerabilidades a la infraestructura tecnológica del sistema.
- El Proveedor del PREP 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 estructura 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 llevarán a cabo tanto desde el interior como desde el exterior de la red de datos 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 registro de datos en el que, de forma conjunta el ente auditor y el Proveedor del PREP, puedan dar seguimiento a los mismos.

II. Validación de reporte de hallazgos. El Proveedor del PREP 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 Proveedor del PREP 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 IEEPCO pueda atender los hallazgos.

IV. Validación de la atención de los hallazgos. El ente auditor validará que el Proveedor del PREP 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*), los siguientes documentos:

Tabla 2. Entregables derivados de las pruebas de penetración

Nombre del documento	Contenido mínimo del documento	Fecha límite de entrega	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	Conforme al plan de trabajo elaborado en coordinación con el IEEPCO, referido en el numeral 1 del punto 1.3 de este documento (**Recomendaciones generales para el instrumento jurídico que sea celebrado con el ente auditor)**	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEPCO ubicadas en Heroica Escuela Naval Militar 1212, colonia Reforma, Oaxaca de Juárez, Oaxaca, junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la cuenta que EL IEEPCO determine y que queden asentadas en dicho documento.
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	Conforme al plan de trabajo elaborado en coordinación con el IEEPCO, referido en el numeral 1 del punto	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEPCO ubicadas en Heroica Escuela

	• Resultado de las pruebas • Recomendaciones generales	1.3 de este documento (**Recomendaciones generales para el instrumento jurídico que sea celebrado con el ente auditor)**		Naval Militar 1212, colonia Reforma, Oaxaca de Juárez, Oaxaca, junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la cuenta que EL IEEPCO determine y que queden asentadas en dicho documento
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	Conforme al plan de trabajo elaborado en coordinación con el IEEPCO, referido en el numeral 1 del punto 1.3 de este documento (**Recomendaciones generales para el instrumento jurídico que sea celebrado con el ente auditor)**	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEPCO ubicadas en Heroica Escuela Naval Militar 1212, colonia Reforma, Oaxaca de Juárez, Oaxaca, junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la cuenta que EL IEEPCO determine y que queden asentadas en dicho documento.

d. Entregables

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

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

Nombre del documento	Contenido mínimo del documento	Fecha de entrega	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	Conforme al plan de trabajo elaborado en coordinación con el IEEPCO, referido en el numeral 1 del punto 1.3 de este documento (**Recomendaciones**	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEPCO ubicadas en Heroica Escuela Naval Militar 1212, colonia Reforma, Oaxaca de Juárez, Oaxaca, junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la cuenta que EL IEEPCO determine y que queden asentadas en dicho documento.

		generales para el instrumento jurídico que sea celebrado con el ente auditor)		
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	Conforme al plan de trabajo elaborado en coordinación con el IEEPCO, referido en el numeral 1 del punto 1.3 de este documento (**Recomendaciones generales para el instrumento jurídico que sea celebrado con el ente auditor)**	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEPCO ubicadas en Heroica Escuela Naval Militar 1212, colonia Reforma, Oaxaca de Juárez, Oaxaca, junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la cuenta que EL IEEPCO determine y que queden asentadas en dicho documento.
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	Conforme al plan de trabajo elaborado en coordinación con el IEEPCO, referido en el numeral 1 del punto 1.3 de este documento (**Recomendaciones generales para el instrumento jurídico que sea celebrado con el ente auditor)**	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEPCO ubicadas en Heroica Escuela Naval Militar 1212, colonia Reforma, Oaxaca de Juárez, Oaxaca, junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la cuenta que EL IEEPCO determine y que queden asentadas en dicho documento.

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 siguiente:

Tabla 4. Tabla de entregables finales

Nombre del documento	Contenido mínimo del documento	Fecha límite de entrega	Responsable de la entrega	Forma de entrega
Informe final del análisis de vulnerabilidades a la infraestructura tecnológica	Documento que contiene el resultado del análisis de vulnerabilidades a la infraestructura tecnológica: • Introducción • Resultados generales • Observaciones y recomendaciones	Conforme al plan de trabajo elaborado en coordinación con el IEEPCO, referido en el numeral 1 del punto 1.3 de este documento (**Recomendaciones generales para el instrumento jurídico que sea celebrado con el ente auditor)**	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEPCO ubicadas en Heroica Escuela Naval Militar 1212, colonia Reforma, Oaxaca de Juárez, Oaxaca, junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la cuenta que EL IEEPCO determine y que queden asentadas en dicho documento
Informe de desempeño de la operación del sistema informático	Documento que contiene el resultado de la operación del sistema informático: • Introducción • Resultados generales • Observaciones y recomendaciones	Conforme al plan de trabajo elaborado en coordinación con el IEEPCO, referido en el numeral 1 del punto 1.3 de este documento (**Recomendaciones generales para el instrumento jurídico que sea celebrado con el ente auditor)**	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEPCO ubicadas en Heroica Escuela Naval Militar 1212, colonia Reforma, Oaxaca de Juárez, Oaxaca, junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la cuenta que EL IEEPCO determine y que queden asentadas en dicho documento.

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.

1.4 Pruebas de denegación de servicio al sitio de publicación del PREP y al sitio principal del IEEPCO

a. Objetivo

Llevar a cabo los 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 IEEPCO, 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 IEEPCO, 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 realizarse 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 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 Proveedor del PREP efectúe 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.

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, los cuales preferentemente deberán observar buenas prácticas y estándares internacionales. Respecto de las metodologías, se sugiere que en el Anexo Técnico se establezca la o las metodologías a utilizarse y que éstas sean detalladas o en su defecto que se establezca en el marco de trabajo del propio instrumento las condiciones de tiempo y forma para establecer dicha metodología de manera conjunta.

A continuación, se mencionan algunas metodologías de seguridad 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

Asimismo, se debe considerar lo siguiente:

- 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 IEEPCO para este proyecto.

Dentro del marco de normatividad aplicable para cada OPL, 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 OPL 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.

1.6 Por parte del IEEPCO.

Para la realización de las pruebas, el Proveedor del PREP conjuntamente con el Proveedor del PREP 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, candidaturas comunes, coaliciones y candidaturas 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 Proveedor del PREP 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 Proveedor del IEEPCO en donde se encuentre instalado el sistema informático, además de brindar la capacitación inicial y apoyo técnico necesario para habilitar la operación de esta.

Cabe mencionar que, en caso de que un tercero implemente el PREP del IEEPCO, se debe especificar en el instrumento jurídico que se suscriba, que el tercero debe permitir al ente auditor el acceso a todos los módulos del sistema para que pueda ejecutarse la auditoría. Lo anterior, deberá ser especificado tanto en el instrumento jurídico firmado con el ente auditor como, en su caso, con el tercero que auxilie en la implementación y operación del PREP.

Respecto a las adecuaciones que se hagan a los distintos módulos del sistema informático del PREP derivadas de los hallazgos del ente auditor, el Proveedor del PREP , preferentemente, deberán contar una bitácora de seguimiento, en la que se detallen dichas adecuaciones, a fin de que el ente auditor cuente con un registro de las observaciones subsanadas y de las distintas versiones del sistema.

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

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 IEEPCO, de los hallazgos derivados de la revisión del sitio de publicación, al menos, 4 meses antes del día de la Jornada Electoral, para que estos puedan ser presentados a los integrantes del Comité Técnico Asesor del PREP.

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 IEEPCO.

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, 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 Proveedor del PREP.
- 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. Manifestación bajo protesta de decir verdad, que cuenta con la capacidad técnica, financiera y operativa para la operación de la auditoría.
IX. Cartas de referencia y certificados.