

Enero 2024

Anexo Técnico para la contratación del
Ente Auditor del Programa de Resultados
ElectORAles Preliminares (PREP)

Proceso Electoral Local 2023 – 2024

Anexo Técnico para la contratación de servicios de auditoría

1.	Descripción general.....	4
1.1	Fundamento normativo.....	4
1.2	Requerimiento general de los servicios	4
2.	Servicios de auditoría al sistema informático e infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP	5
2.1	Pruebas funcionales de caja negra al sistema informático del PREP	5
a.	Objetivo.....	5
b.	Alcance	5
c.	Entregables.....	6
d.	Calendario de entregables	8
2.2	Validación del sistema informático del PREP y/o servicios relacionados con Tecnologías de la Información y Comunicaciones, así como de sus bases de datos, ante un tercero con fe pública.....	8
a.	Objetivo.....	8
b.	Alcance	9
c.	Entregables.....	10
d.	Calendario de trabajo	11
2.3	Análisis de vulnerabilidades a la infraestructura y servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP	11
a.	Objetivos.....	11
b.	Alcance	11
c.	Pruebas de penetración (pentest)	12
d.	Revisión de configuraciones a la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP	14
e.	Entregables.....	14
f.	Informe final de análisis de vulnerabilidades a la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP	16
g.	Calendario de trabajo	17
2.4	Pruebas de negación de servicio al sitio de publicación del PREP y al sitio principal del OPL .	17
a.	Objetivo.....	17
b.	Alcance	17
c.	Entregables.....	19
d.	Calendario de trabajo.	19
3.	Condiciones generales	19

3.1	Por parte del ente auditor	19
3.2	Por parte del OPL	20
3.3	Revisión de las pantallas del sitio de publicación del PREP, verificando el apego a las plantillas base de la interfaz proporcionadas por el INE	22
3.4	Marco de trabajo.....	22
3.5	Comunicación Social Conjunta.....	23
3.6	Estructura de la propuesta	23

1. Descripción general

1.1 Fundamento normativo

En el marco de las actividades para el diseño, implementación y operación del Programa de Resultados Electorales Preliminares (PREP) para el Proceso Electoral Concurrente 2023-2024 en el estado de [Campeche](#), 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. Asimismo, se detallan los requerimientos de cada línea de trabajo que deberán considerarse en la propuesta técnico-económica que se presente ante el OPL de [Campeche](#).

Las líneas de trabajo a considerar son:

- 1.1. Pruebas funcionales de caja negra al sistema informático del PREP y a la aplicación que se utilizarán para operar el mecanismo de digitalización de las Actas desde las casillas, para evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares.
- 1.2. Análisis de vulnerabilidades, considerando al menos pruebas de penetración y revisión de configuraciones a la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP.
- 1.3. **En caso de que el OPL 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.**
- 1.4. Pruebas de negación de servicio al sitio de publicación del PREP y al sitio principal del OPL.

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

2. Servicios de auditoría al sistema informático e infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el 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 PTO, considerando al menos, la **digitalización, captura de datos, verificación y publicación de resultados**, mediante flujos completos e interacción entre los diversos módulos (*escenarios principales*).
- Se debe analizar el funcionamiento del aplicativo desarrollado 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 PTO.

- 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 OPL**.
- 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

- 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.
- Captura de la información contenida en las Actas PREP.
- Verificación 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 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 3.2 del presente Anexo. Es importante señalar que, de acuerdo con el plan de trabajo establecido, se deben llevar a cabo las pruebas necesarias, a fin de dar cumplimiento a lo establecido en la norma y a los objetivos del PREP.

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 entrega	Responsable de la entrega	Forma de entrega
Plan de pruebas funcionales de caja	Describe los elementos generales que deben	06/03/2024	El ente auditor	Debe entregarse por escrito, en físico, en las

Nombre del documento	Contenido mínimo del documento	Fecha límite de entrega	Responsable de la entrega	Forma de entrega
negra del sistema informático y/o servicios relacionados con Tecnologías de la Información y Comunicaciones	considerarse para la ejecución de las pruebas funcionales de caja negra: <ul style="list-style-type: none"> • 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 			oficinas de EL IEEC ubicadas en Av. Fundadores 18, Área Ah-Kim-Pech, CP. 24014, San Francisco de Campeche, Camp. , junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la(s) cuenta(s) que EL IEEC determine y que queden asentadas en dicho documento.
Informe preliminar de las pruebas funcionales de caja negra del sistema informático y/o servicios relacionados con Tecnologías de la Información y Comunicaciones	Documento que contiene el detalle de cada una de las observaciones identificadas en la revisión y pruebas del sistema y que incluya, al menos: <ul style="list-style-type: none"> • Introducción • Metodología • Criterios utilizados para la auditoría • Metodología para clasificar los hallazgos • Observaciones y recomendaciones • Conclusiones <p><i>Software en la nube para la Gestión de hallazgos bajo control del Ente Auditor</i></p>	10/04/2024	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEC ubicadas en Av. Fundadores 18, Área Ah-Kim-Pech, CP. 24014, San Francisco de Campeche, Camp. , junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la(s) cuenta(s) que EL IEEC determine y que queden asentadas en dicho documento.
Informe final de las pruebas funcionales de caja negra del sistema informático y/o servicios relacionados con Tecnologías de la Información y Comunicaciones	Documento que contiene el resultado final de las pruebas del sistema: <ul style="list-style-type: none"> • Introducción • Metodología • Criterios utilizados para la auditoría • Resumen ejecutivo • Resultados 	30/05/2024	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEC ubicadas en Av. Fundadores 18, Área Ah-Kim-Pech, CP. 24014, San Francisco de Campeche, Camp. , junto con copia en formato digital en unidades de

Nombre del documento	Contenido mínimo del documento	Fecha límite de entrega	Responsable de la entrega	Forma de entrega
				almacenamiento en la misma dirección o bien, vía correo electrónico a la(s) cuenta(s) que EL IEEC determine y que queden asentadas en dicho documento.
Informe de desempeño de la operación del sistema informático y/o servicios relacionados con Tecnologías de la Información y Comunicaciones	Documento que contiene el resultado de la operación del sistema: <ul style="list-style-type: none"> • Introducción • Metodología • Criterios utilizados para la auditoría • Resumen ejecutivo • Resultados • Observaciones y recomendaciones 	10/06/2024	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEC ubicadas en <i>Av. Fundadores 18, Área Ah-Kim-Pech, CP. 24014, San Francisco de Campeche, Camp.</i> , junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la(s) cuenta(s) que EL IEEC 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, la remisión de los entregables establecidos en el plan de trabajo, y los avances esperados en cada periodo de trabajo.

2.2 Validación del sistema informático del PREP y/o servicios relacionados con Tecnologías de la Información y Comunicaciones, así como de sus bases de datos, ante un tercero con fe pública

a. Objetivo

Validar que los componentes, programas, configuraciones y, en su caso códigos auditados del sistema informático del PREP y/o servicios relacionados con Tecnologías de la Información y Comunicaciones, sean los utilizados al inicio, durante la operación del PREP y al cierre del mismo. 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. Ambos procedimientos deberán concluirse antes del inicio de la publicación y tendrán que ser atestiguados y validados por un tercero con fe pública, quien deberá dejar constancia de lo anterior.

La validación respecto a la correspondencia del software auditado y el utilizado en la operación del PREP se tendrá que ejecutar por lo menos una vez al inicio, otra durante y una más 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 OPL** designe para tal efecto, contemplando los siguientes aspectos como mínimo, por tanto, el procedimiento deberá:

- Contar con un diagrama de flujo.
- Incluir los roles y responsabilidades de las personas involucradas.
- Documentar como mínimo, las siguientes etapas:
 - Generación, obtención y validación de huellas criptográficas en SHA-256 del software del PREP auditado.
 - Generación, obtención y validación de huellas criptográficas en SHA-256 del software del PREP instalado en el ambiente productivo que operará al término de la Jornada Electoral.
 - Validación de la información inicial y final de las bases de datos del PREP.

- Constancia de hechos.

El procedimiento deberá ejecutarse el día de la operación del PREP, y deberá ser atestiguado y validado por un tercero con fe pública designado por **EL OPL**, 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.

El procedimiento deberá tomar en cuenta las consideraciones particulares dependiendo del modelo de aprovisionamiento de infraestructura, considerando, al menos; infraestructura tecnológica (on-premise) o servicio de nube publica conforme a lo que EL OPL determine.

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 de 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 componentes, programas, configuraciones y, en su caso códigos auditados; 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 OPL** y el ente auditor.
- **Constancia de hechos de la generación de huellas criptográficas** de los componentes, programas, configuraciones y, en su caso códigos auditados del sistema informático del PREP. Esta constancia deberá describir el protocolo de la actividad, fecha y lugar, hora de inicio y término, objetivo, actividades para llevar a cabo, resultados obtenidos y las firmas autógrafas del personal participante por parte del **OPL** y del ente auditor.
- **Constancias de hechos de la validación de los componentes, programas, configuraciones y, en su caso códigos auditados; 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 operación 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 **OPL** 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 y servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP

a. Objetivos

- Identificar debilidades de seguridad en la infraestructura y servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP 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 **OPL** las posibles medidas para la mitigación de las vulnerabilidades que previamente fueron identificadas y documentadas.
- Verificar que las medidas implementadas por **EL OPL** hayan atendido adecuadamente las vulnerabilidades reportadas.

b. Alcance

El análisis de vulnerabilidades de la infraestructura y servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP deberá hacerse con base en las etapas que se describen a continuación.

- I. **Junta de inicio.** Se convocará al personal involucrado en la ejecución 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 llevará a cabo la auditoría, así como los tiempos generales de ejecución.
- **EL OPL** pondrá a consideración del ente auditor una lista de activos durante la junta de inicio.
 - **EL OPL** proporcionará espacios de trabajo a los integrantes del ente auditor para que ejecuten el análisis de vulnerabilidades a la infraestructura y servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP.
 - **EL OPL** 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 y servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP. Este documento integrará la información necesaria durante y después del proceso de auditoría e incluirá, como mínimo, lo siguiente:

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

c. Pruebas de penetración (pentest)

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

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

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

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

II. **Validación de reporte de hallazgos.** **EL OPL** 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 OPL** 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 OPL** pueda atender los hallazgos.

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

V. **Entregables.** El ente auditor deberá elaborar y entregar derivado de la ejecución de pruebas de penetración (pentest), los documentos siguientes:

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 y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP.	Describe los elementos generales de planeación que deben considerarse para el desarrollo de las pruebas de penetración: <ul style="list-style-type: none"> • Alcance • Calendario de trabajo • Responsables técnicos 	06/03/2024	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEC ubicadas en <i>Av. Fundadores 18, Área Ah-Kim-Pech, CP. 24014, San Francisco de Campeche, Camp.</i> , junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la(s) cuenta(s) que EL IEEC determine y que queden asentadas en dicho documento.
Informe preliminar de las pruebas de penetración a la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP.	Documento que contiene el resultado de las pruebas ejecutadas sobre los activos: <ul style="list-style-type: none"> • Resumen ejecutivo • Alcance • Resultado de las pruebas <i>Software en la nube para la Gestión de hallazgos bajo control del Ente Auditor</i>	13/05/2024	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEC ubicadas en <i>Av. Fundadores 18, Área Ah-Kim-Pech, CP. 24014, San Francisco de Campeche, Camp.</i> , junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la(s) cuenta(s) que EL IEEC determine y que queden asentadas en dicho documento.
Informe de la aplicación de recomendaciones de las pruebas de penetración a la	Documento que describe el estado de seguridad de la infraestructura y/o servicios relacionados con Tecnologías de la	10/05/2024	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEC ubicadas en <i>Av. Fundadores 18, Área Ah-Kim-</i>

Nombre del documento	Contenido mínimo del documento	Fecha límite de entrega	Responsable de la entrega	Forma de entrega
infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP.	<p>Información y Comunicaciones donde se implemente el PREP una vez que fueron aplicadas las recomendaciones emitidas por parte del ente auditor.</p> <ul style="list-style-type: none"> • Resumen ejecutivo • Alcance • Resultado de la verificación 			<i>Pech, CP. 24014, San Francisco de Campeche, Camp.,</i> junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la(s) cuenta(s) que EL IEEC determine y que queden asentadas en dicho documento.

d. Revisión de configuraciones a la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP

El objetivo es analizar las configuraciones de los dispositivos que conforman la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP con base en mejores prácticas de seguridad informática, para identificar oportunidades y emitir recomendaciones orientadas al fortalecimiento de ésta.

e. Entregables

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

Tabla 3. Entregables derivados del análisis de las vulnerabilidades a la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP

Nombre del documento	Contenido mínimo del documento	Fecha límite de entrega	Responsable de la entrega	Forma de entrega
Plan de revisión de configuraciones de la infraestructura y/o servicios relacionados con Tecnologías de la Información y	<p>Describe los elementos generales de planeación que deben considerarse para el desarrollo de la revisión:</p> <ul style="list-style-type: none"> • Alcance • Calendario de trabajo 	06/03/2024	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEC ubicadas en <i>Av. Fundadores 18, Área Ah-Kim-Pech, CP. 24014, San Francisco de Campeche, Camp.,</i>

Nombre del documento	Contenido mínimo del documento	Fecha límite de entrega	Responsable de la entrega	Forma de entrega
Comunicaciones donde se implemente el PREP	<ul style="list-style-type: none"> Responsables técnicos 			junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la(s) cuenta(s) que EL IEEC determine y que queden asentadas en dicho documento.
Informe preliminar de la revisión de configuraciones de la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP	<p>Documento que contiene el detalle de cada hallazgo identificado en la revisión de configuraciones:</p> <ul style="list-style-type: none"> Resumen ejecutivo Objetivos Alcance Hallazgos y recomendaciones <p><i>Software en la nube para la Gestión de hallazgos bajo control del Ente Auditor</i></p>	20/04/2024	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEC ubicadas en <i>Av. Fundadores 18, Área Ah-Kim-Pech, CP. 24014, San Francisco de Campeche, Camp.</i> , junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la(s) cuenta(s) que EL IEEC determine y que queden asentadas en dicho documento.
Informe de la aplicación de recomendaciones de la revisión de configuraciones de la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP	<p>Documento que contiene el resultado final de la revisión de configuraciones:</p> <ul style="list-style-type: none"> Resumen ejecutivo Objetivos Alcance 	10/05/2024	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEC ubicadas en <i>Av. Fundadores 18, Área Ah-Kim-Pech, CP. 24014, San Francisco de Campeche, Camp.</i> , junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la(s) cuenta(s) que EL IEEC determine y que queden asentadas en dicho documento.

f. Informe final de análisis de vulnerabilidades a la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP

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 y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP, de acuerdo con lo siguiente:

Tabla 4. 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 y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP	Documento que contiene el resultado final del análisis de vulnerabilidades: <ul style="list-style-type: none"> • Introducción • Resultados Generales • Observaciones y recomendaciones 	30/05/2024	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEC ubicadas en <i>Av. Fundadores 18, Área Ah-Kim-Pech, CP. 24014, San Francisco de Campeche, Camp.</i> , junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la(s) cuenta(s) que EL IEEC 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: <ul style="list-style-type: none"> • Introducción • Resultados • Observaciones y recomendaciones 	10/06/2024	El ente auditor	Debe entregarse por escrito, en físico, en las oficinas de EL IEEC ubicadas en <i>Av. Fundadores 18, Área Ah-Kim-Pech, CP. 24014, San Francisco de Campeche, Camp.</i> , junto con copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la(s) cuenta(s) que EL IEEC determine y que

Nombre del documento	Contenido mínimo del documento	Fecha límite de entrega	Responsable de la entrega	Forma de entrega
				queden asentadas en dicho documento.

g. Calendario de trabajo

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

2.4 Pruebas de negación de servicio al sitio de publicación del PREP y al sitio principal del OPL

a. Objetivo

Llevar a cabo ataques de negación 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 OPL, 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. Para los casos en que el software del PREP, sea aprovisionado a través de una nube pública, se deberá considerar un proveedor autorizado de acuerdo con lo establecido por cada proveedor de nube, hacia los servicios web que se publican dentro del dominio del **OPL**, ya sea en su propia infraestructura o en la que provea un tercero.

Se debe tener en consideración que el tráfico generado deberá ejecutarse tomando en consideración si el software del PREP se encuentra desplegado en ambiente de tipo on-premise o servicio de nube pública.

Las pruebas de negación de servicio deberán considerar dos apartados:

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

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

- Para despliegue on-premise:
 - Ataques volumétricos por protocolo TCP:
 - Al menos de 400 Gbps 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 ATTACK.
 - HTTP FLOOD
 - DNS QUERY FLOOD
- Para despliegue en nube publica:
 - Ataques en la capa de aplicación:
 - Al menos de 20 Gbps de throughput.
 - Al menos ejecutar:
 - DNS QUERY FLOOD.
 - SLOWLORIS Attack.
 - CACHE-BUSTING.
 - HTTP FLOOD.

Las pruebas mencionadas anteriormente, deberán ejecutarse de manera concurrente, considerando la generación de tráfico malintencionado (SYN FLOOD, DNS AMPLIFICATION, ICMP FLOOD, SLOWRIS ATTACK, DNS QUERY FLOOD, HTTPS FLOOD, CACHE-BOSTING) 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 OPL** efectuó la contramedida para la mitigación.

c. Entregables

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

d. Calendario de trabajo.

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

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 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.

A continuación, se mencionan algunas metodologías de seguridad 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

Metodología	Dirección Web
Technical Guide to Information Security Testing and Assessment	https://csrc.nist.gov/publications/detail/sp/800-115/final

Asimismo, se debe considerar lo siguiente:

- Acreditar con soporte documental que su personal designado para ejecutar las auditorías cuenta con 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 últimos tres años.
- En su caso, carta de la máxima autoridad del ente auditor seleccionado, donde se acepte la colaboración con **EL OPL** 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, fracción 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 las y 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 OPL

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

- Normatividad aplicable y vigente.

- Documentación técnica del sistema informático y/o servicios relacionados con Tecnologías de la Información y Comunicaciones sobre la arquitectura tecnológica implementada (tanto de software como de hardware) y el proceso que se automatiza.
- Relación de los partidos políticos, candidaturas independientes, coaliciones y candidaturas comunes 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 y/o servicios relacionados con Tecnologías de la Información y Comunicaciones que se audite.

Durante el periodo de trabajo, **EL OPL** proporcionará al ente auditor: el espacio físico, equipo de cómputo y periféricos para instalar una maqueta con la infraestructura tecnológica necesaria para la ejecución de las pruebas funcionales de caja negra, así como los accesos a los servidores centrales del **OPL** en donde se encuentre instalado el sistema informático y/o servicios relacionados con Tecnologías de la Información y Comunicaciones, además de brindar la capacitación inicial y apoyo técnico necesario para habilitar la operación de ésta.

Cabe mencionar que, en caso de que un tercero implemente el PREP del **OPL**, 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 y/o servicios relacionados con Tecnologías de la Información y Comunicaciones 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 y/o servicios relacionados con Tecnologías de la Información y Comunicaciones derivadas de los hallazgos del ente auditor, **EL OPL** o el tercero, 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.

3.3 Revisión de las pantallas del sitio 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 de la 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 **OPL**, 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.

3.4 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 **OPL**.

3.5 Comunicación Social Conjunta

En el marco de trabajo se deberá considerar lo siguiente:

- Sesiones formales entre las autoridades competentes del **OPL** y el ente auditor 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 las y los integrantes del Comité Técnico Asesor del PREP. Se deberán elaborar minutas de las sesiones celebradas y llevar un control del cumplimiento de los acuerdos asumidos durante éstas.
- Comunicado público para informar la colaboración entre el ente auditor y **EL OPL**.
- Comunicado público para informar los resultados de la auditoría.

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, en la que se dé respuesta a los rubros señalados en el documento del anexo técnico.
- II. Propuesta económica. La cual, se sugiere, deberá desglosar el monto por línea de trabajo y el monto total (con y sin IVA).
- 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.