ANEXO TÉCNICO PARA LA CONTRATACIÓN DEL SERVICIO ESPECIALIZADO PARA LA ACTUALIZACIÓN, IMPLEMENTACIÓN, ACOMPAÑAMIENTO Y SOPORTE DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES DEL PROCESO ELECTORAL ORDINARIO DE GUBERNATURA DEL ESTADO, DIPUTACIONES LOCALES Y AYUNTAMIENTOS 2026-2027.

Contenido

1. Descripción general 6

1.1 Fundamento normativo 6

1.2 Requerimiento general de los servicios 7

1.3 Recomendaciones generales para el instrumento jurídico que sea celebrado con el Tercero especializado. 8

2. Requerimientos específicos para el diseño, la actualización, acompañamiento y soporte en la implementación y operación del sistema informático 10

1.4 Diseño, actualización, implementación, acompañamiento y soporte del sistema informático 10

2.1.1 Aplicativo móvil (digitalización desde las casillas) 10

2.1.2 Sistema informático PREP 12

3. Aprovisionamiento y habilitación de CATD y, en su caso, CCV 34

3.1 Actividades por hacer 35

3.1.1 Identificación de adecuaciones en CATD y CCV 35

3.1.2 Adecuaciones de infraestructura en CATD y CCV 36

3.1.3 Recursos humanos 37

4. Prueba o pruebas de funcionalidad 39

5. Simulacros 40

5.1 Entregables de los simulacros 42

6. Operación del PREP 44

7. Publicación 45

8. Confidencialidad y tratamiento de datos personales 46

9. Consultoría y soporte operativo 48

9.1 Administración de personal 48

9.2 Administración de infraestructura 49

9.3 Administración de sistemas 50

9.4 Administración de proyecto 50

9.5 Involucrados 50

9.6 Entrega del sistema y documentación final 51

9.6.1 Entrega del sistema 51

9.6.2 Documentación final 51

10. Servicio especializado de aseguramiento de ciberseguridad y ciberresiliencia del PREP 51
11.1 Independencia del aseguramiento de ciberseguridad 52
11.2 Evaluación y autorización de proveedores especializados de ciberseguridad 52
11.3 Modelo de amenazas PREP 52
11.4 Aseguramiento del desarrollo seguro 53
11.5 Seguridad del aplicativo PREP Casilla 54
11.6 Seguridad criptográfica e integridad de las Actas 55
11.7 Pruebas de penetración especializadas 55
11.8 Seguridad de APIs y microservicios 56
11.9 Hardening y configuración segura 57
11.10 Protección del sitio público del PREP 57
11.11 Monitoreo de ciberseguridad 58
11.12 Respuesta a incidentes 58
11.13 Simulacros de ciberseguridad y ciberrresiliencia 58
11.14 Ciberresiliencia y continuidad 59
11.15 Gestión de vulnerabilidades 59
11.16 Entregables mínimos 60
11.17 Consideraciones 61
Anexo Único Funcionalidad del mecanismo para la digitalización de Actas desde las casillas 61
1. Preparación de usuarios y sus roles 62
1.1 Administrar roles de usuarios 62
1.2 Administrar usuarios 64
2. Operación del mecanismo para la digitalización de Actas desde las casillas 66
2.1 Acceder a la Aplicación 66
2.2 Autenticar usuario 67
2.3 Autorizar usuario 67
2.4 Menú principal 68
2.5 Acta digitalizada con QR 69
2.6 Acta digitalizada sin QR 69
2.7 Procesamiento del acta digitalizada 70
2.8 Historial de Actas 71

Glosario.

AEC: Acta de Escrutinio y Cómputo.

Acta PREP: Primera copia del Acta de Escrutinio y Cómputo destinada para el PREP o, en su ausencia, cualquier otra copia de esta.

Anexo 13: Anexo del Reglamento de Elecciones del INE referente a los Lineamientos del Programa de Resultados Electorales Preliminares (PREP), que regula la operación, seguridad y requerimientos técnicos del sistema.

CAEL: Capacitador-Asistente Electoral Local.

CATD: Centro de Acopio y Transmisión de Datos.

CCV: Centro de Captura y Verificación.

Código Fuente: Instrucciones escritas por un programador en un lenguaje comprensible, traducidas posteriormente para ser ejecutadas por una computadora.

COTAPREP: Comité Técnico Asesor del Programa de Resultados Electorales Preliminares.

El Proveedor: Persona física o moral adjudicada para brindar los desarrollos o servicios tecnológicos requeridos para la implementación y operación del PREP, conforme a las especificaciones y normativas solicitadas.

El Sistema PREP: Conjunto de software e infraestructura tecnológica destinado al acopio, digitalización, captura, verificación y publicación de las Actas PREP y sus datos.

Encriptación: Proceso informático que cifra datos legibles mediante algoritmos para garantizar su confidencialidad e integridad al transmitirse o almacenarse.

Framework: Estructura de trabajo estandarizada que proporciona herramientas y reglas predefinidas para optimizar el desarrollo de software.

FrontEnd: Capa visual de la aplicación (*interfaz de usuario*) con la que interactúa directamente el usuario.

Hash: Código o huella digital única generada mediante algoritmos criptográficos para verificar la autenticidad e integridad de un archivo o imagen del Acta PREP.

IEPC GRO: Instituto Electoral y de Participación Ciudadana del Estado de Guerrero.

INE: Instituto Nacional Electoral.

OPLE: Organismos Públicos Locales de las entidades federativas.

PEL 2026-2027: Proceso Electoral Ordinario de Gubernatura del Estado, Diputaciones Locales y Ayuntamientos 2026-2027.

PREP: Programa de Resultados Electorales Preliminares.

PTO: Proceso Técnico Operativo.

QR: Código de barras bidimensional cuadrado que almacena datos codificados legibles al instante mediante la cámara de un dispositivo móvil.

RE: Reglamento de Elecciones.

SIE: Sistema Informático Electoral.

Sistema informático: Conjunto de elementos tecnológicos (software, bases de datos e infraestructura) y procedimientos que interactúan para procesar datos y generar resultados.

Testing: Proceso de ejecución de pruebas (manuales o automatizadas) para evaluar el funcionamiento del software, detectar errores y garantizar su calidad.

1. Descripción general

1.1 Fundamento normativo

Que de conformidad con lo dispuesto en los artículos 41 Base V; 116 párrafo segundo, fracción IV, inciso c), de la Constitución Política Federal; 98 y 99 de la Ley General de Instituciones y Procedimientos Electorales, artículos 124 y 125 de la Constitución Política del Estado Libre y Soberano de Guerrero; 173 y 175 de la Ley número 483 de Instituciones y Procedimientos Electorales del Estado de Guerrero; el Instituto Electoral y de Participación Ciudadana del Estado de Guerrero, es un organismo público autónomo, de carácter permanente, independiente en sus decisiones y funcionamiento, con personalidad jurídica y patrimonio propio, garante de otorgar el derecho a votar y ser votado en las elecciones y demás instrumentos de participación ciudadana , así como de promover la participación política de los ciudadanos a través del sufragio universal, libre, secreto y directo; con patrimonio destinado al cumplimiento de su objeto y las partidas que anualmente se le señalen en el presupuesto de egresos del Estado; cumpliendo con sus actividades bajo los principios de certeza, imparcialidad, independencia, legalidad, máxima publicidad y objetividad.

Que, bajo esta misma tesitura, el artículo 352 de la Ley número 483 de Instituciones y Procedimientos Electorales del Estado de Guerrero, establece que el PREP, es el mecanismo de información electoral encargado de proveer los resultados preliminares y no definitivos, de carácter estrictamente informativo a través del acopio, captura, digitalización y publicación de los datos plasmados en las AEC de las casillas que se reciben en los CATD, autorizados por el Instituto. Su objetivo será el de informar oportunamente garantizando la seguridad, transparencia, confiabilidad, credibilidad e integridad de los resultados y la información en todas sus fases.

El artículo 338, numerales 5, 6 y 7 del Reglamento de Elecciones, establece la posibilidad de que los Organismos Públicos Locales (OPL) puedan auxiliarse de terceros para el diseño, implementación y operación del Programa de Resultados Electorales Preliminares (PREP), de acuerdo con su capacidad técnica y financiera, debiendo dar cumplimiento a las disposiciones establecidas en la normatividad aplicable. **EL OPL**, a través de la instancia interna responsable de coordinar el desarrollo de las actividades del PREP, será el responsable de la vigilancia del cumplimiento de las disposiciones que rigen el PREP tratándose de elecciones locales, además de la elaboración de documentos que permitan proporcionar consideraciones mínimas con las que debe cumplir, en su caso, **EL TERCERO**.

En este sentido, el presente documento tiene por objeto estipular los requisitos mínimos que deben tomarse en consideración para la contratación del **TERCERO**.

1.2 Requerimiento general de los servicios

EL OPL de **GUERRERO** (en lo sucesivo IEPC GRO), debe contar con los servicios que se describen en el presente documento, a través de un **TERCERO** que lo auxilie en el diseño, la actualización, implementación, operación, acompañamiento y soporte del PREP, (en lo sucesivo, **EL PROVEEDOR**), ya que para el Proceso Electoral 2026-2027, se considera conveniente contar con el apoyo de un **tercero especializado para la actualización del sistema informático del PREP**, aprovechando la experiencia operativa adquirida por el Instituto en el proceso 2023-2024 y garantizando que las adecuaciones tecnológicas se realicen con el nivel de especialización requerido, conforme a la normativa del INE y bajo criterios de seguridad, estabilidad y continuidad operativa.

para lo cual debe llevarse a cabo lo siguiente:

1. Levantamiento de requerimientos, análisis, diseño, actualización de software para la implementación y operación del sistema informático que permita llevar a cabo las actividades descritas en el Proceso Técnico Operativo del PREP aprobado por el Órgano Superior de Dirección del **IEPC GRO**, así como las condiciones establecidas en el Reglamento de Elecciones, su Anexo 13 relativo a los Lineamientos del PREP, su Formato 18.5 correspondiente a la Estructura de los archivos CSV para el tratamiento de la base de datos del PREP, su Formato 18.10 correspondiente al Catálogo de abreviaturas de las entidades federativas, el Anexo Único del presente documento y la demás normatividad aplicable.

1.1 Actualización de los sistemas PREP que actualmente posee **EL IEPC GRO**, asegurando que la propiedad de estos, al finalizar el PREP, continúe siendo de este OPLE. A continuación, se enlistan la cantidad de aplicaciones web y/o móviles propiedad del **IEPC GRO** que deberán actualizarse por **EL PROVEEDOR.**

1. **Módulo de administración y configuración del Sistema PREP.**
2. **Módulo de Identificación/Foliación.**
3. **Módulo de Captura/Verificación.**
4. **Módulo de Resolución de Incidencias.**
5. **Sitio de publicación.**
6. **Módulo para Cotejo PREP.**
7. **Módulo de Reportes para PRENSA.**
8. **Monitor PREP.**
9. **Reportes COORD.**
10. **Aplicativo ASPREP.**
11. **Aplicación para celular PREP Casilla.**
12. **Aplicación CATD Celular.**

13. Aplicación para Celular para Supervisar al personal técnico de campo.
14. Aplicación para Celular para el Coordinador de los CATD

1.2 Contar con toda la documentación referente a los sistemas, tanto de su composición como manuales de usabilidad.

1.3 Que el personal del **IEPC GRO** que coordinará la implementación del sistema PREP, así como al personal que el **IEPC GRO** designe y contrate para su operación posea todo el conocimiento necesario en materia de sistemas para el desarrollo de sus actividades.

2. Asesoría, configuración y blindaje técnico para el funcionamiento de los Centros de Acopio y Transmisión de Datos (CATD) y, en su caso, los Centros de Captura y Verificación (CCV) aprobados mediante acuerdo del Consejo General del **IEPC GRO**. Para tal efecto, EL PROVEEDOR brindará el servicio de consultoría especializada para la configuración de la seguridad perimetral, esquemas de red y equipos de cómputo/digitalización propios de EL **IEPC GRO**. Adicionalmente, EL PROVEEDOR capacitará y transferirá el conocimiento técnico al personal del Instituto que coordinará y operará dichos centros, garantizando su correcta ejecución durante los simulacros y en la Jornada Electoral.

3. Asesoría en la selección, adquisición e implementación de la infraestructura en la nube; monitoreo para mantener los centros de trabajo libres de vulnerabilidades medias y críticas; y soporte técnico para la resolución de observaciones emitidas por el INE, el COTAPREP, el Ente Auditor y el Consejo General del **IEPC GRO**.

1.3 Recomendaciones generales para el instrumento jurídico que sea celebrado con el Tercero especializado.

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

1. Acordar la elaboración de un Plan de trabajo en coordinación con **EL IEPC GRO**, a través de su instancia interna, con la finalidad de definir las actividades, fechas, responsabilidades, así como los recursos necesarios para llevarlas a cabo.
2. Establecer en todo momento que **EL IEPC GRO** será el responsable directo de coordinar el diseño, la actualización, la implementación y operación del PREP.
3. Convenir que la propiedad de la información que se genere con motivo del diseño, actualización, implementación y operación del PREP, corresponde a **EL IEPC GRO,** por ejemplo, gráficos, videos, bases de datos, entre otros.

4. Indicar los recursos que proporcionará **EL PROVEEDOR** para el diseño, actualización, implementación y operación del PREP con el objetivo de establecer con claridad los alcances y las responsabilidades de las partes.
5. Estipular la obligación del tercero de brindar las facilidades para llevar a cabo la auditoría, en concordancia con los alcances que se establezcan con el ente auditor.
6. Estipular la obligación del tercero de coadyuvar con **EL IEPC GRO**, otorgando la información que requiera para la ejecución de sus actividades. En caso de que **EL IEPC GRO** determine llevar a cabo la auditoría al código fuente, dicha previsión debe ser incorporada tanto en el instrumento jurídico firmado con el ente auditor como, en su caso, con el tercero.
7. **El IEPC GRO** 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 un plan de trabajo. En ese sentido, **EL PROVEEDOR** debe entregar dichos productos de trabajo en las oficinas de **EL IEPC GRO,** ubicadas en *Paseo Alejandro Cervantes Delgado S/N, Fracción A, Colonia El Porvenir, Chilpancingo de Los Bravo, Guerrero. C.P.39030* y/o una copia en formato digital en unidades de almacenamiento en la misma dirección o bien, vía correo electrónico a la cuenta *informatica.sistemas@iepcgro.mx,* según le sea indicado.
8. Acordar la obligación del tercero de brindar las facilidades necesarias para el seguimiento y supervisión que realice **EL IEPC GRO**, el COTAPREP y, en su caso, el Instituto.
9. Convenir que en la realización de la o las pruebas y ejecución de los simulacros se haga uso de los formatos de las Actas de Escrutinio y Cómputo aprobadas por EL IEPC GRO, con los partidos políticos, candidaturas independientes, candidaturas comunes (en el supuesto de que la legislación local las contemple) y coaliciones aprobadas por EL IEPC GRO.
10. Convenir el procesamiento de los resultados electorales preliminares emitidos mediante todas las modalidades de votación que se aprueben (por ejemplo, voto de las y los mexicanos residentes en el extranjero, voto anticipado, voto de personas en prisión preventiva, urna electrónica).
11. Convenir reuniones de trabajo conjuntas con **EL IEPC GRO**, el ente auditor, el COTAPREP que haya integrado **EL IEPC GRO** y, en su caso, el Instituto.
12. Coadyuvar con **EL IEPC GRO**, en la elaboración de los planes de seguridad y de continuidad, así como apegarse a los mismos.
13. La participación de **EL PROVEEDOR** no debe implicar un conflicto de interés con las personas involucradas en el diseño, actualización, implementación y operación del PREP, tales como la instancia interna designada por **EL IEPC GRO**, el ente auditor, el COTAPREP, así como con integrantes de algún partido político o candidatura independiente.
14. Establecer la vigencia de dicho instrumento jurídico.

15. 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.
16. Acordar las causales de rescisión del instrumento jurídico, así como las penas convencionales a que las partes se sujetarán.

2. Requerimientos específicos para el diseño, la actualización, acompañamiento y soporte en la implementación y operación del sistema informático

1.4 Diseño, actualización, implementación, acompañamiento y soporte del sistema informático

De conformidad con el Anexo 13 del Reglamento de Elecciones, el Sistema Informático del PREP, en lo sucesivo **EL SISTEMA**, es el conjunto de programas e infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones utilizados para el acopio y digitalización de las Actas PREP −primera copia del Acta de Escrutinio y Cómputo destinada para el PREP, o cualquier copia de ésta−, así como para la captura, verificación y publicación de los datos asentados en las mismas y sus imágenes digitales.
En este sentido, se establece un esquema de operación indicado en el artículo 339, numeral 1, inciso d) del Reglamento de Elecciones el cual señala que el Proceso Técnico Operativo debe contemplar la digitalización de las Actas desde las casillas, el cual permitirá agilizar el procesamiento de éstas, sin necesidad de esperar a que sean trasladadas y acopiadas en los CATD, agilizando de esta forma la publicación de los resultados electorales preliminares.

Por tal motivo, para las próximas elecciones, **EL IEPC GRO** considera la actualización de un mecanismo de digitalización que permita digitalizar las Actas desde las casillas, a través de dispositivos móviles –con o sin asistencia de un Tercero- utilizando como marco de referencia la funcionalidad descrita en el Anexo Único, y considerando los apartados relacionados al desarrollo del sistema del presente documento.

En resumen, **EL PROVEEDOR** debe actualizar las siguientes aplicaciones:

2.1.1 Aplicativo móvil (digitalización desde las casillas)

El numeral 15 del Anexo 13 del Reglamento de Elecciones, establece que los OPL deben contar con mecanismos que permitan la digitalización y, en su caso, la captura de datos, del mayor número de Actas posible desde las casillas. En este sentido, **EL PROVEEDOR** debe actualizar el aplicativo móvil propiedad de **EL IEPC GRO,** para llevar a cabo dicha fase. El aplicativo y su

operación deberán apegarse a las disposiciones y procedimientos que el INE establezca para tal efecto.

2.1.1.1 Actividades por hacer

2.1.1.1.1 De los dispositivos móviles

EL IEPC GRO debe considerar los mecanismos necesarios para llevar a cabo la fase de digitalización de las Actas desde las casillas. En este sentido, de acuerdo con lo establecido en el Convenio General de Coordinación y Colaboración celebrado entre **EL IEPC GRO** y **EL INE**, y sus Anexos Técnico y Financiero, el procedimiento para la digitalización de las Actas desde las casillas será implementado por las y los Capacitadores Asistentes Electorales (CAE) de EL **IEPC GRO** y con los dispositivos móviles con los que **EL IEPC GRO** los aprovisione. La generación de los usuarios y claves de autenticación necesarios para que las y los CAEL tengan acceso al aplicativo, será una actividad conjunta entre **EL IEPC GRO** y EL PROVEEDOR, donde EL PROVEEDOR debe capacitar a quien **EL IEPC GRO** designe para la generación de los usuarios, no obstante, además de capacitar, se debe contribuir con la gestión de los usuarios durante la operación del PREP a modo de soporte técnico, para ello **EL IEPC GRO** proporcionará a EL PROVEEDOR los datos que requiera, observando las disposiciones y procedimientos que EL INE establezca para tal efecto y siempre **BAJO LAS RESERVAS DE LA LEY PARA LA INFORMACIÓN RESERVADA O SUSCEPTIBLE DE SER RESERVADA.**

La entrega de la actualización del aplicativo de PREP Casilla deberá ser agendada en el plan del proyecto, previo al cierre del año 2026, no obstante, es posible que de las pruebas y ejercicios se susciten actualizaciones, nuevos requerimientos y/o observaciones, por lo que, es posible que se genere una nueva versión, EL PROVEEDOR debe garantizar que **EL IEPC GRO** pueda entregar una versión preliminar al menos, 90 días previos a la Jornada Electoral y la versión final debe entregarse, al menos, 50 días previos a la Jornada Electoral, tomando en consideración las disposiciones y procedimientos que **EL IEPC GRO** establezca.

2.1.1.1.2 Transmisión de Actas digitalizadas mediante el aplicativo desde las casillas

Durante los ejercicios y simulacros que lleve a cabo **EL IEPC GRO**, **EL PROVEEDOR** debe proporcionar algún mecanismo para generar un registro, en valores absolutos y relativos, de las Actas transmitidas mediante el aplicativo. Cabe señalar que se deben catalogar de la siguiente forma:

- Transmitidas ilegibles.
- Transmitidas legibles publicadas.
- Transmitidas legibles no publicadas.

EL PROVEEDOR debe entregar el registro en físico en las oficinas de **EL IEPC GRO** de acuerdo con las consideraciones establecidas en el punto 7 del apartado “1.3 Recomendaciones generales para el instrumento jurídico que sea celebrado con el Tercero”, o en su defecto, entregar el mecanismo previo al inicio de ejercicios y simulacros.

2.1.2 Sistema informático PREP

EL PROVEEDOR debe considerar las actividades que se describen, de manera enunciativa y no limitativa, en el siguiente apartado.

2.1.2.1 Actividades por llevar a cabo

2.1.2.1.1 Levantamiento de los requerimientos

EL PROVEEDOR debe identificar las necesidades de **EL IEPC GRO** tomando como base el Reglamento de Elecciones y su Anexo 13 referente a las actividades descritas en el Proceso Técnico Operativo del PREP, su Formato18.5, así como las necesidades de **EL SISTEMA**, además de considerar el Anexo Único del presente documento; con el propósito de llevar a cabo el levantamiento de requerimientos del Sistema en comento, con la estructura mínima indicada en la Ilustración 1.

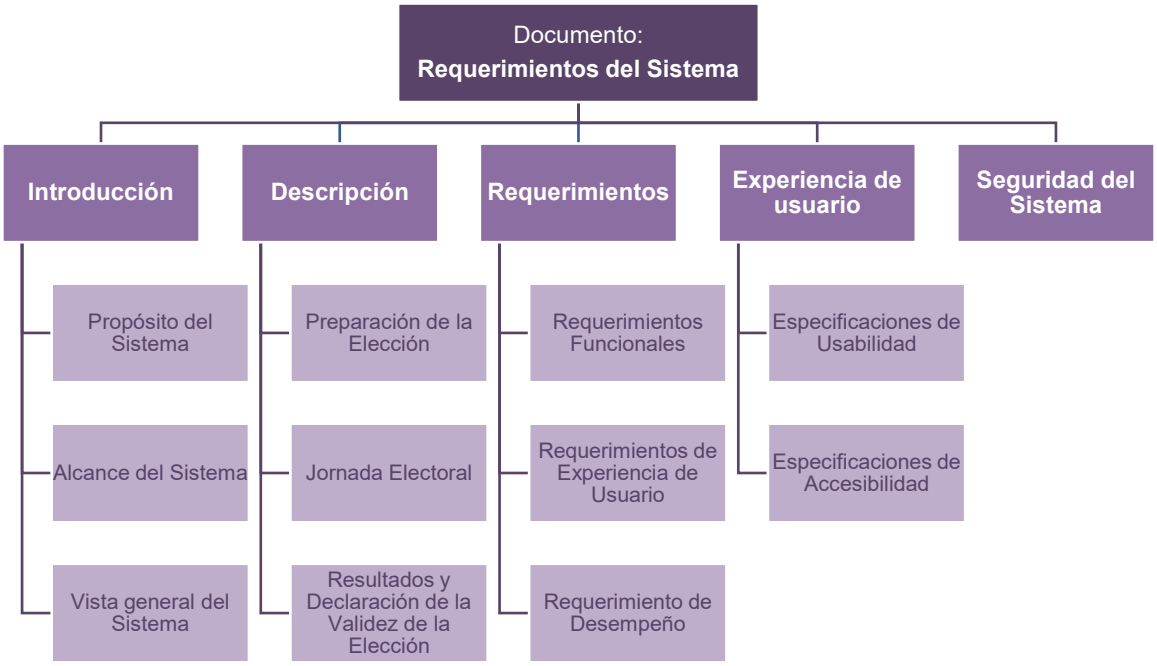
Toda vez que el servicio contempla principalmente la actualización de los sistemas propiedad de **EL IEPC GRO** en esta etapa, el **IEPC GRO** compartirá a **EL PROVEEDOR** el código fuente del sistema actual, además de ejecutar una demostración de cómo funciona el sistema informático, entrega de documentación de cómo se compone el sistema, así como de uso de este, además, en el marco de esta etapa se deberán tener reuniones de análisis donde se notifique a **EL PROVEEDOR** todas las nuevas funcionalidades requeridas y aquellas por actualizar.

Del resultado de este levantamiento, **EL PROVEEDOR** deberá remitir un informe de análisis de necesidades a **EL IEPC GRO**, cuya fecha de entrega deberá ser acordada en el cronograma de trabajo, así mismo, se aclara que este informe puede ser uno solo que incluya los resultados de análisis de necesidades de todo **EL SISTEMA** o, varias entregas de análisis de cada uno de los aplicativos.

La actividad de levantamiento de requerimientos hecha por **EL PROVEEDOR** debe seguir la metodología de actualización que se describe en la sección “Metodología de actualización” del presente documento, misma que debe entregarse por escrito, en físico, en las oficinas de **EL IEPC GRO** ubicadas en *Paseo Alejandro Cervantes Delgado S/N, Fracción A, Colonia El Porvenir, Chilpancingo de Los Bravo, Guerrero. C.P.39030*, 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 IEPC GRO** determine y que queden asentadas en dicho documento.

En su caso, **EL PROVEEDOR** proporcionará todo el licenciamiento que se requiera para el funcionamiento de **EL SISTEMA**, excluyendo el necesario para los diversos ambientes de trabajo, los cuales serán proporcionados por **EL IEPC GRO**.

Ilustración 1. Estructura mínima del documento de requerimientos del Sistema[1]



EL PROVEEDOR debe garantizar que el sistema registre todas las acciones que realicen los usuarios, como altas, bajas y cambios en las bitácoras o historiales de **EL SISTEMA**, para tener la trazabilidad de todas las operaciones.

[1] **Accesibilidad.** Medida en que los productos, sistemas, servicios, entornos o instalaciones pueden ser utilizados por personas de una población con la más amplia gama de características y capacidades para lograr un objetivo específico en un contexto de uso específico.

Experiencia del Usuario. Percepciones y respuestas del usuario que resultan del uso y/o uso anticipado de un sistema, producto o servicio.

Usabilidad. Punto en el que un sistema, producto o servicio puede ser utilizado por determinados usuarios para lograr objetivos específicos con efectividad, eficiencia y satisfacción en un contexto de uso.

EL PROVEEDOR debe capacitar a quien **EL IEPC GRO** *designe* para utilizar la herramienta "Google Analytics" en **EL SISTEMA**.

Finalmente, la fecha de entrega de la documentación será definida en el cronograma de trabajo, el cual, formará parte integral del respectivo Plan de Trabajo.

2.1.2.1.2 Análisis del Sistema

EL PROVEEDOR debe llevar a cabo la actividad de análisis de sistemas de información con el propósito de establecer la definición de la arquitectura de **EL SISTEMA,** el cual podrá ser el mismo que ya se tiene, sufrir modificaciones o ser completamente distinta, bajo la autorización de **EL IEPC GRO**. Durante esta actividad, se deben definir los distintos elementos estructurales que lo conformarán, incluyendo las interfaces de los componentes y su forma de interacción para cumplir con el objetivo del mismo.

EL PROVEEDOR debe remitir un entregable de este análisis el cual será un documento relativo a la arquitectura de **EL SISTEMA**, mismo que debe contener los siguientes apartados:

Tabla 1. Vistas que componen el documento de arquitectura del Sistema

Apartado	Contenido
Vista lógica	Descripción de los distintos módulos que integrarán **EL SISTEMA**, agrupándolos en módulos de capa de datos, lógica de negocio o presentación.
Vista de proceso	Descripción de los aspectos de interacción entre los diversos componentes de **EL SISTEMA**, así como los aspectos de concurrencia y paralelismo asociados.
Vista de desarrollo	Descripción de **EL SISTEMA** desde la perspectiva del programador, enfocada en la administración de los artefactos de software (documentos, diagramas y modelo de procesos).
Vista física	Descripción de los componentes de hardware (servidores, bases de datos, dispositivos de comunicación) de los que **EL SISTEMA** hará uso. Muestra los componentes físicos en los que residen cada uno de los componentes de software de **EL SISTEMA**.
Vista de casos de uso	Descripción de los casos de uso, a través de los cuales se describirá la interacción de los distintos actores con **EL SISTEMA**, y la secuencia de acciones que estos actores llevan a cabo en cada escenario o caso de uso.

EL PROVEEDOR debe entregar la documentación de la arquitectura de **EL SISTEMA**, la cual debe apegarse a la metodología de actualización descrita en la sección "Metodología de actualización" del presente documento.
Finalmente, la fecha de entrega de la documentación será definida en el cronograma de trabajo.

2.1.2.1.3 Diseño del Sistema

Se requiere que **EL PROVEEDOR** lleve a cabo las actividades relativas al diseño de **EL SISTEMA**, mismas que deben llevarse a cabo a través de un conjunto de artefactos (documentos, diagramas y modelo de procesos) que permitan describir el hardware, software, componentes, módulos y datos de **EL SISTEMA**, los cuales satisfagan los requerimientos especificados, se apeguen a la arquitectura de éste, y contengan el detalle suficiente para desarrollar y probar **EL SISTEMA**.

Para la elaboración de los artefactos de diseño de **EL SISTEMA**, **EL PROVEEDOR** debe llevar a cabo, al menos, las siguientes actividades:

1. **Diseño de lógica de negocio**. Se identificarán, diseñarán y documentarán los componentes lógicos de **EL SISTEMA** a través de diagramas, esquemas, textos u otro medio. Lo anterior, se debe hacer con un nivel de detalle que permita al equipo de desarrollo, construir **EL SISTEMA** a partir de dicho diseño.
2. **Diseño de interfaces.** Se diseñarán y documentarán las interfaces de cada uno de los componentes que requieran mostrar información a sus usuarios. Lo anterior, se debe hacer con el nivel de detalle que permita al equipo de desarrollo, actualizar **EL SISTEMA** a partir del diseño propuesto. Para las interfaces de publicación se tendrá que revisar lo establecido en el artículo 353, numeral 3 del Reglamento de Elecciones, particularmente en lo que refiere al prototipo navegable y las plantillas base de la interfaz, para la elección de que se trate, proporcionadas por el Instituto a los OPL. Lo anterior, se debe tomar en consideración, observando lo establecido en el Anexo 13 del Reglamento de Elecciones, particularmente, en lo que se refiere a los datos mínimos a publicar.
3. **Diseño de pruebas.** Se identificarán, diseñarán y documentarán los procedimientos de pruebas de cada componente y de **EL SISTEMA** en su totalidad.
4. **Diseño de datos.** Se desarrollará y documentará la estructura de la base de datos de **EL SISTEMA**. Para cumplir con lo anterior, se generarán los diagramas necesarios del modelo de datos.
5. **Evaluación de conformidad con requerimientos y arquitectura**. Se harán las verificaciones necesarias para asegurar que los diseños anteriores cumplen los requerimientos establecidos y se alinean a la arquitectura definida previamente.

La documentación relativa al diseño de **EL SISTEMA** debe incluir, como mínimo, los apartados que se mencionan en la siguiente tabla:

Tabla 2. Artefactos de diseño de EL SISTEMA y su contenido mínimo.

Artefacto (Documento)	Contenido
Documento de diseño del Sistema	Este artefacto mencionará y documentará **EL SISTEMA** con base en lo obtenido de las actividades de diseño de lógica de negocio y diseño de interfaces. Este documento incluirá, al menos, las siguientes secciones: 1) Introducción. 2) Identificación y diseño de componentes de **EL SISTEMA** que satisfacen la lógica del negocio. 3) Identificación y diseño de interfaces de los componentes de **EL SISTEMA**. 4) Identificación y diseño de pruebas de cada componente y de **EL SISTEMA** en su totalidad.
Modelo de datos	Este artefacto documentará la estructura de la base de datos de **EL SISTEMA** y debe contener, al menos, lo siguiente: 1) Diagramas de base de datos. 2) Scripts para la generación de la base de datos. 3) Específicamente, se deben tener los scripts de consulta de base de datos que permitan consultar los votos registrados y realizar las sumatorias correspondientes.
Reporte de conformidad con requerimientos y arquitectura	Este artefacto mostrará la evaluación de conformidad con el diseño de los requerimientos y arquitectura de **EL SISTEMA**. Dicho reporte debe contener, al menos, los siguientes apartados: 1) Introducción. 2) Evaluación de conformidad de componentes e interfaces con: a) Requerimientos, y b) Arquitectura. 3) Evaluación de conformidad de modelo de datos con: a) Requerimientos, y b) Arquitectura.

La documentación de diseño de **EL SISTEMA** que genere **EL PROVEEDOR** debe elaborarse siguiendo la metodología de actualización, descrita en el presente documento.

La fecha de entrega de la documentación será definida en el cronograma de trabajo.

2.1.2.1.4 Actualización de código del Sistema

Se requiere que **EL PROVEEDOR** lleve a cabo las actividades relativas a la actualización de **EL SISTEMA** para generar el código fuente, la documentación del código fuente, las interfaces gráficas funcionales y la ejecución de pruebas unitarias. En el desarrollo y/o actualización se debe

implementar lo especificado en el diseño, siempre asegurando la conformidad con los requerimientos y arquitectura.

Para llevar a cabo el desarrollo de **EL SISTEMA**, **EL PROVEEDOR** debe desarrollar, al menos, las siguientes actividades:

- Pruebas a los distintos componentes de **EL SISTEMA**.
- Pruebas a **EL SISTEMA** en su totalidad.

El contenido de las versiones finales de los entregables relativos a la construcción del Sistema se menciona en la siguiente tabla:

Tabla 3. Artefactos de desarrollo del Sistema y su contenido mínimo.

Artefacto (Documento)	Contenido
Reporte de ejecución de pruebas	Este entregable se refiere a un documento que muestre los resultados obtenidos de la ejecución de los procedimientos de pruebas de los componentes y de **EL SISTEMA** en su totalidad. Este reporte contendrá, al menos, los siguientes apartados: Introducción. 1. Descripción de las pruebas por componente. 2. Descripción de las pruebas del Sistema en su totalidad. 3. Resultados obtenidos de las pruebas. 4. Evaluación de conformidad de los resultados con los requerimientos asociados a cada componente.
Reporte de conformidad con requerimientos, arquitectura y diseño	Este entregable se refiriere a un documento que muestre la evaluación de conformidad del código fuente con los requerimientos, arquitectura y diseño de **EL SISTEMA**. Este reporte incluirá, al menos, los siguientes apartados: 1. Introducción. 2. Evaluación de conformidad de componentes e interfaces con: ● Requerimientos. ● Arquitectura. ● Diseño.

EL PROVEEDOR debe adicionar a los reportes de pruebas, los resultados obtenidos en las pruebas de volumetría y de estrés efectuadas por **EL IEPC GRO** que garanticen el funcionamiento eficiente el día de la operación del PREP. **EL PROVEEDOR** hará entrega de la documentación generada durante el desarrollo de **EL SISTEMA**, la cual debe apegarse a la metodología de actualización descrita en el presente documento.

EL PROVEEDOR capacitará a quien **EL IEPC GRO** *designe* para habilitar **EL SISTEMA** en las fechas establecidas en el cronograma de trabajo para la adecuada ejecución de ejercicios, pruebas, simulacros y la operación de **EL SISTEMA**. Asimismo, **EL PROVEEDOR** se compromete asesorar a **EL IEPC GRO** y a las y los funcionarios designados por éste, para la revisión en materia de seguridad informática, de funcionalidad, así como para recibir las posibles propuestas de mejora que se soliciten en el marco de las sesiones del COTAPREP que instalará **EL IEPC GRO,** con fundamento en el Reglamento de Elecciones, su Anexo 13 y Formato 18.5, y demás normatividad aplicable.

Derivado de las mejoras o hallazgos que se identifiquen por parte del ente auditor designado por **EL IEPC GRO**, las y los integrantes del COTAPREP, **EL IEPC GRO** o el Instituto Nacional Electoral, **EL PROVEEDOR** en conjunto con **EL IEPC GRO** definirá los cambios aplicables, mismos que deben llevarse a cabo en conjunto entre **EL PROVEEDOR** y **EL IEPC GRO** estableciendo las responsabilidades y fechas para su entrega y liberación.

2.1.2.1.5 Metodología de actualización

Para la actualización de los sistemas PREP con los que cuenta el **IEPC GRO**, éste hará entrega del código fuente actual de estos, así como una transferencia de conocimiento sobre su funcionamiento, además, en esta etapa, el **IEPC GRO** expresará requerimientos específicos sobre nuevas funcionalidades deseadas para los sistemas, de forma que, de acuerdo con la viabilidad de estos nuevos requerimientos sean o no agregados en los planes de trabajo.

Tanto para la actualización de los sistemas PREP, como para el desarrollo de nuevas funcionalidades o incluso nuevos módulos o sistemas, deberá utilizarse alguna metodología ágil de desarrollo de sistemas informáticos por parte del **EL PROVEEDOR** para el desarrollo de las actividades.

Se entenderá por metodología ágil de trabajo, al marco de desarrollo que se caracteriza por el uso de una estrategia de desarrollo incremental, en contraste con un esquema en el que se hace la planificación y ejecución completa de las actividades.

Derivado de lo anterior, **EL PROVEEDOR** se debe apegar a dicho esquema de trabajo, además debe programar y llevar a cabo entregas parciales. El desarrollo incremental estará conformado por entregas parciales (iteraciones) y una entrega consolidada. Cada iteración debe tener una duración de 10 o 20 días naturales, mientras que las fechas de inicio y término de cada iteración, será definida en el cronograma de trabajo correspondiente. Tanto las entregas parciales como la entrega consolidada deben ser revisadas y validadas por **EL IEPC GRO.**

Para efecto de la revisión por parte de **EL IEPC GRO, EL PROVEEDOR** debe organizar sesiones donde se muestre el funcionamiento de la parcialidad entregada, **EL IEPC GRO** contará con 10

días naturales para entregar observaciones correspondientes, entendiendo que no se entregará el código fuente hasta la entrega consolidada una vez finalizados todos los trabajos de actualización y desarrollo.

2.1.2.1.6 Pruebas del Sistema

EL PROVEEDOR debe llevar a cabo pruebas a **EL SISTEMA** para garantizar su adecuado funcionamiento, y verificar que se cuente con un nivel de seguridad adecuado de la información de **EL SISTEMA**. De conformidad con lo anterior, **EL PROVEEDOR** debe hacer las pruebas definidas durante las etapas anteriormente descritas y, adicionalmente, debe llevar a cabo, al menos, las siguientes actividades:

2.1.2.1.6.1 Pruebas de aseguramiento de calidad

1. Pruebas de funcionalidad, para verificar que **EL SISTEMA** hace exclusivamente lo que debe hacer, conforme a la especificación técnica.
2. Pruebas de desempeño, para evaluar la respuesta de **EL SISTEMA** bajo condiciones en donde se simule la totalidad de usuarios con un porcentaje de solicitudes simultáneas.

2.1.2.1.6.2 Pruebas de seguridad informática

1. Análisis de vulnerabilidades a **EL SISTEMA** e infraestructura tecnológica, aprovisionada, instalada y configurada por parte de **EL IEPC GRO** con asesoría de **EL PROVEEDOR**, que utilice **EL SISTEMA** de manera central y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP.
2. Pruebas de negación de servicio, que serán realizadas por un ente auditor contratado por **EL IEPC GRO,** posterior a la adquisición y configuración de protección de nube por parte del **EL IEPC GRO**, con asesoría de **EL PROVEEDOR** para verificar la respuesta de **EL SISTEMA** y la infraestructura tecnológica y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP bajo un escenario simulado de ataque informático.
3. Pruebas de penetración, que serán realizadas por un ente auditor contratado por **EL IEPC GRO** posterior a la adquisición y configuración de protección de nube por parte del **EL IEPC GRO**, con asesoría de **EL PROVEEDOR** para verificar la correcta resistencia ante posibles ataques que intenten modificar la funcionalidad de **EL SISTEMA**.

EL PROVEEDOR debe llevar a cabo las pruebas de calidad de EL SISTEMA indicadas con personal especializado en cada uno de los temas descritos con el objeto de que sean lo más realistas y objetivas posibles. Así, se espera que aporten comentarios y observaciones en beneficio del proyecto y para la mejora de **EL SISTEMA**.

La documentación relativa a la ejecución de pruebas de **EL SISTEMA** debe incluir como mínimo, los apartados que se mencionan en la siguiente tabla:

Tabla 4. Artefactos de evidencia de pruebas ejecutadas a EL SISTEMA y su contenido mínimo.

Artefacto (Documento)	Contenido
Reporte de ejecución de pruebas	Este entregable consistirá en un documento que muestre los resultados obtenidos a partir de la ejecución de los procedimientos de pruebas de los componentes y de **EL SISTEMA** en su totalidad. Este reporte incluirá, al menos, los siguientes apartados: 1. Introducción. 2. Descripción de las pruebas de **EL SISTEMA** en su totalidad. 3. Resultados obtenidos de las pruebas.

EL PROVEEDOR hará entrega de la documentación generada durante las pruebas a **EL SISTEMA**, apegándose a la metodología de actualización descrita en el presente documento a **EL IEPC GRO.**

La fecha de entrega de la documentación será definida en el cronograma de trabajo.

2.1.2.1.7 Ambiente de desarrollo

EL PROVEEDOR debe establecer y proporcionar el ambiente para desarrollo de **EL SISTEMA**. El usuario principal será **EL PROVEEDOR**, teniendo como alcance contar con su propio ambiente para hacer sus pruebas. Las tecnologías y características específicas de dicho ambiente deben seleccionarse de manera que se dé cumplimiento a los requerimientos del proyecto.

2.1.2.1.8 Ambiente de pruebas

EL PROVEEDOR debe proporcionar y establecer el ambiente de pruebas de **EL SISTEMA**, en donde se llevarán a cabo las revisiones de las funcionalidades que fueron desarrolladas por él y se debe liberar para su evaluación por parte de **EL IEPC GRO.** Las tecnologías y características específicas de dicho ambiente deben seleccionarse de manera que se dé cumplimiento a los requerimientos del proyecto. En su caso, deben ser aprobadas por **EL IEPC GRO**.

2.1.2.1.9 Ambiente de producción

EL PROVEEDOR será el encargado y responsable de asesorar al **IEPC GRO** en la adquisición, instalación y operación del ambiente productivo en el que estará alojado **EL SISTEMA**. Durante

los ejercicios, pruebas, simulacros y la operación del PREP, el ambiente referido debe estar basada en la documentación de arquitectura proporcionada por **EL PROVEEDOR.**

El ambiente productivo que instalará y operará **EL IEPC GRO**, debe cumplir con los siguientes requisitos:

1) Estar compuesto de dos sitios físicamente separados, uno principal o primario y otro secundario o de respaldo, de tal forma que se pueda garantizar la continuidad de la operación ante una contingencia.
   a) En cada sitio se debe tener instalada una infraestructura de hardware similar para soportar las cargas de información y flujos de datos correspondientes.
   b) Cada sitio debe ubicarse de manera que se mantengan condiciones apropiadas de temperatura, humedad, suministro de energía eléctrica y de respaldo para el óptimo desempeño de los equipos de telecomunicaciones y servidores. Además, deben considerar la seguridad física de las instalaciones.

2) Los enlaces de telecomunicaciones proporcionados por **EL IEPC GRO** deben ser redundantes por diversos medios, preferentemente mediante la contratación de proveedores diferentes, con anchos de banda que deben ser calculados para permitir una operación óptima, un intercambio de información ágil y con estándares de seguridad de acuerdo con las mejores prácticas.

2.1.2.1.10 Ambiente de auditoría

Para la revisión de **EL SISTEMA** por parte del ente auditor, **EL IEPC GRO** debe proporcionar el ambiente productivo bajo el asesoramiento de **EL PROVEEDOR**, y si es necesario, un ambiente de auditoría totalmente equipado y con los permisos necesarios para que se realicen todas las pruebas requeridas. Los tiempos deben ser especificados en el cronograma de trabajo.

2.1.2.1.10.1 Auditoría al sistema informático

Como lo establece el Reglamento de Elecciones y su Anexo 13, **EL SISTEMA** que se utilizará para la operación del PREP tendrá que ser auditado. Para ello, **EL IEPC GRO** debe celebrar un instrumento jurídico con un ente auditor con el propósito de desarrollar un proyecto de Auditoría en materia de Tecnologías de Información y Comunicaciones al PREP. En este sentido, **EL IEPC GRO** dará el acceso del personal del ente auditor a las instalaciones para la ejecución de la auditoría y a facilitar la información que le sea requerida por el mismo.

El ente auditor debe entregar a **EL IEPC GRO,** un reporte con las observaciones identificadas, preferentemente mediante alguna herramienta para la gestión de incidencias. El propósito de este reporte será analizar y evaluar la factibilidad de atención a las observaciones que se presenten,

con el fin de determinar las acciones a implementar para el seguimiento. Derivado del reporte de auditoría, **EL PROVEEDOR** debe hacer los ajustes que **EL IEPC GRO** determine procedentes.

Finalmente, el ente auditor debe verificar que dichas observaciones se hayan subsanado.

2.1.2.1.10.2 Seguridad operativa

EL PROVEEDOR debe acompañar en la implementación de las medidas de seguridad necesarias para la protección, procesamiento y publicación de datos, imágenes y bases de datos. Asimismo, **debe colaborar con EL IEPC GRO en la elaboración de los planes de seguridad y continuidad del PREP y ejecutarlos, con base en el desarrollo del análisis de riesgos en materia de seguridad de la información** que permita identificarlos y priorizarlos. También debe implementar los controles de seguridad aplicables en los distintos procedimientos del PREP conforme a las consideraciones mínimas descritas en los numerales 12, 13 y 14 del Anexo 13 del Reglamento de Elecciones.

EL PROVEEDOR debe colaborar en la elaboración y hacer entrega del documento del Plan de Continuidad, mismo que debe ser probado y evaluado en conjunto con **EL IEPC GRO.** Dicho Plan debe incluir a los responsables y los medios de contacto para llevar a cabo la resolución de contingencias, es decir, un esquema de comunicación de contingencias que permita una correcta comunicación para implementar las medidas necesarias a fin de solventarlas.

EL PROVEEDOR debe asesorar al **EL IEPC GRO** para establecer un procedimiento que garantice y deje evidencia de que **EL SISTEMA** auditado es el mismo que será utilizado durante la operación del PREP y se debe considerar que cualquier modificación sobre alguno de los elementos objeto de la auditoría, sea informada al ente auditor. Asimismo, **debe proporcionar herramientas y capacitación para establecer un procedimiento que garantice que el sitio de publicación y las bases de datos no cuenten con información referente a los resultados electorales preliminares antes de su puesta en operación el día de la Jornada Electoral**. Cabe señalar que, los campos de las bases de datos cuyo contenido corresponda a los datos de identificación de las Actas que pertenecen al catálogo de Actas esperadas de las casillas aprobadas, la información relativa a la lista nominal, a representaciones de partidos políticos y candidaturas independientes que se acrediten ante la mesa directiva de casilla, así como los mecanismos de traslado que se utilizarán, podrán contener datos, previo conocimiento al día de la operación del PREP.

EL **IEPC GRO** debe hacer las gestiones necesarias a fin de que dichos procedimientos sean atestiguados y validados por un tercero con fe pública, quien debe dejar constancia de lo anterior.

2.1.2.1.11 Respuesta a incidentes

EL PROVEEDOR debe proporcionar el procedimiento para que, **EL IEPC GRO** pueda reportar los incidentes que se presenten durante las revisiones que realice el ente auditor designado por **EL IEPC GRO.** El procedimiento debe remitirse por correo electrónico, durante los primeros 15 días naturales a partir del fallo de la licitación de **EL PROVEEDOR** o la determinación correspondiente, a la cuenta *informatica.sistemas@iepcgro.mx.* **EL PROVEEDOR** debe incluir en el procedimiento referido, por lo menos, los niveles de servicio, cuentas de correo, números telefónicos locales, nombres de contactos, y procedimientos para distribuir los reportes en cuestión.

Para efecto de la atención de incidentes derivados de las revisiones a **EL SISTEMA**, **EL PROVEEDOR** debe poner a disposición del personal de **EL IEPC GRO** una consola de incidentes, a través de la cual se dará el seguimiento apropiado. La entrega de accesos por parte de **EL PROVEEDOR** a **EL IEPC GRO** debe llevarse a cabo dentro de los <<20 días naturales a partir del fallo de la licitación de **EL PROVEEDOR** o la determinación correspondiente>>, mismos que deben ser enviados por correo electrónico a la cuenta *informatica.sistemas@iepcgro.mx.*

EL PROVEEDOR se debe comprometer por escrito, a cumplir con los niveles de servicio, SLA o Service Level Agreement (Acuerdos de Nivel de Servicio), que sean especificados de manera detallada en su oferta técnica y que incluyan de manera precisa y clara los tiempos máximos de respuesta, conforme a lo siguiente:

1. Tiempos de atención en periodos normales.

Los días y horarios de atención serán de *<<lunes a viernes de 09:00 a 19:00 horas, hora local>>*.

2. Tiempo de atención en periodos críticos.

EL IEPC GRO debe proporcionar –a más tardar en la tercera sesión de trabajo-, un calendario con los periodos críticos de las siguientes actividades:

i) **Ejercicios:** Se ejecutarán previo a cada simulacro y a la jornada electoral, en donde **EL PROVEEDOR** debe cubrir un horario de atención de *<<12 horas>>.*

ii) **Prueba o pruebas de funcionalidad del sistema informático del PREP:** Conforme a lo establecido en el numeral 16 del Anexo 13 del Reglamento de Elecciones, se deberá ejecutar, al menos, una prueba que tendrá como objetivo verificar el correcto funcionamiento del sistema informático del PREP en la que se contemplen, como mínimo, las fases de digitalización, captura, verificación y publicación de los datos asentados en los formatos aprobados del Acta de Escrutinio y Cómputo, durante este periodo **EL PROVEEDOR** debe cubrir un horario de atención de *<<12 horas>>*.

iii) **Simulacros:** Conforme a lo establecido en el artículo 349, numeral 3 del Reglamento de Elecciones, se deben ejecutar como mínimo tres simulacros, los tres domingos previos al día de la jornada electoral, durante este periodo **EL PROVEEDOR** debe cubrir un horario de atención de *<<24 horas>>*.

iv) **Operación del PREP:** Se efectuará al concluir el cierre de casillas instaladas el día de la Jornada Electoral durante un plazo máximo de 24 horas; por lo que, **EL**

PROVEEDOR debe operar de *<<24 a 72 horas>>*, o bien hasta que se dé aviso de su término.

En todos los casos, no se podrá rebasar las 120 horas de operación continua.

1. Descripción de los niveles de servicio atribuibles a errores o fallas de **EL SISTEMA**:
   i) **Nivel Alto:** cuando no se puede operar **EL SISTEMA**.
   ii) **Nivel Medio:** cuando se presente una falla que afecte la funcionalidad de **EL SISTEMA**.
   iii) **Nivel Bajo:** cuando se presente una falla que no impide operar **EL SISTEMA**, pero impide su administración.

Nivel de servicio 1: Soporte técnico

	Del SISTEMA			
	Periodo normal		Periodo crítico	
	Desde la solicitud hasta la generación del reporte (ya sea por Internet, teléfono o correo)	Desde la generación del reporte (ya sea por Internet, teléfono o correo) hasta la resolución de la incidencia	Desde la solicitud hasta la generación del reporte (ya sea por Internet, teléfono o correo)	Desde la generación del reporte (ya sea por Internet, teléfono o correo) hasta la resolución de la incidencia
Nivel alto	15 min.	60 min.	10 min.	30 min.
Nivel medio	15 min.	3 horas.	10 min.	60 min.
Nivel bajo	15 min.	8 horas.	10 min.	90 min.

De la generación y entrega de información. Información relativa a EL SISTEMA o cualquier otra información prevista en el instrumento jurídico.		
Periodo normal	Desde la solicitud hasta la generación del reporte (ya sea que la solicitud se reciba por Internet, teléfono o correo).	Desde la generación del reporte hasta la entrega de la información.
	2 horas	10 días naturales

Soporte de sistemas

Si bien, del levantamiento de requerimientos se obtendrá información sobre las nuevas funcionalidades que se deben incorporar a **EL SISTEMA** por parte de **EL PROVEEDOR**, es probable que a lo largo del Proceso Electoral Ordinario 2026-2027 se detecten áreas de oportunidad u observaciones de instancias competentes, por lo que **EL PROVEEDOR** en conjunto con el **IEPC GRO** determinarán cuáles deben ser atendidas y con qué prioridad para que **EL PROVEEDOR** ejecute esa atención, lo que puede implicar nuevas actualizaciones o incluso nuevos desarrollos. Lo anterior, deberá quedar asentado en el instrumento jurídico que sea celebrado con **EL PROVEEDOR.**

Soporte operativo
A lo largo del proyecto pueden surgir áreas de oportunidad o inconvenientes con la infraestructura, sistemas o personal, por lo que **EL PROVEEDOR** debe brindar apoyo con lo siguiente:

- Atención de solicitudes de soporte técnico a través del personal técnico adscrito a EL **IEPC GRO**.
- Reforzamiento en las capacitaciones de uso de **EL SISTEMA**, de cumplimiento del PTO establecido por EL **IEPC GRO**, uso adecuado de material electoral o cualquier área de oportunidad detectado.
- Apoyo con la administración de sistemas y gestión de usuarios durante los ejercicios, simulacros y la operación del PREP, entiéndase desde capacitación a personal designado para tal efecto por EL **IEPC GRO** o a través de ejecución de actividades por sí mismo, como recuperación de contraseñas, desbloqueo de usuarios, apoyo en la definición de tareas programadas, entre otras.
- Apoyo durante eventos, mediante la preparación del personal, infraestructura y sistemas durante estos, por ejemplo, pruebas de funcionalidad y simulacros.

Al concluir, se deberán informar todas las actividades de soporte ejecutadas a través de la remisión de un reporte, remisión que debe ser registrada en el cronograma del proyecto.

2.1.2.1.12 Criterios de Seguridad del sistema

2.1.2.1.12.1 Integridad de la información

- **Validación de entrada:** Se deberán implementar mecanismos para validar y verificar la entrada de datos en el sistema. Esto implica comprobar la integridad de los datos recibidos y asegurarse de que cumplan con los requisitos establecidos.
- **Control de acceso y permisos:** Se deberán establecer controles de acceso adecuados para garantizar que solo los usuarios autorizados puedan modificar o manipular la

información. Esto puede incluir la implementación de roles y privilegios, así como la autenticación y autorización adecuadas.

- **Protección contra modificaciones no autorizadas:** Se deberán implementar mecanismos de seguridad, como firmas digitales o hashes, para verificar la integridad de los datos y detectar cualquier alteración no autorizada.

2.1.2.1.12.2 Confidencialidad de la información

- **Encriptación:** Los datos confidenciales deben ser encriptados tanto en reposo como en tránsito. Esto asegura que solo las personas autorizadas puedan acceder a la información sensible.
- **Control de acceso basado en roles:** Es necesario establecer políticas y controles de acceso adecuados para proteger la información confidencial. Esto incluye la autenticación de usuarios, la asignación de permisos y la implementación de medidas de seguridad física y lógica para restringir el acceso no autorizado.
- **Auditoría y seguimiento:** Se deberán implementar mecanismos de auditoría que registren y supervisen el acceso a la información confidencial. Esto permite detectar cualquier actividad sospechosa y proporciona un rastro de auditoría para futuras investigaciones.

2.1.2.1.12.3 Disponibilidad de la información

- **Respaldo y recuperación de datos:** Es fundamental realizar copias de seguridad regulares de los datos y establecer procedimientos de recuperación en caso de fallos o desastres. Esto garantiza la disponibilidad continua de la información en caso de interrupciones.
- **Tolerancia a fallos y redundancia:** Se deberán implementar mecanismos de redundancia, como sistemas de clúster o servidores espejo, para asegurar la continuidad del servicio en caso de fallos en los componentes del sistema, estos serán adquiridos por el **IEPC GRO** bajo la asesoría de **EL PROVEEDOR**.
- **Monitoreo y mantenimiento:** Es necesario monitorear constantemente la infraestructura y los componentes del sistema para detectar posibles problemas y tomar medidas preventivas o correctivas. Esto ayuda a garantizar que el sistema esté siempre disponible y funcionando correctamente, por lo tanto, **EL PROVEEDOR** deberá asesorar al **IEPC GRO** a la adquisición, configuración y uso de herramientas de monitoreo.

2.1.2.1.13 Módulos a actualizar

Los sistemas que se deberán actualizar por parte de **EL PROVEEDOR** son los que actualmente posee el **IEPC GRO**, dichos sistemas podrán estar divididos en más o menos sistemas, siempre y cuando posean los módulos que cumplan con las siguientes funcionalidades.

Sistemas divididos por módulos:

2.1.2.1.13.1 Módulos Básicos

- **Módulo de configuración:** Módulo que permite administrar la configuración del sistema, pudiendo variar parámetros, encender y apagar otros módulos, generar reportes y demás funcionalidades que en su momento se determinen.
- **Módulo de usuarios y perfiles:** Módulo que permite crear cuentas para los diferentes usuarios que interactúan con el sistema, así como definir los perfiles y/o roles que cuenten cada uno de ellos. También se encarga de implementar las políticas y controles de seguridad de los usuarios.
- **Módulo de transmisión de datos:** Módulo que permite la transmisión segura de la información bajo protocolos criptográficos y canales seguros de transmisión. Se encarga de establecer los canales internos y externos de comunicación de acuerdo con la funcionalidad de los subsistemas.
- **Módulo de replicación:** Módulo que permite configurar la copia de datos en tiempo real hacia un repositorio secundario, con el objetivo de proteger ante una contingencia en el repositorio primario.

2.1.2.1.13.2 Módulos de operación

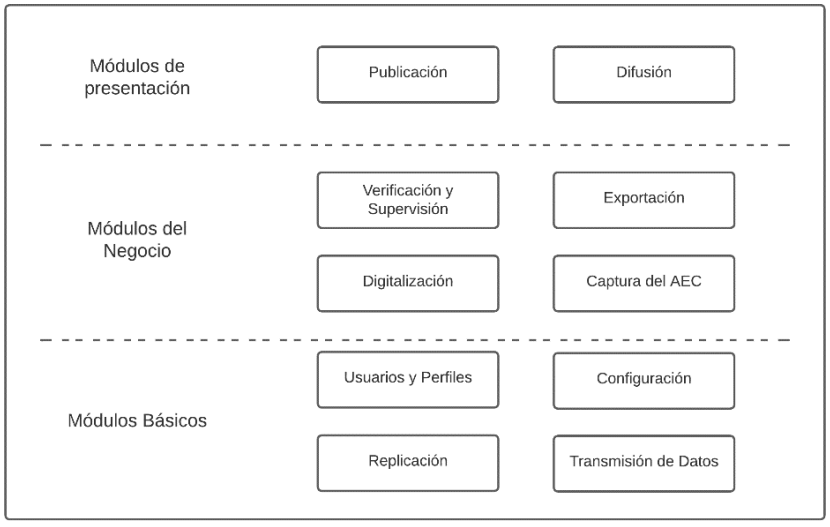
- **Módulo de digitalización:** Este módulo permite la digitalización del AEC de acuerdo con las medidas definidas por la Dirección Ejecutiva de Organización Electoral. Este módulo también permite la lectura de código de barras y/o QR para la identificación de los tipos de elecciones y datos de las casillas.
- **Módulo de captura y verificación del AEC:** En este módulo se realiza la captura del AEC siguiendo las reglas para controlar los posibles errores: dos capturas de la misma acta, comparación automática, trazabilidad de las actividades para poder corregir algún error. Lo anterior requiere de la captura de los datos como son la fecha y la hora correspondiente a la entrega y captura del AEC.
- **Módulo de transmisión de datos:** En este módulo se realiza la verificación de los datos capturados y de la digitalización del AEC mediante dos procesos bien definidos que constan de 6 pasos identificados. Este módulo permite atender los casos que caen fuera del comportamiento regular y que requieran un trato especial y bajo un mecanismo de autorización bien definido, por ejemplo: actas no contabilizadas (SIN ACTA POR PAQUETE NO ENTREGADO, SIN ACTA POR PAQUETE ENTREGADO SIN SOBRE, SIN ACTA POR CASILLA NO INSTALADA) o algún supuesto de inconsistencia de los

datos contenidos en las Actas PREP.

2.1.2.1.13.3 Módulos de presentación

- **Módulo de publicación.** Esté módulo es el encargado de desplegar la información que se encuentra registrada en la base de datos:
    1. Utilizando la plantilla autorizada por parte de INE para administrar varios elementos como son: los resultados electorales preliminares, las secciones y casillas, partidos políticos, coaliciones, candidaturas comunes e independientes, los candidatos registrados.
    2. Publicación se realizará en el lugar donde se desarrolle la sesión del Consejo General y en el portal Web.
    3. Se definirá en la etapa de diseño de **EL SISTEMA** la forma y el lugar en donde se contarán los votos, es decir, donde estará el algoritmo del conteo y su definición. De manera preliminar, se puede decir que el módulo de la publicación lee los resultados de un archivo JSON y genera una página adecuada de resultados.
- **Módulo de difusión.** Este módulo es el encargado de retransmitir los resultados del PREP a otros difusores previamente registrados y autorizados, en caso de existir.

La actualización y desarrollo de los nuevos componentes también deberá estar apegada a los establecidos por el INE para el PEL 2026-2027.



Los módulos por actualizar y/o desarrollar nuevos requerimientos podrán estar contenidos en el mismo número de sistemas o aplicativos, o bien, ser más o menos, dependiendo de la arquitectura que en su momento se defina.

A continuación, se enlistan la cantidad de aplicaciones web y/o móviles propiedad del **IEPC GRO** que deberán actualizarse por **EL PROVEEDOR**.

- **Módulo de administración y configuración del Sistema PREP:** Aplicativo central que permite, entre otras funciones, administrar datos y parámetros del sistema, como lo son (centros de captura y verificación, casillas, partidos, coaliciones y, en su caso, candidaturas independientes, apagar y encender otros aplicativos, configurar logotipos, programar tareas, como los cortes o el encendido de la publicación, así como gestión de usuarios operativos y de PREP Casilla, también la generación de reportes, simulacros y administración de ciertas funciones de la base de datos como acceder a una bitácora y limpiar la base).

- **Módulo de Identificación/Foliación:** Aplicativo web que permite la recepción digital del AEC digitalizada, que permite hacer la identificación automática mediante la lectura de códigos de barra y/o QR así como de forma manual en caso de que estos sean ilegibles por daños, o que, en su defecto, el AEC no los tenga, además, que reconoce cuando las imágenes digitalizadas no sean AEC y permite redirigirlas al aplicativo correspondiente, o en su defecto, rechazarlas.

- **Módulo de Captura/Verificación:** Aplicación web que permite registrar los votos asentados en el AEC, a través de la visualización de los fragmentos correspondientes a cada registro o visualización del AEC completa de acuerdo con la calidad de la imagen, el número de capturas por las que un AEC debe pasar debe ser configurable.

- **Módulo de Resolución de Incidencias:** Módulo que posee funcionalidades tanto de identificación y foliación de AEC, como de su captura y verificación, diseñado para toda vez que las AEC no han coincidió en ninguna de las capturas, que lo que se recibió no sea un AEC, pero si sea un formato de ausencia o bien, que un AEC se haya identificado erróneamente.

- **Sitio de publicación**: Esté módulo es el encargado de desplegar la información que se encuentra registrada en la base de datos apegándose a las plantillas emitidas por el INE.

- **Módulo para Cotejo PREP:** Este se utiliza para el cotejo de la información de todas las actas PREP publicadas. Esta actividad no interfiere con las fases de acopio, digitalización y captura/verificación.

- **Módulo de Reportes para PRENSA:** Este permite visualizar todos los cortes realizados a lo largo de la jornada electoral. Esto nos facilita el acceso a aquellos cortes que se hayan realizado y no descargado en su momento del corte.

- **Monitor PREP:** Este permite supervisar el avance de los centros de captura de información PREP, así como el desempeño de los capturistas.

- **Reportes COORD:** Este se utiliza para el seguimiento al acopio de los paquetes electorales y visualizar en que módulo se encuentra dentro del sistema.

- **Aplicativo ASPREP:** Permite generar, de manera aleatoria y apegado al RE, la información que se usará para el llenado de las AEC PREP durante los simulacros oficiales del PREP.

- **Aplicación para celular PREP Casilla:** Este aplicativo sirve para dispositivos móviles, tipo celular. La función del aplicativo es tomar la imagen de las actas PREP, incluyendo su identificación, desde la casilla.

- **Aplicación CATD Celular:** Esta es una aplicación para dispositivos móviles, tipo celular, y cuya función es principalmente la de un escáner para las Actas PREP. Después de eso, se puede enviar el acta al módulo correspondiente para su revisión.

- **Aplicación para Celular para Supervisar al personal técnico de campo:** Aplicativo que permite al personal técnico registrar los resultados de las inspecciones de los centros de trabajo, así como la habilitación de estos.

- **Aplicación para Celular para el Coordinador de los CATD:** Aplicativo que permite dar de alta las actividades que los Coordinadores de los CATD tienen a su cargo, permitiendo dar seguimiento a su cumplimiento.

Independientemente de si existan o no nuevas funcionalidades solicitadas para los distintos aplicativos, deberán ser actualizados a lenguajes y frameworks con las versiones más recientes y estables y con soporte de los que las constituyen, o bien migrarlos a nuevos que cumplan con los requisitos de calidad y seguridad de estándares mundiales.

Debido a que los aplicativos anteriormente mencionados ya son propiedad del instituto, no se admitirá la sustitución de estos, por lo que, estos deben ser actualizados y la propiedad de estos al finalizar debe ser transferida al **IEPC GRO**, por lo que, los servicios de renta de software o de venta de nuevos sistemas no será admitida.

2.1.2.1.14 Transferencia de conocimiento

Al finalizar con los trabajos de actualización y desarrollo de nuevos componentes, **EL PROVEEDOR** deberá de capacitar al personal adscrito al **IEPC GRO** que éste designe para tal

efecto, esta capacitación deberá incluir de forma enunciativa más no limitativa al menos lo siguiente:

- Guías de uso de cada aplicativo o un manual de uso del sistema completo.
- Sesiones de capacitación.
- Demostración presencial del funcionamiento de todo el sistema.
- Entrega de código fuente de los aplicativos.

La transferencia de conocimiento deberá ser documentada en un informe y remitida al **IEPC GRO**, la fecha de ejecución de estas actividades deberá ser acordada en el cronograma de trabajo.

2.1.2.1.15 Entregables del sistema

Todos los documentos que genere **EL PROVEEDOR** deben hacer uso de los formatos correspondientes que proporcione **EL IEPC GRO** como parte de la conformación del plan de trabajo y deben entregarse en calidad de borrador, en formato digital, vía correo electrónico a la cuenta *informatica.sistemas@iepcgro.mx.*

Posterior a la revisión y aprobación de los documentos por parte de **EL IEPC GRO, EL PROVEEDOR** debe entregar la versión final, en original y por escrito, en las oficinas de **EL IEPC GRO** ubicadas en el domicilio mencionado, junto con una copia en formato digital en unidades de almacenamiento a la misma dirección o bien, vía correo electrónico a la cuenta *informatica.sistemas@iepcgro.mx.*

Las fechas de entrega de los borradores y de las versiones finales serán establecidas en el cronograma de trabajo. Se debe considerar el tiempo necesario entre ambas entregas, de manera que **EL PROVEEDOR** pueda hacer los ajustes correspondientes para los casos en los que **EL IEPC GRO** presente observaciones.

Los entregables mínimos del desarrollo del Sistema Informático son:

Tabla 5. Entregables del desarrollo del Sistema.

Nombre del documento	Contenido mínimo del documento	Fecha límite de entrega	Responsable de la entrega	Forma de entrega
Documentos de Requerimientos	El propósito de **EL SISTEMA**, su alcance, la vista general, los requerimientos funcionales y no funcionales, los requerimientos de experiencia de usuario, el desempeño, la seguridad e interfaces del mismo.	2 días naturales posteriores a la aprobación del documento por parte del EL IEPC GRO.	**EL PROVEEDOR**	Debe entregarse por escrito, en físico, en las oficinas de **EL IEPC GRO** ubicadas en *Paseo Alejandro Cervantes Delgado S/N, Fracción A, Colonia El Porvenir, Chilpancingo de Los Bravo, Guerrero. C.P.39030 ,* 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 IEPC GRO** determine y que queden asentadas en dicho documento.
Documentos de la arquitectura	La vista lógica, la vista de procesos, la vista de desarrollo, la vista física y la vista de casos de uso.	2 días naturales posteriores a la aprobación del documento por parte de EL IEPC GRO	**EL PROVEEDOR**	Debe entregarse por escrito, en físico, en las oficinas de **EL IEPC GRO** ubicadas en *Paseo Alejandro Cervantes Delgado S/N, Fracción A, Colonia El Porvenir, Chilpancingo de Los Bravo, Guerrero. C.P.39030 ,* 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 IEPC GRO** determine y que queden asentadas en dicho documento.
Documento de Diseño	El diseño de lógica de negocio, el diseño de las interfaces, el	2 días naturales posteriores a la aprobación del	**EL PROVEEDOR**	Debe entregarse por escrito, en físico, en las oficinas de **EL IEPC GRO** ubicadas en *Paseo*

Nombre del documento	Contenido mínimo del documento	Fecha límite de entrega	Responsable de la entrega	Forma de entrega
	diseño de pruebas, el diseño de datos, y la evaluación de conformidad con los requerimientos y la arquitectura aprobados.	documento por parte de EL IEPC GRO.		*Alejandro Cervantes Delgado S/N, Fracción A, Colonia El Porvenir, Chilpancingo de Los Bravo, Guerrero. C.P.39030 ,* 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 IEPC GRO** determine y que queden asentadas en dicho documento.
Modelo de datos	Diagramas de base de datos, scripts de generación de la base de datos, diccionario de datos.	2 días naturales posteriores a la aprobación del documento por parte de EL IEPC GRO.	**EL PROVEEDOR**	Debe entregarse por escrito, en físico, en las oficinas de **EL IEPC GRO** ubicadas en *Paseo Alejandro Cervantes Delgado S/N, Fracción A, Colonia El Porvenir, Chilpancingo de Los Bravo, Guerrero. C.P.39030 ,* 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 IEPC GRO** determine y que queden asentadas en dicho documento.
Documento de reporte de ejecución de Pruebas	Resultados obtenidos de la ejecución de los procedimientos de pruebas de los componentes y del Sistema en su totalidad.	2 días naturales posteriores a la aprobación del documento por parte de EL IEPC GRO.	**EL PROVEEDOR**	Debe entregarse por escrito, en físico, en las oficinas de **EL IEPC GRO** ubicadas en *Paseo Alejandro Cervantes Delgado S/N, Fracción A, Colonia El Porvenir, Chilpancingo de Los Bravo,*

Nombre del documento	Contenido mínimo del documento	Fecha límite de entrega	Responsable de la entrega	Forma de entrega
				Guerrero. C.P.39030 , 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 IEPC GRO** determine y que queden asentadas en dicho documento.
Documento de conformidad con requerimientos, arquitectura y diseño	Evaluación de conformidad del código fuente, con los requerimientos, arquitectura y diseño del Sistema.	2 días naturales posteriores a la aprobación del documento por parte de EL OPL.	**EL PROVEEDOR**	Debe entregarse por escrito, en físico, en las oficinas de **EL IEPC GRO** ubicadas en *Paseo Alejandro Cervantes Delgado S/N, Fracción A, Colonia El Porvenir, Chilpancingo de Los Bravo, Guerrero. C.P.39030 ,* 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 IEPC GRO** determine y que queden asentadas en dicho documento.

3. Aprovisionamiento y habilitación de CATD y, en su caso, CCV

De conformidad con la normatividad aplicable, el Órgano Superior de Dirección de **EL IEPC GRO** determinará la cantidad y ubicación de Centros de Acopio y Transmisión de Datos (CATD) y, en su caso, Centros de Captura y Verificación (CCV) que se instalarán para llevar a cabo las actividades establecidas en el Proceso Técnico Operativo del PREP, sin embargo, se recomienda que todas las sedes para la ubicación de CCV sean dentro del territorio de la entidad en la que

se llevará a cabo la elección. **EL IEPC GRO** debe entregar a **EL PROVEEDOR** el listado de los lugares aprobados, incluyendo las dimensiones físicas de los espacios designados.

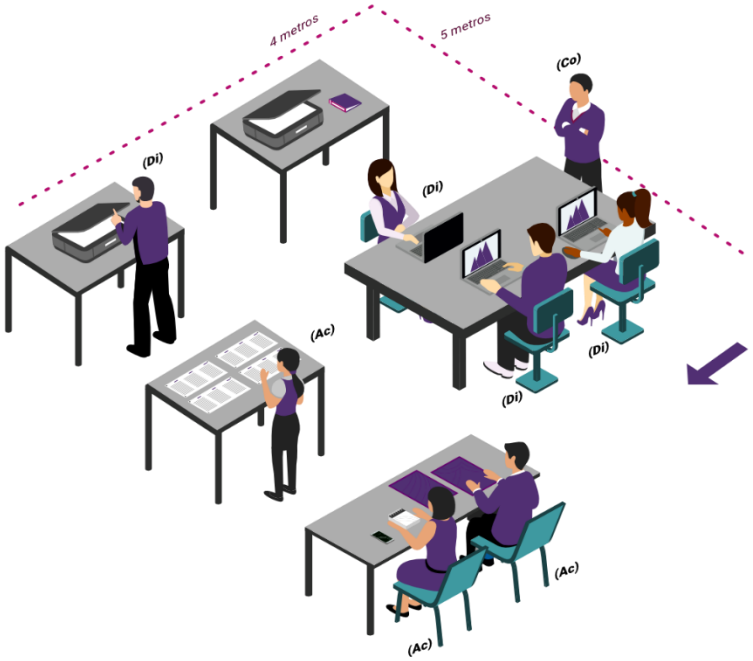
3.1 Actividades por hacer

3.1.1 Identificación de adecuaciones en CATD y CCV

EL PROVEEDOR debe capacitar al personal que **EL IEPC GRO designe** para ejecutar tareas de inspección en los inmuebles en los que se instalarán los CATD, y en su caso los CCV aprobados, de tal forma que se identifiquen los espacios y condiciones en las que se encuentran.

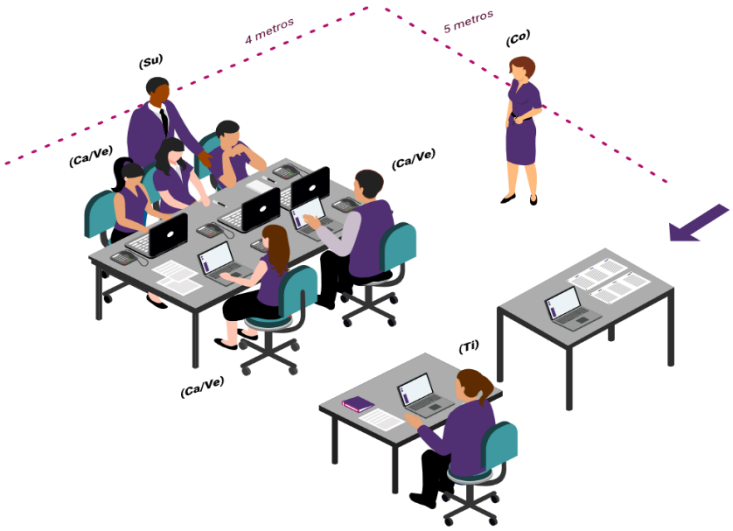
EL IEPC GRO debe considerar, a manera de ejemplo, las ilustraciones que se muestran a continuación en las que se describe la distribución de lugares, equipo de cómputo, mobiliario, entre otros, para diseñar los planos que mostrarán la distribución de los CATD y, en su caso, los CCV a instalar.

Ilustración 2. Ejemplo de distribución en el CATD



Leyenda:

Ac = Persona Acopiadora
Di = Persona Digitalizadora
Co = Persona Coordinadora

	**Leyenda:** Ca/Ve = Persona Capturista/Verificadora Su=Persona Supervisora Co=Persona Coordinadora TI=Personal Técnico Informático (opcional)

De manera conjunta, **EL PROVEEDOR** y **EL IEPC GRO deben** definir la cantidad de personas, que cubrirán los roles establecidos en el numeral 21 del Anexo 13 del Reglamento de Elecciones. **EL IEPC GRO** debe aprovisionar y habilitar los CATD y, en su caso los CCV, de manera que se generen las condiciones necesarias para la ejecución de las actividades descritas en el Proceso Técnico Operativo aprobado por el Órgano Superior de Dirección de **EL IEPC GRO,** bajo la asesoría de **EL PROVEEDOR** La contratación de este personal debe apegarse a los perfiles de puesto autorizados previamente por la autoridad administrativa correspondiente.

EL PROVEEDOR deberá apoyar en la generación de planos de instalación de los CATD y, en su caso, CCV que designe **EL IEPC GRO** siempre y cuando el personal adscrito a **EL IEPC GRO** haya utilizado el aplicativo correspondiente para el registro de información de la inspección

3.1.2 Adecuaciones de infraestructura en CATD y CCV

EL PROVEEDOR debe capacitar y asesorar al personal designado por **EL IEPC GRO** para acondicionar los espacios establecidos de acuerdo con los planos previamente autorizados por **EL IEPC GRO**.

EL IEPC GRO debe suministrar y habilitar el mobiliario para el personal de los CATD, y en su caso de los CCV, así como los equipos de cómputo, equipo multifuncional o escáner, y demás componentes que permitan la adecuada digitalización y captura de las Actas de Escrutinio y

Cómputo y su inclusión en el flujo del Sistema para su procesamiento, de conformidad con el Proceso Técnico Operativo que defina **EL IEPC GRO**.

Todos los equipos de cómputo y de comunicaciones que instale **EL IEPC GRO** deben tener respaldo eléctrico mediante No-break (UPS) o baterías en caso de utilizar equipos portátiles para soportar las posibles variaciones eléctricas y seguir operando de forma ininterrumpida, en tanto la planta de emergencia entra en funcionamiento. Esta última también debe ser suministrada por **EL IEPC GRO**.

Con relación a lo anterior, **EL IEPC GRO** debe revisar, suministrar e instalar la red de computadoras (LAN, wifi) en cada sitio para contar con la infraestructura de telecomunicaciones necesaria, tomando en consideración equipos de red, tales como routers, switches y cableado para interconectar los equipos de cómputo y de digitalización de manera local, además de los equipos necesarios para la interconexión con el o los sitios centrales.

EL PROVEEDOR debe considerar dentro de asesoría la configuración de los enlaces de Internet o de MPLS, o los que **EL IEPC GRO** determine de acuerdo con la conceptualización de su arquitectura tecnológica, que permitirá interconectar a los diferentes CATD y, en su caso los CCV, con el o los centros de datos. Los enlaces que habilite **EL IEPC GRO** deben operar de manera redundante y, preferentemente harán uso de diferentes proveedores, de forma que, en caso de presentarse algún problema con uno de los enlaces, de forma automática se realice el cambio hacia otro servicio y se mantenga la continuidad en la comunicación.

Toda la configuración realizada por **EL IEPC GRO** será probada por **EL PROVEEDOR** con el objetivo de realizar análisis de vulnerabilidades, mismos que serán externados a **EL IEPC GRO** para en conjunto, determinar su atención.

3.1.3 Recursos humanos

EL IEPC GRO debe llevar a cabo el reclutamiento, selección, contratación y pago de los recursos humanos necesarios que operarán en los CATD y, en su caso, CCV para la ejecución de las actividades descritas en el presente documento.

Para efectos de los requisitos que **EL IEPC GRO** solicitará a las y los candidatos, se debe apegar a lo estipulado en el artículo 351, numeral 2 del Reglamento de Elecciones. Como mínimo, las y los candidatos deben cumplir con lo siguiente:

1. Tener ciudadanía mexicana y pleno ejercicio de sus derechos civiles y políticos.

2. Estar inscrita o inscrito en el Registro Federal de Electores y contar con credencial para votar vigente.

3. No haber sido registrada como candidata o candidato ni haber desempeñado cargo alguno de elección popular en los cuatro años anteriores a la designación.

4. No ser ni haber sido miembro de dirigencias nacionales, estatales o municipales de partido político alguno en los últimos cuatro años.

5. No ser consejera o consejero ciudadano, propietario o suplente, ante algún Consejo Electoral Local, Distrital, Estatal o Municipal.

De manera conjunta, **EL IEPC GRO** y **EL PROVEEDOR** establecerán los perfiles, cantidad y requisitos mínimos de tal forma que se lleve a cabo la selección y contratación de los siguientes roles, de conformidad con la normatividad en materia del PREP.

Tabla 6. Roles mínimos a considerar en los CATD y CCV

Rol	Actividades mínimas
Acopiador	Recepción del Acta PREP, verificación de los datos de identificación de ésta y registro de la fecha y hora que se recibe en el CATD.
Digitalizador	Digitalización de las Actas PREP acopiadas y revisión de calidad de la imagen digitalizada.
Capturista	Registro de los datos asentados en las Actas PREP o sus imágenes digitalizadas a través del Sistema.
Verificador	Verifica que los datos capturados en **EL SISTEMA** coincidan con los datos asentados en las Actas de Escrutinio y Cómputo acopiadas o sus imágenes digitales
Coordinador	Dar seguimiento a las tareas operativas en el CATD y en su caso CCV, elaborar un informe de avances de la operación.

EL IEPC GRO debe otorgar materiales de identificación a todo el personal, mismo que debe ser exhibido o portado para tener acceso a los CATD y, en su caso, a los CCV.

EL PROVEEDOR debe proporcionar material didáctico y entrenar a quien el **EL IEPC GRO** designe para brindar capacitación al personal operativo en los siguientes temas:

1. Inducción **a EL IEPC GRO**;

2. Tipo de elecciones;

3. PREP;

4. CATD y, en su caso, CCV.

5. Proceso Técnico Operativo.

6. Seguridad de la información y comunicaciones.

7. Manejo del sistema informático.

En caso de ser necesario, **EL PROVEEDOR** deberá apoyar con la capacitación del personal operativo. **EL PROVEEDOR** debe elaborar y entregar un informe a **EL IEPC GRO** respecto a la capacitación llevada a cabo; ésta debe incluir una galería fotográfica, el material utilizado para la capacitación y las listas de asistencia.

4. Prueba o pruebas de funcionalidad

De conformidad con el numeral 16 del anexo 13 del Reglamento de Elecciones, debe ejecutarse, al menos, una prueba que tendrá como objetivo verificar el correcto funcionamiento del sistema informático del PREP en la que se contemplen, como mínimo, las fases de digitalización, captura, verificación y publicación de los datos asentados en los formatos aprobados del Acta de Escrutinio y Cómputo.

Asimismo, el sistema informático que sea sometido a la o las pruebas, deberá integrar todos los componentes que permitan verificar la totalidad de las funcionalidades necesarias para ejecutar íntegramente el Proceso Técnico Operativo aprobado.

La responsabilidad del desarrollo de la o las pruebas de funcionalidad será conjunta entre **EL PROVEEDOR** y **EL IEPC GRO**, por lo que la documentación que debe emitirse antes, durante y posterior deberá elaborarse de manera coordinada por ambas partes y de acuerdo con los criterios mínimos que emita **EL INE**.

El objetivo de la o las pruebas es verificar el correcto funcionamiento del sistema informático del PREP mediante el análisis y seguimiento puntual, uno a uno, de los distintos flujos de procesamiento de la información contenida en las Actas PREP de acuerdo con las fases establecidas en el Proceso Técnico Operativo correspondiente. Por ello, **EL PROVEEDOR** y **EL IEPC GRO** deberán considerar, por lo menos, los siguientes aspectos:

1. Deberá ejecutarse, a más tardar, mes y medio antes del día de la jornada electoral, en el día establecido por cada OPL.
2. Deberá contar con la participación presencial de las y los integrantes de la Comisión que dé seguimiento a la implementación y operación del PREP, del COTAPREP y del ente auditor, de acuerdo con sus atribuciones y funciones.
3. Se procesará la cantidad de Actas que permita verificar los distintos flujos del funcionamiento integral del sistema informático del PREP, considerando para ello los criterios mínimos que establezca **EL INE**.

Si como resultado de la prueba no ha sido posible verificar el correcto funcionamiento del sistema informático, se deberán ejecutar las pruebas necesarias hasta cumplir con el objetivo de la misma.

EL PROVEEDOR deberá capacitar y asesorar a **EL IEPC GRO** en la preparación y ejecución de la o las pruebas de funcionalidad, ya que será **EL IEPC GRO** quien realice la ejecución.

5. Simulacros

De conformidad con el artículo 349, numeral 3 del Reglamento de Elecciones, deben ejecutarse como mínimo, tres simulacros, mismos que serán ejecutados directamente en los ambientes productivos los tres domingos previos al día de la Jornada Electoral. La responsabilidad de la operación será conjunta entre **EL PROVEEDOR** y **EL IEPC GRO**, por lo que es recomendable que, previamente se elabore un plan para la ejecución de los simulacros. Este plan debe detallar las actividades a ejecutar en cada uno de los simulacros programados y definir claramente quiénes serán las personas responsables de supervisar la ejecución de cada una de éstas. Asimismo, el plan presentado debe especificar los tiempos de ejecución de cada proceso, tomando en consideración la infraestructura tecnológica disponible y los aspectos humanos que intervienen en la ejecución de las actividades. Es importante que **EL IEPC GRO** brinde a las representaciones de los Partidos Políticos y, en su caso, de las Candidaturas Independientes, así como a las y los integrantes del COTAPREP, las facilidades para que asistan y realicen el seguimiento al desarrollo de los simulacros.

El objeto de los simulacros es que **EL IEPC GRO** replique en su totalidad, la operación del PREP, desarrollando cada una de las fases del Proceso Técnico Operativo en el orden establecido. Al ejecutar estos simulacros, **EL IEPC GRO** reproduce experimentalmente el PREP, sujetándolo a diversas manipulaciones con el propósito de analizar su comportamiento, y de este modo poder evaluar diferentes estrategias, incluyendo pruebas de conmutación ante fallas (failover) entre los sitios principal y secundario. Por lo anterior**, EL IEPC GRO** debe aplicar, total o parcialmente, el plan de seguridad y continuidad en el que se prevean mecanismos de respuesta ante posibles contingencias.

Durante los simulacros, **EL IEPC GRO** debe considerar, al menos, los siguientes aspectos:

1. Aplicar los protocolos y medidas de seguridad sanitaria determinados por **EL IEPC GRO** y **EL PROVEEDOR** para proteger la salud de todas las personas que participan en el PREP.

2. **Ejecutar todos los procesos** y procedimientos operativos relacionados con el acopio, digitalización **(incluyendo la digitalización de Actas desde las casillas),** captura de datos, verificación y publicación de las Actas PREP.

3. **Aplicar total o parcialmente los planes de seguridad y continuidad.** Principalmente, se deben considerar aquellos riesgos y escenarios con mayor probabilidad de ocurrencia y mayor impacto para **EL SISTEMA**, así como la activación de los mecanismos para su atención en función a los planes previamente elaborados.

4. **Procesar el total de Actas esperadas para el día de la Jornada Electoral.**

5. **Formato de Acta.**

   a) **Utilizar el formato de Acta aprobado** para cada tipo de elección y con las candidaturas aprobadas de acuerdo con los calendarios oficiales; siempre que éste sea previamente proporcionado por **EL IEPC GRO**. El uso de este formato permite que el personal contratado se familiarice con la distribución de la información dentro de las Actas y conozca la cantidad de datos que deben procesarse. Asimismo, se recomienda que el formato de Acta empleado contenga una marca de agua que indique que se trata de un simulacro.

   b) **Utilizar Actas llenadas a mano**. Se recomienda utilizar Actas llenadas a mano, lo anterior, con el fin de contar con distintas caligrafías para tener un escenario apegado a lo que será la operación del Programa, para lo cual se debe definir si el llenado de las Actas para el simulacro lo hará **EL IEPC GRO**, **EL PROVEEDOR** o en conjunto.

   c) **Incluir Actas con todos los supuestos de inconsistencias,** establecidos en el numeral 31 del Anexo 13 del Reglamento de Elecciones, en todos los ejercicios, pruebas y simulacros que lleve a cabo **EL IEPC GRO** con la finalidad de capacitar y evaluar el desempeño del personal operativo en el tratamiento adecuado de las mismas.

   d) **EL PROVEEDOR debe elaborar y proporcionar a EL IEPC GRO las herramientas y capacitación necesarios** para el desarrollo de los ejercicios y simulacros, por ejemplo, Actas a utilizar para la digitalización desde las casillas, Actas a utilizar en los CATD, manuales de uso de la aplicación para la digitalización desde las casillas, etcétera.

6. **Operación y conexión de todos los CATD y, en su caso, CCV**.

   a) **Recursos humanos.** Para la ejecución de los simulacros es indispensable contar con la totalidad del personal operativo de cada CATD y, en su caso, CCV.

   b) **Recursos materiales**. Deben participar todos los CATD y, en su caso, CCV previstos para operar el día de la Jornada Electoral. Por lo anterior, durante la ejecución de los simulacros éstos deben estar totalmente instalados y habilitados de acuerdo con los requerimientos establecidos en la norma.

7. **Publicación y bases de datos.**

   a) **Sitio de publicación del PREP**. Con la finalidad de facilitar el seguimiento de los simulacros por parte de los distintos actores involucrados, durante los simulacros se debe utilizar una versión terminada del sitio de difusión del PREP, de acuerdo con las plantillas de pantallas definidas por el INE. En este sitio, se deben presentar los datos en los niveles de agregación que estipula el numeral 30 del Anexo 13 del Reglamento de Elecciones y se deben publicar las Actas digitalizadas. Asimismo, se recomienda que dicho sitio de publicación mantenga una marca de agua que indique que se trata de un simulacro.

   b) **Base de Datos.** El formato de base de datos debe apegarse a lo establecido en el Formato 18.5 del Reglamento de Elecciones y las bases de datos deben estar disponibles para su descarga. Asimismo, se debe verificar que los cálculos de las variables resumen de dicha base se realicen conforme la normatividad referida.

      Asimismo, de conformidad con lo establecido en el artículo 349, numeral 4 del Reglamento de Elecciones, para el diseño de las bases de datos que servirán para el llenado de las Actas de Escrutinio y Cómputo que se utilizarán durante la ejecución de los simulacros, se deberá considerar, en la medida que las condiciones lo permitan, que el resultado total de votos que obtenga cada Partido Político en lo individual, así como el resultado total que obtengan todas las Candidaturas Independientes agrupadas como una sola, sea un empate; es decir, la suma de los votos de todas las Candidaturas Independientes deberá ser igual a los votos de cada Partido Político en lo individual.

   c) **Incluir a difusores oficiales**. En caso de que se tenga previsto utilizar a difusores oficiales, éstos deben participar en los simulacros, *<<preferentemente desde el primer simulacro>>*.

   d) **URL de consulta.** Se debe habilitar una liga de consulta, que permita dar seguimiento tanto en las instalaciones del OPL como vía remota.

5.1 Entregables de los simulacros

EL PROVEEDOR debe generar y entregar a **EL IEPC GRO** las herramientas y capacitación para que pueda generar un informe por cada uno de los simulacros efectuados. En el informe se reportarán todas las actividades llevadas a cabo durante el desarrollo de los simulacros, siendo las siguientes:

1. Participantes,

2. Desarrollo, así como horarios, resultados y actividades,

3. Ejecución del Proceso Técnico Operativo en cada una de sus fases,

4. Incidentes con el personal e infraestructura,

5. Los hallazgos y riesgos detectados, incluyendo el detalle de los eventos que hubiesen podido impactar en las fases de acopio, transmisión, captura o verificación de datos,

6. **El registro del número de Actas PREP transmitidas y publicadas a través del mecanismo de digitalización desde casillas**, así como, las razones por la que, en su caso, el número de Actas PREP publicadas y transmitidas no es coincidente. Dicho registro debe generarse en valores absolutos y relativos, de las Actas transmitidas mediante el aplicativo. Cabe señalar que se deben catalogar de la siguiente forma:

   a) Transmitidas ilegibles.

   b) Transmitidas legibles publicadas.

   c) Transmitidas legibles no publicadas.

7. Imprevistos que hayan tenido un impacto en el desarrollo del simulacro, y la forma en que fueron resueltos, y

8. Las posibles mejoras a la operación de **EL SISTEMA** y conclusiones.

Lo anterior, con el objetivo de que sean corregidas de forma inmediata por el personal de **EL PROVEEDOR** y **EL IEPC GRO** según corresponda, de manera que la infraestructura y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP y **EL SISTEMA** se encuentren listos para el siguiente simulacro y la operación del PREP. Cabe señalar que **EL IEPC GRO**, con el apoyo de **EL PROVEEDOR**, debe elaborar un informe general de los tres simulacros, el cual debe apegarse al formato definido por el INE.

Asimismo, de conformidad con el numeral 16, sexto párrafo, fracción III del Anexo 13 del Reglamento de Elecciones, se deben procesar, al menos, la cantidad total estimada de Actas PREP, que se prevé acopiar el día de la Jornada Electoral. Al término de los simulacros, se debe hacer una evaluación, a efecto de tomar las medidas preventivas y correctivas que correspondan. Asimismo, la instancia interna responsable de coordinar el PREP debe elaborar un informe general del desarrollo de los simulacros, mismo que debe hacerse del conocimiento de las y los integrantes del Órgano Superior de Dirección de **EL IEPC GRO**.

EL PROVEEDOR deberá capacitar y asesorar a **EL IEPC GRO** en la preparación y ejecución de los simulacros, ya que será **EL IEPC GRO** quien realice la ejecución.

6. Operación del PREP

EL PROVEEDOR deberá capacitar al personal designado por **EL IEPC GRO** para que esté último pueda verificar lo siguiente previo a la operación del PREP:

a) Aplicar los protocolos y medidas de seguridad sanitaria determinados por **EL IEPC GRO** y **EL PROVEEDOR** para proteger la salud de todas las personas que participan en el PREP.

b) Verificar que las bases de datos cuenten con los elementos, catálogos y cargas de datos necesarios para iniciar la operación del PREP.

c) Verificar el estado operativo de la infraestructura de comunicaciones del ambiente de producción previo al inicio del PREP, y/o servicios relacionados con Tecnologías de la Información y Comunicaciones donde se implemente el PREP.

d) Instalar e iniciar el proceso de extracción y publicación tanto primario como secundario, en caso de que se cuente con secundario.

e) Validar y garantizar que los equipos en los que se ejecutará el aplicativo de digitalización cuenten con los requisitos mínimos de software y comunicaciones para el correcto uso de la aplicación.

f) Verificar que no exista contenido en los sitios de publicación, con el objetivo de asegurar que los datos generados durante pruebas y ejercicios anteriores han sido eliminados.

g) Asegurar la correcta sincronización de los equipos de la sala de monitoreo, así como el correcto funcionamiento de los sistemas de detección de intrusiones.

h) Verificar que las bitácoras se encuentren en blanco y garantizar que la configuración, la conectividad y el espacio disponible de los servidores sean los adecuados para su correcto funcionamiento.

i) Validar el funcionamiento de los servidores en los que se ejecuta el aplicativo, verificando que realice su función de procesamiento, distribución y clasificación de Actas. Además, se debe garantizar que se ejecute la última versión de la aplicación.

j) Validar el correcto funcionamiento de los equipos donde se ejecutará el aplicativo de captura.

k) Ofrecer las facilidades necesarias para que las y los integrantes del COTAPREP puedan verificar, validar o certificar cualquiera de los procesos enlistados para el día de la operación del PREP.

7. Publicación

Para la publicación de los resultados del PREP, **EL PROVEEDOR** debe actualizar el prototipo navegable del sitio de publicación, mismo que debe considerar el apego a las plantillas base de la interfaz definidas por el INE y proporcionadas por **EL IEPC GRO,** observando lo establecido en el Anexo 13 del Reglamento de Elecciones, en lo referente a los datos mínimos a publicar. Dicho prototipo navegable debe ser revisado en el marco de las sesiones del COTAPREP, a más tardar cuatro meses antes del día de la Jornada Electoral. Las observaciones emitidas por las y los integrantes del COTAPREP deben ser discutidas entre **EL PROVEEDOR** y **EL IEPC GRO** para determinar su atención.

En lo que refiere al formato de las bases de datos a publicar, **EL PROVEEDOR** debe cumplir con las especificaciones previstas en el Formato 18.5 del Reglamento de Elecciones.

Aunado a lo anterior, **EL PROVEEDOR** someterá a consideración del COTAPREP y de la instancia interna responsable de coordinar el PREP, el diseño de la página de Internet en la que se publicarán los resultados preliminares.

Los resultados electorales preliminares serán publicados en el portal de **EL IEPC GRO**.
En este sentido, **EL PROVEEDOR** también debe apegarse a lo establecido en el Anexo 13 del Reglamento de Elecciones en lo referente a los datos a publicar. Asimismo, la publicación de los resultados electorales preliminares se hará con base en los datos a capturar y calcular, así como en los niveles de agregación que se detallan de igual forma en los numerales 28, 29 y 30 del Anexo 13 del Reglamento de Elecciones.

EL IEPC GRO determinará por acuerdo, la fecha y hora de inicio de la publicación de los datos, las imágenes y las bases de datos; el número de actualizaciones por hora de los datos y las bases de datos, que deberán actualizarse, como mínimo, tres veces por hora incluso cuando la publicación de datos se realice en tiempo real; así como la fecha y hora de publicación de la última actualización de dicha información.

En caso de que la legislación local en materia electoral lo contemple o se determine implementar el voto de las y los mexicanos residentes en el extranjero o cualquier otra modalidad de votación, y éstas se lleven a cabo en el Proceso Electoral Concurrente en cuestión, **EL PROVEEDOR** debe incluir los resultados de dicha votación en el Prototipo navegable.

8. Confidencialidad y tratamiento de datos personales

EL PROVEEDOR debe declarar que cualquier información de carácter confidencial, reservada y/o susceptible de ser reservada, no podrá ser divulgada y estará sujeta a la normatividad aplicable, tales como: la Ley General de Transparencia y Acceso a la Información Pública, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, *<< Ley Número 466 de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Guerrero>>* y demás disposiciones vigentes. En este sentido, debe incluir como mínimo, la siguiente información:

1. Nombre y domicilio del Área Responsable del Sistema.
2. Fundamento legal.
3. Datos personales que obran en el sistema.
4. Finalidad del tratamiento de los datos.
5. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de datos.
6. Transferencia de datos que, en su caso, se efectúen.
7. Domicilio para ejercer los derechos de acceso, rectificación, cancelación y oposición de datos personales.
8. Vigencia del tratamiento de los datos.
9. El procedimiento y medio por el cual el responsable comunicará a los titulares de los datos las modificaciones al aviso de privacidad.

Por otro lado, con el fin de proteger y conservar la confidencialidad de la información que sea utilizada, El PROVEEDOR y su personal involucrado en el PREP, deben firmar cartas de confidencialidad cuyo texto será validado previamente por EL **IEPC GRO**.

EL IEPC GRO y **EL PROVEEDOR** deben establecer el plan de trabajo del proyecto, durante los primeros 10 días naturales posteriores a la formalización del instrumento jurídico. El plan referido debe contener lo siguiente:

- **Cronograma de trabajo.** En el que se especifique la secuencia de ejecución de actividades, las cuales deben abarcar como mínimo las especificadas en el presente documento (la actualización del sistema, transferencia de conocimiento, capacitación al personal), tiempo de duración de las actividades, así como la especificación de las fechas de los entregables parciales y finales, y responsables de las mismas. Asimismo, se calendarizarán las sesiones que se tendrán para revisar el estado del proyecto.
- **Monitoreo y control del proyecto.** Con el propósito de verificar el cumplimiento de las actividades. **EL PROVEEDOR** debe generar y entregar vía correo electrónico a la cuenta *informatica.sistemas@iepcgro.mx* un informe de avance con una periodicidad semanal,

las fechas de entrega deberán estar estipuladas en el cronograma de trabajo que se defina en conjunto.

Los informes para el seguimiento tienen el objetivo de reportar el avance que se tiene del proyecto hasta el momento de la generación del mismo, la periodicidad se definirá con **EL PROVEEDOR** en la reunión inicial, éstos deben contener por lo menos:

1. Fecha de elaboración del informe.
2. Periodo reportado.
3. Actividades en curso y porcentaje de avance completado, hasta la fecha en que se genere el informe.
4. En caso de existir un retraso en las actividades, se debe dar una justificación del mismo.
5. Riesgos y/o asuntos identificados.
6. Formatos. **EL IEPC GRO** debe entregar a **EL PROVEEDOR**, durante los primeros 5 días naturales posteriores a la formalización del instrumento jurídico, los formatos que éste debe utilizar para la conformación de entregables. Los documentos por su naturaleza podrán tener más o menos secciones, sin embargo, deben apegarse a la siguiente estructura:
   a) Título del documento.
   b) Subtítulo del documento.
   c) Versión.
   d) Fecha de elaboración.
   e) Historial de versiones:
      i) Número de versión.
      ii) Fecha de actualización.
      iii) Responsable de actualización.
   f) Resumen de la actualización Responsables:
      i) De la elaboración:
         (1) Nombre.
         (2) Organización.
         (3) Puesto.
         (4) Firma.
      ii) De la revisión:
         (1) Nombre.
         (2) Organización.
         (3) Puesto.
         (4) Firma.
      iii) De la aprobación:
         (1) Nombre.
         (2) Organización.
         (3) Puesto.
         (4) Firma.

g) Tabla de contenido.
h) Listado de tablas (cuando aplique).
i) Listado de figuras (cuando aplique).
j) Definiciones (cuando aplique).
k) Acrónimos y abreviaciones (cuando aplique).
l) Introducción.
m) Cuerpo del documento.
n) Conclusiones (cuando aplique).
o) Referencias bibliográficas (cuando aplique).

El plan de trabajo que se defina y los posibles cambios que se realicen en la duración del proyecto deben ser validados y aprobados por **EL IEPC GRO.**

EL PROVEEDOR deberá considerar las siguientes fechas clave para la definición del cronograma de trabajo que posteriormente se acordará con **EL IEPC GRO.**

Fase	Descripción	Octubre 2026	Noviembre 2026	Diciembre 2026	Enero 2027
1	Diagnóstico y análisis del SIE				
2	Actualización y desarrollo de nuevos componentes				
4	Pruebas y Laboratorios				
6	Pruebas funcionales PREP				
7	Documentación y transferencia Tecnológica				

Entiéndase que el soporte operativo y servicio de consultoría deberá comprender los meses de febrero a julio del 2027.

9. Consultoría y soporte operativo

9.1 Administración de personal

EL PROVEEDOR deberá asesorar al **IEPC GRO** con la contratación del personal que desempeñará las actividades especificadas en el PTO establecido por el **IEPC GRO**, dicha asesoría debe incluir, pero no limitarse a:

- Actualización y desarrollo de perfiles de puesto.

- Asesoría en la adquisición de herramientas de aplicación de pruebas psicométricas.
- Implementación de herramientas para la gestión de vacantes.
- Asesoría en la definición de personal operativo necesario para la operación de la Jornada Electoral.

La ejecución de estas actividades deberá registrarse en el cronograma de trabajo, así como el debido informe de cumplimiento de estas.

9.2 Administración de infraestructura

EL PROVEEDOR deberá asesorar a el **IEPC GRO** en la adquisición, administración y configuración de la infraestructura necesaria para la operación del PREP, por lo que al menos, deberá realizar lo siguiente:

- Revisión de activos de infraestructura que actualmente posee EL **IEPC GRO**.
- Identificar y acordar con EL **IEPC GRO** la infraestructura que será necesario adquirir para operar el PREP garantizando el cumplimiento de características de calidad y seguridad internacionales.
- Definir la configuración de la infraestructura por utilizar, así como capacitar a quien el **IEPC GRO** designe para efectos de ejecutar la configuración definida.
- Asesoramiento con la adquisición de servicios de nube, incluyendo instancias y la seguridad necesaria para la operación del PREP.
- Asesoramiento y en su caso, capacitación en la configuración de las instancias físicas o en nube necesarias para la implementación de **EL SISTEMA**.
- Asesoramiento y en su caso, capacitación en el despliegue de **EL SISTEMA**,
- Asesoramiento en la adquisición y configuración de herramientas de monitoreo de la infraestructura.
- Ejecución de análisis de vulnerabilidades de la red y la infraestructura implementada y asesoría en la solución de estas.
- Asesoramiento y acompañamiento durante las revisiones ejecutadas por Ente Auditor, integrantes del COTAPREP, del INE y de EL **IEPC GRO** y asesoría en la atención de las observaciones que pudieran existir por parte de estos.
- Entrega de una memoria técnica de adquisición y configuración de la infraestructura.

Todas las actividades deberán ser registradas en el cronograma de trabajo.

9.3 Administración de sistemas

EL PROVEEDOR debe proveer servicios de asesoría y acompañamiento durante las etapas de configuración inicial del sistema, coadyuvando con la configuración de partidos políticos, parámetros, candidatos, entre otros, así como elaborar y participar en los programas de capacitación dirigidos al personal que operara **EL SISTEMA**.

Todas las actividades deben ser acordadas en el cronograma de trabajo.

9.4 Administración de proyecto

EL PROVEEDOR debe proveer servicios de asesoría con la administración de proyecto, los cuales pueden incluir al menos, lo siguiente:

- Definición de planes de trabajo.
- Implementación de herramientas y metodologías de trabajo, que permitan minimizar los riesgos y alinear a todas las personas involucradas.
- Gestionar los entregables que se deban hacer al INE, así como atender los que este emita.

Todas las actividades deben ser acordadas en el cronograma de trabajo.

9.5 Involucrados

EL PROVEEDOR en su central debe designar los siguientes roles para el desarrollo de nuevos componentes y actualización de sistemas.

- Coordinador de Software e Implementación / Coordinador Líder
- Desarrolladores FrontEnd
- Desarrolladores BackEnd
- Desarrolladores Móviles
- Testers

EL PROVEEDOR deberá involucrar un equipo de trabajo para el correcto desempeño de las tareas necesarias para llegar a los objetivos del proyecto, que al menos deberá tener la siguiente estructura:

- Coordinador de Infraestructura y Seguridad.
- Coordinador de Software e Implementación
- Coordinador de Personal y Talento

Mismos que deberán estar instalados en la sede del **IEPC GRO** durante todo el servicio de consultoría y soporte operativo.

9.6 Entrega del sistema y documentación final

9.6.1 Entrega del sistema

Si bien el despliegue de los sistemas debe ejecutarse durante el proyecto en fechas establecidas en el cronograma de trabajo que permitan la ejecución de simulacros y operación del PREP, **EL PROVEEDOR** al finalizar el proyecto debe entregar el código fuente del **EL SISTEMA** asegurando que este sea propiedad del **IEPC GRO** y de libre uso interno, con la consideración que este no será compartido parcial o totalmente con otros OPL o ningún tercero a título gratuito u oneroso.

9.6.2 Documentación final

EL PROVEEDOR deberá entregar una memoria técnica del proyecto que incluya todas las actividades realizadas durante este, su entrega debe definirse en el cronograma de trabajo.

10. Servicio especializado de aseguramiento de ciberseguridad y ciberresiliencia del PREP

El **IEPC GRO** deberá contratar un Servicio Especializado de Aseguramiento de Ciberseguridad y Ciber resiliencia que permita identificar, evaluar, prevenir, detectar y atender riesgos, vulnerabilidades y amenazas que pudieran comprometer la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información procesada por **EL SISTEMA.**

El servicio deberá considerar integralmente la cadena tecnológica del PREP, desde la digitalización y transmisión de las Actas de Escrutinio y Cómputo, hasta su identificación, captura, verificación, cotejo, almacenamiento, procesamiento y publicación.

Las actividades de aseguramiento de ciberseguridad deberán ejecutarse durante las etapas de diseño, desarrollo, pruebas, implementación, simulacros y puesta en operación de **EL SISTEMA**.

El servicio que será contratado por el **IEPC GRO** tendrá por objeto de revisión **EL SISTEMA** actualizado por **EL PROVEEDOR**, por lo que, **El PROVEEDOR** debe comprometerse con la subsanación de observaciones que pudieran surgir como resultado de dichas revisiones.

11.1 Independencia del aseguramiento de ciberseguridad

Con el propósito de garantizar objetividad técnica y evitar que las actividades de aseguramiento dependan exclusivamente de los controles implementados por **EL PROVEEDOR**, el servicio que contrate **EL IEPC GRO** deberá ser independiente del equipo de **EL PROVEEDOR**.

Las pruebas especializadas deberán ejecutarse bajo metodologías documentadas, con personal especializado y generando evidencia técnica reproducible de los hallazgos identificados.

11.2 Evaluación y autorización de proveedores especializados de ciberseguridad

Los proveedores, subcontratistas o terceros especializados que participen en la prestación de servicios, evaluaciones, pruebas, monitoreo, aseguramiento o cualquier otra actividad relacionada con la ciberseguridad y ciberresiliencia de EL SISTEMA deberán ser previamente evaluados y expresamente autorizados por EL INE, a través de la Unidad Técnica de Servicios de Informática (UTSI).

Para dicha evaluación, EL INE, a través de la UTSI, podrá verificar la experiencia, capacidades técnicas, personal especializado, certificaciones, metodologías, herramientas, independencia y demás elementos que considere necesarios para determinar la idoneidad del proveedor.

Ningún proveedor, subcontratista o tercero podrá intervenir, acceder o realizar actividades de ciberseguridad sobre EL SISTEMA, su infraestructura, código fuente, aplicativos, información o componentes tecnológicos sin contar previamente con la autorización correspondiente.

La autorización otorgada no limitará las facultades de supervisión, evaluación o revocación que correspondan a EL INE durante la prestación del servicio.

11.3 Modelo de amenazas PREP

El servicio que contrate el **IEPC GRO** deberá mantener un modelo de amenazas específico para **EL SISTEMA** actualizado por el **PROVEEDOR**.

El análisis deberá considerar, al menos:

- Aplicativo móvil PREP Casilla.
- Dispositivos utilizados para la digitalización.

- Comunicaciones entre dispositivos y servicios centrales.
- APIs y microservicios.
- Sistemas de identificación de actas.
- Módulos de captura y verificación.
- Módulo de Resolución de Incidencias.
- Módulo de Cotejo.
- Bases de datos.
- Consolas administrativas.
- Sistemas de autenticación y autorización.
- Repositorios de código.
- Infraestructura tecnológica.
- Servicios de publicación.
- Sitio público del PREP.
- Dependencias y componentes de terceros.

El modelo deberá identificar activos críticos, actores de amenaza, vectores de ataque, superficies de exposición, escenarios de abuso, controles existentes, riesgos inherentes, controles compensatorios y riesgos residuales.

El PROVEEDOR deberá asesorar a **EL IEPC GRO** en el tratamiento de las amenazas encontradas por este servicio independiente.

11.4 Aseguramiento del desarrollo seguro

Independientemente de que **EL PROVEEDOR** que realice la actualización de EL SISTEMA propiedad del **IEPC GRO** sea seguro (Secure SDLC/DevSecOps), **EL PROVEEDOR** deberá dar apertura a este servicio independiente contratado por el **IEPC GRO** para realizar, al menos, lo siguiente:

a) análisis estático de seguridad del código fuente (SAST);

b) análisis de composición de software y dependencias de terceros (SCA);

c) identificación de vulnerabilidades conocidas en librerías y componentes;

d) detección de secretos, credenciales, certificados, tokens o llaves criptográficas incorporados accidentalmente en código fuente;

e) generación y mantenimiento de Software Bill of Materials (SBOM);

f) revisión de configuraciones de seguridad;

g) análisis dinámico de seguridad (DAST);

h) pruebas especializadas de seguridad de APIs;

i) seguimiento y remediación de vulnerabilidades;

j) validación posterior a la remediación.

Los análisis deberán ejecutarse sobre las versiones relevantes del código previo a su liberación y sobre la versión candidata a producción.

Todas las observaciones pertinentes realizadas por este servicio independiente deberán ser subsanadas por **EL PROVEEDOR.**

11.5 Seguridad del aplicativo PREP Casilla

El Servicio independiente contratado por el **IEPC GRO** deberá realizar pruebas especializadas de seguridad sobre el aplicativo móvil utilizado para la digitalización y transmisión de las Actas.

Las pruebas deberán considerar, cuando resulte aplicable:

- almacenamiento seguro;
- comunicaciones;
- autenticación;
- autorización;
- manejo de sesiones;
- protección de información sensible;
- mecanismos criptográficos;
- protección de llaves;
- manipulación del aplicativo;
- ingeniería inversa;
- modificación o reempaquetado;
- integridad del dispositivo;
- integridad de las imágenes;
- manipulación de metadatos;
- mecanismos offline/online;
- protección de información almacenada temporalmente;
- mecanismos de actualización del aplicativo.

Particularmente deberá verificarse que los mecanismos implementados permitan preservar la integridad y autenticidad de las imágenes y metadatos desde su generación hasta su recepción en los sistemas centrales.

Todas las observaciones pertinentes realizadas por este servicio independiente deberán ser subsanadas por **EL PROVEEDOR.**

11.6 Seguridad criptográfica e integridad de las Actas

El Servicio independiente contratado por el **IEPC GRO** deberá realizar una revisión especializada de los mecanismos criptográficos utilizados por EL SISTEMA.

La revisión deberá considerar:

- algoritmos criptográficos;
- generación de llaves;
- almacenamiento de llaves;
- distribución;
- rotación;
- revocación;
- certificados digitales;
- firmas digitales;
- cifrado de comunicaciones;
- cifrado de información;
- integridad de archivos;
- identificación criptográfica de dispositivos;
- mecanismos de prevención contra alteración y repetición de transmisiones.

Deberá demostrarse técnicamente la trazabilidad e integridad de la información durante las diferentes etapas del procesamiento del PREP.

Todas las observaciones pertinentes realizadas por este servicio independiente deberán ser subsanadas por **EL PROVEEDOR.**

11.7 Pruebas de penetración especializadas

El Servicio independiente contratado por el **IEPC GRO** deberá realizar pruebas de penetración controladas sobre los componentes tecnológicos de EL SISTEMA.

Como mínimo deberán contemplarse:

- aplicativos web;
- APIs;
- microservicios;
- aplicativo móvil;
- infraestructura expuesta;
- mecanismos de autenticación;
- mecanismos de autorización;
- interfaces administrativas;
- servicios de publicación;
- sitio público del PREP.

Las pruebas deberán realizarse antes de la puesta en producción y repetirse sobre aquellos componentes que hayan presentado vulnerabilidades críticas o altas una vez realizada su remediación.

Todas las observaciones pertinentes realizadas por este servicio independiente deberán ser subsanadas por **EL PROVEEDOR.**

11.8 Seguridad de APIs y microservicios

Considerando la arquitectura desacoplada de EL SISTEMA que será actualizado por **EL PROVEEDOR**, el servicio independiente contratado por el **IEPC GRO** deberá implementar pruebas específicas de seguridad sobre APIs y microservicios.

Deberán evaluarse, entre otros:

- autenticación;
- autorización;
- control de acceso;
- exposición indebida de información;
- validación de entradas;
- gestión de tokens;
- abuso de lógica de negocio;
- consumo automatizado;
- limitación de solicitudes;
- comunicación entre servicios;
- registro y trazabilidad de operaciones.

Todas las observaciones pertinentes realizadas por este servicio independiente deberán ser subsanadas por **EL PROVEEDOR.**

11.9 Hardening y configuración segura

EL PROVEEDOR deberá realizar revisiones de configuración segura de los componentes tecnológicos donde opere EL SISTEMA.

Las revisiones deberán generar una línea base de configuración y un reporte de desviaciones que permita identificar configuraciones que incrementen la superficie de ataque.

Las desviaciones identificadas deberán ser corregidas o contar con una aceptación documentada del riesgo.

El servicio independiente contratado por **EL IEPC GRO** podrá hacer revisión de estas configuraciones y realizar observaciones, los resultados y posibles remediaciones deberán ser discutidos con **EL IEPC GRO** y **EL PROVEEDOR.**

11.10 Protección del sitio público del PREP

El sitio público deberá contar con mecanismos que permitan mitigar ataques dirigidos a afectar su disponibilidad o integridad.

Deberán considerarse mecanismos para:

- protección de aplicaciones web;
- mitigación de ataques de denegación de servicio;
- protección contra automatización maliciosa;
- control de solicitudes;
- protección de APIs públicas;
- detección de tráfico anómalo;
- protección contra explotación de vulnerabilidades;
- preservación de la disponibilidad del servicio.

La arquitectura deberá evitar que un ataque dirigido contra la infraestructura pública permita alcanzar directamente los componentes internos responsables del procesamiento de resultados.

El encargado de asesorar a **EL IEPC GRO** en la adquisición y configuración de protecciones WEB será **EL PROVEEDOR,** no obstante, el servicio independiente contratado por **EL IEPC GRO** podrá realizar revisiones y observaciones, que deberán ser discutidas con **EL IEPC GRO** y **EL PROVEEDOR.**

11.11 Monitoreo de ciberseguridad

Durante los simulacros y periodo de operación que determine **EL INE, EL PROVEEDOR** deberá proporcionar monitoreo especializado de ciberseguridad.

Deberán integrarse y correlacionarse eventos relevantes generados por:

- aplicativos;
- APIs;
- sistemas operativos;
- bases de datos;
- infraestructura;
- mecanismos de autenticación;
- dispositivos de seguridad;
- aplicativo PREP Casilla;
- componentes de publicación.

El servicio deberá permitir detectar comportamientos anómalos, intentos de intrusión, accesos no autorizados, manipulación de información y eventos que pudieran comprometer la operación del PREP.

El servicio especializado contratado por **EL IEPC GRO** podrá hacer revisión y observaciones sobre los mecanismos de monitoreo de ciberseguridad implementados, los resultados deberán ser discutidos con **EL IEPC GRO** y **EL PROVEEDOR.**

11.12 Respuesta a incidentes

El servicio independiente contratado por **EL IEPC GRO** podrá hacer revisión de los procedimientos y mecanismos de respuestas proporcionados por **EL PROVEEDOR.**
Los incidentes críticos deberán ser atendidos bajo los niveles de servicio que determine EL INE.

11.13 Simulacros de ciberseguridad y ciberrresiliencia

EL PROVEEDOR deberá coordinarse con el servicio independiente contratado por **EL IEPC GRO** para incluir en los simulacros oficiales que determine EL INE e incorporar escenarios específicos de ciberseguridad.

Los ejercicios podrán contemplar:

- indisponibilidad de componentes;
- ataques contra el sitio público;

- ataques contra APIs;
- compromiso de credenciales;
- comportamiento anómalo de dispositivos;
- intento de manipulación de información;
- pérdida de conectividad;
- degradación controlada de servicios;
- activación de mecanismos de contingencia;
- recuperación tecnológica.

Al término de cada simulacro el servicio independiente contratado por **EL IEPC GRO** deberá entregar un informe de resultados, hallazgos, riesgos y acciones de mejora independiente del informe de simulacro elaborado por **EL IEPC GRO**.

11.14 Ciberresiliencia y continuidad

El servicio independiente contratado por **EL IEPC GRO** deberá evaluar que EL SISTEMA cuente con capacidades suficientes para mantener o recuperar sus funciones críticas ante incidentes de ciberseguridad.

Deberán identificarse los componentes críticos, dependencias tecnológicas, puntos únicos de falla, mecanismos de redundancia, respaldos, procedimientos de recuperación y mecanismos de continuidad.

Las capacidades deberán validarse mediante ejercicios técnicos y simulacros, las observaciones y recomendaciones deberán ser discutidas con **EL IEPC GRO** y **EL PROVEEDOR,** donde **EL PROVEEDOR** deberá garantizar su resolución a través de si mismo o de asesoría a **EL IEPC GRO.**

11.15 Gestión de vulnerabilidades

Todos los hallazgos deberán registrarse en una matriz centralizada de vulnerabilidades que contenga, como mínimo:

- identificador;
- activo afectado;
- descripción;
- evidencia;
- criticidad;
- vector de ataque;
- impacto;

- recomendación;
- responsable de remediación;
- fecha compromiso;
- estado;
- evidencia de corrección;
- resultado de la validación.

Las vulnerabilidades críticas y altas deberán ser atendidas conforme a los niveles de servicio establecidos por EL INE previo a la puesta en producción, salvo aceptación expresa y documentada del riesgo.

El registro de vulnerabilidades estará a cargo del servicio independiente contratado por **EL IEPC GRO** mientras que su resolución estará a cargo de **EL PROVEEDOR.**

11.16 Entregables mínimos

El servicio independiente contratado por **EL IEPC GRO** deberá entregar, al menos:

1. Plan Maestro de Ciberseguridad del PREP.
2. Modelo de amenazas.
3. Arquitectura de seguridad.
4. Reporte SAST.
5. Reporte SCA.
6. SBOM.
7. Reporte de análisis de secretos.
8. Reporte DAST.
9. Reporte de seguridad de APIs.
10. Reporte de seguridad del aplicativo móvil.
11. Reporte de revisión criptográfica.
12. Reporte de hardening.
13. Reporte de pruebas de penetración.
14. Matriz de vulnerabilidades.
15. Evidencias de remediación.
16. Reporte de revalidación de vulnerabilidades.
17. Procedimiento de respuesta a incidentes.
18. Plan de monitoreo de seguridad.
19. Reportes de simulacros.
20. Reporte de evaluación de ciberresiliencia.
21. Informe final de postura de ciberseguridad y riesgos residuales.

Todos los entregables deberán ser compartidos de forma oportuna tanto con **EL IEPC GRO** como con **EL PROVEEDOR** según sea aplicable y conveniente para el aseguramiento de la ciberseguridad y ciberresiliencia del PREP.

11.17 Consideraciones

El servicio independiente contratado por **EL IEPC GRO** podrá ser el mismo o diferente del Ente Auditor que se contrate, por lo que, **EL PROVEEDOR** debe garantizar la apertura con este servicio independiente para hacer las revisiones pertinentes y atender las observaciones que resulten aplicables.

Anexo Único
Funcionalidad del mecanismo para la digitalización de Actas desde las casillas

En este Anexo se presentan los casos de uso correspondientes a cada etapa de operación de los mecanismos para la digitalización de las Actas desde las casillas, considerando los escenarios en los que el aplicativo es desarrollado por **EL IEPC GRO** o por un tercero.

A continuación, se presentan las consideraciones que implican estos escenarios:

Logísticas:

1. Generación de un plan de actividades. Es necesario generar un calendario global que contemple todas las actividades del Instituto y los OPL, con la finalidad de que no se traslapen actividades, como la capacitación y el desarrollo de ejercicios y pruebas.

2. Capacitación. Se deben desarrollar programas de capacitación claros con el fin de garantizar que las y los CAE obtengan los conocimientos necesarios sobre la logística de la toma de la imagen en la operación y la forma de actuar ante eventuales incidencias.

Tecnológicas:

1. Seguimiento al desarrollo de aplicaciones. Será necesario dar seguimiento al desarrollo de las aplicaciones, proceso de instalación y los criterios de seguridad de las aplicaciones desarrolladas por los OPL. Esto se hace con la finalidad de garantizar que las aplicaciones no comprometan la seguridad de los dispositivos móviles y/o afecten el funcionamiento del aplicativo móvil.

Seguridad informática:

El desarrollo independiente por parte de los OPL de una aplicación móvil para la digitalización de las Actas desde las casillas implica tener en cuenta los siguientes aspectos:

1. Elección de mecanismos de seguridad. Se debe hacer una adecuada elección de mecanismos de seguridad informática, a fin de garantizar la integridad y confiabilidad en la transmisión de las imágenes desde los dispositivos móviles a los repositorios que establezca **EL IEPC GRO**, durante la operación.
2. Ejecución de auditorías. Cada aplicación desarrollada por parte de los OPL debe pasar por una serie de pruebas y auditorías en materia de seguridad de la información.

A continuación, se presentan los casos de uso para estos escenarios:

1. Preparación de usuarios y sus roles

En esta sección se muestran los casos de uso correspondientes a la funcionalidad de la aplicación durante la preparación de los distintos actores y el rol que desempeñarán; toda esta funcionalidad se administrará por medio de un portal web, en el que se cuente con la funcionalidad para actualizar las bases de datos, se almacenen los roles y usuarios que tendrán uso del aplicativo.

1.1 Administrar roles de usuarios

Caso de uso	Administrar roles de usuarios.	
Descripción	El administrador crea, modifica o elimina roles de usuarios.	
Actores	Administrador.	
Precondición	1. La aplicación está instalada en el portal correspondiente. 2. Todos los componentes de la Aplicación se encuentran operacionales. 3. El administrador se ha autenticado correctamente en la Aplicación.	
Flujo normal	1	El administrador accede al portal de administración de roles de usuarios.

	2		La aplicación muestra las opciones de administración de roles de usuarios siguientes: 1. Crear nuevo rol de usuario; 2. Modificar rol de usuario, y 3. Eliminar rol de usuario.
	3		El administrador selecciona la opción deseada. Si selecciona: 1. “Crear nuevo rol de usuario”, se hace lo indicado en el paso 4; 2. “Modificar rol de usuario”, se hace lo indicado en el paso 5, o 3. “Eliminar rol de usuario”, se hace lo indicado en el paso 6.
	4	4.1	La aplicación muestra la pantalla para crear un nuevo rol de usuario.
		4.2	El administrador indica el nombre del nuevo rol de usuario.
		4.3	El administrador indica las secciones de la aplicación a las que dicho rol tendrá acceso: 1. Pantallas, y 2. Controles en las pantallas.
		4.4	El administrador instruye a la aplicación guardar la información del nuevo rol de usuario.
		4.5	La aplicación guarda la información del nuevo rol de usuario.
	5	5.1	La aplicación muestra una pantalla con la lista de roles de usuario existentes.
		5.2	El administrador selecciona el rol que desea modificar.
		5.3	La aplicación muestra la pantalla para modificar un rol de usuario. Esta pantalla presenta: 1. El nombre actual del rol de usuario; 2. Pantallas a las que tiene acceso el rol de usuario, y 3. Controles en las pantallas a los que tiene acceso el rol de usuario.
		5.4	El administrador modifica la información deseada para el rol de usuario mostrado.
		5.5	El administrador instruye a la aplicación guardar la nueva información del rol de usuario.
		5.6	La aplicación guarda la información del rol de usuario.
	6	6.1	La aplicación muestra una pantalla con la lista de roles de usuario existentes.

		6.2	El administrador selecciona el rol que desea eliminar.
		6.3	El administrador instruye a la aplicación eliminar el rol de usuario.
		6.4	La aplicación elimina la información del rol de usuario.
Postcondición	1. Cuando se haya creado un nuevo rol, la aplicación contiene la información del nuevo rol de usuario. 2. Cuando se haya actualizado un rol, la aplicación contiene la nueva información del rol de usuario. 3. Cuando se haya eliminado un rol, la aplicación ya no contiene la información del rol de usuario. 4. Existen registros en bitácora del acceso y las actividades llevadas a cabo.		
Excepciones	1	Cuando se haya creado un nuevo rol, si la aplicación no lo almacena, el administrador revisa la aplicación y corrige los errores encontrados.	
	2	Cuando se haya actualizado un rol, si la aplicación no almacena la nueva información, el administrador revisa la aplicación y corrige los errores encontrados.	
	3	Cuando se haya eliminado un rol, si la aplicación no lo elimina, el administrador revisa la aplicación y corrige los errores encontrados.	

1.2 Administrar usuarios

Caso de uso	Administrar usuarios.	
Descripción	El administrador crea, modifica o elimina usuarios.	
Actores	Administrador.	
Precondición	1. La aplicación está instalada. 2. Todos los componentes de la Aplicación se encuentran operacionales. 3. El administrador se ha autenticado correctamente en la aplicación.	
Flujo normal	1	El administrador accede al portal de administración de usuarios.
	2	La aplicación muestra las opciones de administración de usuarios siguientes: 1. Crear nuevo usuario; 2. Modificar usuario, y 3. Eliminar usuario.
	3	El administrador selecciona la opción deseada. Si selecciona: 1. “Crear nuevo usuario”, se hace lo indicado en el paso 4; 2. “Modificar usuario”, se hace lo indicado en el paso 5, o

		3.	“Eliminar usuario”, se hace lo indicado en el paso 6.
	4	4.1	La aplicación muestra la pantalla para crear un nuevo usuario.
		4.2	El administrador indica el nombre del nuevo usuario.
		4.3	El administrador asocia los roles de usuario requeridos.
		4.4	El administrador indica los mecanismos de autenticación del usuario.
		4.5	El administrador instruye a la aplicación guardar la información del nuevo usuario.
		4.6	La aplicación guarda la información del nuevo usuario.
	5	5.1	La aplicación muestra una pantalla con la lista de usuarios existentes.
		5.2	El administrador selecciona el usuario que desea modificar.
		5.3	La aplicación muestra la pantalla para modificar un usuario. Esta pantalla presenta: 1. El nombre de usuario; 2. Roles de usuario asociados, y 3. Mecanismos de autenticación.
		5.4	El administrador modifica la información deseada para el usuario mostrado.
		5.5	El administrador instruye a la aplicación guardar la nueva información del usuario.
		5.6	La aplicación guarda la información del usuario.
	6	6.1	La aplicación muestra una pantalla con la lista de usuarios existentes.
		6.2	El administrador selecciona el usuario que desea eliminar.
		6.3	El administrador instruye a la aplicación eliminar el usuario.
		6.4	La aplicación elimina la información del usuario.
Postcondición	1. Cuando se haya creado un nuevo usuario, la aplicación contiene la información del nuevo usuario. 2. Cuando se haya actualizado un usuario, la aplicación contiene la nueva información del usuario. 3. Cuando se haya eliminado un usuario, la aplicación ya no contiene la información del usuario.		
		1.	Existen registros en bitácora del acceso y las actividades llevadas a cabo.

Excepciones	1	Cuando se haya creado un nuevo usuario, si la aplicación no lo almacena, el administrador revisa la aplicación y corrige los errores encontrados.
	2	Cuando se haya actualizado un usuario, si la aplicación no almacena la nueva información, el administrador revisa la aplicación y corrige los errores encontrados.
	3	Cuando se haya eliminado un usuario, si la aplicación no lo elimina, el administrador revisa la aplicación y corrige los errores encontrados.

2. Operación del mecanismo para la digitalización de Actas desde las casillas

En esta sección se muestran los casos de uso correspondientes a la funcionalidad del aplicativo móvil para digitalización desde las casillas, el cual operará en los dispositivos móviles de las y los CAE.

2.1 Acceder a la Aplicación

Caso de uso	Acceder a la aplicación	
Descripción	La aplicación presenta una interfaz la cual permite a las y los CAE iniciar una sesión en la aplicación móvil.	
Actores	1. Administrador. 2. Las y los CAE. 3. Soporte.	
Precondición	1. El aplicativo se encuentra instalado y configurado en el dispositivo móvil. 2. Se han creado y configurado usuarios en el aplicativo. 3. Las y los CAE deben contar con nombres de usuario institucionales activos para ingresar a la aplicación. 4. Todos los componentes de la aplicación se encuentran operacionales.	
Flujo normal	1	El usuario accede con un doble clic sobre el ícono del aplicativo en el dispositivo móvil o el portal del aplicativo, el cual solicita el nombre de usuario y contraseña para inicio de sesión.
	2	Se ejecuta lo especificado en el caso de uso “Autenticar al usuario”.
	3	Se ejecuta lo especificado en el caso de uso “Autorizar usuario”.
	4	La aplicación le otorga acceso al usuario y despliega las pantallas y controles a los que tiene acceso dependiendo del rol del usuario asociado.
	5	Se presenta el menú principal del aplicativo.
Postcondición	1. El usuario ha iniciado sesión en la aplicación. 2. La Aplicación registra en bitácora las actividades llevadas a cabo.	

Excepciones	1	Acceso denegado: el usuario debe verificar que ingresó correctamente su información de autenticación.
	2	Error de configuración: el administrador debe corregir el error.
	3	Error en alguno de los componentes: el administrador debe diagnosticar y corregir el error.

2.2 Autenticar usuario

Caso de uso	Autenticar al usuario	
Descripción	La aplicación verifica que los datos de inicio de sesión proporcionados por el usuario son correctos.	
Actores	1. Administrador. 2. Las y los CAE. 3. Soporte.	
Precondición	1. Se han creado y configurado usuarios en la aplicación. 2. Los usuarios de las y los CAE deben contar con nombres de usuario institucionales activos para ingresar a la aplicación. 3. Todos los componentes de la aplicación se encuentran operacionales.	
Flujo normal	1	El usuario proporciona sus datos de inicio de sesión.
	2	La aplicación verifica los datos proporcionados.
	3	La aplicación permite el ingreso al usuario.
Postcondición	1. La aplicación registra en bitácora el éxito o fracaso al autenticar al usuario.	
Excepciones	1	Usuario/contraseña incorrecta: el usuario debe verificar sus datos de inicio de sesión.
	2	Acceso denegado: el usuario debe verificar con el administrador que su cuenta tenga asignados los permisos necesarios.

2.3 Autorizar usuario

Caso de uso	Autorizar usuario
Descripción	La aplicación verifica qué acciones puede hacer el usuario que se encuentra dentro de la misma.
Actores	1. Administrador. 2. Las y los CAE. 3. Soporte.

Precondición	1. Se han creado y configurado usuarios en la aplicación. 2. Los usuarios de las y los CAE deben contar con nombres de usuario institucionales activos para ingresar a la aplicación. 3. Todos los componentes de la aplicación se encuentran operacionales. 4. El usuario ha sido autenticado de forma exitosa.	
Flujo normal	1	La aplicación verifica los permisos asignados a la cuenta del usuario.
	2	La aplicación incluye la información de permisos en las variables de sesión.
	3	La aplicación determina las pantallas y controles a los que el usuario tiene acceso dependiendo del rol del usuario asociado.
Postcondición	1. La sesión del usuario se inicia con las variables de sesión inicializadas de acuerdo con los permisos que tiene asociados el rol del usuario. 2. El sistema registra en bitácora los permisos concedidos al usuario.	
Excepciones	1	Error de configuración: el administrador debe corregir el error.
	2	Error en alguno de los componentes del sistema: el administrador debe diagnosticar y corregir el error.

2.4 Menú principal

Caso de uso	Seleccionar opción del menú principal.	
Descripción	Esta pantalla permitirá al CAE seleccionar el tipo de digitalización que desea hacer, dependiendo de la información con la que cuente al momento de ingresar a la aplicación; la y el CAE puede digitalizar un Acta con QR o bien digitalizar un Acta ingresando los datos de identificación, manualmente.	
Actores	• CAE	
Precondición	1. La aplicación se encuentra sincronizada con la zona horaria local. 2. Se han creado y configurado usuarios en la aplicación. 3. Todos los componentes de la aplicación se encuentran operacionales. 4. El usuario se ha autenticado correctamente en la aplicación.	
Flujo normal	1	La o el usuario selecciona la opción para digitalizar el Acta “Con QR” o “Sin QR”; o selecciona la opción “Historial” para visualizar las capturas realizadas
	2	Se despliega una pantalla correspondiente con la información del estado de la aplicación.
	3	El usuario verifica que no existan problemas o irregularidades con el comportamiento del sistema.
Postcondición	1. La aplicación registra en bitácora las actividades llevadas a cabo.	
Excepciones	1	Acceso denegado: el usuario debe verificar con el administrador que su cuenta tenga asignados los permisos necesarios.

	2	Error de configuración: el administrador debe corregir el error.
	3	Error en alguno de los componentes: el administrador debe diagnosticar y corregir el error.

2.5 Acta digitalizada con QR

Caso de uso	Digitalización del Acta cuando se cuenta con el código QR en la misma.	
Descripción	Cuando la o el CAE selecciona la digitalización con QR se debe mostrar un tutorial para la captura del código QR y la lectura y prellenado de datos se hará de manera automática para cada uno de los siguientes campos: Entidad, Distrito, Sección, Tipo Casilla, Ext. Contigua y Núm. Acta Impresa (tipo de elección, ubicado en la esquina superior derecha).	
Actores	CAE	
Precondición	1. Se cuenta con los datos de: Entidad, Distrito, Sección, Tipo Casilla, Ext. Contigua y Núm. Acta Impresa (tipo de elección, ubicado en la esquina superior derecha). 2. La o el CAE se ha autenticado correctamente. 3. Todos los componentes del sistema se encuentran operacionales.	
Flujo normal	1	Confirmar los datos presentados, en caso de que alguno no corresponda, se procede a su captura manual.
	2	Se enfocará la cámara para la toma de la imagen.
	3	Si la definición es clara se acepta.
	4	En caso de que la imagen no pueda leerse, se repiten los pasos 2 y 3.
	5	Se procede con aceptación y envío del Acta.
Postcondición	1. La aplicación genera bitácoras de Actas con código QR registradas. 2. La aplicación registra en bitácora el acceso y las actividades llevadas a cabo.	
Excepciones	1	Error de configuración: el administrador debe corregir el error.
	2	Error en alguno de los componentes del sistema: el administrador debe diagnosticar y corregir el error.
	3	En caso de que la o el CAE modifique alguno de los datos prellenados en automático y no sea válido, no se permitirá la toma de la imagen de esa Acta, desplegándose el mensaje correspondiente.

2.6 Acta digitalizada sin QR

Caso de uso	Digitalización del Acta cuando son se cuenta con el código QR en la misma.

Descripción	Cuando la o el CAE selecciona la digitalización sin QR, la aplicación le permitirá hacer la captura de los siguientes datos: Entidad, Distrito, Sección, Tipo Casilla, Ext. Contigua y Núm. Acta impresa (tipo de elección, ubicado en la esquina superior derecha); dicha información puede ser modificada en caso de ser necesario o bien validada para continuar el proceso de digitalización.	
Actores	CAE.	
Precondición	1. Se cuenta con los datos de: Entidad, Distrito, Sección, Tipo Casilla, Ext. Contigua y Núm. Acta Impresa (tipo de elección, ubicado en la esquina superior derecha). 2. La o el CAE se ha autenticado correctamente. 3. Todos los componentes del sistema se encuentran operacionales.	
Flujo normal	1	Captura de los datos solicitados.
	2	Se enfocará la cámara para la toma de la imagen.
	3	Si la definición es clara se acepta.
	4	En caso de que la imagen no pueda leerse se repiten los pasos 2 y 3.
	5	Se procede con aceptación y envío del Acta.
Postcondición	1. La aplicación genera bitácoras de Actas sin código QR registradas. 2. La aplicación registra en bitácora el acceso y las actividades llevadas a cabo.	
Excepciones	1	Error de configuración: el administrador debe corregir el error.
	2	Error en alguno de los componentes del sistema: el administrador debe diagnosticar y corregir el error.
	3	En caso de que la o el CAE proporcione alguno de los datos que no sea válido, no se permitirá la toma de la imagen de esa Acta desplegándose el mensaje correspondiente.

2.7 Procesamiento del acta digitalizada

Caso de uso	Se procede al procesamiento del Acta digitalizada.
Descripción	Una vez que la imagen del Acta es capturada, la aplicación debe ejecutar un proceso interno mediante un algoritmo para corroborar que sea un Acta válida, dicho algoritmo debe considerar los puntos siguientes.
Actores	N/A

Precondición	1. Se ha digitalizado un Acta. 2. Todos los componentes de la aplicación se encuentran operacionales. 3. Será necesario tener habilitado el servicio de datos para hacer el envío de Actas digitalizadas, en caso de no ser así, la imagen se almacenará con un estatus de pendiente para su posterior envío.	
Flujo normal	1	Análisis de la imagen: 1. Identificación de las 3 marcas que se encuentran en las esquinas del Acta, no importando si la captura de la imagen fue hecha de manera horizontal o de manera vertical. 2. Optimización de la imagen, ya que la imagen original obtenida del dispositivo puede llegar a pesar hasta 6 MB. 3. Rotación de la imagen a una distribución horizontal. 4. Corte excedente de la imagen obteniendo como resultado final solo la sección de los votos del Acta.
	2	Si la imagen del Acta cumple con los requisitos del análisis de la imagen, será un Acta aceptada y la aplicación notificará que ha encontrado un Acta válida lista para ser enviada.
	3	En la pantalla, la o el CAE revisará que los votos sean visibles y podrá enviar el Acta capturada.
	4	En caso de que la imagen del Acta no cumpla con los requisitos del análisis, la aplicación notificará al usuario que no se encontró un Acta válida y podrá “Tomar otra foto” del Acta o “Ver tutorial” por si tiene dudas sobre cómo hacer la captura.
Postcondición	1. La aplicación genera bitácoras de Actas registradas con y sin código QR. 2. La aplicación registra en bitácora el acceso y las actividades llevadas a cabo. 3. El aplicativo debe enviar las Actas almacenadas como pendientes en cuanto se detecte conexión con el servidor.	
Excepciones	1	Error en alguno de los componentes del sistema: el administrador debe diagnosticar y corregir el error.

2.8 Historial de Actas

Caso de uso	Historial de Actas.
Descripción	Desde el menú principal, la o el CAE podrá revisar el avance de Actas enviadas, además de poder consultar el detalle de un Acta enviada al dar clic en una de ellas.
Actores	CAE.
Precondición	1. Existen AEC digitalizadas y almacenadas previamente. 2. Todos los componentes de la aplicación se encuentran operacionales. 3. La o el CAE se ha autenticado correctamente en la aplicación.

Flujo normal	1	Dentro de la ventana de detalle de Actas, el usuario podrá ver la vista previa del Acta.
Postcondición	1. La aplicación registra en bitácora el acceso y las actividades llevadas a cabo.	
Excepciones	1	Error en alguno de los componentes del sistema: el administrador debe diagnosticar y corregir el error.