



**Propuesta de la Universidad Autónoma  
Metropolitana Unidad Iztapalapa (UAMI) para una  
auditoría al sistema informático e infraestructura  
tecnológica del Programa de Resultados  
Electtorales Preliminares (PREP)**

---



## Contenido

I. Propuesta técnica	2
I.1. Pruebas funcionales de caja negra	2
a) Objetivo	2
b) Alcance	2
c) Propuesta técnica	3
d) Entregables	4
I.2. Validación del sistema informático del PREP	5
a) Objetivo	5
b) Alcance	5
c) Propuesta técnica	6
d) Entregables	6
I.3. Análisis de vulnerabilidades a la infraestructura y servicios relacionados con TIC donde se implemente el PREP	7
I.4. Auditoría al Código fuente	13
I.5. Pruebas de negación de servicio al sitio de publicación del PREP y al sitio principal del IEPCG	15
I.6. Revisión de las pantallas del sitio de publicación del PREP, verificando el apego a las plantillas base de la interfaz proporcionadas por el INE	16
II. Propuesta económica	18
III. Plan de trabajo	19
IV. Cronograma	21
V. Presentación de metodología propuesta	23
VI. Curriculum del ente auditor (UAM Iztapalapa)	25

## ***Presentación***

Este documento describe la propuesta para una Auditoría Informática al Sistema Informático del PREP para el Instituto Electoral y de Participación Ciudadana de Guerrero (IEPCG). El documento inicia con la Propuesta Técnica de los trabajos a realizar. A continuación se presenta la propuesta económica asociada con sus condiciones de pago. A continuación se describe brevemente la metodología de trabajo que será utilizada para hacer las revisiones y las pruebas indicadas en el punto I. Propuesta técnica. Enseguida se muestra el plan de trabajo tentativo para cada una de las líneas de trabajo. En la parte final se describe el currículo de la UAMI en trabajos relacionados.



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
**Unidad Iztapalapa**

## ***I. Propuesta técnica***

Las líneas de trabajo para la realización de la auditoría informática al sistema informático del PREP 2024 son:

- 1.1. Pruebas funcionales de caja negra al sistema informático del PREP y a la aplicación que se utilizarán para operar el mecanismo de digitalización de las actas desde las casillas.
- 1.2. Validación del sistema informático del PREP y/o servicios relacionados con TIC, así como sus bases de datos, ante un tercero con fe pública.
- 1.3. Análisis de vulnerabilidades a la infraestructura y servicios relacionados con TIC donde se implemente el PREP.
- 1.4. Auditoría al Código fuente, considerando el sistema informático y componentes en el aplicativo móvil del PREP.
- 1.5. Pruebas de negación de servicio al sitio de publicación del PREP y al sitio principal del IEPCG, considerando la complejidad de ejecutar este tipo de pruebas, éstas pueden llevarse a cabo directamente por el ente auditor, o a través de un tercero que cuente con los recursos de cómputo y ancho de banda necesarios para enviar un volumen de tráfico suficiente para simular las condiciones de saturación que se dan durante un ataque de este tipo.
- 1.6. Revisión de las pantallas del sitio de publicación del PREP, verificando el apego a las plantillas base de la interfaz proporcionadas por el INE.

A continuación se describen las principales actividades a realizar en cada línea de trabajo.

### ***I.1. Pruebas funcionales de caja negra***

#### ***a) Objetivo***

Se analizará el sistema informático del PREP, mediante la realización de pruebas funcionales de caja negra, para evaluar su integridad en el procesamiento de la información y la generación de resultados preliminares, conforme a la normatividad aplicable que se encuentre vigente.

#### ***b) Alcance***

Las Pruebas Funcionales de Caja Negra deberán realizarse en términos de funcionalidad del sistema informático del PREP, donde:

- Analizar el funcionamiento del sistema informático del PREP, en relación con las fases del Proceso Técnico Operativo (PTO), considerando al menos, la digitalización en casilla y en los CATD, la captura de datos, verificación y



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
**Unidad Iztapalapa**

publicación de resultados, mediante flujos completos e interacción entre los diversos módulos.

- Analizar el funcionamiento del aplicativo desarrollado para la digitalización de las actas desde las casillas y los CATD, y, en su caso, la captura de datos desde las casillas. Dicho análisis se hará mediante flujos completos e interacción entre los diversos módulos y fases del PTO.
- Verificar el cumplimiento de las especificaciones funcionales y los requerimientos contenidos en la documentación técnica y normatividad aplicable que será proporcionada por el IEPCG.
- Verificar la correspondencia de la captura de los datos plasmados en las Actas PREP con los presentados en la publicación, mediante los distintos tipos de reportes desplegados por el PREP, considerando datos, imágenes y bases de datos.

Las Pruebas Funcionales de Caja Negra se deberán realizar a los siguientes módulos del sistema informático del PREP:

#### 1. Módulo de Digitalización (casilla y CATD), Captura de Datos y Verificación

- a) Obtención de la imagen digital del Acta PREP, considerando el mecanismo que permita la digitalización y, en su caso, la captura de datos, de las Actas desde las casillas.
- b) Captura de la información contenida en las Actas PREP.
- c) Verificación de la información capturada.

#### 1. Módulo de Publicación de resultados

- a) Revisión de la obtención de los resultados, así como de la emisión de reportes y su despliegue, de acuerdo con la documentación técnica y la normatividad aplicable.

### **c) Propuesta técnica**

Para realizar estas pruebas se estarían siguiendo los lineamientos del ISTQB (International Software Testing Qualifications Board). El tipo de pruebas por la naturaleza del sistema PREP sería a través de:

- Pruebas de Casos de Uso.
- Pruebas de Historias de Usuario.

Se propone seguir una metodología de pruebas de aceptación por flujos completos End-to-End donde sea posible, estableciendo un plan de pruebas implementado a través de dos o tres ciclos de pruebas, los cuales podrán ser integrando a todos los módulos, o por módulo, dependiendo de las condiciones del Sistema Informático y previa consulta con personal de IEPCG. El último ciclo de pruebas será con todos los módulos integrados.



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
**Unidad Iztapalapa**

La propuesta de 2 a 3 ciclos de prueba puede ser modificada para que se ajuste a la estrategia de versiones del IEPCG y pueda proporcionar retroalimentación oportuna, permitiendo actuar de manera más ágil al IEPCG para realizar los ajustes necesarios.

El plan de pruebas identificará y documentará los casos de prueba a realizar.

Como primer paso para la elaboración del plan de pruebas se analizarán los módulos y sus interacciones con los usuarios del Sistema y en consenso con el IEPCG se determinarán las transacciones que serán consideradas para pruebas manuales y las que son susceptibles para aplicarles pruebas automatizadas.

El diseño de los casos de prueba estará basado en los requerimientos del IEPCG. En primer lugar considerará los flujos correctos de las transacciones y en segundo, todos los flujos alternos derivados de detección de condiciones erróneas o de otra naturaleza que lleven a un procesamiento diferente al principal de las transacciones.

Los ciclos de prueba tendrán:

- elaboración de planeación detallada del ciclo,
- diseño detallado de los casos de prueba,
- escritura de los casos de pruebas,
- ejecución de casos de prueba de manera manual,
- generación de reportes preliminares y/o final.

Las pruebas serán realizadas por personal que estará capacitado en pruebas de software y que será capacitado en el uso de los módulos a probar. Se contará con personal suficiente para asegurar un cubrimiento de las funciones, así como para poder asegurar un nivel de utilización significativo.

Los resultados de la aplicación de las pruebas pueden integrarse a informes y administración de incidencias.

#### **d) Entregables**

Los productos para entregar incluirán:

- Plan de pruebas funcionales de caja negra del sistema informático y/o servicios relacionados con TIC, considerando, los siguientes elementos generales: Introducción, objetivo, alcance, pruebas por aplicar, planeación de las pruebas, necesidades de ambiente, casos de prueba, datos de prueba, criterios de pruebas, administración de riesgos y entregables.
- Informe preliminar de las pruebas funcionales de caja negra del sistema informático y/o servicios relacionados con TIC, con el detalle de cada una de las observaciones identificadas en las pruebas y que incluya: Introducción, metodología, criterios utilizados para la auditoría, método para clasificar los hallazgos, observaciones y recomendaciones y conclusiones.



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
**Unidad Iztapalapa**

- Informe final de las pruebas funcionales de caja negra realizadas al sistema informático y/o servicios relacionados con TIC, que contenga: Introducción, metodología, criterios utilizados para la auditoría, resumen ejecutivo, resultados.
- Informe de desempeño de la operación del sistema informático y/o servicios relacionados con TIC, que contenga: Introducción, metodología, criterios utilizados para la auditoría, resumen ejecutivo, resultados.

## ***1.2. Validación del sistema informático del PREP***

### **a) Objetivo**

Validar que el sistema informático del PREP 2024 que operará el día de la Jornada Electoral del Proceso Electoral Federal 2023-2024, corresponda al software auditado, así como que la base de datos se encuentre sin registros adicionales a los necesarios para que el sistema opere. Estas validaciones se tendrán que realizar al inicio, durante y al final de la operación del sistema informático del PREP.

### **b) Alcance**

Se realizará un procedimiento técnico para verificar que los programas auditados se encuentren operando desde el inicio y hasta el cierre de operación del sistema informático del PREP 2024, así como que las bases de datos se encuentren debidamente inicializadas.

Dicho procedimiento deberá ser validado por el personal que el IEPCG designe para tal efectos contemplando los siguientes aspectos:

- Diagrama de flujo.
- Los roles y responsabilidades de los involucrados en el procedimiento.
- Documentación de las siguientes etapas:
  - Generación, obtención y validación de huellas criptográficas en SHA-512 del software PREP auditado.
  - Generación, obtención y validación de huellas criptográficas SHA-512 del software del sistema informático PREP que se habilite en el ambiente productivo y que operará el día de la jornada electoral.
  - Validación de la información inicial y final de la base de datos del PREP.
  - Constancia de hechos.

Será considerado realizar un simulacro del procedimiento en las Oficinas Centrales del IEPCG contemplando todas las etapas mencionadas. Dicho simulacro se llevará a cabo a al menos en uno de los simulacros del PREP que programe el IEPCG para tal efecto.

El procedimiento deberá realizarse el domingo 2 de junio de 2024 en las Oficinas Centrales del IEPCG, concluyendo el 3 de junio y debiéndose atestiguar por un tercero con fe pública designado por el IEPCG.



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
**Unidad Iztapalapa**

### c) Propuesta técnica

#### Huellas criptográficas

Se elaborará un procedimiento que incluirá:

- Desarrollar programas/scripts para tomar los códigos binarios de los aplicativos y con ellos generar la huella criptográfica de c/u de los elementos que constituyan el Sistema Informático.
- Generar huellas criptográficas del Software Auditado.
- Elaborar programas/procedimientos que comparen los conjuntos de huellas criptográficas de un software a auditar contra las huellas criptográficas del Software Auditado.
- Probar los programas/procedimientos/scripts desarrollados.
- Aplicar los programas/procedimientos/scripts de la manera indicada en el alcance.

#### Validación de la BD del Sistema Informático

Dentro del procedimiento de validación se considera:

- Generar consultas a las tablas concentradoras de información para determinar el número de registros presentes.
- Generar un vaciado de la tabla y generar la huella criptográfica del vaciado.
- Elaborar programas/scripts de comparación de huellas criptográficas del vaciado de información contra la referencia.

#### Consideraciones

La obtención de las huellas criptográficas así como la información relativa al contenido de la Base de datos depende del nivel de acceso que se tenga al Sistema Informático.

Para las huellas criptográficas es necesario tener acceso a los contenedores en los que residan los aplicativos a ser auditados y/o a ser utilizados en la jornada electoral.

Para la validación es necesario que la Base de Datos se encuentre sin registros, lo deseable es tener acceso a la misma y poder consultarla directamente.

En caso de que las condiciones anteriores no sea posible tenerlas, se generará un procedimiento que se ajuste a las condiciones presentes tratando en todo momento de lograr los objetivos de la validación.

### d) Entregables

Los productos para entregar en esta línea de trabajo son:

- Plan de trabajo detallado con: el desglose de actividades, entregables, duración, fecha inicio, fecha fin y responsables de las actividades.
- Procedimiento técnico con el esquema de validación de los componentes, programas, configuraciones y códigos auditados y de las bases de datos del sistema informático previamente auditado del PREP, con las etapas de validación,





Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
**Unidad Iztapalapa**

generación de diagramas y descripciones correspondientes, que se acuerden conjuntamente entre el IEPCG y el ente auditor.

- Constancia de hechos de la generación de huellas criptográficas de los componentes, programas, configuraciones y códigos auditados del sistema informático del PREP que describa el protocolo de la actividad: fecha y lugar, hora de inicio y término, objetivo, actividades realizadas, resultados obtenidos con las firmas autógrafas del personal participante por parte del IEPCG y la UAMI.
- Constancias de hechos de la validación de los componentes, programas, configuraciones y códigos auditados; y de las bases de datos del sistema informático del PREP. Previo al inicio, durante y posterior al cierre de operaciones del PREP, que describan el protocolo de validación en el ambiente de producción del sistema informático del PREP: fecha y lugar, hora de inicio y término, objetivo, actividades realizadas, resultados y las firmas autógrafas del personal participante por parte del IEPCG y la UAMI.

### ***1.3. Análisis de vulnerabilidades a la infraestructura y servicios relacionados con TIC donde se implemente el PREP***

#### **a) Objetivos**

- Identificar debilidades de seguridad en la infraestructura y servicios relacionados con TIC donde se implemente el PREP mediante la ejecución de pruebas de penetración y revisión de configuraciones de seguridad.
- Clasificar el impacto y documentar las vulnerabilidades identificadas con el propósito de recomendar al IEPCG las posibles medidas para la mitigación de las vulnerabilidades que previamente fueron identificadas y documentadas.
- Verificar que con las medidas implementadas por el IEPCG se hayan atendido adecuadamente las vulnerabilidades reportadas.

#### **b) Alcance**

Se consideran todos los sistemas informáticos e infraestructura que habilitan los módulos y submódulos incluidos en las Pruebas funcionales de caja negra. Asimismo, se considera la realización de las siguientes pruebas:

- a) Revisión de configuraciones de la plataforma de nube pública
- b) Pruebas de penetración

Se considera:

Junta de inicio para la definición de roles y responsabilidades del la UAMI y del IEPCG, establecer las metodologías y estándares con los que se llevará a cabo esta línea de trabajo así como los tiempos generales de la ejecución. Se realizarán notificaciones de hallazgos



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
**Unidad Iztapalapa**

críticos al Instituto en cuanto se detecten, por los medios que se establezcan en la reunión inicial.

### **c) Propuesta técnica**

A continuación se describen brevemente la forma en que se estará realizando el análisis de las vulnerabilidades y a detalle las pruebas específicas planteadas.

Las actividades de esta línea de trabajo toman como referencia las vulnerabilidades registradas en las bases de datos de vulnerabilidades y debilidades conocidas como CWE (Common Weakness Enumeration), CVE (Common Vulnerabilities and Exposures) así como en otras fuentes neutrales y acreditadas como NIST -National Institute of Standards and Technology-, CIS -Center for Internet Security-, DISA -Defense Information System Agency-, entre otras.

La metodología de análisis de vulnerabilidades comprende las siguientes actividades:

#### Planeación:

Se define el alcance de las pruebas a realizar y se declaran los activos a analizar en búsqueda de vulnerabilidades. También se realiza un proceso de descubrimiento de activos en el alcance de la prueba que no hayan sido declarados explícitamente.

#### Identificación de vulnerabilidades (Pruebas):

Se construye una lista de las vulnerabilidades y debilidades de los activos definidos previamente. Esta lista es el resultado de pruebas de seguridad realizadas con herramientas automatizadas específicas y también de pruebas manuales. La búsqueda toma como fuente las bases de datos de vulnerabilidades y debilidades conocidas, como CWE, CVE, así como los informes de los fabricantes de software, entre otras.

#### Calificación de vulnerabilidades y análisis de riesgo:

Se analiza la lista de vulnerabilidades detectadas y se descartan los falsos positivos. Se asignan métricas y se priorizan las vulnerabilidades mediante calificaciones que asignan un rango o una puntuación de severidad a las diferentes propiedades relacionadas con cada vulnerabilidad (confidencialidad, integridad o disponibilidad) así como a las de los posibles ataques: tipo de ataque, complejidad, facilidad de explotación, etc. La referencia principal para esta calificación es CVSS (Common Vulnerability Scoring System) versión 3.1. Se evalúan los riesgos a partir de la calificación individual de las vulnerabilidades y se establece su prioridad de atención.

#### Remediación:

Se proponen medidas de remediación a las vulnerabilidades priorizadas anteriormente. Estas medidas de remediación pueden incluir la corrección del código fuente vulnerable, el desarrollo e implementación de parches, la ejecución de cambios operativos o de configuración o la introducción de nuevos procedimientos, medidas o herramientas de seguridad.



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
**Unidad Iztapalapa**

Las herramientas que se utilizarán en esta etapa son:

Analizadores de protocolos que buscan protocolos, puertos y servicios de red vulnerables.

Escáneres de red que ayudan a visualizar redes, equipos y servicios y a descubrir señales de advertencia de vulnerabilidades.

Escáneres de aplicaciones web que prueban y simulan patrones de ataque conocidos.

También se implementarán pruebas manuales específicas para ejecutar pruebas no cubiertas por las herramientas.

#### c.1 Pruebas de penetración

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

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

Las pruebas que se realizarían son:

##### Pruebas de control de acceso

Se realizará la validación del ingreso de los usuarios con privilegios, así como la validación de los diferentes roles con los que cuenta el Sistema para evaluar su capacidad de ejecutar funcionalidades dentro de los mismos, considerando al menos las siguientes pruebas:

Esquema de autenticación, incluyendo al menos las siguientes validaciones:

- Pruebas de enumeración de usuarios.
- Pruebas de fuerza bruta y diccionario.
- Pruebas para sobrepasar el esquema de autenticación (ByPass).
- Pruebas de autenticación basadas en múltiples factores.
- Pruebas a la generación de tokens (OTP) en envío de mensajes “push notification” o SMS's.

Gestión de sesiones, incluyendo al menos las siguientes validaciones:

- Pruebas sobre los atributos de las cookies.
- Pruebas de fijación de sesión.
- Pruebas sobre exposición de variables de sesión.
- Pruebas de Cross-Site Request Forgery (CSRF).

Esquema de autorización, incluyendo al menos las siguientes validaciones:

- Pruebas de acceso a recursos protegidos.



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
**Unidad Iztapalapa**

- Pruebas para sobrepasar el esquema de autorización.
- Pruebas de elevación de privilegios.

#### Validación de los datos de entrada

Pruebas de los mecanismos de validación de datos del Sistema PREP 2024, incluyendo al menos las siguientes validaciones:

- Pruebas de Cross-Site Scripting “XSS” (stored, reflected y basados en el DOM).
- Pruebas de Cross Site Flashing.
- Pruebas de inyección de código SQL.
- Pruebas de inyección de código remoto.
- Pruebas de inyección de comandos de sistema operativo.
- Pruebas de desbordamiento de memoria.
- Pruebas de HTTP Splitting/Smuggling.
- Path Traversal.
- Desbordamiento de buffer.

Las actividades de la fase de pruebas de penetración están dirigidas por una metodología basada en las mejores prácticas internacionales para esta actividad, tales como las establecidas según NIST SP 800-115 Technical Guide to Information Security Testing and Assessment y Open Source Security Testing Methodology Manual (OSSTMM), así como por los marcos de referencia OWASP Web Security Testing Guide v4.1 y OWASP Mobile Security Testing Guide v1.1.3 de la fundación OWASP, considerando al menos las siguientes actividades:

#### Pruebas pasivas:

Búsqueda de información en fuentes abiertas acerca de activos en el dominio del IEPCG y que pudiera llegar a ser útil para la explotación de vulnerabilidades del sistema PREP 2024.

#### Exploración de la red y fingerprinting:

Identificación de equipos visibles, mediante técnicas de evasión de protección perimetral. Esta etapa también sirve para tener una primera idea de los servicios, plataformas, y versiones de los mismos que están dentro del alcance, así como las políticas de seguridad de la organización.

#### Enumeración de puertos y servicios:

Exploración y recorrido de puertos y servicios relacionados con el alcance del proyecto para detectar, según su huella, banner y versión, cuáles de ellos tienen vulnerabilidades documentadas en CVE, Exploit-db, Security Focus, entre otras fuentes.

#### Análisis y evaluación de debilidades:

Evaluación de los servicios y activos detectados en los puntos anteriores, mediante la ejecución de herramientas automatizadas y pruebas manuales. Se detectarán



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
**Unidad Iztapalapa**

vulnerabilidades conocidas, así como configuraciones predeterminadas o inseguras que pudieran poner en peligro la confidencialidad, la integridad o la disponibilidad de los activos.

#### Escaneo de aplicaciones y servicios web:

Pruebas con el objetivo de determinar cuáles de las aplicaciones o servicios web pueden contar con vulnerabilidades de inyección, XSS, CSRF, Directory Traversal, manejo de errores deficiente y revelación de información entre otros.

#### Creación de planes de ataque:

A partir de los resultados obtenidos de las pruebas anteriores, se desarrollarán los criterios de explotación de las vulnerabilidades detectadas.

#### Explotación de vulnerabilidades:

De acuerdo con los criterios de ataque creados, se ejecutarán los planes de ataque para explotar las vulnerabilidades detectadas con el fin de demostrar su existencia y medir su impacto sobre los activos.

#### Escalamiento de privilegios:

Pruebas que intentan acceder al sistema con privilegios superiores (escalamiento vertical) a los del usuario de prueba o acceder con privilegios de otros usuarios del mismo nivel (escalamiento horizontal).

#### Movimientos laterales:

Una vez lograda la intrusión, se ejecutarán pruebas para extender el dominio hacia otros activos, tomándolos como base para iniciar nuevos ataques.

#### Creación de evidencias de acceso:

En caso de que la configuración de los sistemas a los que se intentará acceder lo permitan, se dejará una bandera como evidencia de haber vulnerado dicho sistema. Estas banderas estarán registradas en un documento para que posteriormente sean removidas.

#### Eliminación de trazas:

Con excepción del punto anterior, se buscarán eliminar las huellas derivadas de los ataques efectuados.

Herramientas que se emplearán

Durante el proceso de las pruebas se emplearán varias herramientas que permiten tanto automatizar cómo disminuir los tiempos de identificación y verificación de vulnerabilidades como considerar aquellas vulnerabilidades que se han descubierto más recientemente. A continuación, se presenta una lista (no exhaustiva) de algunas de las herramientas que se emplearán:

- WireShark Network Sniffer
- Nmap Network Scanner



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
**Unidad Iztapalapa**

- Burp Suite
- OWASP ZAP App Security Scanner
- Metasploit Framework
- Nikto Web App scanner
- Nessus Professional

Nota: es necesario precisar que las licencias comerciales y open source de las herramientas empleadas durante estas pruebas no son transferibles al IEPCG ni durante la duración del proyecto ni al finalizarlo.

Respecto a la aplicación para la digitalización de actas en las casillas, se realizarán pruebas de ingeniería inversa (y posiblemente decompilación y tampering) con la finalidad de intentar vulnerar los controles de autenticación, control de acceso, integridad y confidencialidad de datos (en reposo y en tránsito) de la aplicación, así como para intentar configurar ataques hacia los métodos implementados en el back-end.

Se estarían presentando los hallazgos encontrados.

El IEPCG validaría los hallazgos y proporcionaría las nuevas versiones corregidas para su validación.

Se validarían las nuevas versiones para asegurar que el hallazgo fue atendido.

Los entregables de las pruebas de penetración serían:

- Plan de Pruebas de Penetración
- Informes preliminares de Pruebas de penetración
- Informe de la aplicación de las Pruebas de penetración

## c.2 Revisión de configuraciones

Se realizará la recolección y el análisis posterior de la información técnica de seguridad sobre los sistemas operativos y otros productos de software de infraestructura.

El acopio de información de configuración se realiza mediante la ejecución de programas (scripts) en los ambientes del sistema operativo y del software de infraestructura. En ciertos casos especiales, será necesaria la ejecución manual directa para la recopilación de información. La información recolectada se contrasta respecto a las buenas prácticas de seguridad definidas por fuentes confiables y neutrales (como NIST, CIS, DISA y otras), así como por los fabricantes de los productos de software utilizados.

Esta revisión de configuración de seguridad incluye los servicios en la nube pública que conforman el Sistema PREP (mismos que serán definidos por el IEPCG), considerando al menos los siguientes componentes:

- Servicio de Base de datos



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
**Unidad Iztapalapa**

- Servicio de ejecución de Tecnología Serverless
- Servicios de exposición de servicios web
- Mecanismos de autenticación
- Servicios de almacenamiento
- Servicios de manejador de APIs
- Servicios subyacentes de seguridad como son: Redes virtuales privadas, Reglas y/o grupos de seguridad, API Gateway, Manejador de llaves, WAF y DDoS.

#### Equipamiento

Se verificarán los equipos de cómputo y dispositivos (scanner, switch de acceso) que conforman un Centro de Acopio y Transmisión de Datos, así como los equipos de cómputo que tengan acceso a los módulos que conforman sistema PREP definidos por el Instituto, a fin de validar que cuentan con el nivel de seguridad adecuado, por lo cual se realizará una revisión de configuración en materia de seguridad

Los entregables de esta sublínea de trabajo son:

- Plan de revisión de configuraciones
- Informe preliminar de revisión de configuraciones
- Informe de la aplicación de recomendaciones de la revisión de configuraciones.

Los entregables finales de la Línea de Trabajo de Análisis de Vulnerabilidades son:

- Informe final del análisis de vulnerabilidades a la infraestructura tecnológica y/o servicios relacionados con TIC donde se implemente el PREP.
- Informe de desempeño de la operación de sistema informático.

## ***1.4. Auditoría al Código fuente***

### **a) Objetivos**

- Identificar las debilidades de seguridad mediante la ejecución de pruebas de análisis de código fuente del PREP y componentes en el aplicativo móvil.
- Clasificar el impacto y documentar las vulnerabilidades o fallas en el código, identificarlas con el propósito de recomendar al IEPCG las posibles medidas para la mitigación de las vulnerabilidades documentadas.
- Verificar que las medidas implementadas por el IEPCG hayan atendido adecuadamente las vulnerabilidades o fallas reportadas.

### **b) Alcance**

Realizar una auditoría al código fuente del sistema Web y de la aplicación móvil del PREP.

### **c) Propuesta técnica**

Se realizará análisis estático de código fuente, tomando como referencia normativa los documentos de buenas prácticas de OWASP en materia de codificación segura y las bases



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
**Unidad Iztapalapa**

de datos públicas de debilidades en lenguajes de programación. Se realizará un análisis automático (en caso de que esté disponible alguna herramienta para los lenguajes de programación utilizados) así como una inspección directa del código. Los hallazgos se clasificarán siguiendo la taxonomía de siete dominios (Seven Kingdoms) y se calificarán según su nivel de riesgo a partir de las referencias documentadas en fuentes confiables.

El análisis de código fuente incluye los siguientes puntos de revisión:

- Validación de entradas.
- Codificación de salidas.
- Administración de autenticación y contraseñas.
- Administración de sesiones.
- Prácticas criptográficas débiles o bibliotecas criptográficas vulnerables.
- Control de acceso.
- Código malicioso
- Seguridad en API y web services
- Manejo de errores y logs.

#### Aplicación móvil

Con respecto al Aplicativo Móvil, la revisión incluye al menos los siguientes tópicos de revisión, referidos al documento OWASP Mobile Top 10 2016:

- Uso adecuado de la Plataforma
- Almacenamiento seguro de información
- Comunicaciones seguras
- Autenticación segura
- Autorización
- Codificación del programa

Los entregables de esta línea de trabajo son:

- Plan de trabajo detallado
- Informe de resultados.





Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
**Unidad Iztapalapa**

## ***1.5. Pruebas de negación de servicio al sitio de publicación del PREP y al sitio principal del IEPCG***

### **a) Objetivo**

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

### **b) Alcance**

Generar tráfico de red hacia los servicios web que se publican dentro del dominio del IEPCG. Este tráfico será de dos tipos:

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

### **c) Propuesta técnica**

Se llevará a cabo una reunión de planeación para la ejecución de las pruebas, donde en conjunto, la UAMI y el IEPCG definirán el horario y fecha que serán realizadas las simulaciones de ataques de negación de servicio (DoS/DDoS) mediante la inyección de tráfico de red especialmente manipulado y controlado cumpliendo con los siguientes requerimientos:

- Ataques volumétricos por protocolo TCP:
  - Al menos de 400 Mbps de throughput.
  - Al menos ejecutar SYN FLOOD.
- Ataques volumétricos por protocolo UDP:
  - Al menos de 400 Mbps de throughput.
  - Al menos ejecutar DNS AMPLIFICATION.
- Ataques volumétricos por protocolo ICMP:
  - Al menos de 400 Mbps de throughput.
  - Al menos ejecutar ICMP FLOOD.
- Ataques en la capa de aplicación (HTTP):
  - Al menos ejecutar SLOWRIS ATTACK.

Las pruebas mencionadas se ejecutarán de manera concurrente, considerando la generación de tráfico malintencionado (SYN FLOOD, DNS AMPLIFICATION, ICMP FLOOD, SLOWRIS ATTACK) en un volumen que represente las condiciones de un ataque.



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
**Unidad Iztapalapa**

Durante las pruebas, cada simulación se apegará a las condiciones de un ataque que puede hacer que el sitio web que se esté probando quede fuera de línea (no disponible), por al menos 2 minutos, previo a que el IEPCG efectué la contramedida para la mitigación.

Para la ejecución de esta actividad se deberá considerar el hardware y software necesario para llevar a cabo las pruebas de negación de servicio distribuido y ésta debe permitir la ejecución de la simulación.

Los entregables de esta línea de trabajo son:

- Plan de trabajo detallado
- Plan de atques de negación de servicio
- Informe de resultados
- Estadísticas del tráfico de red generado.

Segunda revisión de seguridad:

En todas las líneas de trabajo de la Auditoría acerca de seguridad a la plataforma del PREP se realizará una segunda revisión con el objetivo de validar la efectividad de las medidas de remediación realizadas sobre los activos evaluados en la primera revisión.

Esta segunda revisión estará limitada en su alcance e incluirá solamente aquellos activos que hayan sido identificados con vulnerabilidades previamente. Las pruebas de seguridad de la segunda revisión estarán dirigidas a comprobar que las vulnerabilidades reportadas hayan sido remediadas, por lo que ya no será necesario ejecutar pruebas sobre vulnerabilidades no identificadas en la primera revisión.

## ***1.6. Revisión de las pantallas del sitio de publicación del PREP, verificando el apego a las plantillas base de la interfaz proporcionadas por el INE***

### **d) Objetivo**

- Asegurar que las páginas de consulta de información del PREP cumplen con los lineamientos del Instituto Nacional Electoral.

### **e) Alcance**

Revisar todas las interfaces de las páginas de consulta de los resultados del PREP, tanto en dispositivos de escritorio como en móviles.

Esta revisión considera los siguientes elementos:



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
**Unidad Iztapalapa**

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

#### **f) Propuesta técnica**

Se realizará simultáneamente con las Pruebas Funcionales de Caja Negra para los componentes de consulta de resultados, así que se estarán reportando de la misma manera que en dichas pruebas.

## ***II. Propuesta económica***

Por la realización de los trabajos de la auditoría informática al sistema informático del PREP se plantea un monto de \$1,500,000.00 (un millón quinientos mil pesos 00/100 M.N.) más el impuesto al valor agregado IVA.

El monto será pagado a la UAM Iztapalapa de la siguiente forma:

- \$700,000.00 A la firma del convenio entre el IEPCG y la UAM Iztapalapa.
- \$400,000.00 A la entrega de los informes preliminares 1º de abril de 2024.
- \$400,000.00 A la entrega del informe de desempeño 5 de junio de 2024.



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
**Unidad Iztapalapa**

### **III. Plan de trabajo**

El plan de trabajo presentado es una propuesta, pues como se indica en el punto I. Propuesta técnica, cada línea de trabajo definirá a detalle los planes de trabajo correspondientes. Este plan supone que las tres líneas de trabajo pueden realizarse en paralelo y deja un espacio de tiempo antes del 2 de junio que es el día en que el PREP será utilizado.

Los tiempos propuestos para las actividades también son susceptibles de ajuste cuando se disponga de más información en cada línea de trabajo.

Las estrategias para cada línea de trabajo son:

#### Pruebas funcionales de Caja Negra

Se plantean 2 ciclos de pruebas que pueden ser completos revisando todos los flujos en cada ciclo o de manera progresiva.

Cada ciclo de pruebas tendrá una duración de 3 a 4 semanas lo que plantea que aproximadamente 2 meses para llevar a cabo la línea de trabajo.

Para llevar a cabo la actividad los recursos necesarios son:

- Administrador de la Línea de trabajo.
- Analista de pruebas caja negra
- Desarrollador de casos de prueba automatizados.
- Desarrollador de casos de prueba manuales.
- Testers para aplicación móvil.

#### Validación del Sistema Informático y sus BD

La estrategia es analizar la disponibilidad de acceso al sistema informático en términos de sus programas fuentes y/o ambientes de ejecución, así como a sus Bases de Datos, pues las huellas criptográficas que pueden obtenerse están determinadas por el acceso a tales recursos.

Una vez identificados la disponibilidad de acceso al sistema informático se estará terminando de definir el procedimiento de validación el cual podría incluir la realización de los programas/scripts de generación de huellas criptográficas así como los procedimientos que garanticen consistencia en las huellas obtenidas, así como la forma de validación de la Base de Datos.

Se plantean pruebas de tales programas/scripts y procedimientos antes del simulacro.

Los recursos necesarios son:

- Administrador de la línea de trabajo.
- Analista de validación del sistema informático.
- Desarrollador para programas/scripts de generación de huellas criptográficas y consultas de la Bases de Datos.
- Coordinador de actividades con el INE.



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
Unidad Iztapalapa

#### Análisis de Vulnerabilidades, Revisión de Código y pruebas de negación de servicio

Como primera acción del plan de trabajo en esta Línea, se realizará un plan completo, así como, la metodología de pruebas y revisiones para todas las pruebas de seguridad.

Después cada elemento de Pruebas de Seguridad seguridad será realizado un reporte de hallazgos para su atención por parte del IEPCG y continuación una reevaluación para validar su solución o reportar el riesgo.

El desglose se indica a continuación:

a) Pruebas de penetración, análisis de vulnerabilidades y revisión de configuraciones

Se plantea la ejecución de las actividades correspondientes, elaborar un reporte preliminar con los hallazgos, entregarlo al IEPCG para su análisis y solución. Aplicar un ciclo de verificación de incidencias corregidas y elaborar el reporte final de la actividad.

Para las actividades se deja un espacio de 6 semanas.

b) Análisis de código fuente

Se plantea la ejecución de las actividades correspondientes, elaborar un reporte preliminar con los hallazgos, entregarlo al IEPCG para su análisis y solución. Aplicar un ciclo de verificación de incidencias corregidas y elaborar el reporte final de la actividad.

Por su naturaleza para estas las actividades se deja un espacio de 6 semanas.

c) Pruebas de negación de servicio

Se plantea tener una elaboración de casos de prueba detallados, configurar las herramientas de prueba, hacer pruebas internas.

Después tener 2 ciclos de simulaciones de ataque acordados con el IEPCG. El primero corresponde a determinar situaciones de riesgo por ataques de DDoS, el segundo para asegurar que cualquier hallazgo haya sido corregido y que no han cambiado el estado de seguridad en vista del proceso electoral.

Los recursos que participarán en esta Línea de trabajo son:

- Administrador de la Línea de Trabajo
- Analista en configuraciones de seguridad
- Especialista de codificación segura
- Especialista en ataques DDoS
- Analista en pruebas de penetración y análisis de vulnerabilidades
- Testers de seguridad
- Asistentes

## IV. Cronograma

A continuación se presenta el cronograma de actividades resumen de acuerdo a las líneas de trabajo indicadas 1. Propuesta Técnica y consistente con lo mencionado en III. Plan de Trabajo.

Se muestran diagramas de Gantt indicando las semanas del proyecto y las semanas calendario del.

### Pruebas Funcionales Caja Negra

Elemento	Resp	Febrero		Marzo					Abril					Mayo				Junio	
		s0	s1	s2	s3	s4	s5	s6	s7	s8	s9	s10	s11	s12	s13	s14	s15	s16	
		19	26	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	
Pruebas Funcionales de Caja Negra del SI del PREP																			
Elaboración del Plan de pruebas funcionales	UAM		x																
1er ciclo de pruebas																			
Elaboración del plan de pruebas del 1er ciclo	UAM		x	x															
Ejecución del plan de pruebas del 1er ciclo	UAM				x	x	x												
Elaboración del Informe preliminar de pruebas del 1er ciclo	UAM						x												
Corrección de incidencias	IEPCG					x	x	x											
Verificación de corrección incidencias	UAM						x	x											
Entrega de Informe preliminar de pruebas funcionales	UAM							x											
2º ciclo de pruebas																			
Elaboración del plan de pruebas del 2º ciclo	UAM							x											
Ejecución del plan de pruebas del 2º ciclo	UAM								x			x	x	x					
Corrección de incidencias	IEPCG										x			x					
Verificación de corrección incidencias	UAM														x		x		
Elaboración de reporte final de pruebas funcionales	UAM																x		
Entrega de Informe final de pruebas funcionales																	x		
Elaboración y entrega de informe de desempeño	UAM																	x	

### Validación del Sistema Informático del PREPy de su Bases de Datos

Elemento	Resp	Febrero		Marzo					Abril					Mayo				Junio	
		s0	s1	s2	s3	s4	s5	s6	s7	s8	s9	s10	s11	s12	s13	s14	s15	s16	
Validación del Sistema Informático del PREP y de sus BD		19	26	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	
Elaboración del Plan de trabajo	UAM			x															
Elaboración del procedimiento técnico	UAM				x	x													
Validación del procedimientos técnico	IEPCG						x												
Generación de huellas criptográficas																			
Desarrollo de programación	UAM					x	x	x											
Pruebas	UAM						x	x	x										
Generación de huella criptográfica	UAM								x		x								
Simulacro																			
Generación de huella criptográfica software auditado	U - I												x						
Generación de huella criptográfica software en amb productivo	U - I													x					
Validación de información inicial y final de la BD	U - I													x					
Constancia de hechos	U - I													x					
Constancias de hechos de la validación de programas y BD																			
Generación de huella criptográfica software auditado	U - I																x		
Constancia de hechos previo a la Inicio de la jornada	U - I																x	x	
Constancia de hechos después de Fin de la jornada	U - I																	x	



Casa abierta al tiempo

UNIVERSIDAD AUTÓNOMA METROPOLITANA

Unidad Iztapalapa

## Auditoría y Pruebas de Seguridad a la Plataforma del PREP

Elemento	Resp	Febrero		Marzo					Abril					Mayo				Junio	
		s0	s1	s2	s3	s4	s5	s6	s7	s8	s9	s10	s11	s12	s13	s14	s15	s16	
Auditoría de seguridad a la IT del PREP		19	26	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	
Reunión inicial	U - I		x																
Elaboración de propuesta de plan de trabajo AV RC AC DDoS	UAM		x																
Elaboración de metodología de pruebas y revisiones	UAM		x																
Revision del plan de trabajo	IEPCG			x															
Ajustes al plan de trabajo	UAM			x															
Entrega de plan de trabajo	UAM			x															
Entrega de metodología de pruebas y revisiones	UAM			x															
Revisión de documentos	IEPCG			x	x														
Ajustes a los documentos	UAM				x														
Entrega de versiones finales de documentos	UAM				x														
Inicio de ejecución de auditoría	U - I				x														
Pruebas de penetración y análisis de vulnerabilidades																			
Pruebas de penetración	UAM				x	x	x												
Análisis de vulnerabilidades	UAM				x	x	x												
Elaboración de reporte preliminar de PENTEST y AnVul	UAM						x												
Entrega de Informe preliminar de PENTEST y AnVul								x											
Análisis de incidencias	IEPCG						x	x											
Corrección de incidencias	IEPCG						x	x											
Verificación de incidencias corregidas	UAM							x	x		x								
Elaboración de informe final AV, PP y RC	UAM												x	x			x		
Elaboración de aplicación de recomendaciones	UAM																x		
Revisión de configuraciones de la plataforma																			
Ejecución	UAM				x	x	x												
Elaboración de reporte preliminar	UAM						x												
Análisis de incidencias	IEPCG						x												
Corrección de incidencias	IEPCG						x	x											
Verificación de incidencias corregidas	UAM								x		x	x							
Elaboración de aplicación de recomendaciones	UAM																x		
Análisis de código fuente																			
Ejecución	UAM				x	x	x												
Elaboración de reporte preliminar	UAM						x												
Análisis de incidencias	IEPCG						x												
Corrección de incidencias	IEPCG						x	x											
Verificación de incidencias corregidas	UAM								x										
Elaboración de reporte final Análisis de código fuente	UAM						x	x											
Pruebas de negación de servicio distribuido (DDoS)																			
Elaboración de casos de prueba detallados	UAM								x		x								
Configuración de herramientas de prueba	UAM											x	x						
Pruebas internas de casos de prueba	UAM												x						
Simulación 1 de ataque	UAM																		
Análisis de incidencias	IEPCG														x				
Corrección de incidencias	IEPCG													x		x			
Simulación 2 de ataque	UAM																		
Análisis de incidencias	IEPCG																		
Corrección de incidencias	IEPCG																x		
Elaboración de informe final de DDoS	UAM																x		





Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
**Unidad Iztapalapa**

## ***V. Presentación de metodología propuesta***

Se utilizarán los principios planteados en los estándares de auditoría de ISACA (Information Systems Audit and Control Association) aplicables de acuerdo a los requerimientos los cuales son: Planeación, Desempeño del trabajo de auditoría y Reporte.

Se aplicarán las mejores prácticas de la industria en materia de revisiones y pruebas.

Las fases principales de la metodología de revisiones son:

- Estudio de la normatividad
- Estudio de la documentación relacionada con el objeto de la revisión
- Generación de las listas de revisión a ser utilizadas
- Determinación de la estrategia a seguir
- Dimensionamiento del esfuerzo
- Elaboración del plan para la revisión
- Ejecución de las actividades del plan
- Análisis de los resultados
- Generación de reporte de hallazgos y recomendaciones

Las revisiones deben cumplir con criterios de calidad para asegurar su efectividad, como la velocidad máxima de revisión que está planteada en 4 páginas de documentación textual por hora.

Las fases principales de la metodología de pruebas son:

- Estudio de la normatividad
- Estudio de la documentación relacionada con el objeto de la revisión
- Determinación de la estrategia a seguir
- Elaboración del esquema del plan de pruebas
- Dimensionamiento del esfuerzo
- Elaboración del plan de trabajo
- Elaboración de los casos de prueba
- Configuración de ambientes
- Ejecución de los casos de prueba
- Análisis de los resultados
- Generación de reporte de hallazgos y recomendaciones

Dependiendo de las condiciones que se tengan al momento de hacer las pruebas específicas, se buscará usar mecanismos de pruebas automatizadas, frameworks de pruebas, control de incidencias, etc. Que facilite el control de las mismas.

Para las pruebas de seguridad se estarán utilizando las guías de prueba de OWASP V4 (agosto 2015).

Se utilizarán los principios planteados en las guías de prueba, que aunque son planteados para aplicaciones Web, son aplicables para las pruebas de cualquier tipo de aplicación.

Las guías están planteadas para un ciclo de vida de software completo, sin embargo como el sistema informático PREP ya fue desarrollado, se estarán utilizando los principios que sean aplicables.

Las actividades de la fase de análisis de vulnerabilidades y pruebas de penetración están dirigidas por una metodología basada en las mejores prácticas internacionales para esta actividad, tales como las establecidas según NIST SP 800-115 Technical Guide to Information Security Testing and Assessment y Open Source Security Testing Methodology Manual (OSSTMM), así como por el marco de referencia de OWASP Web Security Testing Guide v4.1 de la fundación OWASP.

También se considerarán:

- El estándar NIST 800-115.
- Open Source Security Testing Methodology Manual (OSSTMM).
- Information Systems Security Assessment Framework (ISSAF).
- Penetration Testing Execution Standard (PTES).



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
**Unidad Iztapalapa**

## ***VI. Curriculum del ente auditor (UAM Iztapalapa)***

El equipo de la UAM Iztapalapa ha participado en distintos proyectos de vinculación con entidades privadas y públicas. Las más relevantes con respecto a ejercicios electorales ha sido:

### **2024. Instituto Estatal Electoral del Estado de México**

**Auditoría de la aplicación que se utilizará para llevar a cabo la insaculación electrónica para la designación de consejerías electorales municipales y distritales, en la elección de diputaciones locales y ayuntamientos 2024.** Revisar la aleatoriedad utilizada, la seguridad de la base de datos y que los criterios de asignación estén correctamente implementados como lo especifica el ANEXO TÉCNICO que establece cumplir con las siguientes actividades:

1. Revisar la seguridad de la base de datos.
2. Revisar la generación de números aleatorios
3. Revisar la Integridad de los datos
4. Verificación de los resultados.

### **2023. Instituto Estatal Electoral del Estado de México**

**Auditoría al sistema informático y del Programa de Resultados Preliminares “PREP 2023”**, para las elecciones de gubernatura del 2023. Con la finalidad de evaluar la integridad, disponibilidad y seguridad en el procesamiento de la información y la generación de los resultados conforme a la normativa aplicable y vigente, y en términos del Reglamento de Elecciones, en su Anexo 13, Capítulo III, numeral 5, relativo a los Lineamientos del Programa de Resultados Electorales Preliminares así como al ANEXO TÉCNICO que establece los requisitos mínimos para la contratación del servicio de auditoría; lo anterior, con la finalidad de alcanzar los objetivos siguientes:

1. Evaluar la integridad en el procesamiento de la información y generación de resultados del “PREP 2023”.
2. Evaluar la disponibilidad de la información y generación de resultados del “PREP 2023”.
3. Evaluar la seguridad en el procesamiento de la información y generación de resultados.

### **2022. Instituto Estatal Electoral y de Participación Ciudadana de Oaxaca**

**Auditoría al sistema informático y del Programa de Resultados Preliminares “PREP 202”**, para las elecciones de gubernatura del 2022. Con la finalidad de evaluar la integridad, disponibilidad y seguridad en el procesamiento de la información y la generación de los resultados conforme a la normativa aplicable y vigente, y en términos del Reglamento de Elecciones, en su Anexo 13, Capítulo III, numeral 5, relativo a los Lineamientos del Programa de Resultados Electorales Preliminares así como al ANEXO TÉCNICO que establece los requisitos mínimos para la contratación del servicio de auditoría; lo anterior, con la finalidad de alcanzar los objetivos siguientes:



Casa abierta al tiempo

**UNIVERSIDAD AUTÓNOMA METROPOLITANA**  
**Unidad Iztapalapa**

1. Evaluar la integridad en el procesamiento de la información y generación de resultados del “PREP 2022”.
2. Evaluar la disponibilidad de la información y generación de resultados del “PREP 2022”.
3. Evaluar la seguridad en el procesamiento de la información y generación de resultados.

#### **2021. Instituto Nacional Electoral**

**Auditoría al sistema informático y del Programa de Resultados Preliminares “PREP 2021”**, para las elecciones federales realizadas en junio de 2021. Con la finalidad de evaluar la integridad, disponibilidad y seguridad en el procesamiento de la información y la generación de los resultados conforme a la normativa aplicable y vigente, y en términos del Reglamento de Elecciones, en su Anexo 13, Capítulo III, numeral 5, relativo a los Lineamientos del Programa de Resultados Electorales Preliminares así como al ANEXO TÉCNICO que establece los requisitos mínimos para la contratación del servicio de auditoría; lo anterior, con la finalidad de alcanzar los objetivos siguientes:

1. Evaluar la integridad en el procesamiento de la información y generación de resultados del “PREP 2021”.
2. Evaluar la disponibilidad de la información y generación de resultados del “PREP 2021”.
3. Evaluar la seguridad en el procesamiento de la información y generación de resultados.

#### **2018. Instituto Electoral del Estado (Estado de Puebla)**

**Servicio de Auditoría de verificación y análisis del sistema informático y a la infraestructura tecnológica del Programa de Resultados Preliminares “PREP 2018”**, con la finalidad de evaluar la integridad, disponibilidad y seguridad en el procesamiento de la información y la generación de los resultados conforme a la normativa aplicable y vigente, y en términos del Reglamento de Elecciones, en su Anexo 13, Capítulo III, numeral 5, relativo a los Lineamientos del Programa de Resultados Electorales Preliminares así como al ANEXO TÉCNICO que establece los requisitos mínimos para la contratación del servicio de auditoría; lo anterior, con la finalidad de alcanzar los objetivos siguientes:

1. Evaluar la integridad en el procesamiento de la información y generación de resultados del “PREP 2018”.
2. Evaluar la disponibilidad de la información y generación de resultados del “PREP 2018”.
3. Evaluar la seguridad en el procesamiento de la información y generación de resultados.

#### **2006: Instituto Electoral del Distrito Federal**

**Desarrollo de una prueba piloto mediante el uso de urnas electrónicas semi-industriales, en un simulacro, durante la jornada electoral del 2 de julio de 2006 en el Distrito Federal**, la cual consistió en desarrollar una prueba para una urna electrónica y auditar todo el software desarrollado tanto para la urna electrónica como para la integración de resultados para el entonces Instituto Electoral del Distrito Federal, así como proponer pruebas que pudieran validar

el correcto funcionamiento de todo el proceso, desde su configuración, puesta en operación de la urna, proceso de votación, cierre de casilla, integración de información de la votación y publicación de los resultados.

El equipo además cuenta con certificaciones en auditoría de arquitecturas de software en Architecture Trade-off Analysis Method ATAM (método de Análisis de compromisos de Arquitecturas de software). Esta certificación la proporciona el Software Engineering Institute (Instituto de Ingeniería de Software) con sede en Pittsburgh EUA. Este método es una auditoría a la arquitectura tecnológica utilizada, en la cual se identifican situaciones que, en ciertos escenarios provocarán que el sistema informático no se comporte como está esperado. Lo que permite resolverlas con anticipación antes de poner los sistemas en producción. Este método de auditoría se aplica al final del diseño arquitectónico o bien antes de la liberación de los sistemas como es el caso del Sistema Informático del PREP del IEE de Puebla.

Adicionalmente el equipo se ha especializado en temas de Arquitectura de Software y Arquitectura Tecnológica que les ha permitido participar en varios proyectos asesorando a organizaciones privadas y públicas en esos temas. Los temas de asesoría han sido como apoyando a equipos de desarrollo para las propuestas de elementos de seguridad, confiabilidad, desempeño de los sistemas informáticos y virtualización de servidores. Así como para señalar posibles riesgos que la arquitectura de software propuesta pudiera incurrir.

De ahí se ha desprendido la publicación de dos libros que son referencias en el tema: ***“Arquitecturas de Software”, Cervantes (UAM), Velasco (UAZ), Castro (UAM), Cengage, 2015***, y ***“Designing Software Architectures”, Cervantes (UAM), Kazman (SEI), Addison Wesley, 2016***.

En el pasado miembros del equipo han participado como instructores en diplomados de auditoría informática para la presentación de la Certified Information Systems Auditor CISA (Certificación de Auditor de Sistemas de Información) que otorga el Information Systems Audit and Control Association ISACA (Asociación de Auditoría y Control de Sistemas de Información).

Adicionalmente se integran al equipo personal con las credenciales de seguridad suficientes para garantizar el éxito del proyecto (ver sección de personal).