



**Tecnológico  
de Monterrey**

PROPUESTA TÉCNICA ECONÓMICA:

**Servicio de Auditoría de Infraestructura Tecnológica y  
Sistema Informático del Programa de Resultados  
Electtorales Preliminares (PREP) para las elecciones de  
2024 a cargo del Instituto Electoral y de Participación  
Ciudadana del Estado de Guerrero (IEPC)**

---

*Base*

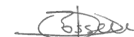
*Lucas*

15 de Enero 2024

## Índice

<b>1</b>	<b>SERVICIOS DE AUDITORÍA AL SISTEMA INFORMÁTICO Y A LA INFRAESTRUCTURA TIC DONDE SE IMPLEMENTA EL PREP .....</b>	<b>5</b>
1.1	PRUEBAS FUNCIONALES DE CAJA NEGRA .....	5
1.1.1	Alcance:.....	5
1.1.2	Metodología: .....	6
1.1.3	Entregables:.....	6
1.1.4	Requerimientos:.....	7
1.2	VALIDAR EL SISTEMA INFORMÁTICO DEL PREP Y SUS BASES DE DATOS .....	9
1.2.1	Alcance:.....	9
1.2.2	Metodología: .....	9
1.2.3	Entregables:.....	10
1.3	ANÁLISIS DE VULNERABILIDADES Y PRUEBAS DE DESEMPEÑO .....	11
1.3.1	Análisis de Vulnerabilidades .....	11
1.3.2	Alcance.....	11
1.3.3	Metodología .....	11
1.3.4	Herramientas .....	11
1.3.5	Entregables:.....	12
1.3.6	Requerimientos .....	13
1.4	PRUEBAS DE NEGACIÓN DE SERVICIO AL SITIO DE PUBLICACIÓN DEL PREP Y AL SITIO PRINCIPAL DEL OPL .....	14
1.4.1	Alcance:.....	14
1.4.2	Metodología: .....	14
1.4.3	Entregables .....	14
1.4.4	Requerimientos .....	15
1.5	REVISIÓN DE CONFIGURACIONES A LA INFRAESTRUCTURA Y/O SERVICIOS RELACIONADOS .....	16
1.5.1	Metodologías.....	16
1.5.2	Entregables .....	16
1.5.3	Requerimientos .....	17
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. ....	18
<b>2</b>	<b>SERVICIOS OPCIONALES .....</b>	<b>19</b>
2.1	PRUEBAS DE DESEMPEÑO: .....	19
2.1.1	Alcance.....	19
2.1.2	Metodología .....	19
2.1.3	Herramientas .....	20
2.1.4	Entregables .....	20
2.1.5	Requerimientos .....	20
2.2	AUDITORÍA AL CÓDIGO FUENTE .....	21
2.2.1	Pruebas de código estático (SAST).....	21
2.2.1.1	Metodología:.....	21

2.2.1.2	Requerimientos para realizar las pruebas.....	22
2.2.1.3	Herramientas. ....	22
2.2.1.4	Entregables. ....	22
2.2.2	<i>Pruebas de código dinámico (DAST)</i> .....	22
2.2.2.1	Metodología:.....	22
2.2.2.2	Herramientas: .....	22
2.2.2.3	Entregables .....	23
<b>3</b>	<b>PROPUESTA ECONÓMICA.....</b>	<b>24</b>
<b>4</b>	<b>PLAN DE TRABAJO .....</b>	<b>26</b>
<b>5</b>	<b>CRONOGRAMA (NOTA: ESTE ES UN EJEMPLO DEL PLAN DE TRABAJO QUE SE DESARROLLARÁ UNA VEZ QUE ESTÉ AUTORIZADO EL PROYECTO) .....</b>	<b>27</b>
<b>6</b>	<b>TÉRMINOS Y ACRÓNIMOS.....</b>	<b>29</b>
<b>7</b>	<b>ANEXO B REQUERIMIENTOS Y DATOS PARA INICIO .....</b>	<b>31</b>
<b>8</b>	<b>ANEXO: CV DEL INSTITUTO TECNOLÓGICO Y DE ESTUDOS SUPERIORES DE MONTERREY .....</b>	<b>32</b>
<b>9</b>	<b>ANEXO: CV COMPLETOS.....</b>	<b>35</b>
<b>10</b>	<b>MANIFESTACIÓN BAJO PROTESTA DE DECIR VERDAD, DE QUE CUENTA CON LA CAPACIDAD TÉCNICA, FINANCIERA Y OPERATIVA PARA LA EJECUCIÓN DE LA AUDITORÍA. ....</b>	<b>55</b>
<b>11</b>	<b>CARTAS DE REFERENCIA Y CERTIFICADOS .....</b>	<b>56</b>




15 de Enero de 2024, Monterrey, N.L.

**MTRA. LUZ FABIOLA MATILDES GAMA**  
**PRESIDENTA**  
**INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA**  
**DEL ESTADO DE GUERRERO**  
**P R E S E N T E.-**

Por medio del presente le comparto la propuesta técnica económica relativa a la invitación para participar como Ente Auditor para el “El Programa de Resultados Electorales Preliminares para el proceso electoral ordinario 2023-2024” a cargo del Instituto Electoral y de Participación Ciudadana del Estado de Guerrero (IEPC).

El Instituto Electoral y de Participación Ciudadana del Estado de Guerrero (IEPC) requiere que se realice una auditoría a los sistemas que integran el PREP de la Organización Publica Local (OPL) previo a la jornada electoral del 2 de Junio del 2024.

Los requerimientos de análisis de los sistemas se subdividen en los siguientes partes:

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.
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.
3. Pruebas de Vulnerabilidades y Pruebas de Desempeño a la infraestructura y servicios relacionados con TIC donde se implemente el PREP.
4. Pruebas de negación de servicio al sitio de publicación del PREP y al sitio principal del OPL, 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.
5. Reportes parciales, y uno final, de los resultados de la auditoría.
6. Pruebas estáticas y dinámicas (Código fuente y en ejecución), considerando el sistema informático y componentes en el aplicativo móvil del PREP (Opcional).

En el presente documento presentamos una propuesta técnico-económica para atender dichos requerimientos.

## Propuesta Técnica

Los entregables a la OPL incluyen la documentación de auditoría a entregarse después de los simulacros de jornada electoral, así como la documentación final de la auditoría después de pasada la jornada electoral. Los siguientes entregables se entregarán los siguientes documentos descritos en las siguientes secciones.

# 1 Servicios de Auditoría al sistema informático y a la infraestructura TIC donde se implemta el PREP

La auditoría incluye lo siguiente puntos: pruebas de caja negra, Validación Sistema informático, Pruebas de penetración, Pruebas de negación de servicio al sitio de publicación.

A continuación, se describen cada una de estas pruebas.

## 1.1 Pruebas funcionales de Caja Negra

Mediante el análisis de pruebas funcionales de caja negra, se evaluará la integridad del procesamiento de la información y generación de resultados preliminares. Para tener los entregables correctos.

### 1.1.1 Alcance:

- Se analizará el funcionamiento del sistema informático del PREP, en relación con las fases del Proceso Técnico Operativo (PTO), considerando al menos, la **digitalización, captura de datos, verificación y publicación de resultados**, mediante flujos completos e interacción entre los diversos módulos.
- Se analizará el funcionamiento del aplicativo desarrollado para la digitalización de las Actas desde las casillas (PREPCASILLA), y, en su caso, la captura de datos desde las casillas. Dicho análisis se hará mediante flujos completos e interacción entre los diversos módulos y fases del PTO.
- Se verificará el cumplimiento de las especificaciones funcionales y los requerimientos contenidos en la documentación técnica y normatividad aplicable que será proporcionada por el **OPL**.
- Se verificará 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.

Los módulos del sistema informático del PREP a incluir:

- I. Módulo de Digitalización, Captura de Datos y Verificación
  - a. Obtención de la imagen digital del Acta PREP, considerando en este apartado el mecanismo que permita la digitalización y, en su caso, la captura de datos, de las Actas desde las casillas.
  - b. Captura de la información contenida en las Actas PREP.

c. Verificación de la información capturada.

II. Módulo de Publicación de Resultados

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

1.1.2 Metodología:

Se seguirá la metodología establecida por el **estándar ISO/IEC 29119** para la ejecución de pruebas de software, asegurando una auditoría sistemática, coherente y eficaz.

Las Pruebas Funcionales tienen un enfoque centrado en evaluar si el sistema cumple con los requisitos funcionales especificados. Verifica si el sistema hace lo que se supone que debe hacer. En lo general la sección de contenido detalla los casos de prueba ejecutados y los resultados de estas pruebas. Se incluye el análisis de cómo el sistema se comporta bajo ciertas condiciones y entradas. Así como la identificación de errores o defectos en la funcionalidad del sistema. Asegurando que la evaluación se hace con conformidad de los requisitos funcionales y especificaciones. A continuación se describe el procedimiento:

- Descripción de un Entorno de pruebas.
- Definición de casos de prueba y de los datos requeridos para las pruebas.
- Análisis de comportamiento del sistema bajo ciertas condiciones y entradas.
- Definición de criterios de aceptación de pruebas.
- Desarrollo de las Pruebas y documentación de resultados.
- Identificación de errores o defectos en la funcionalidad del sistema.
- Desarrollo de las Recomendaciones.

**Coordinación y Comunicación**

- Reuniones periódicas con el OPL, COTAPREP, y otros actores relevantes.
- Gestión de incidencias mediante soluciones automatizadas para un seguimiento efectivo.

1.1.3 Entregables:

1. Plan de pruebas funcionales de caja negra del sistema informático y/o servicios relacionados con Tecnologías de la Información y Comunicaciones. El contenido del documento de esta sección sería el siguiente:
  - Introducción
  - Objetivo
  - Alcance
  - Pruebas por aplicar
  - Planeación de las pruebas
  - Necesidades de ambiente
  - Casos de prueba

- Datos de prueba
  - Criterios de pruebas
  - Administración de riesgos
  - Entregables
2. **El Informe preliminar de los hallazgos encontrados** de las pruebas funcionales de caja negra del sistema informático y/o servicios relacionados con TIC. El contenido del documento de esta sección sería el siguiente:
- Introducción
  - Metodología
  - Criterios utilizados para la auditoría
  - Metodología para clasificar los hallazgos
  - Observaciones y recomendaciones
  - Conclusiones
3. **El Informe final** de las pruebas funcionales de caja negra del sistema informático y/o servicios relacionados con TIC. El contenido del documento de esta sección sería el siguiente:
- Introducción
  - Metodología
  - Criterios utilizados para la auditoría
  - Resumen ejecutivo
  - Resultados
4. **Informe de desempeño** de la operación del sistema informático y/o servicios relacionados con TIC. El contenido del documento de esta sección sería el siguiente:
- Introducción
  - Metodología
  - Criterios utilizados para la auditoría
  - Resumen ejecutivo
  - Resultados
  - Observaciones y recomendaciones

Todos los entregables se remitirán física y digitalmente en las fechas establecidas.

#### 1.1.4 Requerimientos:

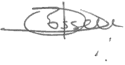
Para la realización de las pruebas de esta sección:

- Se requerirá que la OPL entregue requerimientos de funcionalidad para los diferentes escenarios del PREP.
- **Acceso Continuo y Estable:** Es esencial para probar la funcionalidad del sistema sin conocer su estructura interna. Interrupciones en el acceso podrían impedir la evaluación efectiva de las funcionalidades y los flujos de trabajo.
- **Entorno de Pruebas Dedicado:** Fundamental para asegurar que las pruebas de caja negra no se vean afectadas por otros procesos o datos irrelevantes para el escenario de prueba.

- **Datos de Prueba Representativos:** Son críticos para asegurar que las pruebas de caja negra cubran todos los escenarios de uso posibles, evaluando la respuesta del sistema a diversas entradas.
- **Soporte Técnico y Operativo:** Necesario para resolver dudas o problemas relacionados con la funcionalidad que se está probando.

**NOTAS IMPORTANTES:**

- Las pruebas de caja negra solamente tienen que ver con las funcionalidades de seguridad a revisar del programa.





## 1.2 Validar el Sistema informático del PREP y sus Bases de Datos

El objetivo es validar que los componentes, programas, configuraciones y, en su caso códigos auditados del sistema informático del PREP y/o servicios relacionados con las TIC, sean los utilizados al inicio, durante la operación del PREP y al cierre del mismo. Asimismo, se verificará que el sitio de publicación del PREP y las bases de datos debidamente inicializadas (cero votos) al inicio de las elecciones.

### 1.2.1 Alcance:

Se llevará a cabo, en conjunto con el desarrollador del sistema, **un procedimiento técnico**, validado por el personal que el OPL designe para tal efecto, **para verificar** que los programas auditados se encuentren operando desde el inicio y hasta el cierre de operación del PREP y que las **bases de datos** se encuentren **debidamente inicializadas**. Dicho procedimiento contemplará los siguientes aspectos como mínimo:

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

### 1.2.2 Metodología:

1. Se pedirá al desarrollador que desarrolle un código que genere una clave criptográfica utilizando el código fuente del PREP y el contenido de la configuración.
2. En conjunto con el desarrollador se diseñará un algoritmo que generará una clave criptográfica para garantizar que la(s) bases de datos relacionadas con el voto están vacías y que los catálogos previamente cargados no tuvieron cambios.
3. Se validará la integridad de los componentes y configuración del PREP de la siguiente forma:
  1. Se pedirá que se genere el HASH de componentes y configuración.
  2. Aleatoriamente se pedirá que se modifique algún componente y/o el archivo de configuración.
  3. Se regenerará el HASH de componentes y configuración.
  4. Se verificará que haya cambiado la huella criptográfica.
  5. Se repetirá el paso 2 y paso 3 de acuerdo a los requerimientos del OPL.
  6. Se pedirá que se genere el HASH de las base de datos de votos en su "status" inicial.
  7. Se pedirá simular un procedimiento de captura de acta a una de las bases de datos de votos.
  8. Se regenerará el HASH de las bases de datos.
  9. Se verificará que haya cambiado la huella criptográfica.
  10. Se pedirá que se borre el registro de la base de datos.
  11. Se verificará que la huella criptográfica sea la misma que la generada en el punto 6.
  12. Se repetirá el procedimiento para la base de datos catálogo (datos previamente cargados).
4. El día 2 de junio se ejecutará el procedimiento de validación de componentes y/o archivos de configuración al inicio, durante y al final de la operación del PREP. La validación de la base de

datos de voto que se encuentre en su status inicial (vacía) solo se realizará al iniciode la operación del PREP. Estos procedimientos deberá ser atestiguado y validado por un tercero con fe pública designado por el OPL, quien deberá dejar constancia de lo anterior.

### 1.2.3 Entregables:

1. Documento con el **Plan de Trabajo** – que cuente, como mínimo, con: el desglose de actividades, entregables, duración, fecha inicio, fecha fin y responsables de las actividades.
2. Documento con el procedimiento técnico con el esquema de **validación** de todos los componentes, programas, configuraciones y, en su caso códigos auditados; y de las bases de datos del sistema informático del PREP previamente auditado, junto con las etapas de validación, generación de diagramas y descripciones correspondientes, que se acuerden conjuntamente entre el OPL y el ente auditor.
3. Documento con la **Constancia de hechos de la generación de huellas criptográficas** de los componentes aplicables - deberá describir el protocolo de la actividad, fecha y lugar, hora de inicio y término, objetivo, actividades realizadas, resultados obtenidos y las firmas autógrafas del personal participante por parte del OPL y del ente auditor.
4. Documento con la **Constancia de hechos de la generación de huellas criptográficas** de los componentes, programas, configuraciones y, en su caso códigos auditados del sistema informático del PREP. Esta constancia deberá describir el protocolo de la actividad, fecha y lugar, hora de inicio y término, objetivo, actividades para llevar a cabo, resultados obtenidos y las firmas autógrafas del personal participante por parte del OPL y del ente auditor
5. Documento con la **Constancia de hechos de la validación de los componentes aplicables**- Estas validaciones se deberán realizar previo al inicio, durante y posterior al cierre de operaciones del PREP. Igual que el punto anterior, esta constancia deberán incluir la fecha y lugar, hora de inicio y término, objetivo, actividades llevadas a cabo, resultados y las firmas autógrafas del personal participante por parte del OPL y el ente auditor.

### NOTAS IMPORTANTES:

De haber modificaciones al programa, por cualquier tipo o motivo que altere cualquiera de los programas ya firmado con el HASH previo a las elecciones, la OPL deberá notificar a la entidad auditora previo al día de las elecciones de esta modificación ya que, de haber cambios en el programa, no habrá integridad al momento de verificar las huellas criptográficas al comparar las firmas obtenidas el día de las elecciones con las obtenidas previamente.

## 1.3 Análisis de Vulnerabilidades y Pruebas de Desempeño

### 1.3.1 Análisis de Vulnerabilidades

El objetivo es identificar las debilidades de seguridad en la infraestructura y servicios relacionados con las TICs donde se implementa el PREP mediante la identificación de vulnerabilidades, la ejecución de pruebas de penetración y revisión de configuraciones de seguridad. Así como obtener el impacto, y posible mitigación de las mismas, y recomendar al OPL las posibles medidas de mitigación.

### 1.3.2 Alcance

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 y estaciones de trabajo

### 1.3.3 Metodología

La metodología a utilizar para el análisis de penetración está basada en el *Penetration Testing Execution Standard* (PTES) ([http://www.pentest-standard.org/index.php/Main\\_Page](http://www.pentest-standard.org/index.php/Main_Page)) el cual describe un método estructurado para presentar vulnerabilidades y riesgos de las plataformas involucradas en el PREP 2024. La metodología se complementará con los lineamientos establecidos por OWASP (Open Worldwide Application Security Project) y con el NIST SP 800-115 para el desarrollo de aplicaciones Web. Además, se utilizarán los catálogos estándares de vulnerabilidades como CVE, CWE y NVD.

A continuación se define la metodología a utilizar:

1. Interacción pre-análisis
  - a. En esta etapa, puede consistir en entrevistas y/o cuestionarios técnicos para valoración de activos y de la información que se maneja en la OPL para de ese modo poder establecer una base de referencia al momento del análisis y modelación de riesgos.
2. Análisis de vulnerabilidades
  - a. Este proceso es el descubrimiento de los activos de información indicados por el alcance con la OPL que intervienen en el proceso de las elecciones y que se escanearán para obtener las vulnerabilidades que tengan para poder determinar posteriormente su grado de exposición.
3. Pruebas de Penetración (PENTESTING )
  - a. En esta etapa se usa las vulnerabilidades de las aplicaciones para intentar hacer penetración de las aplicaciones usando herramientas y/o procesos que hacen uso de dichas vulnerabilidades encontradas en la sección anterior.
4. Reportes
  - a. Los reportes que se generarán basados en los entregables definidos en la sección 1 de este documento de acuerdo a lo que la OPL determina requieren como parte de estos informes.

### 1.3.4 Herramientas

A continuación se listan las herramientas a utilizar para realizar en la etapa de **análisis de vulnerabilidades** en los activos de la OPL:

- NMAP – escáner de puertos y equipos
- METASPLOIT - Desarrolla y ejecuta exploits contra una máquina remota
- ZAP – escanea vulnerabilidades de aplicaciones Web.
- CAT – Cisco Audit Tool, herramienta para auditar equipo CISCO (en caso de que haya equipo CISCO).
- NIKTO – Web crawler, descubre vulnerabilidades en la estructura de una página de web
- GreenBone/Nessus – Herramienta de escaneo de vulnerabilidades a nivel sistema.

Y las siguientes herramientas se utilizarán para la fase de **pruebas de penetración (PENTESTING )**:

- ARMITAGE – software para explotar vulnerabilidades
- METASPLOIT – descubre, explota y confirma vulnerabilidades de los activos en prueba
- HPING3 – Permite construir paquetes de una manera específica para usarlos de prueba contra algún dispositivo a probar.

### Definición de pruebas

A continuación se listan las **pruebas de vulnerabilidad**:

1. Escaneo de vulnerabilidades del Sistema operativo.
2. Escaneo de vulnerabilidades de la aplicación web.
3. Prueba de verificación de puertos abiertos y servicios de la red y del sistema donde está el PREP.

Y a continuación se listan las **pruebas de penetración**:

1. Pruebas de Inyección, i.e. código SQL, Código Remoto, comandos del Sistema Operativo,.
2. Explotación de vulnerabilidades alta y críticas del Sistema.
3. Explotación de vulnerabilidades alta y crítica de la aplicación Web, i.e. XSS (Cross-Site Scripting), SSRF (Server-Side Request Forgery), buffer overflow, memory overflow, Path Traversal, .

Si se detecta una vulnerabilidad explotable se realizarán las siguientes pruebas:

1. Escalación de privilegios,
2. modificación de bitacoras y
3. borrado de huella.

### 1.3.5 Entregables:

1. Documento con el plan de pruebas de penetración a la infraestructura y/o servicios relacionados con las TICs donde se implemente el PREP. El cual contiene: el alcance, el calendario de trabajo y los responsables técnicos.

2. **El Informe preliminar de pruebas** de penetración a la infraestructura y/o servicios relacionados con TIC donde se implemente el PREP. El cual contiene: resumen ejecutivo, alcance, resultado de las pruebas y recomendaciones generales
3. **El Informe de la aplicación de recomendaciones** de las pruebas de penetración. El cual contiene: resumen ejecutivo, alcance y resultado de la verificación.

### 1.3.6 Requerimientos

Para definir los entregables se requiere tener claramente estipulado los alcances y restricciones del análisis a realizar. Los alcances del análisis para el PREP del 2024 son:

- Se requiere tener permiso por escrito y autorización de los responsables técnicos y administrativos para realizarlo para desarrollar las actividades de la metodología.
- Los análisis se llevarán a cabo solamente sobre los activos definidos entre la OPL y la entidad administrativa, los cuales deberán estar dentro de la administración de la OPL.
- Debido el impacto potencial de tráfico, los procesos de análisis de activos externos e internos se llevarán a cabo en horas fuera de la operación de la OPL para evitar afectar la operación del día a día.
- El análisis interno de los activos (por adentro de la red de la OPL) se podrá hacer tanto físicamente conectando el software adentro de la red, o bien desde afuera mediante una conexión VPN que permita hacer este proceso más ágil.
- Se requiere tener acceso vía VPN para escanear la red de activos relacionados con el sistema PREP.
- Se requiere conocer, previo a la entrega de los reportes finales, las acciones a tomar en caso de que los reportes finales arrojen resultados en donde no se hayan tomado en consideración las recomendaciones, riesgos y acciones de mitigación de las vulnerabilidades encontradas.

El análisis de vulnerabilidades de la infraestructura y servicios relacionados con las TIC donde se implemente el PREP deberá realizarse en las siguientes etapas.

1. Junta inicial de Kick-off con el personal involucrado en la ejecución de la auditoría donde se presentan las actividades consideradas como parte de la auditoría, definir los roles y responsabilidades de las partes, establecer las metodologías y estándares con las que se llevará a cabo la auditoría, así como los tiempos generales de ejecución. Se definirá la lista de activos, los espacios de trabajo, y se otorgarán los accesos correspondientes y ventanas de tiempo requeridas para la ejecución de la auditoría.
2. Desarrollo del Plan de trabajo detallado con base en la información obtenida y analizada, donde se incluyan los detalles del proyecto de auditoría de seguridad a la infraestructura y servicios relacionados con la TICs donde se implementa el PREP. Este documento integrará la información necesaria durante y después del proceso de auditoría e incluirá, como mínimo, pruebas de penetración (pentest) y la revisión de configuraciones de seguridad.

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

La realización de pruebas de denegación de servicio tiene como objetivo el identificar las debilidades, evaluar y aplicar las medidas necesarias para asegurar la correcta y continua disponibilidad del servicio Web, así como de los sitios de publicación de resultados del PREP y del sitio principal del OPL, durante el periodo de operación del PREP.

### 1.4.1 Alcance:

Las pruebas de negación de servicio deberán considerar dos apartados:

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

Tráfico de red malintencionado, consistente en paquetes de red malformados. Las pruebas mencionadas anteriormente deberán ejecutarse de manera concurrente.

Los ataques de DDOS se harán solamente a la infraestructura explícitamente definida y que esta sea propiedad de la OPL o que esté bajo la administración de ésta.

### 1.4.2 Metodología:

1. Se desarrollará una planeación con el personal de OPL para la ejecución de las pruebas.
2. El día y fecha planeada se realizarán cuatro tipos de ataque con tráfico malintencionado:
  - Ataque volumétrico por TCP @36 Gbps SYN FLOOD
  - Ataque volumétrico por UDP @36 Gbps DNS Amplification
  - Ataque volumétrico por TCP @36 Gbps ICMP FLOOD
  - Ataque a nivel aplicación (HTTP) mediante un ataque de bajo ancho de banda (SLOWLORIS)

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

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

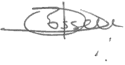
### 1.4.3 Entregables

1. Documento con el **plan de trabajo** detallado que cuente como mínimo con el desglose de actividades, entregables, duración, fecha inicio, fecha fin y responsables de las actividades.
2. Documento con el **plan de ataques** de negación de servicio.
3. **El Informe de resultados** de la prueba DDOS.
4. **Las Estadísticas del tráfico generado** durante la prueba.

#### 1.4.4 Requerimientos

El desarrollo de estas pruebas requiere

- tener la autorización firmada del representante técnico, así como acordar previamente las fechas y horarios para cada tipo de prueba para asegurar la disponibilidad del sistema . (carta anexa en este documento).
- Durante el curso de las pruebas de DOS puede haber afectación a otros servicios y comunicaciones de la OPL por lo que la entidad auditora dará aviso, previa firma de carta de autorización, a la OPL para realizar dicha prueba eximiendo a la entidad auditora de cualquier afectación en tráfico y otras aplicaciones durante la duración de esta prueba.
- autorización explícita del proveedor de nube. Esta autorización será gestionada por el administrador de la cuenta donde está hospedado el sistema.



## 1.5 Revisión de configuraciones a la infraestructura y/o servicios relacionados

El objetivo es analizar las configuraciones de los dispositivos que conforman la infraestructura tecnológica con base a mejores prácticas de seguridad e identificar oportunidades para emitir recomendaciones para su fortalecimiento.

Las buenas prácticas a utilizar serían las establecidas por la filosofía SRE (Site Reliability Engineering).

- Separación de la configuración y de los datos.
- Validación sintáctica y semántica de la configuración.
- Validación del propiedad y la gestión de cambios.
- Validación el procedimiento de despliegue en producción.

### 1.5.1 Metodologías

1. Identificar todos los componentes de la infraestructura Tecnológica y su configuración.
  1. Solicitar el inventario de componentes y sus configuraciones.
2. Gestión de la configuración para ambientes de producción.
  1. Verificar la separación de configuración de los ambientes de desarrollo, prueba y producción.
  2. Validar la separación de la configuración y los datos.
  3. Validar el procedimiento de configuración en producción.
3. Validar que cada elemento de configuración para cada componente se ajuste a las mejores prácticas de la industria en cuestiones de seguridad.
  1. Verificar la gestión de contraseñas, secretos y llaves de criptografía.
  2. Verificar la gestión de usuarios y cuentas.
  3. Verificar la gestión de accesos, permisos y privilegios.
  4. Validar la gestión de cambios de la configuración.
  5. Verificar el uso de herramientas de validación de configuración.
4. Desarrollar documento de recomendaciones.
5. Entregar documento de recomendaciones.
6. Verificar la aplicación de recomendaciones.

### 1.5.2 Entregables

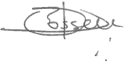
1. **Plan de revisión de configuraciones de la infraestructura y/o servicios relacionados** que contiene lo siguiente: alcance, calendario de trabajo y responsables técnicos.
2. **El Informe preliminar** de revisión de la infraestructura y/o servicios relacionados con TIC donde se implemente el PREP. El cual contiene: alcance, el calendario de trabajo y los responsables técnicos.
3. **El Informe de la aplicación de recomendaciones** de la infraestructura y/o servicios relacionados con TIC donde se implemente el PREP. El cual contiene: resumen ejecutivo, alcance, resultado de las pruebas y recomendaciones generales.



### 1.5.3 Requerimientos

El desarrollo de estas pruebas requiere

- El inventario de componentes
- El documento de arquitectura del sistema
- Acceso a los archivos de configuración
- Entrevista con las personas encargadas de hacer el despliegue en producción



## 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.

Se verificará que el sitio de publicación del PREP se ajuste al diseño definido por el INE para la versión web y la versión móvil, tanto en la interfaz como en la usabilidad, a fin de lograr un mayor nivel de homologación de la información. Esta revisión incluye los siguientes elementos:

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



## 2 Servicios Opcionales

Además de las pruebas que pide el INE, y con el propósito de desarrollar una prueba de seguridad más completa, también ofrecemos las pruebas de estrés y desempeño al sitio de publicación, así como la auditoría de código, tanto su análisis estático como su análisis dinámico.

A continuación se describen estos servicios.

### 2.1 Pruebas de Desempeño:

Para comprobar si una aplicación web puede manejar un número determinado de usuarios y transacciones en condiciones específicas se deben diseñar y ejecutar pruebas de desempeño, que son un tipo de pruebas no funcionales.

Definición de pruebas de desempeño:

- Pruebas de carga
  - Consisten en verificar el comportamiento del sistema bajo una carga anticipada, generalmente determinada en número de peticiones o de usuarios virtuales (VU) por segundo. Si por diseño, el software preestablece una carga, se realiza la comparación de la carga real bajo prueba contra la carga por diseño. Estas pruebas implican simular una carga de trabajo mucho más alta de lo que se espera en condiciones normales, para analizar cómo responde el sistema en situaciones de sobrecarga. El objetivo es identificar los límites del sistema y determinar qué tan bien se comporta en condiciones de estrés.
- Pruebas de estrés
  - Consisten en aplicar un número muy alto de peticiones por segundo para simular un pico de carga por un periodo muy corto de tiempo. Se utilizan para determinar cuellos de botella, mecanismos de recuperación y arquitecturas de alta disponibilidad.

#### 2.1.1 Alcance

El alcance de estas pruebas se limita al sitio de publicación que será accesible por el público en general

#### 2.1.2 Metodología

1. Diseño de pruebas y definición de objetivos de desempeño:
  - Se proponen tres pruebas de carga, con 1000, 2500 y 5000 VU durante 15 minutos, y una prueba de estrés con 10000 VU durante 5 minutos. En todas las pruebas, los usuarios se incrementan de manera regular durante el 25% del periodo de prueba, y durante el tiempo restante se realiza la prueba a carga completa.
2. Identificación de métricas desempeño: Para medir el desempeño de la aplicación se tomarán en cuenta las siguientes métricas:
  - Número promedio de usuarios virtuales por segundo
  - Número promedio de peticiones por segundo

- Tiempo promedio de respuesta por petición
- Número total de peticiones durante la prueba
- 3. Creación de escenarios de prueba
  - Utilizando la herramienta JMeter, se diseñarán los escenarios para cada prueba.
- 4. Establecimiento de entorno de pruebas y ejecución
  - Las pruebas diseñadas en el paso anterior serán configuradas y ejecutadas desde los centros de datos de Microsoft Azure. Durante la ejecución se monitoriza el desempeño y se recopilan datos de las métricas definidas.
- 5. Documentación de resultados
  - Se entrega reporte con métricas. Si el diseño del software determinó parámetro de carga preestablecida, se hace validación sobre este parámetro.

### 2.1.3 Herramientas

- Para ambas pruebas se utilizará la herramienta JMeter para diseñar los escenarios y se ejecutarán de manera distribuida desde centros de datos de Microsoft Azure.

### 2.1.4 Entregables

1. Documento con los **procedimientos de análisis de desempeño**, detallando el desglose de actividades, duración, fechas de inicio y fin. También definirá el alcance de cada prueba, así como los controles aplicables.
2. Documento con **el Informe preliminar** de las pruebas de penetración de la infraestructura y/o servicios relacionados con TIC donde se implemente el PREP.
3. Documento con **Informe final del análisis de las pruebas** realizadas.
4. Documento con **Informe final de la aplicación de recomendaciones** de las pruebas de penetración de la infraestructura tecnológica y/o servicios relacionados con TIC donde se implemente el PREP.

### 2.1.5 Requerimientos

El desarrollo de estas pruebas requiere

- tener la autorización firmada del representante técnico, así como acordar previamente las fechas y horarios para cada tipo de prueba para asegurar la disponibilidad del sistema.
- deshabilitar la funcionalidad que pueda afectar el resultado durante el periodo de ejecución de las pruebas o bien, utilizar mecanismos de lista blanca. Esto es necesario debido a que las pruebas de carga, estrés y desempeño pueden ser detectadas como ataques informáticos de denegación de servicio, de fuerza bruta o bots, por lo que se recomienda.
- notificar al proveedor de infraestructura sobre el tipo, cantidad y duración de estas pruebas para evitar romper con políticas de buen uso.
- la siguiente información técnica sobre la plataforma, incluyendo versiones de cada punto:
  - Infraestructura (física o virtual)
  - Sistema operativo
  - Framework

- Lenguaje de programación
- Web server y configuración de servicio (workers, threads, etc)
- Balanceadores de carga
- CDN
- WAF

**Notas:**

- En caso de realizarse dos o más conjuntos de pruebas, la recomendación es utilizar ambientes iguales en especificaciones para poder realizar las comparaciones pertinentes.
- Las pruebas que requieran algún mecanismo de autenticación<sup>1</sup> está fuera del alcance de esta propuesta, debido a que requieren diseñarse e implementarse en conjunto con el desarrollador del sistema. El desarrollo de una propuesta de pruebas contemplando autenticación es factible, requiriendo la estrecha colaboración del desarrollador del sistema durante el diseño y ejecución de las pruebas.

## 2.2 Auditoría al código fuente

En esta sección se identificará las debilidades que pueda haber en el código mediante dos tipos de análisis:

1. Análisis estático (SAST) al código fuente del PREP.
2. Análisis dinámico (DAST) a la aplicación del PREP.

Mediante estas pruebas se podrá presentar recomendaciones al OPL para la mitigación de dichos hallazgos y posteriormente verificar que estos se hayan atendido adecuadamente de manera que se pueda eliminar las debilidades en el código encontradas en los análisis realizados.

### 2.2.1 Pruebas de código estático (SAST)

Las pruebas SAST (Static Application Security Testing) son un componente clave de un enfoque integral de seguridad en el desarrollo de software, ayudando a identificar y corregir vulnerabilidades en una etapa temprana del ciclo de vida del desarrollo de software a través del análisis del código fuente de la aplicación.

#### 2.2.1.1 Metodología:

La metodología para pruebas SAST sigue varios pasos esenciales para asegurar la detección efectiva de vulnerabilidades y malas prácticas en el código fuente de una aplicación. Los pasos de la metodología son los siguientes:

1. Selección y configuración de la herramienta
  - Seleccionar una herramienta SAST adecuada para el lenguaje de programación y el marco de desarrollo utilizados en el proyecto. Configurar la herramienta SAST adaptarla a las necesidades específicas del proyecto, incluyendo umbrales de severidad y exclusiones.
2. Ejecución de Pruebas:

---

<sup>1</sup> Esta autenticación puede ser básica de HTTP, por intercambio de llaves, por certificado o por algún tipo de biometría.

- Ejecutar la herramienta SAST para analizar el código fuente en busca de patrones que indiquen posibles vulnerabilidades.
- 3. Revisión de Resultados:
  - Revisar los resultados generados por la herramienta para identificar falsos positivos y clasificar las vulnerabilidades detectadas por su severidad y riesgo.
- 4. Informes y Mejora Continua:
  - Se crea informes detallados sobre los hallazgos de vulnerabilidades altas y críticas y recomendaciones para solventar los hallazgos.

#### **2.2.1.2 Requerimientos para realizar las pruebas.**

La disponibilidad del código fuente es un requisito indispensable en la realización de estas pruebas.

#### **2.2.1.3 Herramientas.**

Las herramienta a utilizar dependen del lenguaje que estén utilizando, por ejemplo si se utilizar el lenguaje PHP, se utilizarían las herramientas SonarQube y Lorastan.

#### **2.2.1.4 Entregables.**

Los documentos a entregar son los siguientes:

1. **Plan de trabajo detallado** – Detallando el desglose de actividades, entregables, duración, fechas de inicio y fin, así como los responsables de la ejecución de dichas pruebas.
2. **Informe de resultados** – Este reporte deberá contener los hallazgos que deberán clasificarse por impacto detallando este, así como la recomendación para mitigarlo.

### **2.2.2 Pruebas de código dinámico (DAST)**

Las pruebas DAST (Dynamic Application Security Testing) es el proceso de analizar una aplicación web mediante la interacción con el front-end de modo que se pueda encontrar vulnerabilidades simulando ataques a la aplicación desde el entorno exterior a esta como si fuera el ambiente real de operación.

Mediante las pruebas de DAST se simula la actividad de un usuario mal intencionado sobre la aplicación a probar de manera que el ataque sea lo mas cercano a la realidad; razón por la cual estas pruebas deben llevarse a cabo en un ambiente muy similar a lo que sería la operación regular.

#### **2.2.2.1 Metodología:**

1. Configurar adecuadamente los parámetros de la aplicación.
2. Realizar el escaneo de la aplicación para determinar las vulnerabilidades de la aplicación de web.
3. Realizar el análisis de las vulnerabilidades obtenidas para descartar falsos positivos.
4. Generar el reporte de resultados y recomendaciones para la remediación de las vulnerabilidades encontradas.

#### **2.2.2.2 Herramientas:**

El software que se podría utilizar para realizar pruebas de tipo DAST sobre la aplicación podría ser:

- Nikto - Es un software de escaneo de web con el que se realizan escaneos de vulnerabilidades sobre un servidor de web tanto para la plataforma de web (servidor) como para la aplicación de web montada sobre el servidor.
- Nessus - Es un software de escaneo de vulnerabilidades que se configura para realizar análisis de vulnerabilidades sobre el servidor y la aplicación de web
- ZAP - Es un software de pruebas para aplicaciones web el cual puede ejecutar varios escenarios contra la aplicación de web para determinar que vulnerabilidades pudiese tener la aplicación de web.

### 2.2.2.3 Entregables

La ejecución de las pruebas DAST se hace mediante las herramientas listadas que facilitan el escaneo y ejecución de estas y se proporcionan un reporte final como parte de las pruebas dinámicas de seguridad de la aplicación el cual incluye lo siguiente:

- Documento con el listado de hallazgos de vulnerabilidades así como la descripción de cada uno
- Documento con la clasificación de los hallazgos por severidad.
- Documento con las recomendaciones para la remediación de los hallazgos encontrados.
- Reporte de resultado de pruebas obtenido por la o las herramientas usadas en la ejecución de estas



### 3 Propuesta Económica

Proyecto	SERVICIO DE AUDITORÍA DE INFRAESTRUCTURA TECNOLÓGICA Y SISTEMA INFORMÁTICO DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES (PREP) PARA LA JORNADA DE ELECCIONES DEL 2024 A CARGO DEL INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DEL ESTADO DE GUERRERO (IEPC)		
Cantidad	Concepto	Costo Unitario	Costo Total
1	<b>SERVICIOS REQUERIDOS POR EL INE</b> -PRUEBAS CAJA NEGRA -VALIDACIÓN SISTEMA INFORMÁTICO -ANÁLISIS DE VULNERABILIDADES -PRUEBAS DE PENETRACIÓN (PENTEST) -PRUEBAS DE NEGACIÓN DE SERVICIO AL SITIO DE PUBLICACIÓN DEL PREP -REVISIÓN DE CONFIGURACIONES A LA INFRAESTRUCTURA Y/O SERVICIOS RELACIONADOS	\$1,045,000.00 MX	<b>\$1,045,000.00 MX</b>
1	<b>SERVICIOS OPCIONALES</b> -AUDITORÍA AL CÓDIGO FUENTE -PRUEBAS DE ESTRÉS Y DESEMPEÑO AL SITIO DE PUBLICACIÓN	\$450,000.00 MX	<b>\$450,000.00 MX</b>
<b>Subtotal</b>			<b>\$1,495,000.00 MX</b>
<b>I.V.A.</b>			<b>Exento de IVA</b>
<b>Total</b>			<b>\$1,495,000.00 MX</b>

\*Servicios Exentos de IVA.

El monto señalado en la cotización es **exento del Impuesto al Valor Agregado (I.V.A.)** y corresponde en su totalidad a la cantidad de \$1,495,000.00 MX (Un millón cuatrocientos noventa y cinco mil pesos con 00/100 M.N.).

El **pasado 9 de diciembre de 2019**, fue publicada en el Diario Oficial de la Federación una **Reforma a la Ley del impuesto al Valor Agregado**, (la misma puede ser consultada de manera pública en el sitio electrónico: [0](#)) por medio de la cual “las enajenaciones de bienes, la prestación de servicios y los arrendamientos realizados por donatarias autorizadas serán **exentas de I.V.A. a partir del 1ero. de Enero del 2020...**”

#### **Fundamento de exención para Donatarias**

LEY DEL IMPUESTO AL VALOR AGREGADO



**CAPÍTULO II – De la Enajenación**

Artículo 9. **No se pagará el impuesto en la enajenación de los siguientes bienes:**

[...] X. La de bienes **que realicen las personas morales autorizadas para recibir donativos deducibles** para los efectos del impuesto sobre la renta.

**CAPÍTULO III - De la Prestación de Servicios**

Artículo 15. **No se pagará el impuesto por la prestación de los siguientes servicios:**

[...] VII. Los prestados por las **personas morales autorizadas para recibir donativos deducibles** para los efectos del impuesto sobre la renta.

**CAPÍTULO IV - Del Uso o Goce Temporal de Bienes**

Artículo 20. **No se pagará el impuesto por el uso o goce temporal de los siguientes bienes:**

I. Los otorgados por las **personas morales autorizadas para recibir donativos deducibles** para los efectos del impuesto sobre la renta.

Conforme a esta reforma a la Ley del Impuesto al Valor Agregado a partir del 1 de enero 2020, los **servicios prestados por donatarias autorizadas están exentos de I.V.A.** (Artículo 15 fracción VII), considerando que el Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) es una **donataria autorizada** por el Servicio de Administración Tributaria (SAT), confirmamos que nuestros servicios están exentos de I.V.A. El directorio de las donatarias autorizadas, puede ser consultado en el sitio electrónico del SAT: <https://www.sat.gob.mx/consultas/27717/conoce-el-directorio-de-donatarias-autorizadas>, en el cual el ITESM aparece como donataria autorizada.

**Forma de Pago:**

El costo tal del proyecto se cubrirá en tres pagos:

1. Primer Pago –30 % al arranque del proyecto
2. Segundo Pago – 40 % con la entrega del reporte previo a las elecciones
3. Tercer Pago – 30 % con la entrega del reporte post-evento.

**Vigencia:**

Esta cotización tiene una vigencia de 1 mes a partir de su emisión.

## 4 Plan de Trabajo

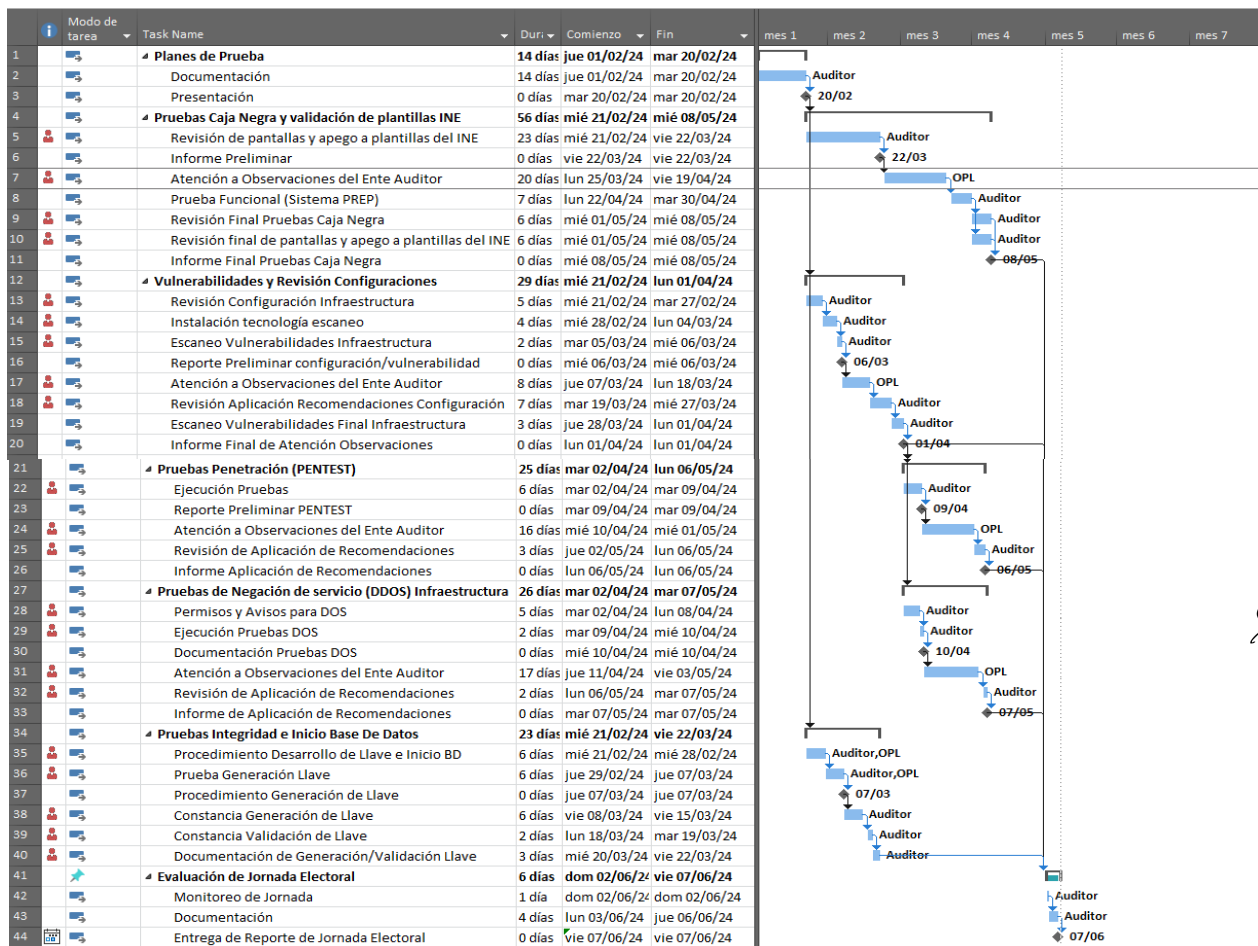
Las actividades del plan de trabajo están hechas para realizarse en cierto orden en base a la metodología descrita en la sección 6 de este documento y aprovechar de la mejor manera los resultados obtenidos en cada actividad.

- **Reconocimiento y análisis** – Para iniciar se requiere tener conocimiento de la infraestructura, de ahí que se inicie con las actividades de análisis de vulnerabilidades y luego con la revisión de configuraciones
- **Ejecución Ataques y Sondeos** – Teniendo la información del reconocimiento y análisis se pasa a efectuar las pruebas de penetración (Pentesting). En el mismo tiempo se efectúan las pruebas de DOS aprovechando las vulnerabilidades encontradas en el análisis.
- **Pruebas de Caja Negra** – Estas pruebas se ejecutarán posterior a las revisiones de infraestructura tecnológica, pentest, ataque de DOS, pero es crítico para esta actividad tener los alcances, así como descripción de funcionalidades del sistema informático PREP desde el inicio de los trabajos para construir los casos de prueba y documentación de los criterios de aceptación de estas actividades.
- **Validación de aplicación** – Esta actividad se documentará como procedimiento previo al inicio de los simulacros en el OPL, la constancia se obtendrá una semana antes de la jornada electoral, durante el último ensayo y posteriormente la prueba de firma se obtendrá previo al inicio de arranque del PREP el día de la jornada. La comprobación de la BD se documentará su proceso previo al último simulacro de actividades del OPL y el día de la jornada electoral se ejecutará para probar la Re inicialización de la Base de datos y probar que esta se encuentra vacía.



## 5 Cronograma (NOTA: Este es un EJEMPLO del plan de trabajo que se desarrollará una vez que esté autorizado el proyecto)

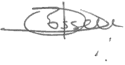
El cronograma comprende actividades y tareas que se acordarán para iniciarse con tiempo previo y adecuado a la jornada electoral.



Dado que algunas fechas aún están en proceso de definición, los tiempos y calendario para las actividades se definirán en sesión de trabajo con el equipo del OPL para con la fecha ya definida de la jornada electoral del 2024.

El plan se hizo para evitar hacer actividades la semana previa a las elecciones, de modo que inicia un mes antes las actividades. Esto asegura evitar problemas antes de las elecciones.

Todas las actividades de los entregables requeridos se realizarán durante las primeras 5 semanas para tener referencia y dejar tiempo para corrección y/o implementación de medidas correctivas. La revisión de estas se hará durante las últimas semanas de abril y la primera de mayo, justo antes de los simulacros de las elecciones.



## 6 Términos y Acrónimos

Acrónimo	Significado
BD	Base de Datos
IEPC	Instituto Electoral y de Participación Ciudadana del Estado de Guerrero
CVSS	Comon Vulnerability Scoring System
DDOS	Distributed Denial Of Service
DNS	Domain Name Server
HTTP	Hypertext Transfer Protocol
HW	Hardware
ICMP	Internet Control Message Protocol
Mbps	Mega bits per second
NIST	National Institute of Standards and Technology
OPL	Organismo Público Local
PREP	Programa de Resultados Preliminares
PTES	Penetration testing execution standard
SHA256	Secure Hash Algorithm 256bits
SW	Software
TCP	Transmission Control Protocol
UDP	User Datagram Protocol




## ANEXO A Carta Autorización para Pen-Testing

<Ciudad Origen>  
A XX de YY del 2020

Para:

Con el propósito de asegurar adecuadamente los activos de la infraestructura de Tecnología de Información del OPL, previo a las elecciones del 2 de junio del 2024, se ejecutará una serie de pruebas, análisis de vulnerabilidades y pruebas de penetración a algunos de los activos de información de la institución. Estas actividades implican el escaneo y pruebas de estrés a ciertos activos de información las cuales pueden causar afectación temporal en los servicios involucrados en dicho análisis. Solo mediante estas pruebas se podrá corregir y modificar la configuración o los programas de la infraestructura para disminuir los riesgos de intrusiones no deseadas en la red del OPL.

El propósito de esta carta es para dar la autorización para la(s) persona(s) en específico que realizarán estas pruebas para análisis de vulnerabilidades, así como para las pruebas de penetración a los activos de esta organización. Para este fin las siguientes personas estarán a cargo de estas pruebas durante las siguientes fechas indicadas:

- a) <NOMBRE\_PENTESTER-1> y <NOMBRE\_PENTESTER-2> tienen permiso para escanear la red del y OPL efectuar análisis de vulnerabilidades y pruebas de penetración, desde el Internet y desde adentro de la red del Instituto. Las fechas propuestas para estas pruebas serán del \_\_\_\_\_ al \_\_\_\_\_ obligando a la entidad auditora a enviar un correo al contacto técnico previo al inicio de cada prueba e indicando las afectaciones que potencialmente puede haber, así como un correo indicado el final de estas al contacto técnico.
- b) <Contacto\_Técnico\_OPL -1> y <Contacto\_Técnico\_OPL-2> tienen la facultad administrativa para otorgar este permiso para la prueba de los activos de información del OPL
- c) <Contacto\_Administrativo\_OPL> tiene la facultad técnica para otorgar este permiso y monitorear internamente la prueba de los activos que se llevará a cabo en las fechas previamente mencionadas de los activos de información del OPL

\_\_\_\_\_  
<NOMBRE\_PENTESTER-1> y/o <NOMBRE\_PENTESTER-2>  
Entidad Auditora del PREP 2024

\_\_\_\_\_  
<Contacto Técnico OPL >  
OPL 2024

\_\_\_\_\_  
<Contacto Técnico OPL >  
OPL 2024


\_\_\_\_\_  
<Contacto Administrativo OPL >  
OPL 2024

c.c.p Expediente

## 7 Anexo B Requerimientos y datos para inicio

Con el propósito de iniciar los análisis y coleccionar resultados para su revisión, se requiere tener a la mano lo siguientes datos y requisitos:

- Rango de direcciones IP públicas a probar desde Internet
- Rango de direcciones IP Privadas a probar desde la red interna del OPL
- Acceso vía IPSEC a la red privada para prueba y escaneo a la red Interna de forma remota
- Carta firmada autorizando las pruebas a realizar sobre la infraestructura del OPL
- Lista de activos enumerando su función
- Acceso a las instalaciones del OPL para conectarse a la red y hacer las pruebas requeridas. Estas se harán con previo aviso al contacto técnico para poder ejecutarlas
- Diagramas del proceso con los roles identificados
- Diagramas de la arquitectura de la red a ser probada
- Entrevista con la persona encargada de la infraestructura tecnológica, el encargado del proceso del PREP
- Acceso al simulacro del evento



## 8 Anexo: CV del Instituto Tecnológico y de Estudios Superiores de Monterrey

Mediante el acta de constancia legal del Instituto Tecnológico de Monterrey expedida el 20 de diciembre de 1988, en la escritura 22,243 en el Volumen LXXXI expedida por el Instituto Registral y Catastral del Estado de Nuevo León, Dirección de Registro Público Primer Distrito, Monterrey se establece la Denominación, Objeto y Domicilio de la Institución, en los artículos 1, 2 y 4, respectivamente.

### Denominación:

La institución particular, con personalidad jurídica propia, reconocida por la Secretaría de Educación Pública, mediante DECRETO publicado en el diario oficial de la Federación del 24 de julio de 1952, se denomina “INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY”.

### Objeto Social:

El Instituto Tecnológico y de Estudios Superiores de Monterrey, no tiene fines de lucro, ni podrá adquirir el dominio sobre tierras, aguas y sus accesiones. El objeto del Instituto Tecnológico y de Estudios Superiores de Monterrey, es iniciar, promover, fomentar, estimular, patrocinar o directamente realizar, administrar y dirigir toda clase de actividades educacionales, de investigación científica y de difusión de la cultura.

### Domicilio:

El domicilio del Instituto es la ciudad de Monterrey, Estado de Nuevo León. El Instituto podrá instalar, cuando lo estime conveniente, oficinas subordinadas, escuelas o cualquiera otra clase de dependencias o establecimientos en cualesquiera otras ciudades del territorio nacional o del extranjero.

### Historia, Descripción, Estructura y Servicios que presta

El Tecnológico de Monterrey fue fundado en 1943 gracias a la visión de don Eugenio Garza Sada y de un grupo de empresarios, quienes constituyeron una asociación civil denominada Enseñanza e Investigación Superior, A. C.

El Tecnológico de Monterrey es una institución de carácter privado, sin fines de lucro, independiente y ajena a partidarismos políticos y religiosos.

Actualmente, el Sistema, está integrado por las siguientes instituciones:

- Tecnológico de Monterrey
- Universidad TecMilenio
- TecSalud



El Tecnológico de Monterrey se distingue por ofrecer un modelo educativo de vanguardia, enfocado al desarrollo del espíritu emprendedor. Los alumnos reciben una formación integral con sentido humano que está basada en la ética y la ciudadanía.

El prestigio de la institución está sustentado: en el aseguramiento de la alta calidad académica; en impulsar un modelo de investigación – acción para transformar, emprender y trascender; por contar con centros de excelencia en las diferentes áreas del conocimiento; y por impulsar la incorporación exitosa de los egresados a la vida profesional.

Además, mantiene una exitosa vinculación con egresados, empresas e instituciones para fortalecer alianzas nacionales e internacionales; promover la internacionalización de alumnos, egresados y profesores; realizar proyectos de colaboración y programas estratégicos, y compartir recursos.

El Tecnológico de Monterrey ha tomado la decisión de evolucionar hacia un nuevo modelo educativo que permitan a sus alumnos convertirse en líderes preparados para enfrentar los retos y oportunidades del siglo XXI.

Este modelo, conocido como Tec21 basa su éxito en mejorar la competitividad al potenciar las habilidades y desarrollar las competencias requeridas en los diferentes campos profesionales. Este modelo tiene su base en 4 componentes que permiten la formación de líderes capaces de enfrentar con éxito los retos del siglo XXI: Aprendizaje basado en retos, flexibilidad, profesores inspiradores y vivencia memorable.

El Tecnológico de Monterrey es una universidad con presencia nacional e internacional que cuenta con 26 campus en todo el país y 18 oficinas internacionales en el mundo. Cuenta con seis escuelas de posgrado nacionales: Escuela de Gobierno y Transformación Pública, EGADE Business School, Escuela de Ingeniería y Ciencias, Escuela de Arquitectura y Diseño, Escuela de Medicina y Ciencias de la Salud, y Escuela de Humanidades y Educación.

La oferta educativa incluye una amplia gama de carreras profesionales, especialidades, maestrías, especialidades médicas y doctorados en diversas áreas del conocimiento; así como tres programas de bachillerato.

El Tecnológico de Monterrey cuenta con acreditaciones nacionales e internacionales tanto como institución como de sus programas académicos que sus diferentes campus ofrecen.

A nivel internacional, el Tecnológico de Monterrey está acreditado por la Comisión de Universidades de la Asociación de Escuelas y Universidades del Sur de Estados Unidos para otorgar títulos profesionales y grados académicos de maestría y doctorado.

La Asociación de Escuelas y Universidades del Sur de Estados Unidos (Southern Association of Colleges and Schools, SACS) es uno de los seis organismos acreditadores regionales de la educación y se encuentra integrada por dos comisiones, una encargada de educación preuniversitaria y otra para educación superior. La Comisión de Universidades (Commission on Colleges) de SACS es la responsable de acreditar

institucionalmente a las universidades en los estados de: Alabama, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, South Carolina, Tennessee, Texas y Virginia. Adicionalmente, esta comisión acredita universidades fuera de los Estados Unidos.

Esta acreditación del Tecnológico de Monterrey incluye los programas y servicios educativos de los niveles de profesional y posgrado, tanto en la modalidad presencial como a distancia.

El Tecnológico de Monterrey ha estado acreditado por SACS desde 1950 y esta acreditación debe reafirmarse cada 10 años. La reafirmación más reciente se obtuvo el 11 de diciembre de 2018, y cubre el período 2018-2028. Esta acreditación ha permitido a la Institución fortalecer su reconocimiento internacional y continuar su liderazgo en la educación superior del país al cumplir con estándares de calidad académica del más alto nivel, así como incorporar importantes mejoras en sus programas académicos y en todos los servicios que ofrece.

A nivel nacional, el Tecnológico de Monterrey está acreditado por la Federación de Instituciones Mexicanas Particulares de Educación Superior (FIMPES).

El Tecnológico de Monterrey realiza investigación científica y tecnológica en áreas estratégicas para satisfacer las demandas sociales, económicas y ambientales del país. Hoy es reconocida por CONACYT, y por otras organizaciones, como una institución comprometida con la investigación, al ser la que más patentes solicita a nivel nacional. Con la Red de Parques Tecnológicos y la transferencia de modelos de desarrollo, así como con las incubadoras y aceleradoras de empresas apoya la generación de riqueza en nuestro país.

Y en el área de desarrollo social, los programas para el Desarrollo Social Sostenible están presentes en comunidades marginadas de todo el país a través de los Centros Comunitarios de Aprendizaje y las Incubadoras sociales con el apoyo de alumnos y profesores.

El Tecnológico de Monterrey, está actualmente estructurado en cuatro Rectorías de Zona, cinco Vicerrectorías y 6 Escuela Nacionales de Profesional y Posgrado y a las que están adscritos diversos Campus. La Escuela de Ciencias Sociales y Gobierno es parte de estas Escuelas Nacionales.

El Tecnológico de Monterrey a través de su Escuela de Ciencias Sociales y Gobierno y con un equipo de expertos de las áreas de ingeniería, como institución estamos conscientes de la importancia de que los procesos electorales en México y en Latinoamérica sean transparentes, objetivos e imparciales, por lo cual hemos participado en procesos electorales como “Ente Auditor”, los cual nos impulsa a seguir apoyando iniciativas que contribuyan en el quehacer democrático.

Como Institución hemos tenido participaciones muy exitosamente en varios procesos electorales que se detallan a continuación:

- 2017:
  - Instituto Electoral de Coahuila (IEC)
  - Comisión Estatal Electoral (CEE) de Nuevo León

- 2018:
  - Instituto Electoral de Coahuila (IEC)
  - Comisión Estatal Electoral (CEE) de Nuevo León (en las elecciones regulares y en las elecciones extraordinarias).
- 2020:
  - Instituto Electoral de Coahuila (IEC)
- 2021:
  - Proyecto "Servicio de Auditoría del Programa de Resultados Electorales Preliminares PREP"- Instituto Electoral de Coahuila
  - Comisión Estatal Electoral (CEE) de Nuevo León
  - Proyecto "Servicio de Auditoría del Programa de Resultados Electorales Preliminares PREP"- Organismo Público Local Electoral de Veracruz
  - Proyecto "Servicio de Auditoría del Programa de Resultados Electorales Preliminares PREP"- Instituto Tlaxcalteca de Elecciones
  - Proyecto "Servicio de Auditoría del Programa de Resultados Electorales Preliminares PREP"- Instituto Electoral y de Participación Ciudadana del Estado de Guerrero
  - Proyecto "Servicio de Auditoría del Programa de Resultados Electorales Preliminares PREP"- Instituto de Elecciones de Participación Ciudadana del Estado de Chiapas
  - Proyecto "Servicio de Auditoría del Programa de Resultados Electorales Preliminares PREP"- Instituto Electoral del Estado de Sinaloa
  - Proyecto "Servicio de Auditoría del Programa de Resultados Electorales Preliminares PREP"- Instituto Estatal Electoral de Hidalgo
  - Proyecto "Servicio de auditoría para la verificación y análisis del Sistema de Cómputo Distrital Municipal (SCDM) 2021"-Organismo Público Local Electoral de Veracruz
- 2022:
  - Instituto de Elecciones de Participación Ciudadana del Estado de Chiapas
  - Instituto Estatal Electoral de Hidalgo
- 2023:
  - Proyecto "Servicio de Auditoría del Programa de Resultados Electorales Preliminares PREP"- Instituto Electoral de Coahuila

## 9 Anexo: CV completos

Los Currículums y semblanzas que se presentan a continuación, son un grupo de especialistas que pudieran participar como parte del equipo auditor, una vez formalizado el proyecto en caso de concretarse, se definirá el equipo que realizará la auditoría, así como los roles y el plan de trabajo.

**Líder:**

**JUAN ARTURO NOLAZCO-FLORES** nació en Gral. Terán, Nuevo León, México. Recibió Licenciatura y de Maestría en el Tecnológico de Monterrey, Monterrey, México, en 1986 y 1988, respectivamente, y el grado de Maestría y doctorado de la Universidad de Cambridge, Cambridge, Inglaterra, en 1992 y 1995, respectivamente. Actualmente es Director del Hub de Ciencia de Datos del Tec de Monterrey.

De 2017 a 2020 fue Decano de la Escuela de Ingeniería y Ciencias, Región Sur, Tecnológico de Monterrey, México. Desde 2011 hasta 2017 fue Director del Área Académica de Tecnologías de la Información y Electrónica en el Tec de Monterrey, campus Monterrey. Fue académico visitante en la Universidad Carnegie Mellon, en Estados Unidos; en la Universidad de Zaragoza, en España; y en las Universidades de Marburg y Mannheim en Alemania. Es autor de más de 70 artículos indexados en Scopus citation report. Ha revisado artículos de *IEEE Transaction on Speech Recognition*, *Speech Communications* y *IEEE Access*, y ha sido evaluador de importantes conferencias internacionales como ICASSP (*International Conference on Acoustic, Speech and Signal Processing*), SLT (*Speech Language Technologies*) y SIP (*Global Signal Information Processing Conference*). Sus intereses de investigación se encuentran en los campos del procesamiento de señales y la ciencia de datos aplicada a las tecnologías del habla y la salud.

Juan Arturo Nolasco ha desarrollado proyectos para las siguientes organizaciones internacionales: para Google, en Estados Unidos; Telefónica, en España; y para las siguientes en organizaciones mexicanas : METALSA; RENAPO; CEMEX; AEROMÉXICO. Específicamente, ha sido líder de más de 15 auditorías del sistema PREP en diferentes estados de México e internacionalmente ha liderado una auditoría en Centroamérica.

El Dr. Nolasco es miembro de la Academia Mexicana de Ciencias, miembro del Sistema Mexicano de Investigación, IEEE Senior Member y ACM Senior Member. En 2005 y 2009 recibió el premio a la Labor Docente y de Investigación de la Escuela de Ingeniería del Tec de Monterrey. Es evaluador certificado de ABET, y ha participado como evaluador de los programas de Ciencias de la Computación de *University of Southern California*, *West Florida University*, *Gran Canyon University*, *Iowa University*, *Miami University* y *Houston Christian University*.

**Coordinador Nacional:**

**JESÚS RAÚL GONZÁLEZ HERNÁNDEZ** es Ingeniero en Cibernética Electrónica y cuenta con una Maestría en Administración de Sistemas Información por el Tecnológico de Monterrey. Así mismo cuenta con certificaciones en CCDA, CCNA, CSSSP, ITIL Foundation, CSSSE, CISSP (en proceso), CDCUCI, CDCUCD. Es consultor independiente en temas de Seguridad de Información y TI y actualmente imparte también cátedra en la Universidad de Monterrey. Así mismo colabora con la empresa VIPRE como responsable de Seguridad y Cumplimiento de los marcos de referencia y estándares de seguridad y privacidad para la empresa. Ha participado desde hace más de 20 años en varias empresas de Tecnologías de Información como TCS, NEORIS, Alestra (Ahora Axtel), CITI en diversas áreas de redes de datos, integración, seguridad y riesgos. Como asesor independiente ha colaborado en la emisión de recomendaciones de vulnerabilidades y mejores prácticas seguridad para la Comisión Estatal Electoral de Nuevo León, como parte de una auditoría general de seguridad y procesos. Así mismo como en el análisis de vulnerabilidades y recomendaciones a diferentes clientes, por otra parte colaboró en el desarrollo de interface web a clientes para consulta segura de estados de cuenta de cheques y tarjeta de crédito para el Grupo Banorte. Actualmente, el Mtro. González es el Coordinador del Centro Ejecutivo SPERTO (Executive Briefing Center) de ALESTRA (AT&T).

Jesús ha participado en más de 15 auditorías del sistema PREP en diferentes estados de México e internacionalmente ha liderado una auditoría en Centroamérica.


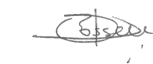
Trabajó en el área de Seguridad de TI con atención a requerimientos de clientes en arquitectura de seguridad y cumplimiento de normas (NIST, ISO27001, SOC2, ISAE, GDPR), diseño campañas de concientización para Seguridad de la Información y revisión de políticas de seguridad para diseño del plan de implementación ISO27001.

**Coordinador Nacional:**

**MARCO O. PEÑA-DÍAZ** nació en Saltillo, Coahuila, México. Recibió Ingeniería en Electrónica por el Tecnológico de Saltillo y Maestría en Inteligencia Artificial por el Tecnológico de Monterrey, en 2000 y 2004 respectivamente. Actualmente es cofundador y director de Appworld S de RL de CV, empresa de consultoría especializada en tecnología desde el 2012. Participó en la creación de Ensitech de México, una de las primeras empresas SAAS en México.

Con 25 años de trayectoria profesional, ha participado en proyectos de implementación tecnológica, ciberseguridad, y habilitación y transformación digital para la iniciativa privada, instituciones educativas superiores y gobierno en los 3 niveles. Los proyectos involucran desde sistemas distribuidos de cómputo hasta soluciones de análisis de datos para empresas de clase mundial en México, Estados Unidos y Europa. Ha participado como consultor estadístico para una de las principales cadenas televisivas en el norte de México. Por la parte de ciberseguridad ha participado en múltiples proyectos de seguridad de software, incluyendo auditorías de cumplimiento bajo lineamientos PCI-DSS, NIST CSF y OEA-CTPAT en su apartado de ciberseguridad; además de diseño de arquitectura de software e infraestructura para aseguramiento de información y auditorías del sistema PREP para el estado de Guerrero (2021) y el sistema TREP para Guatemala (2023). Participó activamente en la fundación del capítulo OWASP Capítulo León.

Ha impartido materias de corte tecnológico para el Tecnológico de Monterrey como profesor de cátedra desde el 2004, y ha dado clases especiales y talleres de software, inteligencia artificial y ciberseguridad para la UNAM Unidad Morelia, Tecnológico de Saltillo, Gobierno Federal y público en general.



**Auditora:**

**JESSICA IZQUIERDO** estudió Ingeniería en Sistemas Electrónicos y obtuvo el grado de Maestra en Ciencias en Ing. Eléctrica con especialidad en Telecomunicaciones por el Tecnológico de Monterrey, Campus Monterrey. Cuenta con 18 años de experiencia docente en los departamentos de Computación, Mecatrónica y Eléctrica en el sistema TEC incluyendo campus Saltillo, Monterrey, Puebla, Tampico y Chihuahua, con diferentes esquemas de enseñanza (presencial, híbrido, FIT).

Actualmente es Directora de la Maestría de Ciberseguridad en el Tec de Monterrey, campus Monterrey, Coordinadora y líder académica de la concentración de ciberseguridad para los estudiantes de profesional que toman la especialización.

Jessica ha coordinado iniciativas académicas en el ámbito de Internet de las cosas con socio-formadores como TERNIUM y CYDSA. Ha participado como experta en la iniciativa Nuevo León 4.0. Ha representado al Tecnológico de Monterrey en procesos de auditoría de infraestructura y ciberseguridad en las elecciones de Coahuila (sistema PREP 2018), elecciones en el estado de Veracruz (sistema PREP y sistema de cómputo final, 2021).

Tiene más de 20 años de experiencia en la industria, cuenta con certificaciones nivel “Associate” e “Instructor” en Redes, seguridad y domótica. Es consultora independiente desde el año 2018 brindando servicios de redes y ciberseguridad a empresas de FEMSA comercio.

Ha recibido reconocimientos de instructora de excelencia por Cisco Systems, vitalidad intelectual, mejor profesora evaluada, círculo de profesores destacados y profesores que dejan huella por el Tec de Monterrey. En el área de vinculación con empresas ha trabajado en el diseño, coordinación e impartición de cursos y consultoría a empresas en el área de ciberseguridad y automatización con redes industriales. Ha participado como organizadora, maestra de ceremonias y ponente/panelista en congresos y concursos regionales y nacionales que abordan temáticas en el área de ciberseguridad.



**Líder Técnico Nacional:**

**HUGO NAVARRO ESPÍNOLA** es Ingeniero Industrial con más de 25 años de experiencia en Tecnologías de la Información, cuenta con una Maestría en Ingeniería de Sistemas Electrónicos y Computacionales, además está diplomado en Gobierno Electrónico para la Competitividad y el Desarrollo por el Instituto Tecnológico y de Estudios Superiores de Monterrey.

Fue Director General de Sistemas de Información de la Secretaría Particular del C. Gobernador del Estado de Guanajuato, Director General de Tecnologías de la Información del Gobierno del Estado de Guanajuato, Director de Innovación y Desarrollo de la empresa KSP Technology, además de impartir por varios años la asignatura de “Seguridad, Integridad y Protección de Datos” en la Maestría en Administración de Redes y Telecomunicaciones, y Especialidad en Redes y Telecomunicaciones en la Universidad de León. Ha impartido diversos cursos de Ciberseguridad en el sector Financiero, empresas y Gobierno, además de participar en entrevistas para diversos medios de comunicación locales y nacionales e impartir conferencias en diferentes universidades. Es Perito autorizado por el Poder Judicial del Estado de Guanajuato en redes de computadoras, cómputo forense, ciberseguridad, seguridad de la información y audio forense.

Desde hace varios años cuenta con las certificaciones en Seguridad de la Información y Tecnologías de la Información más reconocidas a nivel internacional, tales como:

- CERTIFIED ETHICAL HACKER otorgada por el International Council of Electronic Commerce Consultants.
- COMPUTER HACKING FORENSIC INVESTIGATOR otorgada por el International Council of Electronic Commerce Consultants.
- CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL otorgada por el International Information Systems Security Certification Consortium.
- CERTIFIED INFORMATION SYSTEMS AUDITOR otorgada por la Information Systems Audit and Control Association.
- CERTIFIED INFORMATION SECURITY MANAGER otorgada por la Information Systems Audit and Control Association.
- ITIL OPERATIONAL SUPPORT & ANALYSIS otorgada por la Office of Government Commerce (United Kingdom).
- ITIL FOUNDATIONS otorgada por la Office of Government Commerce (United Kingdom).

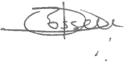
Además, es miembro activo de las siguientes organizaciones:

- Miembro representante de México en el Global Advisory Board del EC-Council para la certificación Computer Hacking Forensic Investigator.
- International Information Systems Security Certification Consortium.
- Information Systems Audit and Control Association.



- International Council of Electronic Commerce Consultants.
- Grupo Examinadores Forenses de Alta Tecnología.

Es consultor del Tec con el que ha participado en la auditoría del Sistema PREP del Instituto Electoral de Participación Ciudadana de Chiapas para el proceso electoral de 2021.



**Auditor:****LCP y MBA Gabriela Reynaga Vargas****CRISC, CISA, CDPSE, GRCP, COBIT 5 & COBIT 2019 Accredited Trainer,  
LA ISO 37001:2016 SGAS, LI ISO/IEC 27001:2022 SGSI**


Gabriela es auditoría y consultoría en Gobierno Riesgo y Cumplimiento para las Tecnologías de la Información. Cuenta con 20+ años de experiencia en temas gobernanza de ciberseguridad, gestión de riesgos, control interno para tecnologías de información (IT) y tecnologías de operación (OT)

Desde 2020 es profesora del Instituto Tecnológico de Monterrey en la Maestría de Ciberseguridad, conferencista internacional, consejera y miembro de comités de auditoría, finanzas, riesgos y tecnologías de información con un enfoque en ciberseguridad.

En 2013 desarrolló la metodología para auditoría de gobernanza de ciberseguridad de sistemas de control industrial para infraestructuras críticas que ha aplicado ya en diferentes países y diferentes sectores.

Ha participado en diversas organizaciones para fortalecer las capacidades de los profesionales de las TIC's como:

- Board Member de ISACA 2018-2019, 2019-2020
- Member of the Advisory Board of the GFCE (The Global Forum on Cyber Expertise) 2018-2020
- Presidente de ISACA Capítulo Guadalajara 2015-2018
- Presidente de la Comisión de TI de la Vicepresidencia del Sector Gubernamental del IMCP 2017-2019
- ISACA Evangelist desde 2022
- Miembro del Comité Estratégico para Latinoamérica ISACA desde 2022



**Auditor:**

**JORGE RODRIGUEZ RUIZ** es originario de Tabasco, México. Recibió la Licenciatura en Sistemas Computacionales y Doctorado en Ciencias de la Ingeniería del Tecnológico de Monterrey, Campus Estado de México en 2011 y 2018 respectivamente. Actualmente es el director nacional de la maestría en ciberseguridad del Tecnológico de Monterrey.

De 2012 a 2014 fue asistente de investigación para HP Labs, trabajando en el desarrollo y aseguramiento de plataformas de analítica de negocios e inteligencia artificial en la nube. Posteriormente, en 2015 participo como profesor en materias como sistemas operativos y seguridad informática en el Tecnológico de Monterrey. A partir de 2020, es el director nacional de la maestría en ciberseguridad. Adicionalmente, es profesor del departamento de computación en campus Santa Fe, miembro del claustro del Doctorado de Ciencias Computacionales, miembro adscrito del grupo de investigación enfocado en inteligencia artificial avanzada. Jorge Rodríguez pertenece al sistema nacional de investigadores con nivel 1, miembro del comité de seguridad en tecnologías de la información de la cámara de la industria de exportación INDEX y miembro de la academia mexicana de computación. Ha participado anteriormente en 2 auditorías del sistema PREP.



**Auditor:**

**GUALBERTO AGUILAR-TORRES** nació en la ciudad de México. Realizó sus estudios de ingeniería en comunicaciones y electrónica, maestría en microelectrónica y doctorado en comunicaciones y electrónica en el Instituto Politécnico Nacional, en 2003, 2005 y 2008 respectivamente. Desde 2019 es profesor de planta en el departamento de computación del Tecnológico de Monterrey campus Santa Fe, donde participa como profesor de licenciatura y posgrado. Cuenta con experiencia en Ciberseguridad, en procesos de investigación, manejo de estrategia y gestión de la información.

Ha participado como líder en el desarrollo de proyectos para aplicaciones forenses. Ha colaborado en materia de combate y persecución de ciberdelitos como robo de información, fraude, amenazas cibernéticas, extorsiones, entre otros. Cuenta con conocimientos en cadena de custodia, algoritmos criptográficos, certificados digitales, así como en servicios preventivos y correctivos en la comisión de delitos informáticos. Ha participado como profesor en distintas universidades públicas y privadas en México.

Tiene más de 30 publicaciones en revistas arbitradas, ha participado en distintos congresos a nivel nacional e internacional, ha sido director de tesis de licenciatura, maestría y doctorado. Cuenta con una patente en reconocimiento de placas y más de 20 registros de software. Ha sido distinguido con el nivel 1 del sistema nacional de investigadores por más de 7 años. Sus intereses de investigación se encuentran en los temas de ciberseguridad, procesamiento de señales y biometría.

El Dr. Aguilar Torres ha participado en proyectos para instituciones federales y estatales como RENAPO, INE, SEDENA, POLICÍA FEDERAL, IEPC GUERRERO, SECRETARÍA DE SEGURIDAD CIUDADANA – QUERÉTARO, entre otras más, donde ha colaborado como líder, instructor, coordinador o auditor.

Ha participado anteriormente en la auditorías del sistema PREP de Guerrero.

**Auditor:**

**AGUSTÍN DOMINGUEZ OVIEDO** estudió Ingeniería en Electrónica y Comunicaciones en el Tec de Monterrey Campus Querétaro, además de una Maestría en Ciencias en Sistemas Electrónicos en el Tec de Monterrey Campus Toluca. Cuenta con un Doctorado en Ingeniería Eléctrica y Computación por la Universidad de Waterloo en Ontario, Canadá. El título de la tesis doctoral es “On Fault-based Attacks and Countermeasures for Elliptic Curve Cryptosystems”. En este trabajo se realizaron experimentos en hardware, en específico con FPGAs (Field Programable Gate

Arrays) de sistemas propuestos que permiten detectar errores en el cómputo de multiplicación escalar basado en curvas elípticas. En el área de criptografía la detección de errores es fundamental desde el punto de vista de seguridad. Es por ello que se realizaron experimentos físicos en circuitos para probar de manera práctica que los sistemas propuestos en la tesis doctoral permiten detectar errores con una muy alta probabilidad.

En el Tec de Monterrey Campus Querétaro es Profesor en el Departamento de Computación y Mecatrónica desde 1997, Director Académico de las Carreras de Ingeniería Electrónica (ITE e ISD) de 2008 a 2016 y de 2018 al 2020. De diciembre de 2020 a la fecha, funge como Director de Departamento Regional del Departamento de Computación en la Región Centro Sur (que integra los Campus Querétaro, Puebla, Cuernavaca, Hidalgo y Tampico).

El Dr. Domínguez escribe y enseña en los ámbitos de Ingeniería Electrónica en las áreas de seguridad de hardware y sistemas digitales. Ha sido supervisor y dado consultoría en proyectos de diseño electrónico con la industria, algunos ejemplos destacados son un administrador telefónico Adtel en la empresa Vantec (1996), programador de microcontroladores ProFlash89 para Valutbbs Inc. (1999), monitor remoto de refrigeradores Mabe (2001), y maqueta interactiva de densidad de población para el Municipio de Querétaro (2017-2018). Fue Borrego de Oro y Profesor Inspirador Campus Querétaro en 2011 y 2019 respectivamente.

**Auditor:**

**JOSÉ MANUEL CÓRDOVA VILLANUEVA** es Ingeniero en Electrónica y de comunicaciones, con cédula profesional número 23168802, maestro en Ingeniería de calidad con cédula 7328331, expedidas por la Secretaría de Educación Pública, con 36 años de experiencia en el área de tecnologías de la información, como desarrollador de software, administrador de redes de computadoras, equipos activos y pasivos, como conmutadores de datos (switches) encaminadores (routers), conmutadores de voz, GrandStream, Alcatel-Lucent, LG-Nortel, ex instructor de Cisco CCNA Academy Connection ID 3712668, administrador de servidores linux, Netware, Windows, True64.

Administrador de tecnologías de la Información en diversas organizaciones como la Universidad Iberoamericana León (Jefe de la oficina de Servicios de Tecnologías de Información y Comunicación) y varias empresas, implementador de sistemas administrativos complejos como los ERP y de administración de los clientes como CRM, fui miembro suplente del Consejo Técnico del Proyecto de Laboratorio de Desarrollo y Pruebas de software del Estado de Guanajuato en el CONCYTEG.

Coordinador de los diplomados de “Redes de cómputo” y “Estrategias de seguridad informática” así como instructor del diplomado en “Hackeo Ético” impartidos en la Universidad Iberoamericana León, catedrático de diversas asignaturas en el rubro de las tecnologías de información y comunicación en la Universidad Iberoamericana León y la Universidad de León en la maestría en “Redes de computadoras”, habiéndome certificado en instalación, configuración y administración de servidores de correo electrónico del fabricante Microsoft.

Perito autorizado #430 en el Poder Judicial del Estado de Guanajuato en Redes de Computadoras, Cómputo Forense.

**Auditor:**

**MARCO ANTONIO GONZÁLEZ GALICIA** MSc., CISSP, CCNP R&S, CCNA Cyberops, CCSI

Ingeniero en Electrónica y Comunicaciones, egresado del ITESM. Estudió la Maestría en Ciencias con especialidad en Telecomunicaciones en la Universidad de Mánchester, Reino Unido. Es profesor del Departamento de Computación del ITESM – Campus Estado de México.

Es socio Director de Mavixel Systems ([www.mavixel.com](http://www.mavixel.com)) y se dedica a actividades de consultoría y capacitación en las área de ciberseguridad e infraestructura de redes y telecomunicaciones. Ha realizado auditorías de seguridad y desempeño así como instalación de infraestructura de seguridad y redes para organizaciones públicas y privadas de todos los tamaños.

Es instructor certificado de Cisco Systems (CCSI) y cuenta con certificaciones tales como CCNA Cyberops, CCNA Security y CCNP Routing and Switching. Sus áreas de especialidad son: ciberseguridad, redes de datos, redes inalámbricas, Voz sobre IP y el análisis y validación de diseños de redes. Es profesional certificado en seguridad informática (CISSP). Ha impartido clases para el Instituto Nacional de Telecomunicaciones (INT) en París, Francia y para la Universidad de Guayaquil en Guayaquil, Ecuador. Desde 1993 y hasta la fecha se ha desempeñado como profesor del ITESM en diferentes modalidades para los Campus Estado de México, Santa Fé, Hidalgo, Cd. de México, Guadalajara, Monterrey, León y Morelia. Del 2008 al 2019 impartió cursos de capacitación para el Instituto Tecnológico de Teléfonos de México (Inttelmex). Participa activamente en los servicios de actualización profesional y asesoría de Mavixel ([www.mavixel.com](http://www.mavixel.com)).



**Auditora:**

**GABRIELA AZUCENA CAMPOS GARCÍA** estudió Ingeniería en Electrónica y Comunicaciones en el Tec de Monterrey Campus Estado de México, además de una Maestría en Ciencias Computacionales con especialidad en Redes de Computadoras.

Desde agosto del 2000 es profesor de planta en el ITESM-CEM impartiendo clases en el área de Lenguajes de Programación, Redes Computacionales y Analítica de Datos.

Ha participado como líder nacional en el diseño de las materias de Implementación de redes de área amplia y servicios distribuidos y Pensamiento computacional para la ingeniería y los negocios.

Es miembro del comité de los programas de Instructores de CISCO y Patrones Hermosos.

Ha realizado consultoría en el área de redes en diversas instituciones como: NBA, CONALEP, PEMEX, BBVA y además ha participado anteriormente como auditora del sistema del PREP del Estado de Veracruz y apoyando la auditoría de Chiapas y Tlaxcala.

Cuenta con las siguientes certificaciones: CCNA Instructor Trainer Qualification, CCNA Routing & Switching, SAS Educator y Google Cloud Professor Facilitator.



**Auditor:**

**RAFAEL EMILIO DÁVALOS VILLARREAL** originario de Monclova Coahuila. Se recibió de Ingeniero en Sistemas Electrónicos con Mención Honorífica y Mejor promedio de su generación en el Tecnológico de Monterrey, Campus Monterrey. Cursó la Maestría en Ciencias, especialidad Ciencias Computacionales en el mismo Instituto.

Actualmente es Director de Entrada de la Avenida de Computación ICT (Ingeniero en Computación y Tecnologías de Información) y Profesor del Departamento de Computación impartiendo cursos de Redes, Ciberseguridad e Internet de las Cosas entre otros cursos.

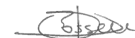
Su trayectoria incluye las áreas de Soporte Técnico, Redes, Seguridad y Desarrollo de aplicaciones en Vitro. Ventas de servidores IBM y HP en Migesa. Educación y procesos de innovación educativa en el Tecnológico de Monterrey, así como experiencia emprendedora en el ramo de la joyería.

Profesor fundador del grupo estudiantil Cybersecurity Tec en el Tecnológico de Monterrey. Ha recibido cursos de ciberseguridad desde 2018 incluyendo preparación para CISSP, Creación de Investigación, Análisis, Administración de Incidentes de Ciberseguridad, CyberOps Associate de Cisco, y otros.

Ha participado en varios eventos relacionados a la Ciberseguridad entre ellos: La importancia de entender la CyberSeguridad para el Centro Virtual de Aprendizaje del Tec de Monterrey, Ciberseguridad, ¿Porqué es tan peligroso el Phishing? Ceddie, Ciberseguridad y el phishing de SecurityCon.

Participó en la Auditoría del INE por parte del Tecnológico de Monterrey en Junio de 2021 revisando los documentos de Auditoría de varios Estados de la República Mexicana.

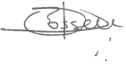
Ha recibido diferentes reconocimientos como Profesor Inspirador (2018), Profesor Dejando Huella (2023), Múltiples reconocimientos entre ellos: Encuesta ECAG (graduandos), ECOA (alumno de clases), Ha sido reconocido como el profesor favorito de varias generaciones de alumnos INT (2 veces), ITI (2 veces), ITC (3 veces). Y otros reconocimientos académicos.



**Auditor:**

**RAIME ALEJANDRO BUSTOS GARDEA** nació en Chihuahua, Chihuahua, México. Recibió Ingeniería en Electrónica por el Tecnológico de Chihuahua en 1994, Maestría en Sistemas Electrónicos con Especialidad de Telecomunicaciones por el Tecnológico de Monterrey en 1997. Actualmente es Director del Programa de Ingeniería en Tecnologías Computacionales en el Tec de Monterrey, campus Chihuahua y forma parte del claustro de la Maestría en Ciberseguridad del Tec de Monterrey.

Actualmente es líder 3 proyectos nacionales de inteligencia artificial aplicada y de innovación educativa dentro del Tecnológico de Monterrey. Tiene 25 años de experiencia en el área docente y Tecnologías de Información, ha liderado proyectos de innovación tecnológica para compañías como Santander, RICOH, Rosslare Security y Salto Systems, en Mexico, Colombia, Chile, Brasil, España y Estados Unidos. Ha representado al Tecnológico de Monterrey en el proceso de auditoría de infraestructura y ciberseguridad en las elecciones de Sinaloa (sistema PREP y sistema de cómputo final, 2021).



Raime ha recibido reconocimientos por excelente labor como profesor, entre ellos al profesor mejor evaluado por los estudiantes, círculo de profesores destacados y el reconocimiento de profesores que dejan huella por el Tec de Monterrey.



**Auditor:**

**PABLO GUTIÉRREZ SALAZAR** es un empresario regiomontano y especialista en ciberseguridad, Pablo Gutiérrez Salazar se ha distinguido por su participación en múltiples iniciativas como experto en estrategias de ciberseguridad y seguridad de la información. Fundador y Director General de WhiteSuit Hacking desde 2014, su liderazgo ha sido crucial en el establecimiento y crecimiento de la empresa.

Es consultor del Tecnológico de Monterrey, y ha participado en diferentes proyectos entre ellos participó como auditor del sistema PREP en las elecciones del 2021.

En 2016, Gutiérrez Salazar fue el cerebro detrás del diseño de la certificación G.H.O.S.T. (Grey Hat Offensive Security Technician), una referencia en la industria de la ciberseguridad, que ha graduado a más de 16,000 profesionales. Esta certificación es un testimonio de su compromiso con la formación de expertos calificados y su influencia en el campo de la ciberseguridad.

En 2019, amplió su contribución al campo con la publicación de su libro "Hacker's WhiteBook: Como convertirte en un hacker profesional", una obra que profundiza en el hacking ético y las metodologías de ciberseguridad. Además, ha obtenido la certificación CEH (Certified Ethical Hacker), reafirmando su expertise y dedicación al campo.

Bajo su dirección, WhiteSuit Hacking ha implementado estrategias de ciberseguridad en una amplia gama de entidades, incluyendo empresas nacionales e internacionales, así como organismos gubernamentales. Estas implementaciones destacan su capacidad para navegar y proteger a organizaciones en un entorno digital cada vez más complejo.

Actualmente, Pablo Gutiérrez Salazar ejerce un rol clave como presidente de la Comisión de Ciberseguridad de la Asociación Mexicana de Empresas de Seguridad Privada (AMESP). En este puesto, continúa su labor de promover prácticas de ciberseguridad seguras y efectivas, marcando una diferencia significativa en la industria de la seguridad privada en México.

En resumen, Pablo Gutiérrez Salazar es un empresario con visión, un especialista en ciberseguridad con una trayectoria notable, y un educador comprometido, cuyo trabajo ha influenciado profundamente el campo de la ciberseguridad en México y más allá. Su liderazgo, conocimiento y dedicación a la excelencia han establecido nuevos estándares en la industria.

**Auditor:**

**LUIS ROBERTO DE LEÓN ELIZONDO** nacido en Monterrey, Nuevo León, Luis Roberto De León Elizondo es reconocido por su sólida formación académica en Tecnologías de Información, obtenida en la Universidad Autónoma de Nuevo León. Esta formación fue el inicio de su destacada carrera en el ámbito de la ciberseguridad y la protección de datos.

Es consultor del Tecnológico de Monterrey en materia de Ciberseguridad, en el que ha contribuido a la integridad de procesos electorales en México, participando en la auditoría del sistema PREP en las elecciones 2021, reflejando su compromiso con la transparencia y seguridad en el ámbito político.

Además es Director de Operaciones en White Suit Hacking, liderando equipos y colaborando con organizaciones para mitigar su exposición a ciberamenazas, crucial en la prevención de pérdidas monetarias significativas. Su vasta experiencia y conocimiento en ciberseguridad son valiosos para empresas en un contexto digital desafiante.

Elizondo también ha participado en proyectos enfocados en normativas y estándares de seguridad, mostrando su compromiso con la adhesión a prácticas de seguridad óptimas en la industria.

Elizondo también ha dejado su marca como autor, escribiendo el libro "Hacker's Purplebook", donde expone metodologías de equipos rojos, enfocadas en ataques y auditorías informáticas, y de equipos azules, dedicadas a la defensa informática. Esta obra destaca su profundo entendimiento tanto de tácticas ofensivas como defensivas en el campo de la ciberseguridad.

En resumen, Luis Roberto De León Elizondo es un experto en ciberseguridad, un educador inspirador y un autor influyente, que ha dejado una huella significativa en su campo y ha contribuido enormemente a la formación de futuros profesionales en seguridad de la información. Su dedicación a la seguridad, ética y excelencia académica lo convierte en un referente clave en su área de especialización.

**Auditor:**

**JOSÉ LUIS GÓMEZ TREVIÑO** graduado en Tecnologías de la Información por la Universidad Autónoma de Nuevo León, José Luis Gómez Treviño se ha establecido como un profesional destacado en el ámbito de la ciberseguridad. Con más de siete años de experiencia en desarrollo de software y una especialización en seguridad ofensiva y defensiva, ha logrado certificarse en desarrollo seguro, lo que subraya su compromiso con la creación de soluciones tecnológicas seguras y confiables.

Actualmente, Jorge actualmente es consultor del Tecnológico de Monterrey y aplica su vasta experiencia y conocimiento como consultor de seguridad informática en WhiteSuit Hacking. En esta posición, juega un rol crucial en la implementación de estrategias innovadoras de ciberseguridad. Su trabajo se enfoca en fortalecer las defensas cibernéticas de los sistemas, mitigando riesgos y asegurando la protección integral de la información.

El enfoque de José Luis en seguridad cibernética no solo abarca la prevención y defensa contra ataques externos, sino también el desarrollo proactivo de sistemas y software que resistan intrusiones. Su habilidad para combinar experiencia en desarrollo de software con especialización en ciberseguridad lo posiciona como un experto en la creación de soluciones integrales de seguridad.

En resumen, José Luis Gómez Treviño es un profesional íntegro y altamente capacitado en el campo de la ciberseguridad. Su enfoque innovador y su experiencia en el desarrollo de software seguro hacen de él un recurso invaluable en la lucha contra las amenazas cibernéticas y en la protección de sistemas críticos. Su trayectoria demuestra un compromiso constante con la mejora de la seguridad informática y la protección de datos en un mundo digitalmente conectado.


**Auditor:**

**JORGE RODRIGO TORRES OCHOA** originario de Monterrey, Nuevo León, Jorge Rodrigo Torres Ochoa es un profesional distinguido en el campo de la ciberseguridad. Su formación académica se centra en la Licenciatura en Seguridad en Tecnologías de la Información, obtenida en la Facultad de Ciencias Físico Matemáticas de la Universidad Autónoma de Nuevo León.

Jorge actualmente es consultor del Tecnológico de Monterrey y ejerce como analista de ciberseguridad en White Suit Hacking, donde su trabajo abarca una variedad de áreas críticas en ciberseguridad, incluyendo consultoría, capacitación, pruebas de penetración y análisis de SOC (Security Operations Center). Su especialización en la implementación de controles CIS (Center for Internet Security) subraya su competencia en fortalecer las defensas cibernéticas y mejorar las prácticas de seguridad.

Con una carrera centrada en la seguridad ofensiva, Jorge se dedica a identificar vulnerabilidades y debilidades en los sistemas informáticos de empresas y organizaciones. Su participación en diversas pruebas de penetración resalta su habilidad para descubrir y mitigar posibles riesgos de seguridad.

Más allá de su rol en White Suit Hacking, Torres Ochoa ha llevado a cabo investigaciones sobre la concienciación en seguridad cibernética del público general, demostrando su compromiso con la educación y la sensibilización en esta área..

En su trayectoria profesional, Torres Ochoa ha abarcado áreas como programación, soporte técnico, seguridad, redes y competencias de CTF (Capture The Flag), lo que demuestra su amplio conocimiento y experiencia práctica en diversos aspectos de la tecnología y la ciberseguridad.


En conclusión, Jorge es un analista de ciberseguridad con una sólida base académica y una amplia experiencia práctica. Su enfoque en la seguridad ofensiva y su habilidad para identificar y contrarrestar amenazas cibernéticas lo convierten en un valioso activo en el campo de la ciberseguridad. Su compromiso con la mejora continua y su enfoque práctico en la resolución de problemas de seguridad lo distinguen como un profesional competente y confiable en su área de especialización.

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

15 de Enero de 2024, Monterrey, N.L.

**MTRA. LUZ FABIOLA MATILDES GAMA  
PRESIDENTA  
INSTITUTO ELECTORAL Y DE PARTICIPACIÓN  
CIUDADANA  
DEL ESTADO DE GUERRERO  
P R E S E N T E.-**

El suscrito **Pablo de la Peña Sánchez**, en nombre y representación del **Instituto Tecnológico y de Estudios Superiores de Monterrey**, vengo manifestando bajo protesta de decir verdad que Institución que represento cuenta con la capacidad técnica, financiera y operativa para la ejecución de la “SERVICIO DE AUDITORÍA DE INFRAESTRUCTURA TECNOLÓGICA Y SISTEMA INFORMÁTICO DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES (PREP) PARA LAS ELECCIONES DE 2024” a cargo del Instituto Electoral y de Participación Ciudadana del Estado de Guerrero (IEPC).



**Dr. Pablo de la Peña Sánchez**  
**Apoderado Legal**  
**INSTITUTO TECNOLÓGICO Y DE ESTUDIOS**  
**SUPERIORES DE MONTERREY**

c.c.p.- Mtra. Ileana Beatriz Rossell González, Decana Asociada de Educación Continua, Escuela de Ciencias Sociales y Gobierno del Tecnológico de Monterrey -Para conocimiento.  
c.c.p.- Dr. Juan Arturo Nolasco Flores, Director del Hub de Datos del Tecnológico de Monterrey -Para conocimiento.  
c.c.p.- Mtro. Jaime Rangel Mancha, Coordinador de Gestión de Proyectos de Educación Continua de la Escuela de Gobierno y Transformación Pública & de la Escuela de Ciencias Sociales y Gobierno del Tecnológico de Monterrey -Para conocimiento.

## 11 Cartas de referencia y certificados

Con base a nuestra experiencia con otros institutos electorales estatales como referencia se encuentran:

**Ing. Jorge Gallegos Valdés**

Director Ejecutivo de Innovación Electoral

Instituto Electoral de Coahuila

+52 (844) 438-62-60 Ext. 142

[jorge.gallegos@iec.org.mx](mailto:jorge.gallegos@iec.org.mx)

[www.iec.org.mx](http://www.iec.org.mx)

**Ing. César Rolando Romero González**

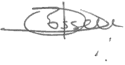
Unidad de Tecnología y Sistemas

Comisión Estatal Electoral de Nuevo León

+528112331543, +528112331571, +528180234921

[crromero@ceenl.mx](mailto:crromero@ceenl.mx)

[www.ceenl.mx](http://www.ceenl.mx)







12 de febrero de 2021, Monterrey, Nuevo León

A QUIEN CORRESPONDA.  
P R E S E N T E -

Por medio del presente hago de su conocimiento que el Instituto Tecnológico y de Estudios Superiores de Monterrey, ha colaborado como ente Auditor del sistema informático e infraestructura tecnología del PREP en varios procesos electorales que se detallan a continuación:


- 2018:
  - Elecciones Ordinarias-Comisión Estatal Electoral (CEE) de Nuevo León
  - Elecciones Extraordinarias-Comisión Estatal Electoral (CEE) de Nuevo León

Los alcances de las Auditorías de Seguridad Informática han sido los siguientes:

- Análisis a caja negra del sistema PREP
- Análisis de la Base de datos
- Vulnerabilidades infraestructura
- Pruebas de penetración

De igual forma confirmamos que todas estas auditorías las han realizado en estricto apego y cumplimiento a los Requisitos mínimos del Instituto Nacional Electoral (INE) para la contratación de servicios de auditoría al sistema informático e infraestructura tecnología del PREP.

Atentamente,

  
Ing. César Rolando Romero González  
Unidad de Tecnología y Sistemas  
Comisión Estatal Electoral de Nuevo León  
+528112331543, +528112331571, +528180234921  
[crromero@ceenl.mx](mailto:crromero@ceenl.mx)  
[www.ceenl.mx](http://www.ceenl.mx)

5 de Mayo 975 oriente, Centro,  
64000, Monterrey, Nuevo León México  
Teléfono: 81 1233 1515 [www.ceenl.mx](http://www.ceenl.mx)



12 de febrero de 2021, Saltillo, Coahuila de Zaragoza

**A QUIEN CORRESPONDA.  
PRESENTE -**

Por medio del presente hago de su conocimiento que el **Instituto Tecnológico y de Estudios Superiores de Monterrey**, ha colaborado como **ente Auditor del sistema informático e infraestructura tecnología del PREP** en varios procesos electorales que se detallan a continuación:

- 2017:
  - Elecciones Ordinarias - Gobernadora/Gobernador, Diputaciones Locales y Ayuntamientos
- 2018:
  - Elecciones Ordinarias- Ayuntamientos
- 2020:
  - Elecciones Ordinarias- Diputaciones Locales

Los alcances de las Auditorías de Seguridad Informática han sido los siguientes:

- Análisis a caja negra del sistema PREP
- Análisis de la Base de datos
- Vulnerabilidades infraestructura
- Pruebas de penetración

De igual forma confirmamos que todas estas auditorías las han realizado en estricto apego y cumplimiento a los Requisitos mínimos del Instituto Nacional Electoral (INE) para la contratación de servicios de auditoría al sistema informático e infraestructura tecnología del PREP.

Atentamente,



**Ing. Jorge Gallegos Valdés**  
Director Ejecutivo de Innovación Electoral  
Instituto Electoral de Coahuila  
(844) 438-62-60 Ext. 142  
jorge.gallegos@iec.org.mx  
www.iec.org.mx



Bldv. Luis Donaldo Colosio No. 6207, Fracc. Rancho La Torreclilla, C.P. 25298 Saltillo, Coahuila. Tel. (844) 438 62 60

**SEGOB**  
SECRETARÍA DE GOBERNACIÓNSubsecretaría de Población, Migración y Asuntos Religiosos  
Dirección General del Registro Nacional de Población e Identificación Personal  
Dirección General Adjunta Técnica  
Dirección de Infraestructura

México, D.F., 21 de enero de 2013

A quien corresponda:

Por medio de la presente se hace constar que el Dr. Juan Arturo Nolasco Flores es el responsable por parte del Tecnológico de Monterrey, Campus Monterrey, del proyecto "ANÁLISIS Y VERIFICACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 2012" que se desarrolló desde el 25 de mayo al 31 de diciembre del 2012; y que como parte del equipo de trabajo también participó el MSc. Renán Rafael Silva Rubio.

Este proyecto de alto impacto es parte del proceso Integral de Seguridad de la Información que se encuentra implementado en el Registro Nacional de Población e Identificación Personal, y es para garantizar la confidencialidad, integridad y disponibilidad de la información relativa al Registro de Menores.

El proyecto estuvo formado por los siguientes tres subproyectos: Análisis y Verificación del Hackeo Ético por una tercera entidad; verificación y desarrollo de procesos de Seguridad de la Información; y propuesta de Evaluación de Riesgos. En el equipo de trabajo también participó el MSc. Renán Rafael Silva Rubio.

Los objetivos principales del proyecto fueron:

- Analizar la metodología actual de Hackeo Ético, con el propósito de encontrar deficiencias y posteriormente proponer una metodología alterna con mejores características.
- Presentar una solución para el Control y Administración de usuarios privilegiados.
- Presentar una solución para la Verificación de uso de bases de datos, archivos críticos y bitácoras.
- Presentar una solución para la Verificación del Monitoreo de Integridad de bases de datos, archivos críticos y bitácoras.
- Presentar una metodología para Evaluación de Riesgos.

Sin más por el momento quedo a sus órdenes para ampliar la información aquí proporcionada o aclarar cualquier duda.

Atentamente

El Director de Infraestructura

  
Lic. Luis Antonio Calderón DamiánAv. Paseo de la Reforma No. 99, piso 15, Col. Tabacalera, C.P. 06030, Delegación Cuauhtémoc, México, D.F.  
Tel.: (55) 5128-0000 ext. 11552 www.rnapi.gob.mx

**Dirección General del Registro Nacional de Población  
e Identificación Personal**

**Dirección de Infraestructura**



SECRETARÍA  
DE GOBERNACIÓN

**SEGOB**

México, D.F., 20 de septiembre de 2012

A quien corresponda:

Por medio de la presente se hace constar que el Dr. Juan Arturo Nolasco Flores es el responsable por parte del Tecnológico de Monterrey, Campus Monterrey, del proyecto "Revisión de Hackeo Ético" y que como parte de equipo de trabajo también participó el MSc. Renán Rafael Silva Rubio.

El proyecto "Revisión de Hackeo Ético" es un proyecto de alto impacto que forma parte del proceso Integral de Seguridad de la Información que se encuentra implementado en el Registro Nacional de Población e Identificación Personal, para garantizar la confidencialidad, integridad y disponibilidad de la información relativa al Registro de Menores.

El objetivo principal del proyecto fue analizar los resultados y conclusiones del Hackeo Ético realizado por el proveedor que opera el Servicio Nacional de Identificación Personal a la infraestructura de captura, procesamiento y almacenamiento de información del Registro Nacional de Población e Identificación Personal.

El alcance de la revisión consideró la etapa de Análisis de Vulnerabilidades y las Pruebas de Penetración; así como los procesos de Seguridad de esta Dirección General. Al finalizar el proyecto, se recibieron los comentarios y sugerencias que han contribuido a mejorar las políticas de seguridad de la Institución.

Sin más por el momento quedo a sus órdenes para ampliar la información aquí proporcionada o aclarar cualquier duda.

**Atentamente**

**El Director de Infraestructura**

  
**Lic. Luis Antonio Calderón Damián**

Av. Paseo de la Reforma # 99, piso 18, Col. Tabacalera, Del. Cuauhtémoc, México, D.F., C.P. 06030  
t. 51-28-00-00 ext. 11552 e-mail: lcalderond@segob.gob.mx










*[Signature]*

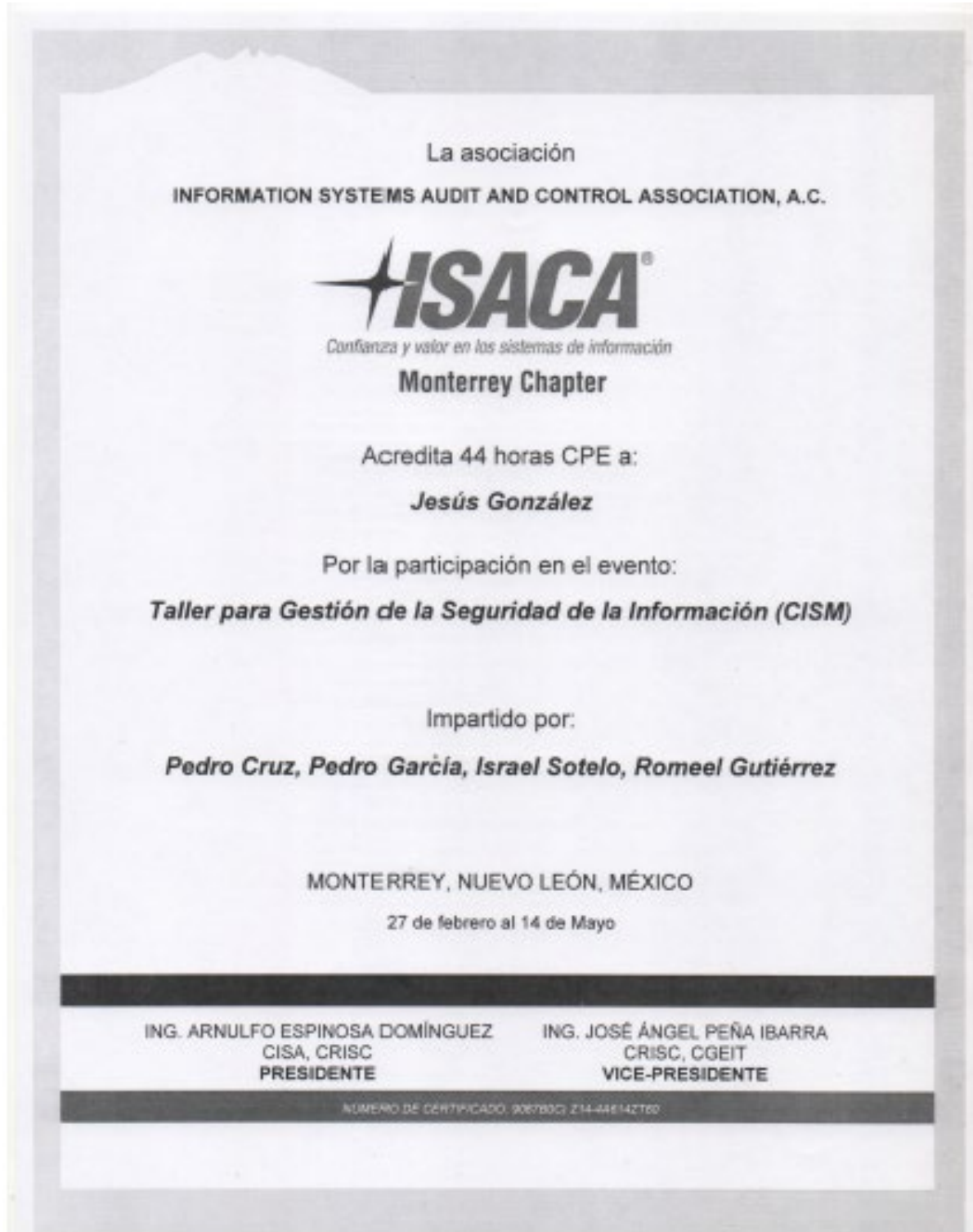
*[Signature]*



*Base*

*Jesus Raul Gonzalez Hernandez*












Sin más por el momento, quedo a sus órdenes,

Atentamente,

**Mtra. Ileana Beatriz Rossell González**  
**Decana Asociada de Educación Continua**  
**Escuela de Ciencias Sociales y Gobierno**  
**INSTITUTO TECNOLÓGICO Y DE ESTUDIOS**  
**SUPERIORES DE MONTERREY**

**Dr. Pablo de la Peña Sánchez**  
**Apoderado Legal**  
**INSTITUTO TECNOLÓGICO Y DE ESTUDIOS**  
**SUPERIORES DE MONTERREY**

c.c.p.- Dr. Juan Arturo Nolasco Flores, Director del Hub de Datos del Tecnológico de Monterrey -Para conocimiento.

c.c.p.- Mtro. Jaime Rangel Mancha, Coordinador de Gestión de Proyectos de Educación Continua de la Escuela de Gobierno y Transformación Pública & de la Escuela de Ciencias Sociales y Gobierno del Tecnológico de Monterrey -Para conocimiento.