



ENTE AUDITOR DEL SISTEMA INFORMÁTICO DEL PREP

Propuesta Técnica y Económica.

Preparado para:



15 de diciembre de 2023

Contenido

Introducción	4
Situación actual	4
Auditoría Técnica del Sistema Informático del PREP	5
Objetivo	5
Enfoque y Metodología	5
Alcance	6
Actividades	6
Análisis de Activos Externos (desde Internet)	6
Análisis de Activos Internos (red LAN)	7
Duración de Servicio	10
Acerca de la ejecución de actividades	12
Aclaraciones sobre las actividades	13
Herramientas a utilizar	13
Entregables	14
Aclaraciones sobre los entregables	14
Equipo de trabajo	15
Organización del proyecto	15
Capacidad técnica y operativa	15
Propuesta Económica	16
Términos y condiciones del servicio	17
Derechos de autor	17
Sobre licencias	17
Criterios y tiempos de aceptación	17
Anexo I. Modelo de carta de autorización	18

MTRA. LUZ FABIOLA MATILDES GAMA

PRESIDENTA DEL IEPC GUERRERO

PRESENTE.

Estimada Maestra, en atención a su oficio 1448, mediante el cual invita al Instituto Nacional de Administración Pública A.C. (INAP) para participar como ente auditor del sistema informático del PREP para el proceso electoral ordinario 2023-2024, enviamos a usted la propuesta técnico-económica solicitada.

Esperamos que esta propuesta cumpla sus expectativas y aprovechamos la ocasión para saludarle.

ATENTAMENTE



DR. RICARDO CORRAL LUNA

DIRECTOR DEL CENTRO DE CONSULTORÍA

EN ADMINISTRACIÓN PÚBLICA

Y APODERADO LEGAL

Introducción

Dado que el pasado 8 de septiembre del año en curso, dio inicio el Proceso Electoral Ordinario 2023-2024 de Diputaciones Locales y Ayuntamientos del Estado de Guerrero, por lo que el **IEPC Guerrero** se encuentra desarrollando diversas actividades para atender las etapas previas a la Jornada Electoral que se celebrará el 2 de junio de 2024.

Entre estas actividades, se encuentra la relacionada con el Programa de Resultados Electorales Preliminares (PREP), siendo éste un mecanismo de información electoral encargado de proveer los resultados preliminares y no definitivos de las elecciones a través de Internet, desde la misma noche de la Jornada Electoral de cada una de las elecciones que se llevarán a cabo en la entidad, de conformidad con las reglas, lineamientos, criterios y formatos que para tal efecto emita el Instituto Nacional Electoral (INE).

Situación actual

Se requiere de la ejecución de una auditoría técnica del sistema informático que será utilizado en la implementación y operación del PREP, con la finalidad de evaluar la integridad, disponibilidad y seguridad en el procesamiento de la información y la generación de los resultados conforme a la normativa aplicable y vigente.

En este contexto, el procedimiento de auditoría es necesario considerar y ajustarse al Reglamento de Elecciones del INE y el Anexo 13 relativo a los Lineamientos del PREP.

En este sentido y en relación con el sistema informático del PREP, el Reglamento de Elecciones aprobado por el Consejo General del INE, en el Título III, Capítulo II, Sección Cuarta, denominada Sistema informático y su auditoría, artículo 347, establece:

1. El Instituto y los opl deberán someter su sistema informático a una auditoría técnica para lo cual se deberá designar un ente auditor. El alcance de la auditoría deberá cubrir, como mínimo, los puntos siguientes:
 - a. Pruebas funcionales de caja negra al sistema informático para evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares.
 - b. Análisis de vulnerabilidades, considerando al menos pruebas de penetración y revisión de las configuraciones de la infraestructura tecnológica del prep.
2. Para la designación del ente auditor se dará preferencia a instituciones académicas o de investigación y deberá efectuarse a más tardar, cuatro meses antes del día de la Jornada Electoral. El ente auditor deberá contar con experiencia en la aplicación de auditorías con los alcances establecidos en el numeral anterior.
3. La instancia interna responsable de coordinar el desarrollo de las actividades del prep será la encargada de validar el cumplimiento de la experiencia del ente auditor.
4. El ente auditor deberá presentar, previo a su designación, una propuesta técnico-económica que incluya el cronograma de las actividades a realizar y que cumpla con el anexo técnico que para tal efecto se establezca, el cual a su vez deberá considerar los requisitos mínimos establecidos por el Instituto.
5. Posterior a su designación, el ente auditor deberá entregar al Instituto o al opl, según corresponda, la aceptación formal de su designación.
6. El Instituto, a través de la instancia interna, será el encargado de vigilar el cumplimiento por parte del ente auditor, de las disposiciones que rigen al prep, tratándose de elecciones federales, mecanismos de participación ciudadana y aquellas elecciones o prep que corresponda al Instituto llevar a cabo. Lo mismo corresponderá a los opl, a través de la instancia interna, tratándose de elecciones locales y ejercicios de participación ciudadana locales.

Auditoría Técnica del Sistema Informático del PREP

Objetivo

Ejecutar una auditoría técnica del sistema informático que será utilizado en la implementación y operación del PREP, con la finalidad de evaluar la integridad, disponibilidad y seguridad en el procesamiento de la información y la generación de los resultados conforme a la normativa aplicable y vigente.

En este contexto, el procedimiento de auditoría se considerará y ajustará al Reglamento de Elecciones del INE y el Anexo 13 relativo a los Lineamientos del PREP.

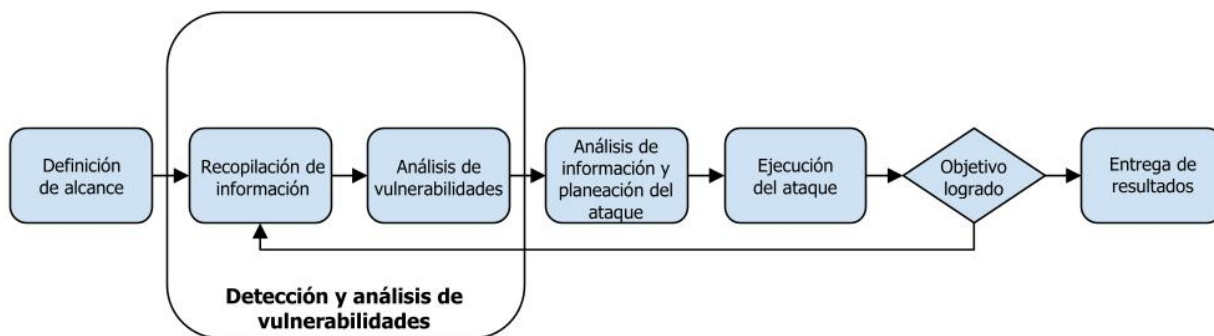
La ejecución de una Auditoría Técnica al Sistema Informático del PREP del **IEPC Guerrero**, *servirá* para su análisis y mejora del nivel de seguridad de la información, los cuales, serán documentados en alcances considerando un Informe Inicial y un Reporte Final, en estos se indicarán los hallazgos y resultados en cada actividad realizada por el Auditor complementando con evidencias y procedimientos realizados, y así, poder establecer medidas adecuadas para su mitigación o sean reducidas a un nivel aceptable con base a las mejores prácticas, estándares y metodologías de seguridad de la información.

Este servicio y sus entregables, brindan conformidad a los controles A.12.6.1, A.18.2.1 y A.18.2.3 del estándar ISO 27001:2013, los requisitos 11.2 y 11.3 de la norma PCI-DSS, controles CA-8 y RA-5 del NIST SP 800-53, el numeral 20.2 del CIS CSC 20, así como al Capítulo III del Anexo 13 Lineamientos del programa de resultados electorales preliminares (Prep).

Enfoque y Metodología

La forma en que se llevarán a cabo las pruebas auditoría técnica de ciberseguridad (Análisis de Vulnerabilidades y/o Pentest), inician por un reconocimiento de infraestructura y de forma coordinada con el **IEPC Guerrero** se procede a realizar la prueba de intrusión y denegación de servicio correspondiente, esto significa que en la ventana de tiempo definida se identificarán y analizarán posibles huecos de seguridad que afecten a la confidencialidad, a la integridad y a la disponibilidad, los cuales se intentarán explotar, para que de esta forma se presenten las evidencias y los vectores de ataque que se utilizaron para aquellos servicios y/o aplicaciones comprometidas durante la ejecución de las pruebas.

- Las pruebas se realizan a los activos externos de la organización sobre Internet y/o de manera interna con acceso a la red LAN.
- Se utilizarán los enfoques **blackbox**, **graybox** y **whitebox** durante todo el proyecto.
- Los objetivos particulares están determinados a lograr el mayor acceso posible y compromiso de los servicios autorizados a analizar.
- Durante todo el proceso se detallarán los hallazgos encontrados, así como el nivel de criticidad y sensibilidad que afectan directamente a los activos evaluados basados en el sistema CVSS y en el contexto del **IEPC Guerrero**.
- Se anexarán las evidencias recopiladas durante todo el análisis para comprobar que se logró comprometer los activos de información.
- También se darán las posibles soluciones, mismas que **IEPC Guerrero** deberá evaluar e implementar si así lo requiere.
- Las pruebas se realizarán de acuerdo a la metodología propia basada en los principales marcos de referencia reconocidos de Test de Intrusión y Análisis de Vulnerabilidades, como: OSSTMM, GPEN SANS, FedRAMP, NIST SP 800-115, OWISAM, OWASP, PTES e ISSAF así como la experiencia del consultor que participará.



Metodología de Auditoría Técnica de Ciberseguridad

Alcance

El análisis se aplicará a la infraestructura del Sistema Informático del PREP del **IEPC Guerrero** de forma coordinada con su área de Sistemas, considerando el siguiente alcance:

- **Activos Externos (Expuestos en Internet):**
 - 2 dominios.
 - 2 aplicativos web.
 - 6 apps móviles
 - 3 aplicaciones iOS.
 - 3 aplicaciones Android.
- **Activos Internos (Alcanzables solo desde red local):**
 - 2 aplicativos web.
 - 2 hosts.

NOTA: Es importante señalar que el alcance propuesto está estrictamente limitado a los elementos de evaluación descritos en la sección Alcance. Si derivado de las adecuaciones al Sistema Informático del PREP del **IEPC Guerrero** o de un interés específico del **IEPC Guerrero**, dicho alcance sufriera modificaciones, este deberá ajustarse en tiempo y condiciones económicas.

Actividades

Las actividades técnicas que se llevarán a cabo durante el análisis externo a la infraestructura serán las siguientes:

Análisis de Activos Externos (desde Internet)

Reconocimiento pasivo

Sirve para detectar posibles debilidades vía elementos informativos relacionados con el **IEPC Guerrero** y su dominio en Internet, utilizando motores de búsqueda públicos que puedan ayudar a generar un vector de ataque interno o externo.

Tiempo estimado: 1 día hábil.

Enfoque: Blackbox.

Reconocimiento activo

Se realiza una serie de pruebas de reconocimiento activo y escaneos automáticos a los sistemas y servicios de red, para lograrlo se sugiere que sea un horario productivo ya que no se tiene riesgo de caída. Este tiempo invertido es previo a la realización de ataques.

Tiempo estimado: 1 día hábil.

Enfoque: Blackbox.

Pruebas a la infraestructura

Se realiza análisis de la información recolectada para que, de forma coordinada, se procede con escaneos intrusivos y explotación de vulnerabilidades conforme a CVE en caso de aplicar.

En caso de detectar en el reconocimiento algún vector de ataque (dependiendo de los servicios y protocolos encontrados), se ejecutarán las herramientas y técnicas manuales necesarias para completar el vector de ataque.

Con la finalidad de mostrar al cliente el grado de vulnerabilidad de sus sitios, **el INAP** intentará obtener información de sus sistemas que pueda clasificarse como confidencial y que sirva como evidencia para el informe. Otro tipo de evidencia válida pueden ser: capturas de pantalla, dejar un archivo bandera en el sistema objetivo o la grabación de un video.

Tiempo estimado: 1 día hábil.

Enfoque: Blackbox.

Pruebas a los aplicativos o portales Web

El INAP considera realizar escaneo de vulnerabilidades web de forma automática a las aplicaciones web que nos autorice, incluyendo la revisión de las principales vulnerabilidades conforme a CWE Top 25 y OWASP Top 10:

- Inyección de comandos
- Pérdida de autenticación y gestión de sesiones
- Secuencia de comandos cruzados (XSS)
- Referencia insegura a objetos
- Configuración de seguridad incorrecta
- Exposición de datos sensibles
- Ausencia de control de acceso a funciones
- Falsificación de peticiones en sitios cruzados (CSRF)
- Utilización de componentes con vulnerabilidades conocidas
- Redirecciones y reenvíos no validados
- Entre otras

En caso de detectar en el reconocimiento algún vector de ataque (dependiendo de los servicios y protocolos encontrados), se ejecutarán las herramientas y técnicas manuales necesarias para completar el vector de ataque.

Con la finalidad de mostrar al **IEPC Guerrero** el grado de vulnerabilidad de sus sitios, se intentará obtener información de sus sistemas que pueda clasificarse como confidencial.

Las pruebas se hacen primeramente sin credenciales desde el punto de vista de un hacker y posteriormente (opcional sin costo adicional) con credenciales para entrar a las páginas en profundidad desde el punto de vista de un usuario del aplicativo.

Todo análisis se realiza sobre el aplicativo en ejecución, no se incluye análisis de código fuente, ni APIs.

Tiempo estimado: 4 días hábiles.

Enfoque: GrayBox.

Análisis de Activos Internos (red LAN)

Para el análisis interno se tendrá una entrevista con el responsable de la infraestructura para que brinde su inventario y señale cada equipo físicamente. Esto quedará registrado ante notario público que dará fe de los equipos que se analizarán internamente.

Reconocimiento activo

Se realiza una serie de pruebas de reconocimiento activo y escaneos automáticos a los sistemas y servicios de red, para lograrlo se sugiere que sea un horario productivo ya que no se tiene riesgo de caída. Este tiempo invertido es previo a la realización de ataques.

Tiempo estimado: 1 día hábil.

Enfoque: Blackbox.

Pruebas a la infraestructura

Se realiza análisis de la información recolectada para que, de forma coordinada, se procede con escaneos intrusivos y explotación de vulnerabilidades conforme a CVE en caso de aplicar.

En caso de detectar en el reconocimiento algún vector de ataque (dependiendo de los servicios y protocolos encontrados), se ejecutarán las herramientas y técnicas manuales necesarias para completar el vector de ataque.

También se realizarán ataques de captura intrusiva de tráfico para detectar protocolos inseguros y ataques de hombre en medio para corroborar el nivel de fortalecimiento de sus switches.

Con la finalidad de mostrar al cliente el grado de vulnerabilidad de sus sitios, el INAP intentará obtener información de sus sistemas que pueda clasificarse como confidencial y que sirva como evidencia para el informe. Otro tipo de evidencia válida pueden ser: capturas de pantalla, dejar un archivo bandera en el sistema objetivo o la grabación de un video.

Tiempo estimado: 1 día hábil.

Enfoque: Blackbox.

Pruebas a los aplicativos o portales web

El INAP considera realizar escaneo de vulnerabilidades web de forma automática a las aplicaciones web que nos autorice, incluyendo la revisión de las principales vulnerabilidades conforme a CWE Top 25 y OWASP Top 10:

- Inyección de comandos
- Pérdida de autenticación y gestión de sesiones
- Secuencia de comandos cruzados (XSS)
- Referencia insegura a objetos
- Configuración de seguridad incorrecta
- Exposición de datos sensibles
- Ausencia de control de acceso a funciones
- Falsificación de peticiones en sitios cruzados (CSRF)
- Utilización de componentes con vulnerabilidades conocidas
- Redirecciones y reenvíos no validados
- Entre otras

En caso de detectar en el reconocimiento algún vector de ataque (dependiendo de los servicios y protocolos encontrados), se ejecutarán las herramientas y técnicas manuales necesarias para completar el vector de ataque.

Con la finalidad de mostrar al cliente el grado de vulnerabilidad de sus sitios, se intentará obtener información de sus sistemas que pueda clasificarse como confidencial.

Las pruebas se hacen primeramente sin credenciales desde el punto de vista de un hacker y posteriormente (opcional sin costo adicional) con credenciales para entrar a las páginas en profundidad desde el punto de vista de un usuario del aplicativo.

Todo análisis se realiza sobre el aplicativo en ejecución, no se incluye análisis de código fuente, ni APIs, pero puede solicitarlo con un costo aparte.

Tiempo estimado: 4 días hábiles.

Enfoque: GrayBox.

Otras Pruebas

Denegación de Servicios

Debido a que la infraestructura pública se encuentra con un proveedor externo se descartan pruebas de disponibilidad, estas solo se ejecutarán si el **IEPC Guerrero** presenta una carta donde el proveedor le brinde autorización explícita para realizar este tipo de pruebas.

Tiempo estimado: 1 día hábil.

Enfoque: Whitebox.

Pruebas funcionales de caja negra

Se propone realizar un análisis de funcionalidad a sus 2 aplicaciones web internas. Con base a la documentación de sus aplicativos web y de los casos de uso funcionales documentados, se realizarán pruebas de verificación para cada uno.

En caso de que no sea facilitada la documentación por parte del cliente, las pruebas quedarán a criterio y tiempos que determine el consultor.

Estas pruebas son llamadas de caja negra debido a que no se tiene acceso al código fuente, pero el enfoque es totalmente con acceso al aplicativo con credenciales para ingresar a sus funcionalidades, por lo que lo clasificamos como WhiteBox.

Tiempo estimado: 10 días hábiles.

Enfoque: WhiteBox.

Apps Móviles

Se le propone realizar un análisis de seguridad a sus 6 aplicaciones móviles basadas, pero no limitadas al Mobile Security Testing Guide (MSTG).

El MSTG es un manual completo para las pruebas de seguridad de aplicaciones móviles y la ingeniería inversa para las aplicaciones de iOS y Android con el siguiente contenido:

- Aspectos internos de la plataforma móvil.
- Pruebas de seguridad en el ciclo de vida del desarrollo de aplicaciones móviles.
- Pruebas básicas de seguridad estática y dinámica.
- Ingeniería inversa y manipulación de aplicaciones móviles.
- Evaluación de las protecciones del software.

Para realizar el análisis tiene que facilitarle al **INAP** las aplicaciones en el estado que se encuentran antes de subirlas al AppStore y al Playstore para realizar un análisis estático y dinámico a los archivos .apk o .ipa. Todas las pruebas están basadas en el nivel 1 de OWASP Mobile App Verification (MASVS), clasificándose en los siguientes requerimientos de seguridad:

- Almacenamiento de datos y privacidad.
- Criptografía.
- Autenticación y manejo de sesiones.
- Comunicaciones a través de la red.
- Interacción con la plataforma.
- Calidad del código y configuración del compilador.
- Resistencia ante la ingeniería inversa.

En el análisis se podrá realizar ingeniería inversa para obtener el código fuente, identificación de bibliotecas con vulnerabilidades, exceso de permisos hacia los dispositivos, análisis de actividad de red y uso de criptografía, así como la identificación de posibles vulnerabilidades, como: exploración para descubrir contenido visible, ataques específicos de autenticación.

Tiempo estimado: 30 días hábiles.

Enfoque: WhiteBox

Apoyo de vigilancia en el día de la elección

Se le propone tener un canal de comunicación directo con el responsable/director del PREP que no incluya terceros que puedan distorsionar la información, con la finalidad de estar presente en el día de la elección con las siguientes actividades:

- Se acudirá de forma presencial el día que se acuerde previo a la elección, cuando el área o empresa desarrolladora de las dos aplicaciones web se encuentren en su versión final y garanticen que ya no habrá cambios ni actualizaciones de última hora.
- La presencia se realizará junto con un notario público que de fe y sea testigo de las actividades.
- Se obtendrá el código hash del ejecutable del aplicativo web.
- Se regresa el día de la elección y se obtendrá el código hash del aplicativo web antes de iniciar la jornada electoral.
- Este nuevo hash nuevamente será observado por el notario público que dé fe de la actividad.
- El código hash deberá ser el mismo para que pueda iniciar la ejecución del aplicativo. En caso contrario se reportará la inconsistencia al responsable del PREP de manera directa y se generará una carta para notificar que no existen las condiciones de integridad solicitadas, este reporte también se entregará a la notaría pública.
- Se supervisarán los equipos a lo largo del día y se obtendrán códigos hash cada 4 horas para validar que sea el mismo hash.
- Se generará un informe 24 horas posteriores al inicio de la jornada, indicando los pormenores y observaciones. Toda negligencia será notificada.

Tiempo estimado: 24 horas.

Enfoque: WhiteBox.

Duración de Servicio

Los tiempos de ejecución de las actividades se han propuesto en función de la información provista al momento de generar esta propuesta, si hubiera alguna modificación estos tiempos deberán ajustarse y no exceder una duración de **todas** las actividades técnicas será de máximo **54 días hábiles**.

Plan de Trabajo

La ejecución de esta Auditoría Técnica se realizará por proyecto basado en el modelo lineal con alcances definidos; cumpliendo objetivos y resultados clave mediante habilidades duras (hard skills) impulsando el teletrabajo.

Se iniciará el proyecto una vez que se tenga:

- Aprobaciones comerciales
- Carta de autorización
- Lista de objetivos

La lista de objetivos deberá ser entregada al INAP por un medio que genere evidencia, por ejemplo, mediante un correo electrónico; puede ser un listado de direcciones IPs o URLs, según sea el caso.

Hasta este momento se podrá agendar una reunión inicial (Kick Off) durante la cual se entregará un **plan de trabajo detallado** con cronograma de las actividades.

Análisis de Activos Externos

Este análisis incluye actividades de reconocimiento pasivo y activo, pruebas intrusivas a la infraestructura vía internet así como el análisis de las aplicaciones web que se encuentren expuestas en la red pública.

	Tiempo Invertido	Fecha	Lugar	Comentarios
Actividad Intrusiva	7 días hábiles	Por definir	Remoto	Requerimientos: 1. Carta de autorización firmada. 2. Exclusión de IP en Firewall perimetral.

Análisis de Activos Internos

Este análisis inicia configurando el acceso remoto para tener alcance de los activos internos de manera remota, ya sea en infraestructura del cliente o en la nube. Posteriormente se realizan actividades de reconocimiento, pruebas intrusivas a la infraestructura así como el análisis de las aplicaciones web que se encuentren en la red interna.

	Tiempo Invertido	Fecha	Lugar	Comentarios
Actividad Intrusiva	6 días hábiles	Por definir	Remoto	Requerimiento: 1. Acceso físico sin restricciones

Otras Pruebas

Se incluyen pruebas funcionales de caja negra, análisis de apps móviles para iOS y para Android y apoyo de vigilancia en el día de la elección incluyendo fé pública para mantener la integridad del aplicativo web.

	Tiempo Invertido	Fecha	Lugar	Comentarios
Actividad Intrusiva	41 días hábiles	Por definir	Remoto	Requerimiento: 1. Acceso a los archivos .ipa y .apk sin subir a stores 2. Acceso físico sin restricciones para obtener hash del aplicativo

Reportes

Se documentan los hallazgos y se prepara el reporte técnico y ejecutivo, se programa la entrega para el siguiente día hábil vía email. También se puede programar la entrega vía reunión virtual.

	Tiempo Invertido	Fecha	Lugar	Comentarios
Actividad Intrusiva	4 días hábiles	Por definir	Remoto	

El desarrollo de la documentación se inicia después del periodo de pruebas y se entrega al día hábil siguiente por email. Se puede programar una reunión virtual con el **IEPC Guerrero** si así lo desea para

explicar el resumen de los hallazgos; esta reunión no se grabará por motivos de confidencialidad a la información que se presentará.

Aclaraciones sobre el plan de trabajo:

- Se requiere carta de autorización en hoja membretada, firmada y sellada para poder iniciar cualquier prueba.
- Considere este documento como nuestra Declaración de Trabajo (statement of work / SOW).
- En caso de no existir inquietudes o preguntas sobre el proyecto o entregables, se da por cerrado a los 15 días naturales una vez entregado el reporte.
- No se considera realizar pruebas de Re-testing y/o verificación Post-remediación, sin embargo, puede solicitarlo con una cotización aparte.
- Cualquier requisito técnico solicitado en esta propuesta, pero que no sea brindado por parte del **IEPC Guerrero**, se procede a descartar sin responsabilidad para el INAP.

Acerca de la ejecución de actividades

Se debe determinar el alcance y objetivos de las pruebas, así como, la ventana de tiempo para ejecutar actividades.

- Las pruebas se coordinarán en conjunto entre el **IEPC Guerrero** y el INAP para considerar las fechas y los horarios convenientes para no afectar el servicio.
- Se cuenta con disponibilidad por parte del INAP para ajustarse a horarios nocturnos si fuera el caso en algunas aplicaciones.
- Las pruebas externas se realizan de manera remota a través del Internet.
- **IEPC Guerrero** tendrá que proporcionar la URL/IP objetivo y firmar una carta de autorización de ejecución de pruebas. (Ver **Anexo I – Carta de autorización**).
- Antes de cada prueba se deberán establecer los puntos de contacto entre un responsable por parte de **IEPC Guerrero** para que se pueda mantener un canal de comunicación con acceso directo al equipo ejecutor de las pruebas que esté realizando las actividades con la posibilidad de detener las pruebas si se detecta alguna afectación al servicio, estos medios de contacto podrán ser de forma directa vía telefónica y correo electrónico.
- Previo a iniciar la ejecución de las pruebas se realizará conferencia telefónica o correo electrónico entre el responsable del proyecto por parte de **IEPC Guerrero** y el equipo ejecutor de las pruebas. El responsable de proyecto será quien instruya a nuestro equipo de ejecución la autorización para dar inicio a las pruebas.
- Si por alguna razón se deshabilita un sistema o no es alcanzable en el momento de hacer las pruebas, se validará con el responsable del proyecto la funcionalidad de la aplicación o servidor para volver a intentarlo o se procede a descartar.
- En caso de que se deban detener las pruebas por parte de **IEPC Guerrero**, deberá indicarlo de forma directa nuestro equipo ejecutor vía telefónica y posteriormente deberá ser enviado por correo electrónico indicando las razones por las cuales se ha solicitado la detención de las pruebas, sólo para mantener un registro y documentación del equipo ejecutor.
- En caso de detectarse una vulnerabilidad de alto riesgo, se deberá avisar inmediatamente al contacto establecido por **IEPC Guerrero** para que se tomen decisiones al respecto.
- El equipo ejecutor de las pruebas podrá reportar la vulnerabilidad para su toma de decisión de **IEPC Guerrero** mediante vía telefónica, correo electrónico u otro medio que sea acordado entre ambas partes.
- **IEPC Guerrero** tendrá que asegurar que no habrá cambios en la infraestructura y/o configuraciones de los dispositivos evaluados en el tiempo autorizado para la ejecución de las pruebas, ya que una finalidad es evaluar los objetivos en el estado normal de utilización.

Aclaraciones sobre las actividades

- No se realizarán pruebas de phishing, client-side attacks ni las consideradas amenazas avanzadas persistentes (APT's), ni de ingeniería social.
- Nuevas amenazas y ataques surgidos durante la ejecución del proyecto o cualquier prueba que no haya sido mencionada anteriormente no se consideran para su evaluación.
- No se considera realizar pruebas que pudieran provocar la caída de los servicios por lo que el INAP no se responsabiliza de interrupciones que pudiera tener su infraestructura en el tiempo que dure el proyecto.
- Si por alguna razón se deshabilita un sistema o no es alcanzable en el momento de hacer las pruebas, se validará con el responsable del proyecto la funcionalidad de la aplicación o servidor para volver a intentarlo o se procede a descartar sin responsabilidad para el INAP.
- En caso de tener un control de seguridad que filtre o bloquee los ataques se le sugiere añadir una exclusión para la dirección IP del consultor (Pruebas externas), debido a que la finalidad de la prueba es conocer el nivel de seguridad de los equipos y no de los controles de seguridad ya que para estos se realizarán las pruebas de caja gris.
 - Esta sugerencia es tomada del punto 4.1.7 de la guía de *Penetration Testing del PCI Data Security Standard* que recomienda añadir una exclusión al consultor que realice las pruebas para evitar "Scan Interference".
- No se considera soporte técnico, ni transferencia de conocimiento, ni ejecución de pruebas a modo de demostración.
- No se considera un programa de capacitación sobre análisis de vulnerabilidades y pruebas de penetración.
- No se consideran actividades de mitigación de vulnerabilidades o cualquier otro tipo de hallazgo.
- No se consideran actividades particulares de revisión y emisión de recomendaciones en la configuración y/o parametrización de la infraestructura tecnológica evaluada.
- **No se considera realizar pruebas de Re-testing y/o verificación Post-remediación**
- No se consideran actividades de seguimiento a mitigación de vulnerabilidades o cualquier otro tipo de hallazgo.
- **IEPC Guerrero** tendrá que asegurar que no habrá cambios en la infraestructura y/o configuraciones de los dispositivos evaluados en el tiempo autorizado para la ejecución de las pruebas, ya que una finalidad es evaluar los objetivos en el estado normal de utilización.

Herramientas a utilizar

Para llevar a cabo satisfactoriamente este proyecto se consideran técnicas, metodologías, análisis, criterios, herramientas, pruebas manuales, identificación de vectores de ataque y la **experiencia del consultor** por lo que no solo nos basamos en la ejecución de herramientas de pruebas automatizadas. La cobertura de las herramientas se mencionan de manera general de acuerdo a los rubros que cubren:

- Escáner de puertos y servicios.
- Escáner de vulnerabilidades.
- Scripts automatizados para prueba de vulnerabilidades.
- Pruebas manuales para la penetración del sistema.
- Frameworks automáticos para la penetración del sistema.
- Scripts y herramientas creadas por hackers para la afectación de servicios web.
- Scripts y herramientas desarrolladas por los consultores.

Todas las herramientas pueden ser comerciales o gratuitas, particulares o creadas por hackers. Las herramientas comerciales son con licenciamiento previo por lo que **IEPC Guerrero** no requiere la adquisición de ningún software en particular.

Entregables

Se entregan 2 informes en **español** con un enfoque basado en evidencias. Sólo se reporta lo que aporte valor y sea relacionado a la seguridad informática de la siguiente manera:

Entregable	Descripción
<i>Informe Previo</i>	Se presenta de forma detallada el estado actual de la seguridad considerando: <ul style="list-style-type: none"> • Fecha y nombre de los responsables. • Listado del alcance autorizado. • Análisis de vulnerabilidades técnicas priorizando conforme al CVSS y al contexto de su organización. • Reporte de hallazgos técnicos y su evidencia, organizados por vulnerabilidad. • Posibles correcciones y sugerencias de remediación para cada vulnerabilidad. • Resultado certero o fallido de la denegación de servicio. • Conclusiones generales, donde también se incluyen recomendaciones de ciberseguridad acordes al contexto de la organización y basadas en las mejores prácticas internacionales.
<i>Informe Final</i>	Se presenta de forma general el estado actual de la seguridad considerando: <ul style="list-style-type: none"> • Presentación del estado actual de la seguridad. • Reporte de hallazgos generales. • Análisis de amenazas a los activos de información. • Vectores de ataque en caso de existir.

La duración de la documentación será de **4 días hábiles** después del periodo de pruebas.

Aclaraciones sobre los entregables

- Para mantener la presentación ecuánime del reporte, no se entregarán logs, bitácoras o capturas de pantalla de las herramientas utilizadas.
- Para mantener la integridad del reporte, no se entregarán informes previos, editables, borradores ni preliminares de las vulnerabilidades encontradas.
- Para mantener la imparcialidad de los hallazgos identificados, ningún hallazgo queda sujeto a negociación.

Equipo de trabajo

Organización del proyecto

El equipo de trabajo que el INAP propone para llevar a cabo el proyecto, se compone de al menos los siguientes perfiles:

Rol	Responsabilidades
Líder de Proyecto	<ul style="list-style-type: none"> Identificar los recursos necesarios. Definir las actividades. Dar seguimiento a los principales riesgos identificados. Establecer compromisos del proyecto. Identificar, analizar y reportar desviaciones. Control de cambios. Enlace entre el equipo de IEPC Guerrero y el equipo Auditor.
Equipo Auditor	<ul style="list-style-type: none"> Ejecutar las actividades de Auditoría Técnica.. Análisis de resultados. Generación de informes.

Capacidad técnica y operativa

<p>Contamos con los recursos humanos especializados para la entrega de servicios en materia de seguridad de tecnologías de la información.</p> <p>El personal responsable que sea designado cuentan con algunas de las certificaciones más reconocidas del mercado como son:</p>	<ul style="list-style-type: none"> Project Management Professional (PMP). ISO/IEC 27001 (Lead Auditor, Implementer, Auditor). ISO/IEC 22301 (Lead Auditor, Implementer, Auditor) OSSTMM Professional Security Analyst/Tester (OPSA/OPST). Certified Data Centre Professional (CDCP). Mile2 Certified Vulnerability Assessor (CVA). Mile2 Certified Penetration Testing Consultant (CPTC). Mile2 Certified Digital Forensics Examiner (CDFE). Certified Ethical Hacker (CEH). Offensive Security Certified Professional (OSCP). Certified Information Systems Auditor (CISA). ITIL v3 Foundation. Certified Information Security Manager (CISM). Otras relacionadas.
	

Propuesta Económica

A continuación, ponemos a su consideración el costo por la ejecución de este servicio de acuerdo a los alcances definidos en esta propuesta:

Concepto	Cantidad	Costo Unitario	Total
Servicio "Ente Auditor al Sistema Informático del PREP - IEPC Guerrero" conforme al los alcances descritos en esta propuesta.	1	\$2,930,000.00	\$2,930,000.00
Subtotal servicios			\$2,930,000.00
IVA			\$468,800.00
Total			\$3,398,800.00

Condiciones comerciales y de pago

- Montos expresados en moneda nacional, el total incluye el IVA.
- Cualquier actividad no listada de forma expresa en esta propuesta de servicios, deberá cotizarse por separado.
- El precio indicado ampara servicios profesionales y no incluye hardware ni licenciamientos.
- El precio total incluye viáticos al estado de Guerrero.
- El precio indicado considera Notario Público durante el apoyo de vigilancia.
- Condiciones de pago: Pago del 50% de anticipo para iniciar el proyecto y dos pagos por 25% cada uno a la mitad de ejercicio y al finalizar.
- Se requiere de Orden de Compra o contrato de servicios para el inicio del proyecto.
- La presente propuesta tiene una vigencia de 60 días.

Fuera del alcance de la propuesta

- Desarrollo e implementación de algún proceso y/o control de seguridad.
- Instalación, configuración ni evaluación de cualquier tipo de software, hardware o equipo de comunicaciones o seguridad.
- No se considera realizar pruebas de Re-testing y/o verificación Post-remediación
- Implementación de cualquier herramienta de software.
- Análisis de otros procesos que estén fuera de alcance mencionado del proyecto.
- Cualesquiera otras actividades no definidas expresamente.

ATENTAMENTE

DR. RICARDO CORRAL LUNA

DIRECTOR DEL CENTRO DE CONSULTORÍA
EN ADMINISTRACIÓN PÚBLICA
Y APODERADO LEGAL

Términos y condiciones del servicio

Derechos de autor

El INAP y el **IEPC Guerrero** manifiestan ser propietarias y/o titulares y/o licenciatarios legítimos de los derechos de propiedad industrial, de autor y de uso en su caso, de los procedimientos, programas, sistemas informáticos, equipo y demás materiales de esta naturaleza que involucren derechos de propiedad intelectual que sean o lleguen a ser utilizados en la prestación de los servicios objeto de la presente propuesta.

Sobre licencias

NO se incluyen las licencias de cualquier producto ni herramientas de terceros tales como Software y Hardware, estas –en caso de requerirse- deberán de ser adquiridas directamente por el **IEPC Guerrero** con el proveedor que él considere adecuado.

Criterios y tiempos de aceptación

Ambas partes – el INAP y el **IEPC Guerrero** - acordarán mutuamente los criterios de aceptación de los Servicios presentados y en casos particulares estos criterios deben ser acordados antes de empezar con pruebas de aceptación y tiene su base en la metodología del INAP para gestión de proyectos, y las condiciones pactadas en los tiempos finales de ejecución de las fases del proyecto o sus correspondientes acuerdos de cambios firmados durante la duración del proyecto.

Anexo I. Modelo de carta de autorización¹

Ciudad de México, XX de XXXXX 2024.

Dr. Ricardo Corral Luna
Director del Centro de Consultoría
en Administración Pública

Por medio de la presente autorizamos a el Instituto Nacional de Administración Pública A.C. (INAP), a ejecutar pruebas de seguridad informática tipo caja negra y gris bajo las siguientes condiciones:

1. **IEPC Guerrero** manifiesta su conocimiento y aprobación del análisis de vulnerabilidades y pruebas de penetración externa e interna del tipo caja negra, gris y blanca, que se realizarán durante el periodo comprendido entre el XXX al XXX 2024 y ejecutado por el personal designado por el INAP, teniendo como objetivo: (*Hostname, IP, URL*).
2. **IEPC Guerrero** aprueba en su totalidad la realización de las pruebas de seguridad de acuerdo al alcance listado a continuación:
 - XXX
3. **IEPC Guerrero** faculta a el INAP para validar vulnerabilidades que puedan permitir el acceso a los sistemas de información.
4. **IEPC Guerrero** reconoce que la ejecución de las pruebas de seguridad por parte del INAP tienen completa autorización y por lo tanto, no se está incumpliendo ninguna normatividad o ley de delitos informáticos vigente en el país.
5. El INAP realizará las pruebas de seguridad mediante técnicas de mínimo impacto sobre la operación de la plataforma tecnológica, sin afectar la integridad, confidencialidad o disponibilidad de la información.

Cordialmente,

XXX
XXX
IEPC Guerrero

¹ Deberá emitirse en papel membretado de la organización. Este modelo de carta es referencial y su versión final será definida en su contenido de manera previa al inicio del proyecto.