

REGISTRO UNAM: 47780-596-2-III-17

CONVENIO DE COLABORACIÓN PARA LA AUDITORÍA DE VERIFICACIÓN Y ANÁLISIS DEL SISTEMA INFORMÁTICO QUE SERÁ UTILIZADO EN LA IMPLEMENTACIÓN Y OPERACIÓN DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES (PREP), PARA EL PROCESO ELECTORAL 2016-2017, EN LO SUCESIVO "LA AUDITORÍA", QUE CELEBRAN POR UNA PARTE, LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, EN LO SUCESIVO "LA UNAM", REPRESENTADA EN ESTE ACTO POR EL DR. LEONARDO LOMELÍ VANEGAS, EN SU CARÁCTER DE SECRETARIO GENERAL, ASISTIDO POR EL M. EN I. FERNANDO MACEDO CHAGOLLA, DIRECTOR DE LA FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN; Y POR LA OTRA PARTE, EL INSTITUTO ELECTORAL DEL ESTADO DE MÉXICO, EN LO SUCESIVO "EL IEEM", REPRESENTADO EN ESTE ACTO POR EL LIC. PEDRO ZAMUDIO GODÍNEZ, CONSEJERO PRESIDENTE DEL CONSEJO GENERAL, Y EL M. EN A.P. FRANCISCO JAVIER LÓPEZ CORRAL, SECRETARIO EJECUTIVO Y REPRESENTANTE LEGAL, CON LA PARTICIPACIÓN DEL DR. JUAN JOSÉ RIVAUD GALLARDO, JEFE DE LA UNIDAD DE INFORMÁTICA Y ESTADÍSTICA, EN LO SUCESIVO "LA UIE" A QUIENES EN CONJUNTO SE DENOMINARÁN "LAS PARTES", CONFORME A LAS DECLARACIONES Y CLÁUSULAS SIGUIENTES:

D E C L A R A C I O N E S

I. Declara "LA UNAM":

- I.1 Que de conformidad con el artículo 1 de su Ley Orgánica publicada en el Diario Oficial de la Federación el 6 de enero de 1945, es una corporación pública, organismo descentralizado del Estado, dotada de plena capacidad jurídica y que tiene por fines impartir educación superior para formar profesionistas, investigadores, profesores universitarios y técnicos útiles a la sociedad; organizar y realizar investigaciones, principalmente acerca de las condiciones y problemas nacionales, y extender con la mayor amplitud posible los beneficios de la cultura.

- I.2 Que la representación legal de esta Casa de Estudios, recae en su Rector, el Dr. Enrique Luis Graue Wiechers, según lo dispuesto en los artículos 9 de su Ley Orgánica y 30 de su Estatuto General, teniendo, conforme a la fracción I del artículo 34 del propio Estatuto, facultades para delegarla.
- I.3 Que el Dr. Leonardo Lomelí Vanegas, en su carácter de Secretario General, cuenta con las facultades necesarias para suscribir el presente instrumento de conformidad con el Acuerdo que delega y distribuye competencias para la suscripción de convenios, contratos y demás instrumentos consensuales en que la Universidad sea parte, publicado en Gaceta UNAM el 5 de septiembre del 2011.
- I.4 Que dentro de su estructura orgánico-administrativa se encuentra la Facultad de Estudios Superiores Aragón, en lo sucesivo **"LA FES ARAGÓN"**, la cual cuenta con la infraestructura y los recursos necesarios para el cumplimiento del objeto del presente Convenio, cuyo director es el M. en I. Fernando Macedo Chagolla.
- I.5 Que cuenta con Registro Federal de Contribuyentes que le han asignado las autoridades hacendarias con clave alfanumérica UNA-290722-7Y5.
- I.6 Que para los efectos del presente Convenio, señala como domicilio legal el piso 9 de la Torre de Rectoría en Ciudad Universitaria, Delegación Coyoacán, Código Postal 04510, en la Cd. Mx.
- I.7 Que para efectos de la ejecución del Convenio referido señala como domicilio el ubicado en Avenida Rancho Seco s/n, Colonia Impulsora, Código Postal 057130, Municipio de Nezahualcóyotl, Estado de México.

II. Declara **"EL IEEM"**:

- II.1 Que es un organismo público dotado de personalidad jurídica y patrimonio propio, autónomo en su funcionamiento e independiente en sus decisiones, responsable de la organización, desarrollo y vigilancia de los procesos electorales, según se desprende del artículo 11, párrafo segundo de la Constitución Política del Estado Libre y Soberano de México.

- II.2 Que de conformidad con lo establecido en el artículo 168, párrafos primero y segundo, del Código Electoral del Estado de México, es autoridad electoral de carácter permanente y profesional en su desempeño, se registrará por los principios de certeza, imparcialidad, independencia, legalidad, máxima publicidad y objetividad.
- II.3 Que el Consejo General de “**EL IEEM**”, es el Máximo Órgano de Dirección, que se conforma con un Consejero Presidente, seis Consejeros Electorales, un Secretario Ejecutivo y un representante de cada uno de los partidos políticos con registro, en términos de los artículos 175 y 176, del Código Electoral del Estado de México.
- II.4 Que en fecha 2 de febrero de 2017, la Junta General de “**EL IEEM**”, aprobó el acuerdo IEEM/JG/12/2017, denominado “*Por el que se designa el Ente Auditor del Sistema Informático del Programa de Resultados Electorales Preliminares para el Proceso Electoral 2016-2017*”; en cuyo punto de acuerdo segundo se designa al **Centro Tecnológico Aragón**, de la Facultad de Estudios Superiores Aragón, de la Universidad Nacional Autónoma de México.
- II.5 Que el Lic. Pedro Zamudio Godínez es Consejero Presidente del Consejo General, y el M. en A.P. Francisco Javier López Corral, Secretario Ejecutivo y Representante Legal, respectivamente, el primero designado por el Consejo General del Instituto Nacional Electoral a través del acuerdo INE/CG165/2014 de 30 de septiembre de 2014; mientras que al segundo lo designó el Consejo General del Instituto Electoral del Estado de México, con base en el diverso IEEM/CG/58/2014 de fecha 3 de octubre de 2014 y ratificado en su cargo, mediante diverso IEEM/CG/234/2015 del 23 de noviembre de 2015, aprobado por el Máximo Órgano de Dirección del Instituto, por lo que cuenta con las más amplias facultades para representarlo y suscribir en su nombre en el presente instrumento.
- II.6 Que de acuerdo a lo dispuesto en el artículo 190 fracción II, del Código Electoral del Estado de México el Presidente del Consejo General, se encuentra facultado para firmar conjuntamente con el Secretario Ejecutivo el presente.

II.7 Que el Secretario del Consejo General, tiene la facultad entre otras, de auxiliar al Consejero Presidente en el ejercicio de sus atribuciones, de conformidad con lo establecido en los artículos 190 y 191 del Código Electoral del Estado de México, quien además como Secretario Ejecutivo, cuenta con la representación legal de **"EL IEEM"**, según el artículo 196, fracción I, del ordenamiento legal invocado.

II.8 Que tiene su domicilio legal en Paseo Tollocan número 944, Colonia Santa Ana Tlapaltitlán, Toluca, Estado de México. C.P. 50160.

III. Declaran **"LAS PARTES"** que:

III.1 Se reconocen mutua y plenamente la personalidad con que se ostentan, así como la capacidad con la que comparecen.

III.2 Deciden que de forma conjunta cumplirán con las obligaciones estipuladas en el presente.

III.3 Y es su voluntad celebrar el presente Convenio, sujetándose al tenor de las siguientes:

C L Á U S U L A S

PRIMERA. OBJETO.

Es la colaboración entre **"LAS PARTES"** a fin de llevar acabo el estadio denominado Auditoría de Verificación y Análisis del sistema informático, que será utilizado en la implementación y operación del Programa de Resultados Electorales Preliminares (PREP) para el Proceso Electoral 2016-2017 de **"EL IEEM"**, en lo sucesivo **"LA AUDITORÍA"** 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.

“**LA AUDITORÍA**” se desarrollará conforme a las especificaciones establecidas en el **Anexo Técnico**, que forma parte integrante del presente, en el cual constan, de manera detallada:

- Los alcances de la misma;
- La metodología;
- El plan de trabajo base, incluyendo actividades, fechas, responsabilidades y recursos necesarios para su cumplimiento;
- La descripción de la información que “**EL IEEM**” entrega a “**LA UNAM**”;
- Las fechas, contenido y términos en los que “**LA UNAM**” presentará los informes parciales y final de “**LA AUDITORÍA**”, así como los correspondientes a la **evaluación de la operación del PREP**.

En todo caso, “**LA AUDITORÍA**” deberá prever, al menos, pruebas funcionales de caja negra y caja blanca al sistema informático para evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares; así como el análisis de vulnerabilidades, considerando pruebas de penetración y revisión de configuraciones a la infraestructura tecnológica del PREP.

SEGUNDA. COMPROMISOS. Para la realización y cumplimiento del objeto del presente Convenio, “**LAS PARTES**” se comprometen a desarrollar las actividades que, de manera enunciativa más no limitativa se mencionan a continuación:

1. De “**LA UNAM**” por conducto de la “**FES ARAGÓN**”:

- a) Designar por oficio, como parte integrante de su equipo de trabajo, a dos doctores o un doctor y dos maestros, todos ellos, en ciencias de la computación, con los grados otorgados por instituciones académicas de reconocido prestigio, así como amplia experiencia comprobada en auditoría informática de sistemas del PREP, para que participen en el desarrollo y cumplimiento del objeto del presente Convenio.
- b) Designar por oficio al personal que ejecutará “**LA AUDITORÍA**”, además, presentar en copia y en original (para cotejo), las certificaciones vigentes de los ingenieros que realizarán la auditoría, debiendo tener al menos 3 años de experiencia cada uno. Puede ser uno o más ingenieros los que realicen la auditoría, debiendo cubrir con todas las líneas que se solicitan a continuación:

Comprobar que el personal designado está capacitado para realizar “**LA AUDITORÍA**”, para lo cual “**LA UNAM**” presentará la acreditación formal de al menos una de las siguientes certificaciones:

- Certificación por EC-Council (CEH, LPT, ECSA, ENSA, ECIH, CHFI, CCISO).
- Certificación por ISACA (CISM, CISA, CRISC, CGEIT).
- Certificación por ISC2 (CISSP, SSCP, CAP, CCFP).
- Auditor/Leader Auditor ISO27001.
- CompTIA: Security+ Profesional.
- CCIE, CCSP.
- En caso de contar con alguna otra certificación de seguridad que no se menciona en la relación anterior, “**LA UNAM**” deberá comprobar la validez de la certificación avalada por alguna instancia a nivel nacional o internacional.

c) Presentará oficio de al menos 2 empresas con las que haya realizado trabajos similares a los solicitados en los últimos tres años, éste estará dirigido al Lic. José Mondragón Pedrero, Director de Administración de “**EL IEEM**” y deberá hacer referencia a este procedimiento.

d) Generar el documento en el que se haga constar la metodología de “**LA AUDITORÍA**”, incluyendo el procedimiento y enfoque para verificar y comprobar los controles a revisar, así como el formato y contenido de los reportes que se deriven de ésta. Se utilizarán dos metodologías: la del Manual de la Metodología Abierta de Comprobación de la Seguridad (OSSTMM, Open Source Security Testing Methodology Manual) y la del Proyecto Abierto de Seguridad de Aplicación Web (OWASP, Open Web Application Security Project).

e) Establecer los alcances de “**LA AUDITORÍA**”, así como los recursos materiales y técnicos necesarios para llevarla a cabo.

Las técnicas de verificación serán realizadas empleando software OpenSource y propietario, para implementar el checklist que de acuerdo a la OWASP, es el siguiente:

- I. Prueba de calidad de todos los aplicativos desarrollados específicamente para **"LA AUDITORÍA"**, en términos de la funcionalidad;
 - II. Análisis de vulnerabilidades en la infraestructura tecnológica de **"LA AUDITORÍA"**, incluyendo pruebas de negación de servicio, pruebas de inyección de código malicioso y pruebas de acceso a los diversos recursos del sistema informático;
 - III. Manejo de los informes emitidos respecto a la calidad del software, vulnerabilidades y hallazgos detectados, con un carácter estrictamente confidencial e inclusión de recomendaciones que permitan a **"EL IEEM"** atender el riesgo identificado durante las pruebas;
 - IV. Realización de pruebas de estrés para determinar los límites de uso del software y estimar los límites de la estructura informática de hardware y red; y
 - V. Emisión de recomendaciones para asegurar la calidad y seguridad del software y de la infraestructura tecnológica.
- f) Entregar a **"EL IEEM"**, con un carácter estrictamente confidencial, los informes que se generen respecto a **"LA AUDITORÍA"**, conforme a los siguientes modelos básicos:
- I. Informes parciales: referentes a los resultados emitidos durante el proceso de **"LA AUDITORÍA"**, debiendo incluir, al menos lo siguiente:
 - a. Los criterios utilizados para realizar **"LA AUDITORÍA"**.
 - b. El método para clasificar los hallazgos que permitan priorizar su atención;
 - c. Los hallazgos identificados y clasificados, y
 - d. Las posibles recomendaciones que permitan a **"EL IEEM"** atenderlos jerarquizadas por su nivel de impacto.

Estos informes tendrán calidad de reservados en términos de las disposiciones aplicables en material de **transparencia y acceso a la información**. En caso de que se detecten vulnerabilidades graves, deberán ser notificadas de manera inmediata al personal designado de **"LA UIE"**, con la finalidad de que sean corregidas a la brevedad.

- II. Informe final correspondiente a los resultados finales de **"LA AUDITORÍA"**, que considera el cierre de operaciones del PREP, así

como también la etapa de evaluación del mismo, éste deberá ser entregado a más tardar el segundo día hábil después de haber concluido **“LA AUDITORÍA”**, el cual será publicado en el portal oficial de **“EL IEEM”**.

III. Informe de evaluación de la operación: deberá incluir:

- Resumen ejecutivo.
- Objetivos y alcance.
- Metodologías utilizadas.
- Vulnerabilidades identificadas, indicando el riesgo, impacto y recomendaciones.
- Validación de los aplicativos.
- Documentación de soporte de la evaluación (en medio electrónico).
- Presentación ejecutiva con los resultados de la auditoria.

2. De **“EL IEEM”**:

- a) Asignar un líder del proyecto, el cual deberá coordinar las actividades de **“LA AUDITORÍA”** con el personal responsable de **“LA UNAM”**. Todos los entregables deberán ser aprobados por el líder de proyecto de **“LA UIE”**.
- b) Proporcionar por escrito a **“LA UNAM”** toda la información necesaria y que tenga relación con el objeto de este Convenio, en los términos establecidos en la cláusula Tercera.
- c) Colaborar con **“LA UNAM”** a efecto de llevar a cabo el desarrollo y ejecución de **“LA AUDITORÍA”**, en los términos establecidos en el Anexo Técnico que forma parte integral del presente instrumento.
- d) Dar acceso a la información indispensable para efectuar **“LA AUDITORÍA”**, salvo aquella que tenga el carácter de confidencial.
- e) Supervisar, en todo momento, a través de **“LA UIE”** el desarrollo y resultados derivados de **“LA AUDITORÍA”**.
- f) Realizar las validaciones de información en los términos y condiciones, conforme a lo señalado en la cláusula Tercera.

- g) Entregar a **"LA UNAM"** en tiempo y forma, la aportación acordada en términos de lo estipulado en la cláusula Cuarta.
- h) Las demás que determinen **"LAS PARTES"** por mutuo acuerdo, y que tengan como finalidad la consecución del objeto del presente Convenio de Colaboración.

TERCERA. FECHAS, TÉRMINOS Y CONDICIONES. **"LA AUDITORÍA"** será realizada de acuerdo a lo establecido en el **Anexo Técnico**, que debidamente firmado por **"LAS PARTES"**, forma parte integral del presente Convenio, en él se integra un cronograma que señala las fechas y particularidades en que serán desarrolladas cada una de las actividades.

Se considerarán los siguientes términos y condiciones:

- a) Para la ejecución de las pruebas en la infraestructura de Tecnologías de la Información de **"EL IEEM"**, **"LA UNAM"** no ejecutará pruebas sin una autorización formal de **"LA UIE"**.
- b) Durante el desarrollo de las pruebas, no se debe causar ningún tipo de daño a la red, a los equipos y a la información. Por lo que, en consecuencia, para la realización de algunas de las pruebas, personal de **"LA UIE"** establecerá los horarios en que no ocasionen inconvenientes en la operación normal.
- c) Los resultados y entregables de **"LA AUDITORÍA"** son propiedad de **"EL IEEM"**, no podrán ser distribuidos, ni divulgados a ningún tercero, en su totalidad o en parte sin consentimiento expreso de **"EL IEEM"**.
- d) La información obtenida durante la realización de las pruebas será estrictamente propiedad de **"EL IEEM"**.
- e) Por tanto, **"LA UNAM"** firmará una cláusula de confidencialidad de la información en donde se compromete a guardar la confidencialidad por un periodo de 5 años, a partir de la firma del convenio.
- f) A la firma del Convenio **"LA UNAM"** firmará la cláusula de confidencialidad de la información referida en el inciso anterior, donde se especificará que la información obtenida del sistema de información del PREP 2017 y la

infraestructura de “EL IEEM”, no podrá ser divulgada por ningún motivo a un tercero. Además, toda información accedida por “LA UNAM” será tratada como confidencial, siendo destruida al final del proyecto, excepto lo que “LA UIE” considere que sea requerido como soporte del proyecto.

CUARTA. APORTACIONES. “EL IEEM” se compromete a aportar a “LA UNAM” la cantidad de **\$1,200,000.00 (un millón doscientos mil pesos 00/100 M.N.)**, dicha cantidad será otorgada por “EL IEEM” de la siguiente forma, dos exhibiciones, la primera dentro de los 5 días posteriores al inicio de “LA AUDITORÍA” por un monto de **\$600,000.00 (seiscientos mil pesos 00/100 M.N.)**; y, la segunda dentro de los 5 días posteriores a la conclusión de los trabajos de “LA AUDITORÍA”, por un monto de **\$600,000.00 (seiscientos mil pesos 00/100 M.N.)**.

QUINTA. FORMA DE OTORGAR LA APORTACIÓN. Las aportaciones serán cubiertas en moneda nacional, mediante transferencia electrónica a solicitud por escrito de “LA UNAM” a la cuenta bancaria número [REDACTED] del Banco BBVA Bancomer, Clave [REDACTED] Sucursal [REDACTED] Plaza [REDACTED] Concepción Béistegui, a nombre de la Universidad Nacional Autónoma de México.

“EL IEEM”, entregará a “LA UNAM” en un plazo no mayor de 5 días naturales posteriores a la realización de las transferencias realizadas en los momentos establecidos en el presente Convenio, copia impresa o electrónica del documento comprobatorio.

Dichas aportaciones serán otorgadas a “LA UNAM” previa presentación del Comprobante Fiscal Digital correspondiente debidamente requisitado, ante la Dirección de Administración de “EL IEEM”, en el domicilio de éste señalado en el presente Convenio, previa autorización y con el visto bueno del Titular de “LA UIE”.

SEXTA. COMISIÓN TÉCNICA. “LAS PARTES” convienen que para la debida ejecución de este Convenio y el adecuado desarrollo de las actividades a que se refiere el mismo, sean designados como Responsables Operativos los siguientes funcionarios:

Por “LA UNAM”:

M. EN I. MARCELO PÉREZ MEDEL

Encargado del Laboratorio de Cómputo del Centro
Tecnológico de Aragón

Por “EL IEEM”: **DR. JUAN JOSÉ RIVAUD GALLARDO**
Jefe de “LA UIE”.

Los Responsables Operativos tendrán las siguientes obligaciones:

- a) Determinar y aprobar oportunamente las acciones o actividades pertinentes factibles de ejecución para el cumplimiento del objeto de este instrumento;
- b) Coordinar la ejecución del objeto del presente Convenio,
- c) Resolver todo conflicto que se derive del presente instrumento, respecto a su interpretación, formalización y cumplimiento.
- d) Dar seguimiento e informar periódicamente de los resultados a cada una de “**LAS PARTES**” que representan.
- e) Las demás que acuerden “**LAS PARTES**”.

Para tal efecto, celebrarán reuniones de trabajo, estableciendo mecanismos de comunicación e interacción y demás acciones a emprender para cumplir con este Convenio.

SÉPTIMA. COMUNICACIONES. “**LAS PARTES**” acuerdan que las comunicaciones relacionadas con este Convenio, deberán dirigirse por escrito a los domicilios precisados por ellas en las Declaraciones I.7 y II.8 del presente Convenio; también podrán ser vía correo electrónico, quedando obligada la parte que así lo haga, a remitir de forma inmediata el original del comunicado (documento) de que se trate, con firma autógrafa.

OCTAVA. SUPERVISIÓN. “**LAS PARTES**” acuerdan que, en todo momento, “**EL IEEM**” a través de “**LA UIE**”, podrá llevar a cabo la supervisión del desarrollo y ejecución de “**LA AUDITORÍA**”, objeto del Convenio, realizada por “**LA UNAM**”.

NOVENA. PROPIEDAD INTELECTUAL. “**LAS PARTES**” se obligan a reconocerse los derechos de autor (derechos morales y patrimoniales) que cada una tiene o llegue a tener por su cuenta, de conformidad a lo establecido en la Ley Federal del Derecho de Autor.

En caso de que con motivo de la ejecución de este convenio se generen productos o conocimientos que sean susceptibles de registro o explotación, en favor de "LA UNAM" en su oportunidad a través del instrumento jurídico correspondiente se debe dar intervención a la Dirección General de Asuntos Jurídicos para que en el ejercicio de sus atribuciones emita el dictamen respectivo, de conformidad con lo establecido en el punto Quinto, fracción IV y VI del Acuerdo que establece la estructura y facultades de la Oficina del Abogado General de la Universidad Nacional Autónoma de México; los derechos patrimoniales sobre los mismos corresponderán a la parte cuyo personal haya realizado el trabajo que sea objeto de protección en la materia, dándole el debido reconocimiento a quienes hayan intervenido en su realización. Si los trabajos se realizarán por el personal de ambas partes, la titularidad les corresponderá en proporción a su participación. **"LAS PARTES"** podrán utilizar la información derivada de las actividades desarrolladas en sus actividades académicas.

DÉCIMA. INFORMACIÓN DE ACCESO RESTRINGIDO. "LAS PARTES" convienen mantener la clasificación de la información de acceso restringido que tenga el carácter de reservada o confidencial y la cual se tenga acceso con motivo del presente, asimismo, no dar publicidad de todos aquellos actos y acciones derivadas de la ejecución del presente instrumento, conforme a lo establecido en las leyes en materia de transparencia y acceso a la información pública y protección de datos personales, aplicable a cada una; en el caso de **"LA UNAM"** aplica el Reglamento de Transparencia y Acceso a la información Pública de la Universidad Autónoma de México, publicado en Gaceta UNAM el 25 de agosto de 2016.

DÉCIMA PRIMERA. RELACIÓN LABORAL. "LAS PARTES" acuerdan que el personal designado, contratado o comisionado para la realización de las actividades objeto de este Convenio estará bajo la dependencia directa de la parte que lo designe, contrate o comisione, y se entenderá relacionado exclusivamente con aquella que lo empleó, por lo que cada una de **"LAS PARTES"** asumirá su responsabilidad al respecto, y en ningún caso se considerará a la otra como patrón solidario, sustituto o indirecto; consecuentemente, no tendrán relación alguna de carácter laboral con dicho personal y quedarán liberadas de cualquier responsabilidad que pudiera presentarse en materia de trabajo y seguridad social.

DÉCIMA SEGUNDA. MODIFICACIONES O ADICIONES. El presente Convenio podrá ser modificado o adicionado, y se deberá realizarse mediante la suscripción

del convenio modificatorio respectivo, previo acuerdo entre **"LAS PARTES"** y pactando que dichas reformas solamente tendrán validez cuando hayan sido hechas por escrito y firmadas por sus representantes legales, las cuales serán obligatorias a partir de la fecha de su suscripción.

"LAS PARTES" aceptan que, lo señalado en el párrafo anterior, también aplicará en caso de que el Instituto Nacional Electoral emita disposiciones generales, que impliquen la realización de actividades adicionales a las establecidas en el presente instrumento jurídico; o en su defecto, las que sean determinadas por el Consejo General de **"EL IEEM"**.

DÉCIMA TERCERA. VIGENCIA Y TERMINACIÓN ANTICIPADA. El presente Convenio entrará en vigor a partir del **21 de marzo** hasta el **30 de agosto de 2017**.

Cualquiera de **"LAS PARTES"** podrá dar por terminado este Convenio, mediante aviso por escrito a la otra, notificándolo con 15 días hábiles de anticipación y, en tal caso, tomarán las medidas necesarias para evitar perjuicios tanto a ellas como a terceros, en el entendido de que aquellas actividades derivadas del presente acuerdo de voluntades que se hayan iniciado antes de la fecha que se pretenda concluir el presente instrumento, deberán desarrollarse y concluirse satisfactoriamente. En caso de darse este supuesto, **"EL IEEM"** cubrirá a **"LA UNAM"**, el monto de los gastos erogados y el costo de los trabajos realizados hasta ese momento. De igual forma, **"LA UNAM"** estará obligada a devolver las cantidades que le hayan sido entregadas en exceso por parte de **"EL IEEM"**, previa cuantificación que hagan en conjunto **"LAS PARTES"**, lo anterior con fundamento en lo dispuesto por el artículo 180 de los Lineamientos para la Administración de los Recursos del Instituto Electoral del Estado de México.

DÉCIMA CUARTA. RESPONSABILIDAD CIVIL. Queda expresamente pactado que **"LAS PARTES"** no tendrán responsabilidad civil por los daños y perjuicios que pudieran causarse como consecuencia de caso fortuito o fuerza mayor, particularmente por el paro de labores académicas o administrativas, en el entendido de que una vez superados dichos eventos se reanudarán las actividades en la forma y términos que determinen las partes.

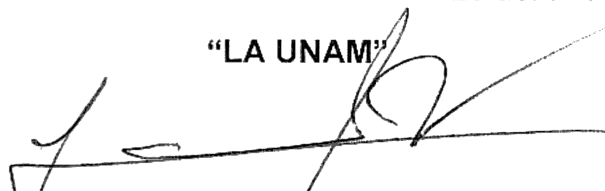
DÉCIMA QUINTA. CESIÓN DE DERECHOS Y OBLIGACIONES. **"LAS PARTES"** convienen que las obligaciones derivadas del presente Convenio, no podrán

cederse o transferirse a ninguna persona física, moral o entidad alguna. Cualquier cesión o traslado de obligaciones realizado en contravención a lo anterior será causa de terminación inmediata del presente Convenio.

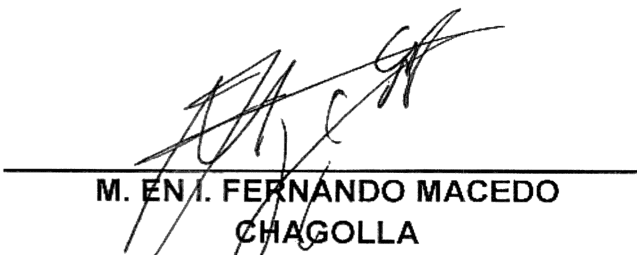
DÉCIMA SEXTA. SOLUCIÓN DE CONTROVERSIAS. El presente convenio es producto de la buena fe por lo que no existe vicio alguno del consentimiento que pudiese implicar su nulidad, por ende, **"LAS PARTES"** convienen en que toda controversia que se suscite en su interpretación y aplicación, será resuelta de común acuerdo por las partes a través de los responsables operativos. Las decisiones que al respecto adopten deberán hacerlas por escrito, anexando dichas constancias al presente instrumento jurídico formando parte integral del mismo. Sin embargo, de subsistir la controversia, **"LAS PARTES"** acuerdan someterse a la jurisdicción de los Tribunales del Fuero Común de Toluca de Lerdo, Estado de México, en el entendido de que el titular de la FES Aragón autorizaría los gastos que para "La UNAM" se originen, en caso de litigio.

Leído el presente Convenio y enteradas **"LAS PARTES"** de su contenido y alcance legal, lo firman al margen y al calce por quintuplicado, en México, Cd. Mx. a los veintidós días del mes de marzo del año dos mil diecisiete.

"LA UNAM"

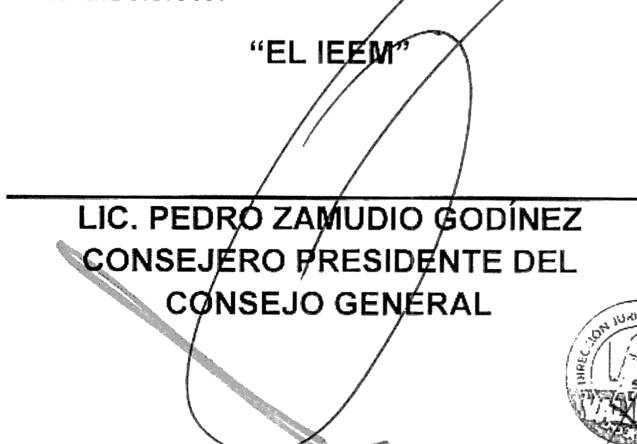


DR. LEONARDO LOMELÍ VANEGAS
SECRETARIO GENERAL

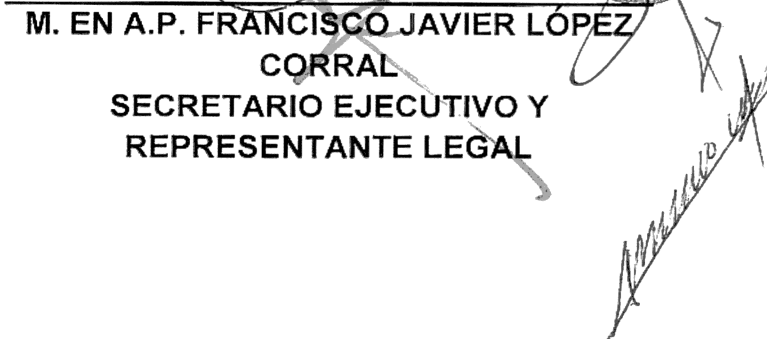


M. EN I. FERNANDO MACEDO
CHAGOLLA
DIRECTOR DE LA FACULTAD DE
ESTUDIOS SUPERIORES ARAGÓN

"EL IEEM"

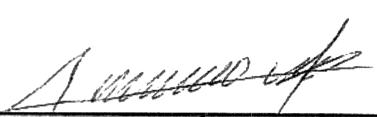


LIC. PEDRO ZAMUDIO GODÍNEZ
CONSEJERO PRESIDENTE DEL
CONSEJO GENERAL



M. EN A.P. FRANCISCO JAVIER LÓPEZ
CORRAL
SECRETARIO EJECUTIVO Y
REPRESENTANTE LEGAL

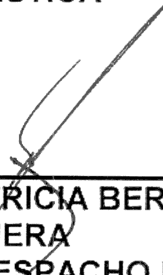




M. EN C. MARCELO PÉREZ MEDEL
ENCARGADO DEL LABORATORIO DE
CÓMPUTO DEL CENTRO TECNOLÓGICO
ARAGÓN



DR. JUAN JOSÉ RIVAUD GALLARDO
JEFE DE LA UNIDAD DE INFORMÁTICA
Y ESTADÍSTICA



MTRA. ALMA PATRICIA BERNAL
OCEGUERA
ENCARGADA DEL DESPACHO DE LOS
ASUNTOS DE LA DIRECCIÓN JURÍDICO
CONSULTIVA
(En términos del artículo 34, párrafo segundo del
Reglamento Interno)
VALIDANDO EL CONTENIDO JURÍDICO

La presente foja forma parte integral del Convenio de Colaboración celebrado entre el Instituto Electoral del Estado de México y la Universidad Nacional Autónoma de México, a través de la Facultad de Estudios Superiores Aragón contenido en quince fojas, de fecha veintiuno de marzo de dos mil diecisiete.

ANEXO TÉCNICO PARA LA AUDITORIA INFORMÁTICA AL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES 2017

I. OBJETIVO GENERAL

Realizar una auditoría informática al Programa de Resultados Electorales Preliminares (PREP) 2017, del Instituto Electoral del Estado de México conforme al reglamento de elecciones aprobado mediante acuerdo del Consejo General del Instituto Nacional Electoral. No. INE/CG661/2016.

De forma general, la auditoría deberá determinar si el sistema del PREP es robusto, confiable, seguro y realiza exclusivamente las operaciones y funciones para las cuales fue diseñado, de acuerdo con el manual de usuario, garantizando la integridad en el procesamiento de toda la información.

II. OBJETIVOS ESPECÍFICOS

1. Revisar el sistema informático y los correspondientes aplicativos desarrollados específicamente para el PREP en términos de funcionalidad. La auditoría deberá determinar, mediante un análisis detallado del código, que los aplicativos PREP realizan las funciones descritas en el manual de usuario y solamente esas, es decir, el programa solamente hace lo que se espera de él, procesando transparente y correctamente la información desde su origen hasta la publicación.

Los aspectos a revisar en el rubro de calidad del sistema son:

- i. Cumplimiento en buenas prácticas de codificación basado en estándares en donde se protejan los componentes por medio de encapsulación, niveles de acceso y buena implementación de estructuras de control.
- ii. Almacenamiento y restauración de datos.
- iii. Manejo de errores.
- iv. Controles adecuados en la entrada de datos.
- v. Verificación de la arquitectura del sistema.
- vi. Evaluación de desempeño y ausencia de leaks de memoria y recursos.

2. Probar todos los aplicativos desarrollados específicamente para el PREP en términos de desempeño, funcionalidad, seguridad y gestión.
3. Analizar las posibles vulnerabilidades de la infraestructura tecnológica del PREP.
4. Probar todos los aplicativos desarrollados específicamente para el PREP en términos de su funcionalidad.
5. Ejecutar pruebas de denegación de servicios, de inyección de código malicioso y de acceso a los diversos recursos del sistema informático. (Ataques de inundación y estrés, paquetes malformados, Envenenamiento de DNS, verificación de pilas TCP/IP fragmentado, Detectar degradación por medio de pruebas Fuzzing)

III. ALCANCES

1. La auditoría se realizará del 27 de febrero al 4 de junio de 2017 con base a siguiente calendario:

Id	Nombre de tarea	Comienzo	Fin	Revisión de los avances
1	Instalación de máquinas virtuales y herramientas para descubrimiento	lun 27/02/17	vie 03/03/17	
2	Organización del personal para repartición de tareas descubrimiento	lun 06/03/17	vie 03/03/17	
3	Selección de autorización para la realización de las pruebas	lun 06/03/17	vie 03/03/17	
4	Inicio de la etapa de descubrimiento	mar 08/03/17	vie 03/03/17	
5	Descubrimiento externo (desde internet)	jue 08/03/17	vie 22/03/17	
6	Descubrimiento interno (en las instalaciones de la infraestructura)	jue 08/03/17	vie 22/03/17	
7	Fin de descubrimiento	mar 22/03/17	vie 22/03/17	
8	Etapas de enumeración	jue 22/03/17	vie 31/03/17	
9	Pruebas de penetración, Prueba DDoS y Análisis de vulnerabilidades	lun 03/04/17	vie 14/04/17	
10	Estructura y entrega del informe parcial	lun 17/04/17	jue 20/04/17	
11	Remediación	vie 21/04/17	jue 27/04/17	
12	Ejecución de nuevos ciclos de pruebas después de remediación	vie 28/04/17	jue 25/05/17	
13	Pruebas de seguridad en centros de captura (Durante simulacros)	lun 05/05/17	vie 26/05/17	
14	Escritura y entrega del segundo informe parcial	vie 26/05/17	mar 02/06/17	
15	Inicio de revisión de calidad de software	lun 17/05/17	lun 27/05/17	
16	Solicitud lista de requerimientos, casos de prueba y manual de usuario	lun 17/05/17	lun 10/06/17	
17	Creación de casos de prueba	lun 13/06/17	lun 27/06/17	
18	Creación de matriz de prueba	lun 13/06/17	vie 30/06/17	
19	Fin de preparación de pruebas	lun 27/06/17	lun 27/06/17	
20	Ejecución de las pruebas de calidad de software en términos de f	mar 22/06/17	vie 30/06/17	
21	Inspección de código fuente	lun 17/06/17	vie 30/06/17	
22	Evaluación del funcionamiento del software en simulacros	lun 04/06/17	jue 29/06/17	
23	Diseño del mecanismo de firma y aseguramiento de la integridad	vie 26/06/17	vie 09/06/17	
24	Escritura del informe final	lun 26/06/17	jue 09/06/17	
25	Revisión de finalización de BD y ejecución de procedimiento de	vie 02/06/17	lun 05/06/17	
26	Escritura del documento de recomendaciones	mar 06/06/17	lun 03/07/17	

2. Se realizará una planificación de la auditoría, identificando claramente los recursos materiales y técnicos necesarios para llevarla a cabo.

3. La auditoría se realizará en:

- i. Centro Estatal de Cómputo (CEsCo)
- ii. Centro Estatal de Cómputo de Respaldo (CEsCoRes)

- iii. En cinco Centros de Acopio y Transmisión de Datos (CATD) que se elegirán posteriormente
 - iv. Centro de Captura y Validación (CCapV)
4. La auditoría se realizará utilizando las siguientes dos metodologías: Manual de la Metodología Abierta de Comprobación de la Seguridad (OSSTMM, Open Source Security Testing Methodology Manual) del Instituto para la Seguridad y Metodologías abiertas (ISECOM, Institute for Security and Open Methodologies), que incluye procedimientos para comprobar los controles a revisar, así como formatos y contenido de los reportes que se deriven de ésta; y la metodología del Proyecto Abierto de Seguridad de Aplicación Web (OWASP, Open Web Application Security Project).
- OSSTM es un estándar para la realización de pruebas y métricas de seguridad desarrollado por un grupo de profesionales especialistas en seguridad informática y agrupados bajo la organización denominada ISECOM (Institute for Security and Open Methodologies). Las siglas OSSTMM hacen referencia al manual o documento guía de OSSTM. Los casos de pruebas de OSSTMM se agrupan en 5 diferentes áreas que, en conjunto, tienen por objeto la verificación de los siguientes aspectos:
- A. Robustez de los controles implementados para la seguridad de la información y de datos.
 - B. Los controles implementados para la infraestructura de cómputo de comunicaciones, de redes inalámbricas y dispositivos móviles.
 - C. Los controles para la detección de intentos de ataques de ingeniería social.
 - D. Los niveles de concientización en relación a los temas de seguridad informática en el personal de una organización.
 - E. Los controles de seguridad física de una organización.
5. Revisar el sistema informático y todos los aplicativos desarrollados utilizando OWASP (www.owasp.org), la cual es una metodología que contiene información de cómo construir un ambiente de pruebas y del tipo de técnicas de verificación que se deben usar en los desarrollos de aplicaciones WEB, teniendo como objetivo principal, el desarrollo de aplicaciones seguras, basándose en lo que se consideran las mejores prácticas de programación.

6. Se verificará que las bases de datos del CEsCo se encuentren vacías, previo al ingreso inicial de los datos que se reciban el día de la jornada electoral (4 de junio d 2017), informando al notario público para que certifique que se está utilizando la aplicación correcta y que las bases de datos están en ceros.

La Metodología utilizada cubrirá las siguientes etapas y actividades:

Para la auditoría a las aplicaciones del sistema informático del PREP

La revisión de:

- Control de ingreso (entrada) de los datos al sistema de aplicación en funcionamiento, así como los demás perfiles del sistema para asegurar que se cumpla con la separación de responsabilidades (administración, dar de alta usuarios, manejo de contraseñas), para asegurar que cada transacción a ser procesada cumpla con los siguientes requisitos:
 - A. Validar la entrada de datos al sistema.
 - B. Procesar solamente datos válidos y autorizados.
 - C. Ingresar los datos una vez por cada transacción.

Se realizará lo siguiente:

- Revisar que las pantallas de captura de datos estén diseñadas en forma consistente con los documentos fuente.
- Revisar que en el ingreso de los datos, la aplicación tenga mensajes de ayuda con el fin de facilitar su captura.
- Restringir el acceso de los usuarios a las diferentes opciones de la aplicación, de acuerdo al perfil.
- Verificar los procedimientos de asignación de permisos a usuarios de la base de datos.
- Verificar en cada pantalla de captura, que los campos de los datos importantes sea de obligatoria digitación.
- En toda la aplicación, revisar que cada campo tenga el formato de datos apropiado.
- Para los campos numéricos y campos fecha, revisar que tengan controles de límite.

- En la captura o modificación de datos críticos revisar que tengan una pista (log o bitácora) donde se identifique lo siguiente: nombre del usuario, fecha y hora, valor del campo y donde se realizó la transacción así como qué tipo de operación fue.
- Verificar que las bitácoras (logs) de la aplicación puedan ser revisados por los responsables para investigar accesos y manipulaciones no autorizadas.
- Verificar la integridad y protección adecuada de las bitácoras.
- En la captura numérica, revisar que se controle la correcta digitación de cantidades.
- En la captura de información revisar que se cuente con los controles adecuados para la disminución de errores de captura.
- Revisar que la aplicación permita imprimir listados de datos ingresados para que estos sean revisados por los usuarios, con el propósito de verificar la correcta inclusión de los datos.
- Validar los procedimientos de excepciones tales como: una acta tenga problemas de origen, datos ilegibles, número de votos mayor que la lista nominal.
- Revisar el funcionamiento del procedimiento del programa que valida al momento que se detecte un error de captura.

Dentro del área de control de entrada de datos se verificarán los siguientes puntos:

- A. Transacciones en línea
- B. Usuario y operador
- C. Terminal o dispositivo de entrada de datos

A. Transacciones en línea.

Revisar que el sistema dispone de los siguientes mecanismos de control:

- Manejo de transacciones erróneas o incompletas.
- Asegurar la consistencia de los datos de las transacciones en la base de datos central.
- Asegurar la integridad de las transacciones en la base de datos central.

- Asegurar que existan mecanismos de detección de errores y de corrección de los mismos.
- Asegurar que existan mecanismos de transacciones en línea que provean de pistas de auditoría para pruebas posteriores.
- Prever la formulación de informes sobre tipos de transacciones desarrolladas.
- Verificar la existencia de manuales y procedimientos de entrenamiento.

B. Usuario y operador de entrada de datos.

Verificar que el sistema cuente con los siguientes controles:

- Minimizar la posibilidad de que se cometan errores humanos durante la captura de datos.
- Asegurar que las funciones que ejecutan los operadores de datos sobre áreas reservadas se ajustan a las políticas y prácticas de control de la organización.
- Permitir el ingreso de datos, consulta y actualización de archivos únicamente a personas propiamente autorizadas e identificadas.
- Desactivar la terminal desde la que se hayan intentado frecuentemente accesos no autorizados o erróneos y validar el procedimiento de reactivación.
- Desactivar terminales después de un número determinado de intentos fallidos de ingreso de datos y el procedimiento de restablecimiento.
- Asegurar el procedimiento para mantener la confidencialidad de las llaves de cifrado de datos y contraseñas en las bases de datos.

C. Terminal o dispositivo de entrada de datos.

Objetivos:

- Asegurar que el sistema sea utilizado por operadores autorizados y desde lugares autorizados.
- Resguardar con seguridad el área destinada a los servidores.
- Asegurar que antes de efectuar una conexión e iniciar una sesión de transmisión de datos, se verifique que la respectiva terminal sea auténtica.

- Asegurar la autenticidad del operador/usuario.

Para la auditoría a la infraestructura de hardware y software que soporta a las aplicaciones.

A. Reconocimiento de la red externa

Identificar los puntos de acceso y consulta que tiene el Instituto para el público en general a fin de ubicar la infraestructura que lo soporta. En este proceso se hará uso de herramientas de mapeo e identificación de red estableciendo los límites de la infraestructura de comunicaciones para desarrollar un modelo para las siguientes etapas:

- Identificación de puntos con presencia en Internet.
- Obtención de registros públicos (NIC).
- Enumeración de nodos externos.
- Enumeración de servicios externos.
- Enumeración de manejadores de base de datos.
- Análisis del contexto general del Instituto.

B. Obtención de equipo objetivo

Basados en los resultados de la etapa anterior se enumerará y conocerán los nodos y servicios activos, así como los que se encuentran en modalidad silenciosa. A partir de esta información, se elaborará un diagrama que registre sistemas operativos, aplicaciones operativas y dispositivos de red alcanzables.

- Documentación de los nodos activos.
- Documentación de los nodos ocultos.
- Enumeración de los nodos confiables.
- Determinar los tipos de sistemas operativos.
- Determinar la configuración de los sistemas operativos.
- Determinar los tipos de manejadores de bases de datos.

C. Valoración de vulnerabilidades

Se realizarán pruebas tanto automatizadas como manuales para obtener acceso a todos los recursos de información de los dispositivos localizados como objetivo en la etapa anterior:

- Identificar riesgos en sistemas operativos y en bases de datos.
- Identificar exploits de acuerdo a las vulnerabilidades encontradas.

D. Pruebas de penetración

Las pruebas se realizarán utilizando las metodologías mencionadas en los alcances. Se analizará la seguridad de la red desde el punto de vista externo (Internet) desde la red local del Instituto (LAN); desde una línea de suscriptor digital asimétrico (ADSL) y mediante la utilización de enlaces privados del Instituto; todas ellas sin el conocimiento previo de la topología de red (caja negra).

Se realizarán estas pruebas con la intención de mostrar el grado de exposición de las aplicaciones, bases de datos e infraestructura del Instituto, las pruebas incluirán:

- Pruebas de "caja negra" y "caja blanca".
 - Pruebas de "man in the middle".
 - Pruebas a las instancias de base de datos.
 - Pruebas de penetración para VMware (en caso de ser utilizado).
 - Pruebas de Active Directory Injection.
 - Pruebas de penetración hacia los aplicativos.
- Depositar banderas en los objetivos que haya sido posible acceder, sin afectar la operación.
 - Evidenciar las vulnerabilidades en aplicaciones, base de datos e infraestructura de TI que permitan acceso o negación de los servicios.
 - Integrar pruebas de penetración a la infraestructura de la red inalámbrica del Instituto, que como mínimo contenga lo siguiente:
 - Obtención de SSID.
 - Obtención de marca de AP.
 - Obtención de APs abiertos.
 - Obtención de tipo de cifrado TKIP (Temporal Key Integrity Protocol) y AES (Advanced Encryption Standard).

- Obtención de autenticación WEP y WPA.
- Pruebas de ruptura de cifrado.
- Direcccionamiento de la red Wireless.
- Identificación de broadcast de SSID.
- Búsqueda de AP sin SSID.
- Validación de tipo de cifrado.
- Captura de tráfico cifrado.

E. Pruebas de negación de servicio

- Pruebas de ataques de negación de servicio distribuidos (DDoS) al sitio principal de difusión del PREP.
- Medir los tiempos de respuesta del servidor mediante la emulación de miles de usuarios simultáneos en la aplicación (pruebas de estrés).
- Aplicar técnicas de inyección de contenido especialmente malformado que permitan sobrecarga del sistema por errores de programación o diseño de la aplicación.
- Realizar pruebas de "fuzzing" en los protocolos identificados y detectar la degradación o la negación de servicio.
- Identificación y análisis de puertos y servicios (UDP / TCP) habilitadas en el perímetro de la red del IEEM.
- Realizar la verificación de manejo de pilas TCP / IP, con técnicas de fragmentación.
- Realizar la inundación de pilas por técnicas ping SYN e ICMP / UDP.
- Aplicar ataques basados en DNS.

IV. EJECUCIÓN DE LA REVISIÓN

La ejecución de la revisión, se realizará en 2 etapas:

Etapas 1 - Verificación de la infraestructura de cómputo y comunicaciones donde operará el PREP con las siguientes actividades:

- Verificar la infraestructura de cómputo y comunicaciones que se encuentre alojada en el Centro de Cómputo propiedad del Instituto.
- Verificar la configuración de la infraestructura de cómputo y comunicaciones que se encuentre alojada en la nube o en el sitio de respaldo del Instituto.

- Comprobar que la arquitectura de la infraestructura de cómputo y comunicaciones corresponda a las necesidades del PREP.
- Verificar que los parches y actualizaciones de los sistemas operativos se encuentren estables; acorde a las necesidades del PREP.
- Comprobar que existan procedimientos que permitan asegurar los accesos físicos y lógicos a la infraestructura de cómputo y comunicaciones del Instituto, además del acceso lógico a la infraestructura ubicada en la nube o en el sitio de respaldo del Instituto.

Etapa 2 – Revisión del software que operará en el PREP con las siguientes actividades:

- Asegurar que la integridad de la información se mantenga en todo momento en el PREP.
- Verificar que el desarrollo del PREP cumpla por lo menos un proceso estándar de Ingeniería de Software: Metodología en cascada, RUP, TSPI, SCRUM, Extreme Programming o semejante.
- Revisión del sistema informático y todos los aplicativos desarrollados utilizando información del OWASP (www.owasp.org), la cual es una organización que provee información de cómo construir un ambiente de pruebas y de técnicas de verificación que se deben usar en el desarrollo de aplicaciones WEB, teniendo como objetivo principal el desarrollo de aplicaciones seguras, con base en lo que se consideran las mejores prácticas de programación a la fecha.
- Las técnicas de verificación serán realizadas empleando software OpenSource o propietario, para implementar el checklist de acuerdo al OWASP, a continuación se presenta:

Authentication. SessionManagement	OWASP-AUTHSM-001	Tamaño de Sesión	Asegurar que la sesión de autenticación tenga una adecuada longitud de con el fin de prevenir que alguien pueda adivinar alguna sesión ya autenticada
	OWASP-AUTHSM-002	"timeout" de sesión	Asegurarse que la Autenticación solo sea válida por un periodo de tiempo
	OWASP-AUTHSM-003	Reuso de sesión	Asegurar que los valores de la Autenticación no sean válidos cuando el usuario se mueve de una sesión protegida (https) a una no protegida (http)
	OWASP-AUTHSM-004	Borrado de sesión	Asegurar que la sesión sea inválida una vez que el usuario se sale de la aplicación
	OWASP-AUTHSM-005	Formato de los valores de sesión	Asegurarse que los valores de autenticación no sean persistentes y que estos no sean escritos en ninguna parte del cache o historial del navegador
Configuration. Management	OWASP-CM-001	Métodos HTTP	Asegurarse que los web servers no permitan las opciones PUT y DELETE
	OWASP-CM-002	Sitios hospedados virtualmente	Determinar si el sitio es hospedado virtualmente
	OWASP-CM-003	Vulnerabilidades conocidas / parches de seguridad	Verificar que las versiones instaladas tengan los últimos parches de seguridad.
	OWASP-CM-004	Archivos de Respaldo	Asegurar que no existe acceso a archivos de respaldo o archivos de configuración de la aplicación públicamente
AppDOS	OWASP-AD-001	"Flooding" de Aplicación	Asegurarse que la aplicación siga funcionando cuando se le envían grandes cantidades de tráfico
	OWASP-AD-002	Bloqueo de Aplicación	Asegurarse que un atacante no pueda provocar que alguna cuenta sea bloqueada
AccessControl	OWASP-AC-001	Análisis de Parámetros	Asegurar que la aplicación mantenga su modelo de análisis de entrada de parámetros de tal manera que el atacante no pueda tener acceso a servicios adicionales
	OWASP-AC-002	Autorización	Asegurar que la aplicación haga una correcta autorización después de la autenticación de usuarios
	OWASP-AC-003	Manipulación de parámetros de Autorización	Asegurar que un usuario una vez autenticado no sea capaz de modificar su "ID" de sesión
	OWASP-AC-004	Autorización de páginas/funciones	Verificar si es posible acceder a páginas que requieren autenticación
	OWASP-AC-005	Ambiente de Aplicación	Verificar que cuando el usuario requiera hacer ciertas acciones antes de hacer otras, estas no puedan ser omitidas
Authentication	OWASP-AUTHN-001	Autenticación por HTTPS	Verificar que las Autenticaciones sean cifradas al menos por SSL
	OWASP-AUTHN-002	Sobrepasar la Autenticación	Asegurar que no se pueda sobrepasar los métodos de autenticación.
Authentication. User	OWASP-AUTHN-003	Envío de credenciales de Autenticación por canal encriptado	Asegurarse que el usuario y contraseña sean enviados en un canal seguro (cifrado)
	OWASP-AUTHN-004	Cuentas por defecto	Verificar que no se usen cuentas y password por defecto
	OWASP-AUTHN-005	Usuarios	Asegurar que el usuario no este público ya sea en correo o en alguna nota
	OWASP-AUTHN-006	Calidad de Contraseñas	Asegurar que la complejidad de las contraseñas sea la correcta.
	OWASP-AUTHN-007	Reinicio de contraseñas	Asegurarse que el usuario responda al menos a una pregunta secreta ante de que la contraseña pueda ser modificada.
	OWASP-AUTHN-008	Bloqueo de contraseñas	Asegurarse que el usuario es bloqueado después de cierto número de intentos fallidos de autenticación
	OWASP-AUTHN-009	Estructura de la contraseña	Asegurarse que la contraseña está bien construida y que al menos use un carácter especial y que la autenticación no pueda ser sobrepasada usando meta caracteres.
	OWASP-AUTHN-010	Contraseñas en Blanco	Asegurarse que no existen contraseñas en blanco

	OWASP-CM-005	Componentes del servidor web	Asegurar que ningún componente de servidor web como apache, tomcat, front page, etc. o módulo de estos provoquen que el servidor este vulnerable.
	OWASP-CM-006	Directorios comunes	Verificar la existencia o no de directorios por defecto en las Aplicaciones
	OWASP-CM-007	Aplicaciones y/o lenguajes cargados por defecto	Verificar que no se estén cargando módulos por defecto de algunas Aplicaciones y/ lenguajes de programación.
Configuration. Management Infrastructure	OWASP-CM-008	Interfaces de Administración	Asegurar que las interfaces administrativas no sean accesibles desde Internet o públicamente.
Error Handling	OWASP-EH-001	Mensajes de errores de la aplicación	Asegurar que los errores que regresa la aplicación no puedan ser usados por un atacante para realizar una fechoría
	OWASP-EH-002	Mensajes de error en usuarios	Asegurar que los errores que regresa la aplicación no puedan ser usados por un atacante para realizar una fechoría
Error Handling	OWASP-EH-001	Errores de Aplicaciones	Asegurar que los errores que regresa la aplicación no puedan ser usados por un atacante para realizar una fechoría
DataProtection	OWASP-DP-001	Datos sensibles en la página HTTP	Asegurar que no existen datos que pueden ser sensibles dentro del cache o historial del navegador
	OWASP-DP-002	Resguardo de Datos	Asegurar que los respaldos mantengan el CIA (Confidentiality, Integrity, Avalability).
Data Protection. Transport	OWASP-DP-003	Versión de SSL	Asegurar que la versión de SSL que se esté usando no tenga vulnerabilidades
	OWASP-DP-004	Métodos de intercambio de SSL KEY	Asegurar que el servidor web no acepte intercambio de llaves de autenticación anónimamente
	OWASP-DP-005	Algoritmos SSL	Asegurar que no existen algoritmos vulnerables
	OWASP-DP-006	Tamaño de las llaves SSL	Asegurar que el sitio mantenga un tamaño apropiado de la llave SSL
	OWASP-DP-007	Validación de Certificados Digitales	Asegurar que la aplicación use certificados digitales validos
Input Validation	OWASP-IV-001	Inyección de scripts	Asegurar que la Aplicación no acepte entradas que no puedan procesar.
Input Validation.SQL	OWASP-IV-002	SQL Injection	Asegurar que la aplicación no procese comandos de SQL desde las entradas de usuario
Input Validation.OS	OWASP-IV-003	Inyección de comandos de SO	Asegurar que la aplicación no permita la inyección de comandos de sistema operativo desde la interfaz de usuario
Input Validation.LDAP	OWASP-IV-004	Inyección de LDAP	Asegurar que la Aplicación no permita procesar comandos de LDAP desde la interfaz de usuario
InputValidation.XSS	OWASP-IV-005	Cross Site Scripting	Asegurar que la aplicación no permita mantener o reflejar scripts maliciosos

- Revisión del sistema informático:
 - Aplica al Programa de Resultados Electorales Preliminares.
 - Se deben revisar los siguientes activos que conforman el sistema informático del Programa, en términos de desempeño, funcionalidad, seguridad y gestión:
 - Aplicación PREP de captura y digitalización (Web y Local).
 - Se deberán validar los 3 aplicativos que conforman el sistema de captura, digitalización y verificación de los datos del PREP, consiste en la compilación y firma de los aplicativos auditados.

- Aplicación Local (concentrador y generador de páginas Web).
 - Base de datos.
 - Servidores WEB.
 - Equipos de comunicaciones y balanceadores de carga.
 - Equipos de seguridad, como firewall, antivirus, etc.
 - Servidores de transferencia segura de archivos.
 - Equipo personal.
 - Servidores.
 - Servidor Web Institucional.
 - Se deberán evaluar los siguientes controles de gestión:
 - Administración de incidentes y problemas.
 - Operaciones y respaldos.
 - Controles de acceso a infraestructura y aplicaciones.
 - Control de cambios.
 - Seguridad física del Centro Estatal de Cómputo, ubicado en la Unidad de Informática del IEEM y en los cinco Centros de Acopio y Transmisión de Datos distritales a seleccionar junto con los dos CCapV.
 - Seguridad en telecomunicaciones.
-
- Verificar que las funcionalidades del PREP, contengan por lo menos el almacenamiento de bitácoras; con el objetivo de que se puedan demostrar los estados en los que se encuentra en cada momento el sistema; lo anterior para solucionar posibles incidentes a presentarse.
 - Verificar que el PREP contenga un catálogo de errores con su respectiva acción correctiva.
 - Comprobar la usabilidad del PREP, la cual tenga accesibilidad a los navegadores a utilizar.
 - Verificar que existan procedimientos para el control de cambios y de versiones del PREP.
 - Comprobar que el PREP, en su caso tenga el licenciamiento requerido para su operación.
 - Verificar que los perfiles de seguridad de los usuarios y/o de acceso a la base de datos, respondan únicamente a las actividades para las cuales fueron creados.
 - Los tipos de vulnerabilidades que se intentarán explotar en aplicativos de los portales externos serán:

- SQL Injection.
 - Cross Site Scripting.
 - Errores en las aplicaciones.
 - Errores en los patrones de base de datos.
 - Directorios ocultos.
 - LDAP Injection.
 - Command Injection.
 - Buffer overflow.
 - Manipulación de parámetros http.
 - Corrupción de archivos.
 - Envenenamiento de Cookies.
- Realizar pruebas en las aplicaciones de los portales que sean necesarias para identificar:
 - Riesgos de seguridad.
 - URLs escaneadas.
 - URLs vulnerables.
 - Causas de los problemas de seguridad clasificados por tipo de amenaza.
 - Responsables de mitigación por cada uno de los problemas de seguridad encontrados durante las pruebas.
 - Tareas necesarias para la mitigación de los problemas de seguridad encontrados.

En caso de obtener acceso a algún servidor de bases de datos o servidor interno, se enumerarán los manejadores de bases de datos que se puedan "ver", el punto desde donde se tuvo acceso y se intentó comprometerlos. Toda la información a la que se tenga acceso, o bien, se obtenga a partir de los resultados de la prueba.

- Realizar el análisis de vulnerabilidades en la infraestructura tecnológica del PREP y contemplará lo siguiente:
 - Ejecución de herramientas automatizadas de búsqueda de vulnerabilidades.
 - Pruebas de inyección de código malicioso.
 - Pruebas de penetración internas y externas que incluirán pruebas de acceso a los diversos recursos del sistema informático.

- Análisis de código estático que consistirán en técnicas de análisis de código fuente.
- Pruebas de código dinámico sobre la aplicación en ejecución.
- El objetivo será la detección de los siguientes tipos de vulnerabilidades:
 - Cross Site Scripting (XSS).
 - SQL Injection.
 - Buffer overflow.
 - Los top 10 más recientes de OWASP.

V. EJECUCIÓN DE LAS PRUEBAS

Para la realización de las pruebas, se empleará la metodología OSSTMM (Open Source Security Testing Methodology Manual).

Las pruebas se realizarán en dos periodos de tiempo:

- Primero: Previo y durante el primer simulacro.
- Segundo: Una vez solventados los posibles hallazgos encontrados en el primer periodo de pruebas.

En el caso de requerir más pruebas para fortalecer el PREP se realizarán conforme lo determinen el Instituto y el auditor.

Se realizarán las pruebas en el sitio central donde operará el PREP y de forma remota en el caso de las pruebas de penetración y búsqueda de vulnerabilidades.

Las pruebas que se ejecutarán para el PREP son:

- Pruebas de Calidad: Todos los aplicativos desarrollados específicamente para el PREP deberán ser revisados en términos de funcionalidad. Se requiere al menos los siguientes:
 - Modularidad del código.
 - Estándares y estilo de codificación.
 - Separación de responsabilidades.
 - Manejo de errores.
 - Leaks de memoria/recursos.

- Seguridad de threads/aislamiento.
 - Desempeño.
 - Encapsulamiento.
 - Estructuras de control.
 - Entrada de datos (Batch/On-line).
 - Transmisión de datos.
 - Procesos en la computadora.
 - Almacenamiento y recuperación de datos.
 - Salida de datos, distribución y recepción de resultados.
- Pruebas de denegación de servicio - en el caso de encontrar hallazgos; estos serán documentados con las evidencias respectivas para su mitigación.
 - Pruebas de vulnerabilidad - se evidenciará y documentará el grado de visibilidad y el nivel de exposición ante ciertos riesgos de inclusión de código malicioso, o algún otro ataque controlado; comprobando así la efectividad de la prueba. Esto es, que para considerar que una vulnerabilidad fue exitosa es necesario contar con la bandera o evidencia de intrusión.
 - Escaneo de puertos - identificando así los sockets del PREP; los cuales deberán ser exclusivamente los necesarios para atender los servicios solicitados.
 - Pruebas de estrés a las aplicaciones que se utilicen en el PREP; identificando así los siguientes umbrales de riesgo: alto, moderado, menor, bajo.

Las pruebas se realizarán ante dos modalidades:

- "Caja negra" - Para los sistemas expuestos a Internet.
- "Caja blanca" - Para los sistemas internos que operan en el PREP.

VI. DEL USO DE EQUIPO POR PARTE DEL AUDITOR

Todo equipo de cómputo propiedad del auditor que requiera conectarse a la infraestructura de red del Instituto, estará protegido y actualizado contra

código malicioso, virus, troyanos, etc., y cumplirá con las políticas de seguridad para equipos de terceros.

Todas la herramientas y software utilizado para la auditoría deben ser del ente auditor, el IEEM no proporcionará ningún tipo de licenciamiento para el levantamiento de dicha auditoría; todo el software instalado por parte de la empresa auditora será removido al final de la auditoría.

VII. DE LA PRESTACIÓN DEL SERVICIO

Una vez que el auditor concluya con su revisión y haya presentado los resultados, deberá eliminar cualquier rastro en la infraestructura del Instituto originado a raíz de las pruebas realizadas.

Sólo se podrán instalar, con previa autorización, aplicaciones de acceso remoto que sean claramente identificables como procesos activos y cuyos puertos, y conexiones sean visibles. Estas aplicaciones deberán permanecer apagadas y desinstaladas mientras no estén en uso. Queda prohibido modificar la configuración de un servidor, estación de trabajo o dispositivo de red. Si se llegase a requerir un cambio temporal, éste deberá ser autorizado y programado con antelación. Al terminar la prueba controlada, se deberá confirmar que la configuración regreso a su estado original y que no hubo ninguna afectación.

Queda prohibido borrar, alterar o apagar el uso de las bitácoras (logs) en cualquier dispositivo, estación de trabajo o servidor. Se requiere que todas las acciones del auditor queden registradas de forma normal en las bitácoras existentes.

VIII. INFORME DE LA REVISIÓN Y RECOMENDACIONES

Los informes de la auditoría se emitirán en 2 momentos diferentes:

- Primero – Consistirá en los resultados emitidos durante el proceso de auditoría enfocada a los hallazgos y recomendaciones los cuales deben estar enfocados a garantizar la integridad de los resultados presentados.

- Segundo – Consistirá en el resultado final de la auditoría donde se argumente las condiciones en que operará.

Los informes de la auditoría tendrán 2 modelos básicos: El primero de ellos consiste en lo referente a los resultados emitidos durante el proceso de auditoría enfocada a los hallazgos y recomendaciones. El segundo de ellos consiste en el resultado final de la auditoría donde se argumenten las condiciones en que operará el PREP.

Las recomendaciones realizadas deberán ser precisas y objetivas, enfocadas a cumplir la continuidad del PREP. Deberán igualmente incluir los datos, hechos y observaciones en que se basen las recomendaciones propuestas.

Los informes se tipificarán de la siguiente manera:

- Informes Parciales: son los referentes a los resultados emitidos durante el proceso de auditoría, los cuales tendrán **calidad de reservados** en términos de las disposiciones aplicables en materia de transparencia y acceso a la información.
- Informe Final: es el correspondiente a los resultados finales de la auditoría, que considera el cierre de operaciones del PREP, así como también la etapa de evaluación del mismo. Dicho informe **será público**.
- Informe de evaluación que considere el cierre de operaciones del PREP, así como la etapa de evaluación del mismo, donde contenga:
 - i. Análisis de vulnerabilidades y pruebas de penetración realizadas a la infraestructura tecnológica del PREP.
 - ii. Nivel de exposición de la información.
 - iii. Desempeño del sistema.
 - iv. Opinión general del comportamiento del sistema (fundamentada).
 - v. Nivel de exposición de la información (evidencias).
 - vi. Observaciones.
 - vii. Sugerencias.

IX. EXCLUSIONES

El desarrollo de las pruebas de seguridad y la revisión de calidad en términos de funcionalidad no incluye:

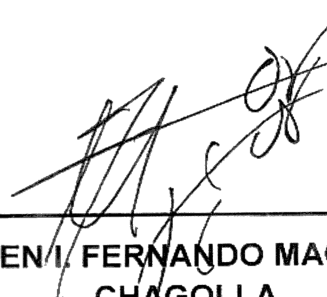
- Cambios a la infraestructura.
- Implementación de las recomendaciones.

Leído el presente Convenio y enteradas **"LAS PARTES"** de su contenido y alcance legal, lo firman al margen y al calce por quintuplicado, en México, Cd. Mx. a los veinte días del mes de febrero del año dos mil diecisiete.

"LA UNAM"

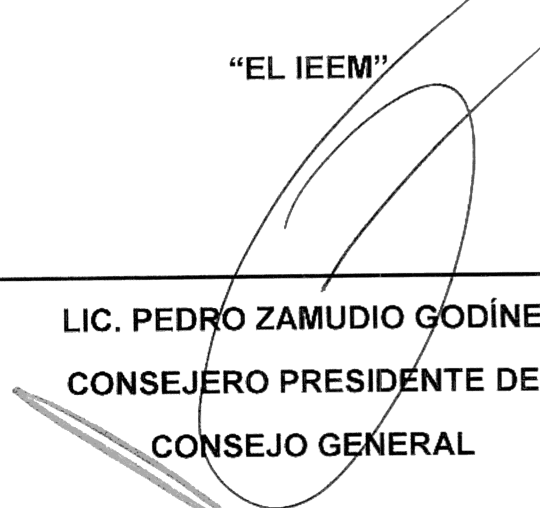


DR. LEONARDO LOMELÍ VANEGAS
SECRETARIO GENERAL

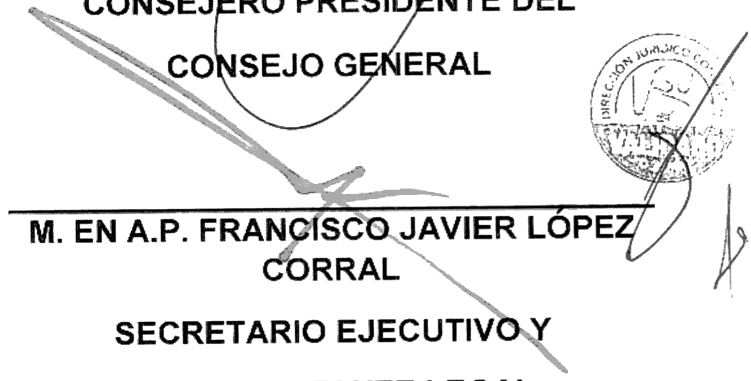


M. EN. FERNANDO MACEDO
CHAGOLLA
DIRECTOR DE LA FACULTAD DE
ESTUDIOS SUPERIORES ARAGÓN

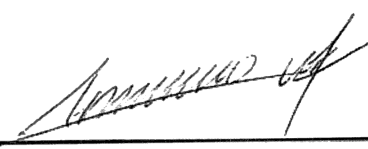
"EL IEEM"



LIC. PEDRO ZAMUDIO GODÍNEZ
CONSEJERO PRESIDENTE DEL
CONSEJO GENERAL



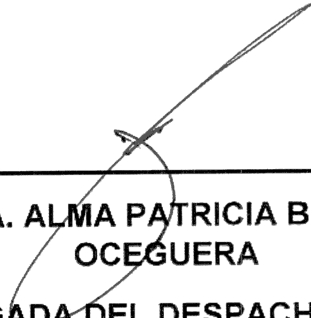
M. EN A.P. FRANCISCO JAVIER LÓPEZ
CORRAL
SECRETARIO EJECUTIVO Y
REPRESENTANTE LEGAL



M. EN C. MARCELO PÉREZ MEDEL
ENCARGADO DEL LABORATORIO DE
CÓMPUTO DEL CENTRO TECNOLÓGICO
ARAGÓN



DR. JUAN JOSÉ RIVAUD GALLARDO
JEFE DE LA UNIDAD DE INFORMÁTICA
Y ESTADÍSTICA



MTRA. ALMA PATRICIA BERNAL
OCEGUERA
ENCARGADA DEL DESPACHO DE LOS
ASUNTOS DE LA DIRECCIÓN JURÍDICO
CONSULTIVA

(En términos del artículo 34, párrafo
segundo del Reglamento Interno)

VALIDANDO EL CONTENIDO JURÍDICO