

ANEXO TÉCNICO NÚMERO UNO AL CONVENIO ESPECIFICO DE COLABORACIÓN CV-COSJ-CFATA-014-X/2017 PARA LA AUDITORÍA DE VERIFICACIÓN Y ANÁLISIS DEL SISTEMA INFORMÁTICO Y A LA INFRAESTRUCTURA TECNOLÓGICA QUE SERÁ UTILIZADA EN LA IMPLEMENTACIÓN Y OPERACIÓN DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES, PARA EL PROCESO ELECTORAL LOCAL ORDINARIO 2017-2018, EN LO SUCESIVO “LA AUDITORÍA”, QUE CELEBRAN POR UNA PARTE EL INSTITUTO ELECTORAL DEL ESTADO DE QUERÉTARO, EN LO SUCESIVO EL “IEEQ”, REPRESENTADO POR EL M. EN A. GERARDO ROMERO ALTAMIRANO, CONSEJERO PRESIDENTE DEL CONSEJO GENERAL Y EL LIC. JOSÉ EUGENIO PLASCENCIA ZARAZÚA, SECRETARIO EJECUTIVO Y REPRESENTANTE LEGAL; Y POR LA OTRA LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, EN LO SUCESIVO LA “UNAM”, REPRESENTADA EN ESTE ACTO POR EL DR. RAMIRO PÉREZ CAMPOS, EN SU CARÁCTER DE PRESIDENTE DEL CONSEJO DE DIRECCIÓN Y DIRECTOR DEL CENTRO DE FÍSICA APLICADA Y TECNOLOGÍA AVANZADA A QUIENES ACTUANDO CONJUNTAMENTE SE LES DENOMINARÁ “LAS PARTES”, CONFORME A LOS ANTECEDENTES, DECLARACIONES Y CLÁUSULAS SIGUIENTES:

ANTECEDENTES

PRIMERO. En el Convenio Específico de Colaboración **CV-COSJ-CFATA-014-X/2017** firmado por “**LAS PARTES**”, se prevé la suscripción de un Anexo Técnico que establezca las especificaciones para desarrollar “**LA AUDITORÍA**” y se precisen alcances, metodología, plan de trabajo base, incluyendo actividades, fechas, responsabilidades y recursos necesarios para su cumplimiento, la descripción de la información que “**EL IEEQ**” entrega a “**LA UNAM**” y 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 Programa de Resultados Electorales Preliminares.

SEGUNDO. En fecha 19 de enero de 2018, se remitió por parte de la Unidad Técnica de Vinculación con los Organismos Públicos Locales del Instituto Nacional Electoral, la circular número INE/UTVOPL/044/2018, mediante la cual hace del conocimiento de “**EL IEEQ**”, los requisitos mínimos para la elaboración del anexo técnico para la contratación de los servicios de auditoría al sistema informático y la infraestructura tecnológica del Programa de Resultados Electorales Preliminares.



[Handwritten signatures and initials]

De esta manera, se suscribe el presente Anexo Técnico, con base en las siguientes:

DECLARACIONES

ÚNICA. "LAS PARTES" reconocen expresamente la personalidad que ostentan como autoridades firmantes y acuerdan tener por reproducidas como si a la letra se insertase las declaraciones contenidas en el Convenio Específico de Colaboración **CV-COSJ-CFATA-014-X/2017** celebrado el 16 de noviembre de 2017, mencionado en el antecedente Primero del presente instrumento.

CLÁUSULAS

PRIMERA. OBJETO. El presente Anexo Técnico Número Uno, tiene por objeto precisar los alcances, metodología, plan de trabajo base, actividades, fechas, responsabilidades y recursos necesarios, la descripción de la información que **"EL IEEQ"** entrega a **"LA UNAM"** y las fechas, contenido y términos en los que **"LA UNAM"** presentará los informes parciales y final, respecto de **"LA AUDITORÍA"**.

APARTADOS

1. GLOSARIO DE TÉRMINOS Y ACRÓNIMOS

Para efectos del presente Anexo Técnico, se entenderá por:

INE. Instituto Nacional Electoral

IEEQ. Instituto Electoral del Estado de Querétaro.

CFATA. Centro de Física Aplicada y Tecnología Avanzada de la Universidad Nacional Autónoma de México, Campus Juriquilla

Proceso Electoral. Proceso Electoral Local Ordinario 2017-2018.

PREP. Programa de Resultados Electorales Preliminares para el Proceso Electoral.

Convenio de Colaboración. Convenio específico de colaboración para la auditoría de verificación y análisis del sistema informático que será utilizado en la implementación y operación del PREP, celebrado entre **"LA UNAM"** y **"EL IEEQ"**.



Auditoría. Auditoría de verificación y análisis de los sistemas informáticos e infraestructura tecnológica del PREP.

Ente Auditor. Entidad encargada de realizar la auditoría.

TIC. Tecnologías de la Información y Comunicación.

Activos. Los activos comprenden equipos informáticos, redes de comunicaciones y aplicaciones de software a través de los cuales se procesa información relacionada con el PREP.

Caja negra. Son pruebas/auditorías que se realizan sin conocimiento de la estructura interna o funcionamiento de un sistema/red o sitio web, el cual simula un ataque real de forma mal intencionada.

Bug tracking system. Aplicación informática que permite registrar y dar seguimiento a los defectos detectados en el software.

Exposición de información. Acto o proceso que revela, presenta una fuga de información o viola la privacidad de datos. Puede derivarse de una vulnerabilidad en algún activo de información (físico, lógico o humano).

Huella criptográfica. Una huella criptográfica (SHA-256) es una clave conformada por caracteres alfanuméricos que es generada como resultado de una función matemática y que permite identificar un archivo electrónico de manera única.

Infraestructura tecnológica. Comprende los equipos de cómputo y las redes de telecomunicaciones, así como el sistema informático con el que opera el PREP.

Reglamento de Elecciones. Reglamento de Elecciones del INE, aprobado por el Consejo General el 7 de septiembre de 2016 y sus modificaciones aprobadas el 22 de noviembre de 2017 y 14 de febrero de 2018.

Lineamientos del PREP. Anexo 13 del Reglamento del INE.

Pentest. Las pruebas de penetración son una serie de técnicas utilizadas para evaluar la seguridad de redes, sistemas y aplicaciones informáticas en un ambiente totalmente controlado el cual simula un ataque real.

Simulacro. Evento previo al día de la Jornada Electoral, en que se reproduce el proceso técnico operativo de manera integral, para evaluar el óptimo funcionamiento del sistema informático y los procedimientos.

4
g
RPC.

Vulnerabilidad. Se puede considerar como una debilidad un ataque de cualquier tipo que afecte la confidencialidad, integridad o disponibilidad de un activo de información. Dicha vulnerabilidad es la intersección de tres elementos: un sistema susceptible a una falla, un atacante con la capacidad de explotar dicha falla y el acceso a la misma.

2. OBJETIVOS

2.1. General

Llevar a cabo **“LA AUDITORÍA”** para el Proceso Electoral de las elecciones locales de Diputaciones y Ayuntamientos del Estado de Querétaro; con la finalidad de evaluar la integridad, disponibilidad y seguridad en el procesamiento de la información y la generación de los resultados conforme a lo dispuesto en la Sección Cuarta, Capítulo II del Reglamento de Elecciones, así como el título II, capítulo III de los Lineamientos del PREP.

2.2. Específicos

- a) Analizar el sistema informático del PREP, mediante la realización de pruebas funcionales de caja negra, para evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares, conforme a lo establecido en el artículo 347, numeral 1, inciso a) del Reglamento de Elecciones.
- b) Validar al inicio, durante y al final de la operación del PREP y ante la presencia de un tercero con fe pública, que los sistemas informáticos del PREP que operarán el día de la Jornada Electoral, correspondan al software auditado, así como que la base de datos se encuentre sin registros adicionales a los necesarios para que el sistema opere.
- c) Identificar debilidades de seguridad en la infraestructura tecnológica mediante la ejecución de pruebas de penetración y revisión de configuraciones de seguridad.
- d) Clasificar el impacto y documentar las vulnerabilidades identificadas con el propósito de recomendar a **“EL IEEQ”** las posibles medidas para la mitigación de las vulnerabilidades que previamente fueron identificadas y documentadas.
- e) Realizar ataques de negación de servicio que permitan identificar, evaluar y aplicar las medidas necesarias para asegurar la correcta y continua disponibilidad del servicio Web de los sitios de publicación de

resultados del PREP y del sitio principal de “EL IEEQ”, durante el periodo de operación del PREP.

- f) Auditar los módulos y/o programas que conforman el PREP para el caso del software así como los activos tecnológicos en el caso de la infraestructura tecnológica.

3. ALCANCES

3.1. Los sistemas informáticos e infraestructura tecnológica que estarán sujetos al análisis, serán aquellos que sean utilizados por el PREP y se encuentren en los siguientes recintos:

- a) Dos Centros de Captura y Verificación, ubicados en los domicilios aprobados mediante acuerdo IEEQ/CG/A/011/18.

CENTRO DE CAPTURA Y VERIFICACIÓN	DOMICILIO
PRINCIPAL	PROLONGACIÓN PINO SUÁREZ 479, COLONIA EJIDO MODELO, QUERÉTARO, QRO.
RESPALDO	AV. CATARATAS 15, BODEGA 5, FRACC. LA NORIA, EL MARQUÉS, QRO.

- b) Centros de Acopio y Transmisión de Datos instalados en las sedes de los 15 Consejos Distritales y 12 Municipales, ubicados en los siguientes domicilios:

CONSEJO ELECTORAL	TIPO	DOMICILIO
QUERÉTARO	DISTRITAL 1	CALLE REAL DE ZIMAPÁN 157, COL. VILLAS DEL PARQUE, QUERÉTARO, QRO.
QUERÉTARO	DISTRITAL 2	AV. BELLAVISTA 2121, PLAZA LAS FLORES, COLONIA RANCHO BELLAVISTA, QUERÉTARO, QRO.

QUERÉTARO	DISTRITAL 3	CALLE REAL DE VALPARAÍSO 418, FRACC. REAL DEL MARQUÉS, QUERÉTARO, QRO.
QUERÉTARO	DISTRITAL 4	CALLE LIQUÍDAMBAR 14, COLONIA ARBOLEDAS, QUERÉTARO, QRO.
QUERÉTARO	DISTRITAL 5	CALLE CERRO DEL AIRE 210, COL. COLINAS DEL CIMATARIO, QUERÉTARO, QRO.
QUERÉTARO	DISTRITAL 6	CALLE ECUADOR 34, COLONIA LOMAS DE QUERÉTARO, QUERÉTARO, QRO.
QUERÉTARO	DISTRITAL 13	CALLE 16 DE SEPTIEMBRE 62, SANTA ROSA JAUREGUI, QUERÉTARO, QRO.
CORREGIDORA	DISTRITAL 7	CALLE RUFINO TAMAYO 4 E, FRACC. PUEBLO NUEVO, EL PUEBLITO CORREGIDORA, QRO.
CORREGIDORA	MUNICIPAL	CALLE FRAY BUENAVENTURA TOVAR 6, COL. LA CIENEGA, CORREGIDORA, QRO.
AMEALCO DE BONFIL	MUNICIPAL	CALLE NOGAL 27, COL. MIRADORES, AMEALCO DE BONFIL, QRO.
SAN JUAN DEL RÍO	DISTRITAL 8	CALLE 20 DE NOVIEMBRE 33, FRACCIONAMIENTO LA PAZ, SAN JUAN DEL RÍO, QRO.
SAN JUAN DEL RÍO	DISTRITAL 9	CALLE FRANCISCO MÁRQUEZ 21, COL. SAN

Handwritten signatures and initials on the right margin, including a large signature that appears to be "RRC" and other smaller marks.

		JUAN BOSCO, SAN JUAN DEL RÍO, QRO.
SAN JUAN DEL RÍO	MUNICIPAL	CALLE CAMINO AL RASTRO 123, FRACC. LOS OLIVOS, SAN JUAN DEL RÍO, QRO.
PEDRO ESCOBEDO	DISTRITAL 10	CALLE HEROICO COLEGIO MILITAR 3, COL. CENTRO, PEDRO ESCOBEDO, QRO.
EL MARQUÉS	DISTRITAL 12	AV. EL MARQUÉS SIN NÚMERO, COLONIA CENTRO, EL MARQUÉS, QRO.
TOLIMÁN	MUNICIPAL	CALLE HEROICO COLEGIO MILITAR S/N, COL. CENTRO, TOLIMÁN, QRO.
CADEREYTA DE MONTES	DISTRITAL 14	CALLE JOSE MA. MORELOS S/N, COL. CENTRO, CADEREYTA DE MONTES, QRO.
JALPAN DE SERRA	DISTRITAL 15	CARR. SAN JUAN DEL RÍO-XILITLA KM 181, COL. EL PUENTE, JALPAN DE SERRA, QRO.
ARROYO SECO	MUNICIPAL	CALLE BENITO JUÁREZ SIN NÚMERO, COL. CENTRO, ARROYO SECO, QRO.
COLÓN	MUNICIPAL	CALLE GUANAJUATO 9, COL. CENTRO, COLÓN, QRO.
EZEQUIEL MONTES	MUNICIPAL	CALLE FRANCISCO I. MADERO 206, BARRIO LA BOLA, EZEQUIEL MONTES, QRO.
HUIMILPAN	MUNICIPAL	CALLE IGNACIO ALDAMA 206, COL. CENTRO, HUIMILPAN, QRO.

RPE

		QRO.
LANDA DE MATAMOROS	MUNICIPAL	CALLE CAYETANO RUBIO 412, COL. CENTRO, LANDA DE MATAMOROS, QRO.
PEÑAMILLER	MUNICIPAL	CALLE PINO SUAREZ S/N COL. CENTRO, PEÑAMILLER, QRO.
PINAL DE AMOLES	MUNICIPAL	CARR. SAN JUAN DEL RÍO-XILITLA S/N COL. CENTRO, PINAL DE AMOLES, QRO.
SAN JOAQUÍN	MUNICIPAL	PROL. INSURGENTES 32, COL. CENTRO, SAN JOAQUÍN, QRO.
TEQUISQUIAPAN	DISTRITAL 11	CALLE PASEO DEL JAZMIN 48 A, BARRIO DE SAN JUAN, TEQUISQUIAPAN, QRO.

c) Oficinas centrales de “**EL IEEQ**” en Av. Las Torres 102, Residencial Galindas, Querétaro, Qro. y

d) Centros de Datos.

3.2. Los sistemas informáticos del PREP deberán generar y almacenar bitácoras para facilitar los procedimientos de verificación, análisis y auditoría de los mismos.

3.3. Las pruebas funcionales de caja negra se efectuarán a todos los sistemas informáticos del PREP, con la finalidad de evaluar la integridad en el procesamiento de la información y la generación de resultados preliminares dentro de un ambiente controlado y homólogo al que se utilizará en la elección local el día de la jornada electoral.

3.4. El análisis de vulnerabilidades consistirá en la realización de pruebas de penetración y revisión de configuraciones a la infraestructura tecnológica del PREP.

3.5. “LA AUDITORÍA” se ejecutará sobre todos los módulos del sistema informático previo al inicio de los simulacros; si de las pruebas y

4



simulacros resultara necesario realizar ajustes al sistema, “EL IEEQ” contará con un margen de tiempo que permita aplicar las medidas que resulten necesarias y garantizar que el sistema auditado sea el que opere para el PREP.

3.6. “LA UNAM” presenciara y evaluará la operación del PREP durante los tres simulacros que “EL IEEQ” realice.

3.7. Comprobar al inicio, durante y al final de la operación del PREP, que las aplicaciones informáticas utilizadas correspondan a los programas auditados.

3.8. Ejecutar un procedimiento que garantice que las bases de datos no cuenten con información de votos para ninguna fuerza política, candidatos no registrados y votos nulos; previo a la puesta en operación del PREP el día de la Jornada Electoral.

4. EXCLUSIONES

4.1. Queda excluida de “LA AUDITORÍA”, la revisión de los procedimientos operativos y la logística del PREP, así como todo lo relacionado a la auditoría de los recursos humanos, materiales y financieros. Se excluye también la revisión de otros aspectos del sistema informático que no sean explícitamente los señalados en los Lineamientos del PREP.

4.2. Queda excluida la revisión de la funcionalidad que no se encuentre directamente relacionada con la captura, procesamiento y despliegue de la información de las actas de escrutinio y cómputo, como son modos de operación diferentes al de la jornada electoral, la generación de certificados digitales de capturistas, configuración de tokens, entre otros.

4.3. No se contempla la evaluación de aspectos de usabilidad, accesibilidad y visibilidad.

4.4. Las pruebas de vulnerabilidades se realizarán en los recintos descritos en el numeral 2.1 del apartado Alcance y quedan excluidas las pruebas a equipos fuera del Estado de Querétaro.

4.5. “EL IEEQ” será el único responsable de llevar a cabo la instalación y configuración de los dispositivos de seguridad (firewalls, routers, switches, entre otros) del PREP, por lo que la “LA UNAM” no brindará asesoría sobre este tipo de actividades.



- 4.6. No se llevarán a cabo pruebas de denegación de servicio a dispositivos no relacionadas con la infraestructura tecnológica del PREP y que no se describan en el alcance.
- 4.7. Queda excluidas las pruebas de penetración a dispositivos que no sean administrados por “EL IEEQ”.
- 4.8. No está dentro del alcance del proyecto implementar las medidas de seguridad de la infraestructura tecnológica del PREP y sitios principales y alternos de “EL IEEQ”.
- 4.9. No se realizará la revisión de la configuración de la infraestructura tecnológica, ni la instalación y configuración de equipo de cómputo y telecomunicaciones.
- 4.10. Queda excluido el monitoreo de incidentes de seguridad.
- 4.11. Queda excluida cualquier actividad, entregable o pruebas a cualquier software, aplicación o servicio que no haya sido especificado expresamente en el alcance y/o que no se haya entregado en los tiempos y forma acordados, la interacción con otros sistemas informáticos y otros componentes desarrollados por entidades externas a “EL IEEQ”.

5. METODOLOGÍA

- 5.1. Se utilizará como metodología, el “**Protocolo de Auditoría del Sistema Informático del PREP 2018**” autorizado por “LA UNAM” en su versión 5 emitido por la Dirección General de Cómputo y de Tecnologías de la Información y Comunicación de la Universidad Nacional Autónoma de México en enero de 2018.

La metodología de revisión contempla tres líneas de trabajo:

1. Pruebas funcionales de caja negra al sistema informático del PREP

Las pruebas funcionales de caja negra deben realizarse en una infraestructura y ambiente tecnológico similar al que se usará durante la jornada electoral, el cual será habilitado por parte de “EL IEEQ”.

Este ambiente debe contemplar la implementación de una maqueta con la infraestructura tecnológica y el sistema informático en

Handwritten signature and initials in the bottom right corner of the page.

operación para realizar la digitalización, captura, procesamiento y despliegue de las actas de escrutinio y cómputo, así como simular algunos Centros de Acopio y Transmisión de Datos con base en una muestra de entidades y distritos seleccionados por el ente auditor.

Durante la ejecución de las pruebas se analizará el funcionamiento de la aplicación con relación a la captura, procesamiento y despliegue de la información de las actas de escrutinio y cómputo, de acuerdo con la normativa aplicable a la elección.

Como resultado de las pruebas funcionales de caja negra se deben identificar, clasificar y priorizar los hallazgos detectados.

Para apoyar la comunicación y el seguimiento de los hallazgos identificados durante las pruebas, es conveniente habilitar una herramienta de seguimiento de incidencias tipo “bug tracking system” con los mecanismos apropiados para garantizar la comunicación segura entre el equipo de trabajo de “LA UNAM” y el equipo de trabajo de “EL IEEQ”.

Revisión del sistema informático y todos los aplicativos desarrollados específicamente para el PREP, en términos de funcionalidad.

- a) Para la revisión de requisitos funcionales será necesario que el sistema informático publique los datos mínimos obligatorios.
- b) Para la revisión de funciones mínimas:
 - Que el sistema informático permita la captura, digitalización y publicación de los datos asentados en las actas de escrutinio y cómputo que se reciben en los Centros de Acopio y Transmisión de Datos.
 - Que el sistema informático integre los procesos de captura, verificación, transmisión, recepción, consolidación y difusión de los resultados electorales preliminares de las elecciones, en el marco de la normatividad vigente.
 - Que se maneje la Integridad en el registro de la información. Que a partir de un acta de escrutinio y cómputo en papel, se genere una imagen digital

Handwritten signature and initials (RPC) on the right margin.

completa y legible de ésta y sea almacenada sin alteraciones en su contenido y publicada para consulta.

- Que la imagen digital del acta de escrutinio y cómputo, así como sus datos capturados manualmente sean debidamente asociados a la casilla, sección y distrito que corresponda. Que los resultados del acta de escrutinio y cómputo capturados sean asociados fielmente al partido político, coalición, candidatura independiente o rubro en el cual se registren.

c) Para la revisión de desempeño se considerará el universo válido de información: únicamente se verificará que el sistema implemente dicha validación o restricción a partir de un catálogo de información el cual deberá tener cargada previamente la información de las casillas válidas. No será competencia del ente auditor ni alcance de la auditoria, garantizar que dichas casillas son las que tendrían que existir en la elección, ya que esto es competencia de la autoridad electoral. También se considerarán la Contabilización de actas de escrutinio y cómputo y la presentación de resultados acumulados.

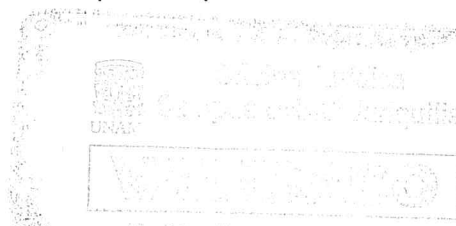
d) Adicionalmente, se revisará que el sistema informático genere y almacene bitácoras y pistas de auditoría que faciliten los procesos de verificación, análisis y auditoría de los sistemas.

2. Validación del sistema informático del PREP y de sus bases de datos

Validación de los programas auditados

Se deberán obtener las huellas criptográficas de la última versión de los programas probados para identificarlos de manera unívoca y contar así con las huellas maestras que sirvan de referente para su posterior cotejo.

Para ello, se sugiere implementar un mecanismo automatizado que permita obtener las huellas criptográficas de los programas instalados en el ambiente de pruebas que fueron auditados, así como resguardar esta información en un medio de almacenamiento seguro y que sea resguardado de manera inviolable por las partes.



Este procedimiento deberá ser atestiguado por un tercero con fe pública, generando como resultado de este acto una constancia de hechos firmada por todas **"LAS PARTES"**.

Previo al inicio de operaciones del sistema informático del PREP, se deberá realizar la obtención de las huellas criptográficas de los programas que se encuentran instalados en los equipos de cómputo y servidores de producción que se pondrán en operación, así como el cotejo de estas huellas respecto a las huellas criptográficas maestras obtenidas en el punto anterior.

Para facilitar el cotejo, se sugiere apoyarse de alguna herramienta de software que permita automatizar esta actividad y generar los reportes de resultados.

Este procedimiento deberá ser atestiguado por un tercero con fe pública, generando como resultado de este acto una constancia de hechos firmada por todas **"LAS PARTES"**.

Adicional a esta validación que se realiza previo al inicio de operaciones del PREP, es conveniente realizar tanto validaciones intermedias durante la operación del PREP, como una validación final, una vez que el PREP ha cerrado operaciones.

Validación de las bases de datos

En relación con la base de datos, deberán analizarse aquellas tablas o catálogos que resultan críticos en el almacenamiento de la información y el procesamiento de los resultados preliminares, identificando tanto los que pudieran sufrir modificaciones durante la operación del PREP, así como los catálogos fijos que deben estar precargados.

Previo al inicio de operaciones del sistema informático del PREP, se deberán obtener los valores iniciales de la base de datos y comprobar que los resultados preliminares se encuentran en ceros. Este procedimiento deberá ser atestiguado por un tercero con fe pública y generar una constancia de hechos que será firmada por **"LAS PARTES"**.

RRC.

Adicional a esta revisión inicial es conveniente realizar una verificación final, una vez que el PREP ha cerrado operaciones.

Emisión de constancias de hechos

Como resultado de la validación del sistema informático del PREP, deberán documentarse al menos las siguientes constancias de hechos:

- Constancia de hechos de la generación de huellas criptográficas maestras de los programas probados.
- Constancia de hechos de la validación de los programas y de la base de datos del PREP, previo al inicio de operaciones del PREP.
- Constancia de hechos de la validación de los programas, durante la operación del PREP.
- Constancia de hechos de la validación de los programas y de la base de datos del PREP, posterior al cierre de operaciones del PREP.

3. Análisis de vulnerabilidades a la infraestructura tecnológica

Esta línea de trabajo se refiere a la aplicación de pruebas de penetración, la revisión de configuraciones de seguridad y la realización de pruebas de denegación de servicio (DoS), con la finalidad de identificar posibles vulnerabilidades en la infraestructura tecnológica del PREP.

Selección de activos para las pruebas y revisión de configuraciones.

El primer paso para el análisis de vulnerabilidades de la infraestructura tecnológica, es establecer los activos sobre los que se realizarán las pruebas y la revisión de configuraciones.

Ejecución de pruebas de penetración (Pentest) a activos seleccionados

Se aplicarán pruebas de seguridad informática de caja negra a los activos de información considerados en el alcance del pentest. Las pruebas consisten en la ejecución de herramientas informáticas para identificar potenciales vulnerabilidades, y posteriormente en la aplicación de diversas técnicas para intentar explotarlas e identificar así el impacto que tienen sobre la infraestructura tecnológica,

Handwritten signatures and initials are present on the right margin of the page. There are three distinct marks: a small 'y' or 'd' at the top, a large stylized signature in the middle, and the letters 'RPE' at the bottom.

determinar el nivel de exposición de información sensible. Estos hallazgos deben ser documentados de manera clara y precisa.

Revisión de configuraciones en activos seleccionados

La revisión de configuraciones se enfocará en el sistema operativo de servidores, consolas y dispositivos, por lo que no considera los servicios y aplicaciones que se ejecuten en los mismos.

Análisis y clasificación de hallazgos de pruebas de penetración y revisión de configuraciones

Todos los hallazgos y oportunidades de mejora que se obtengan como resultado de la ejecución del pentest y de la revisión de configuraciones, serán analizados y clasificados. Por lo que se utilizará un sistema de calificación de vulnerabilidades, que permita determinar su impacto en la infraestructura tecnológica y proporcione elementos para definir prioridades para la aplicación de medidas de mitigación de los mismos.

Esta actividad incluye la emisión de recomendaciones para establecer las medidas de seguridad que se implementarán para mitigar el impacto de los hallazgos detectados.

Verificación de medidas de seguridad implementadas con base en los hallazgos

A partir de los informes de las pruebas de penetración y de la revisión de configuraciones, se verifica la aplicación de las medidas de mitigación aplicadas por “**EI IEEQ**” a fin de identificar la persistencia de los hallazgos reportados en la infraestructura tecnológica.

Posteriormente, “**LA UNAM**”, deberá emitir un informe final con los resultados de la verificación de hallazgos una vez que “**EL IEEQ**” haya implementado las medidas de mitigación.

6. CALENDARIO GENERAL DE TRABAJO

6.1. Para la elaboración de los planes de trabajo y cronogramas relacionadas con la auditoría informática se observará el siguiente calendario:

[Handwritten signature and stamp]

No.	Actividad	Fecha de Inicio	Fecha de Conclusión	Responsable (s)
1.	Llevar a cabo una sesión de inducción sobre el sistema informático PREP.	01/ENE/2018	31/ENE/2018	"LA UNAM"- "EL IEEQ"
2.	Instalación de infraestructura tecnológica.	01/FEB/2018	30/ABR/2018	"EL IEEQ"
3.	Entrega de código fuente, archivos ejecutables y documentación técnica para maqueta de pruebas.	01/MAR/2018	16/ABR/2018	"EL IEEQ"
4.	Análisis de vulnerabilidades a la infraestructura tecnológica.	05/MAR/2018	22/ABR/2018	"LA UNAM"
5.	Ejecución de pruebas de caja negra a las aplicaciones informáticas.	05/MAR/2018	22/ABR/2018	"LA UNAM"
6.	Presentación y remisión de informes parciales de las pruebas funcionales de caja negra a las aplicaciones informáticas y vulnerabilidades a la infraestructura tecnológica.	23/ABR/2018	30/ABR/2018	"LA UNAM"
7.	Presentación y remisión de las recomendaciones para resolver las amenazas detectadas durante la auditoría.	23/ABR/2018	30/ABR/2018	"LA UNAM"
8.	Implementación de acciones correctivas y ajustes derivados de las recomendaciones.	A más tardar el 25/MAY/2018		"EL IEEQ"
9.	Comprobación que las aplicaciones informáticas utilizadas en la operación del PREP correspondan a los programas auditados.	28/MAY/2018	8/JUN/2018	"LA UNAM"
10.	Verificación de las acciones implementadas para atender, las recomendaciones	28/MAY/2018	8/JUN/2018	"LA UNAM"






	emitidas.			
11.	Evaluación del PREP durante su operación en los simulacros.	10/JUN/2018	24/JUN/2018	"LA UNAM"
12.	Pruebas de negación de servicio de ataque volumétrico.	10/JUN/2018	28/JUN/2018	"LA UNAM"
13.	Presentación y remisión del informe final de auditoría.	25/JUN/2018	28/JUN/2018	"LA UNAM"
14.	Comprobación de que las aplicaciones informáticas utilizadas en la operación del PREP correspondan a las auditadas.	01/JUL/2018	01/JUL/2018	"LA UNAM"- "EL IEEQ"
15.	Verificación del procedimiento para comprobar que las bases de datos del PREP no contienen votos almacenados.	01/JUL/2018	01/JUL/2018	"LA UNAM"- "EL IEEQ"
16.	Evaluación del PREP durante su operación el día de la Jornada Electoral.	01/JUL/2018	02/JUL/2018	"LA UNAM"
17.	Presentación y remisión del informe de evaluación de la operación del PREP durante la Jornada Electoral.	A más tardar el 20/JUL/2018		"LA UNAM"

7. REQUERIMIENTOS DE INFORMACIÓN

7.1. Con la finalidad de que **"LA UNAM"** cuente con los elementos suficientes que le permitan llevar a cabo la auditoría informática al PREP, **"EL IEEQ"** le hará entrega o pondrá a su disposición lo siguiente:

1. Acceso a la maqueta de pruebas de la infraestructura tecnológica, análoga a la real para la realización de las pruebas funcionales de caja negra, con los archivos ejecutables y scripts del PREP, así

como los códigos HASH de cada uno y el algoritmo criptográfico utilizado para su generación, estos últimos serán generados por “**LA UNAM**”.

2. Listado de usuarios y contraseñas de las aplicaciones informáticas así como de los dispositivos utilizados.
3. Bitácoras generadas por los sistemas informáticos del PREP.
4. Diagramas de los modelos de bases de datos utilizados.
5. Procedimiento Técnico-Operativo del PREP. Documentación técnica que permita comprender el funcionamiento del sistema informático, esto comprende por ejemplo: requerimientos, casos de uso o historias de usuario, arquitectura y diseño detallado, manuales técnicos y de operación.
6. Procedimiento para garantizar y dejar evidencia que los programas auditados sean los utilizados durante la operación del PREP.
7. Procedimiento de control de cambios del código fuente y configuraciones de las aplicaciones informáticas.
8. Procedimiento para garantizar que las bases de datos no cuenten con información antes de la puesta en operación del PREP el día de la Jornada Electoral.
9. Relación de los activos informáticos que se revisarán en el Análisis de vulnerabilidades.
10. Al menos un ejemplar muestra de las actas de escrutinio y cómputo de los diversos escenarios y elecciones.
11. Escenarios de la elección, relación completa de partidos políticos, coaliciones, candidatura común y candidatos independientes que participan en las elecciones para Diputaciones y Ayuntamientos.
12. Normatividad aplicable y vigente.



13.Relación de las casillas electorales aplicables en las elecciones, que contienen los datos principales para identificar un acta de escrutinio y cómputo, como son: municipio, distrito, sección, casilla, tipo de casilla, tipo de candidatura, circunscripción, lista nominal, entre otros.

14.Calendario de trabajo del PREP, en el que se señalen la fecha en que el sistema informático estará concluido, la fecha en que la infraestructura tecnológica estará instalada y fechas de los simulacros.

15.Capacitación inicial y apoyo técnico necesario.

16.Acceso a un ambiente de auditoría para controlar las versiones de los Sistemas Informáticos que se auditen.

7.2.El acceso a la maqueta de pruebas, así como la información definida en este apartado que **“LA UNAM”** requiera para llevar a cabo las actividades relacionadas con la auditoría, serán solicitadas a **“EI IEEQ”** a través de escrito.

7.3.En caso de que **“LA UNAM”** requiera información adicional, se solicitará mediante oficio en el que se especifique el motivo de su petición. En caso de que la información una vez entregada se actualice por parte de **“EI IEEQ”**, éste deberá informarlo a **“LA UNAM”** por escrito y, remitir nuevamente la información que se hubiere actualizado.

8. ENTREGABLES, PRESENTACIÓN Y ENTREGA DE INFORMES

8.1.**“LA UNAM”** remitirá a **“EI IEEQ”** los documentos derivados de la auditoría y operación del PREP conforme a lo siguiente:

a) Pruebas funcionales de caja negra

Entregable y descripción	Contenido	Criterios de aceptación
Plan de pruebas funcionales de caja negra del sistema informático. <i>Descripción: Contiene los elementos generales de planeación que deben</i>	• Introducción • Objetivo • Alcance • Pruebas a aplicar • Planeación de las pruebas • Necesidades del	Documento en formato electrónico con los contenidos señalados.

<i>considerarse para la realización de las pruebas funcionales de caja negra.</i>	- ambiente - Casos de prueba - Datos de prueba - Criterios de pruebas - Administración de riesgos - Entregables	
Informe preliminar de las pruebas funcionales de caja negra del sistema informático. <i>Descripción: Contiene el detalle de las observaciones identificadas en la revisión y pruebas del sistema informático.</i>	- Introducción - Metodología - Criterios utilizados para la auditoría - Metodología para clasificar los hallazgos - Observaciones y recomendaciones - Conclusiones	Documento en formato electrónico con los contenidos señalados.
Informe final de las pruebas funcionales de caja negra del sistema informático. <i>Descripción: Documento que contiene el resultado final de las pruebas del sistema informático.</i>	- Introducción - Metodología - Criterios utilizados para la auditoría - Resumen ejecutivo - Resultados	Documento en formato electrónico con los contenidos señalados. Fecha de entrega: entre el 25 y 28 de junio de 2018.

b) Validación del sistema informático del PREP y de sus base de datos

Entregable y descripción	Contenido	Criterios de aceptación
Plan de trabajo <i>Descripción: Contiene la descripción de las actividades y los responsables de su ejecución, para garantizar y dejar evidencia de que los programas auditados sean los utilizados en la operación del PREP.</i>	- Alcance - Calendario de trabajo - Responsables técnicos	Documento en formato electrónico con los contenidos señalados.
Procedimiento técnico para verificar que los	- Propósito - Alcance	Documento en formato electrónico con los

programas auditados se encuentren operando al inicio, durante y al final de la operación del PREP. <i>Descripción: Contiene la descripción de las actividades y los responsables de su ejecución, para garantizar y dejar evidencia de que los programas auditados sean los utilizados en la operación del PREP.</i>	• Roles • Políticas • Procedimiento • Diagrama de flujo	contenidos señalados.
Procedimiento técnico para garantizar que las bases de datos no cuenten con información antes de la puesta en operación del PREP. <i>Descripción: Contiene la descripción de las actividades y los responsables de su ejecución, para garantizar que las bases de datos no cuenten con información antes del inicio de operaciones del PREP.</i>	• Propósito • Alcance • Roles • Políticas • Procedimiento • Diagrama de flujo	Documento en formato electrónico con los contenidos señalados.
Constancias de hechos de la generación de huellas criptográficas.	• Circunstancias de tiempo, modo y lugar del acto del que se da fe.	Protocolo notarial
Constancias de hechos de la validación de los programas y de la base de datos del sistema informático del PREP.	• Circunstancias de tiempo, modo y lugar del acto del que se da fe.	Protocolo notarial

c) Análisis de vulnerabilidades a la infraestructura tecnológica

Entregable y descripción	Contenido	Criterios de aceptación
--------------------------	-----------	-------------------------

yl
gr
X
RRC

Plan de pruebas de penetración a la infraestructura tecnológica y de revisión de las configuraciones. <i>Descripción: Contiene los elementos generales de planeación que deben considerarse para la realización de las pruebas de penetración y para el desarrollo de la revisión de configuraciones y la priorización de las remediaciones.</i>	• Alcance • Calendario de trabajo • Responsables técnicos	Documento en formato electrónico con los contenidos señalados.
Informe preliminar de las pruebas de penetración a la infraestructura tecnológica y de la revisión de las configuraciones. <i>Descripción: Contiene el resultado de las pruebas realizadas sobre los activos y de cada hallazgo identificado en la revisión de configuraciones clasificados según su nivel de impacto y su prioridad de atención</i>	• Resumen ejecutivo • Objetivo • Alcance • Resultados de las pruebas • Hallazgos clasificados • Recomendaciones	Documento en formato electrónico con los contenidos señalados.
Informe de aplicación de recomendaciones de las pruebas de penetración a la infraestructura tecnológica y de la revisión de configuraciones. <i>Descripción: Documento que describe el estado de seguridad de la infraestructura una vez</i>	• Resumen ejecutivo • Alcance • Resultado de la verificación	Documento en formato electrónico con los contenidos señalados.

Handwritten signatures and initials: A large stylized signature, and the initials "RPC" below it.

que “EL IEEQ” aplicó las recomendaciones hechas por parte del ente auditor.		
Informe final del análisis de vulnerabilidades a la infraestructura tecnológica. <i>Descripción: Contiene el resultado final del análisis de vulnerabilidades en el que se incluyen los hallazgos clasificados y sus recomendaciones, el software y herramientas utilizadas.</i>	• Introducción • Resultados generales	Documento en formato electrónico con los contenidos señalados. Fecha de entrega: entre el 25 y 28 de junio de 2018.

d) Pruebas de negación de servicio

Entregable y descripción	Contenido	Criterios de aceptación
Plan de trabajo de pruebas de negación de servicio a los sitios web del PREP y el sitio principal de “EL IEEQ” y de ataques de negación de servicio. <i>Descripción: Contiene el desglose de actividades para la realización de las pruebas de ataques.</i>	• Actividades • Entregables • Fecha inicio • Fecha fin • Responsables	Documento en formato electrónico con los contenidos señalados.
Informe de resultados de pruebas de negación de servicio a los sitios web del PREP y principal de “EL IEEQ”. <i>Descripción: Contiene los resultados obtenidos de la realización de las pruebas de ataques.</i>	• Introducción • Resultados	Documento en formato electrónico con los contenidos señalados.

e) Informe de evaluación de la operación

Entregable y descripción	Contenido	Criterios de aceptación
Informe final de evaluación de la operación del PREP. <i>Descripción: Contiene el análisis del desempeño del PREP desde el inicio de operaciones hasta su conclusión así como la etapa de evaluación del mismo.</i>	• Introducción • Resultados generales	Documento en formato electrónico con los contenidos señalados. Fecha de entrega: a más tardar el 20 de julio de 2018.

8.2. Por lo que refiere a las constancias de hechos que deben elaborarse derivado de los actos que el ente auditor lleve a cabo ante la presencia de un tercero con fe pública, corresponderá a este último la elaboración y entrega a “EL IEEQ”.

9. ORGANIGRAMA ESTRUCTURAL

9.1. “LA UNAM” designará un equipo de 6 especialistas en distintas áreas de conocimiento, quienes desarrollarán el servicio bajo estrictos parámetros de calidad, el personal asignado será conforme a la siguiente tabla:

Área de conocimiento o experiencia	Rol	No. de Personas
Doctorado en Ciencias Físicas	Dirección del Proyecto	1
Maestría en Ciencias	Coordinación del Proyecto y Responsable técnico	1
Administración o afín	Coordinación Administrativa	1

[Handwritten signatures and initials on the right margin]

10. CONSIDERACIONES ADICIONALES

10.1. Para el desarrollo de las actividades relativas al servicio descrito, es necesario que **"EL IEEQ"** facilite a **"LA UNAM"** el ingreso a las instalaciones señaladas en el punto 1 de los alcances del presente documento.

11. OBLIGACIONES

11.1. En términos de la en la cláusula segunda, fracción primera, numeral 6 del Convenio de Colaboración **"EL IEEQ"** cubrirá una dieta mensual consistente en \$6,000.00 (seis mil pesos 00/100 m.n.) al equipo de colaboradoras: Diana Abigail Muñoz Bustos, Laura Selene Olguín Martínez y Roxana Yarely Sánchez Salinas.

11.2. **"EL IEEQ"** cubrirá al personal asignado de **"LA UNAM"**, la cantidad correspondiente para apoyo de viáticos que resulten necesarios para el desarrollo de **"LA AUDITORÍA"**. Los gastos que se generen serán cubiertos por **"EL IEEQ"**, observando para ello los procedimientos administrativos aplicables.

SEGUNDA. "LAS PARTES" se comprometen a publicar en sus respectivos portales de internet y, en su caso, a través de los medios electrónicos a su alcance, la colaboración entre **"LAS PARTES"** y los resultados de **"LA AUDITORÍA"**.

TERCERA. Queda expresamente pactado que **"LAS PARTES"** no tendrán responsabilidad civil por los daños y perjuicios que pudieran causarse como consecuencia del caso fortuito o fuerza mayor; en especial, los que provoquen la suspensión de los trabajos que se realicen con motivo del cumplimiento del presente documento, por lo que de ser posible, una vez que desaparezcan las

Handwritten signatures and initials are present on the right margin of the page. There are three distinct marks: a small signature at the top, a larger signature in the middle, and a set of initials 'RAC' at the bottom.

causas que suscitaron su interrupción, se procederá a reanudar las tareas pactadas.

CUARTA. Para la ejecución y seguimiento de las actividades a que se refiere el presente instrumento, **"LAS PARTES"** designan al funcionariado siguiente:

1. El **"IEEQ"** al **Ing. Raúl Islas Matadamas**, en su carácter de Coordinador de Informática, con correo electrónico informatica@ieeq.mx, teléfono 101 98 00, extensión 1107, así como el personal relacionado o que sea asignado a este programa, y
2. Por la **"UNAM"** al M. en C. Guillermo Vázquez Sánchez, en su calidad de Técnico Académico, titular nivel "B" del Centro de Física Aplicada y Tecnología Avanzada, con correo electrónico william@fata.unam.mx, teléfono 238 11 31 así como el personal relacionado o que sea asignado a este programa.

QUINTA. Para efecto de la revisión de los avances y del cumplimiento de las obligaciones derivadas del presente instrumento, **"EL IEEQ"** y **"LA UNAM"** acuerdan reunirse ordinariamente de manera mensual y de manera extraordinaria para atender cualquier situación de contingencia o riesgo, bastando para su celebración que una de las partes la solicite con la debida anticipación.

SEXTA. En las comunicaciones que se lleven a cabo entre **"LAS PARTES"** se privilegiará el uso de tecnologías, equipos y/o herramientas informáticas que permitan agilizar e interactuar en tiempo real, -entre otros- respecto del intercambio de información, la toma de decisiones y en general en la atención pronta y expedita de los asuntos derivados del presente instrumento. Esta medida permitirá abonar al uso racional de recursos, en cumplimiento a los criterios de legalidad, honestidad, eficiencia, eficacia, economía, austeridad, transparencia, control y rendición de cuentas.

SÉPTIMA. El presente instrumento podrá ser modificado por voluntad de **"LAS PARTES"**, quienes se obligarán a cumplir tales modificaciones a partir de la fecha de su suscripción, en el entendido de que éstas tendrán como única finalidad perfeccionar y coadyuvar en el cumplimiento de su objeto.

OCTAVA. **"LAS PARTES"** manifiestan su conformidad en que el presente Anexo Técnico es producto de la buena fe, por lo que todo conflicto que resulte del mismo, en cuanto a su interpretación, aplicación y cumplimiento, serán resueltos de común acuerdo.

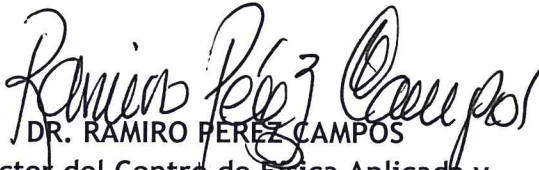


Leído que fue el presente instrumento y enteradas “LAS PARTES” de su contenido y alcances, lo firman por duplicado, en Santiago de Querétaro, Querétaro, 2 de abril de dos mil dieciocho.

POR LA UNIVERSIDAD NACIONAL AUTÓNOMA DE
MÉXICO

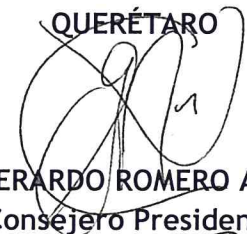


DR. GERARDO CARRASCO NÚÑEZ
Presidente del Consejo de
Dirección del Campus UNAM
Juriquilla



DR. RAMIRO PÉREZ CAMPOS
Director del Centro de Física Aplicada y
Tecnología Avanzada

POR EL INSTITUTO ELECTORAL DEL ESTADO DE
QUERÉTARO



M. EN A. GERARDO ROMERO ALTAMIRANO
Consejero Presidente



LIC. JOSÉ EUGENIO PLASCENCIA ZARAZÚA
Secretario Ejecutivo