



INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS FUNCIONALES DE CAJA NEGRA DEL PREP 2012



**INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA
REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS
FUNCIONALES DE CAJA NEGRA DEL PREP 2012**

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



Contenido

Resumen ejecutivo	3
Introducción	7
Resultados de la aplicación de recomendaciones	18
Conclusiones	20
Anexo 1. Cuadro resumen de las líneas de código del PREP	22
Anexo 2. Sobre la línea de colaboración en seguridad informática	23



**INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA
REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS
FUNCIONALES DE CAJA NEGRA DEL PREP 2012**

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



Resumen ejecutivo

En noviembre de 2011, el Instituto Federal Electoral (IFE) solicitó a la Universidad Nacional Autónoma de México (UNAM), a través de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC), se practicara una auditoría de software al sistema del Programa de Resultados Electorales Preliminares (PREP) con el objetivo de “analizar el aplicativo del PREP 2012, mediante la revisión de código fuente y la realización de pruebas funcionales de caja negra, que permita determinar el cumplimiento con las especificaciones presentadas en la documentación técnica, así como evaluar la integridad en el procesamiento de la información y la generación de los resultados conforme a la normatividad aplicable”.

Lo anterior fue formalizado en el Convenio Específico de Colaboración celebrado entre el IFE y la Universidad con registro UNAM 30863-87-16-I-12, cuya firma fue difundida mediante boletín UNAM-DGCS-050 del 24 de enero de 2012. Adicionalmente y en el marco del mismo Convenio, la UNAM ha prestado apoyo técnico al IFE para complementar su estrategia en materia de seguridad informática, a través de dos líneas de colaboración independientes a la auditoría del sistema PREP 2012: 1) una auditoría en materia de seguridad informática a la infraestructura de RedIFE y del PREP 2012, y 2) el monitoreo y respuesta a incidentes técnicos durante la jornada electoral del 1° de julio. Los trabajos de colaboración sobre seguridad informática concluyen el día 2 de julio. A la fecha, se han realizado pruebas de penetración a la infraestructura contemplada en el convenio y se emitieron recomendaciones que han sido atendidas por el IFE y revisadas por la UNAM.

El trabajo formalizado por el IFE y la UNAM en el Convenio Específico de Colaboración se circunscribe a la auditoría técnica del sistema informático del PREP 2012, mediante la inspección de código fuente y la realización de pruebas funcionales de caja negra. El alcance de esta colaboración fue establecido a partir del análisis de los requerimientos presentados, de la amplitud de los procesos, la información y la infraestructura que comprende el PREP, así como de las restricciones de tiempo con las que se cuenta en el proceso electoral federal para su desarrollo e implementación.

Fecha: 25/Junio/2012	Página: 3 de 23
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO	INSTITUTO FEDERAL ELECTORAL



**INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA
REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS
FUNCIONALES DE CAJA NEGRA DEL PREP 2012**

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



En este sentido, la inspección del software que opera en los Centros de Acopio y Transmisión de Datos (CEDAT) para la captura de los resultados de casilla en el sistema PREP 2012 es materia de la auditoría realizada por la UNAM y no el proceso logístico asociado de donde proviene la información que alimenta a este sistema: el llenado de las actas de escrutinio y cómputo por los funcionarios de casilla ante los representantes de partidos políticos, así como la entrega de estas por los presidentes de casilla a la Junta Distrital Ejecutiva.

La auditoría de software consistió en la inspección visual del código¹, para verificar que las instrucciones de cada uno de los programas implementaran la funcionalidad indicada en la documentación técnica, y que el procesamiento de la información de los resultados electorales preliminares fuera íntegro. Por su parte, las pruebas funcionales de caja negra² se realizaron en un entorno tecnológico con características similares al ambiente de operación de la jornada electoral, con la finalidad de comprobar que los resultados de la operación del PREP fueran consistentes con la funcionalidad que deben cubrir, desde la captura de datos en el sistema hasta el despliegue de resultados preliminares en Internet. Se verificó la integridad en el procesamiento de la información y la generación de resultados electorales preliminares del sistema del PREP 2012, bajo diversos escenarios y casos de prueba, conforme a la normatividad aplicable.

Como resultado de la revisión de 1,501 archivos con un total de 262,540 líneas de código y de la realización de pruebas funcionales, la UNAM emitió diversas observaciones y recomendaciones jerarquizadas por su nivel de impacto. Las de importancia crítica fueron atendidas en su totalidad por el IFE, y la UNAM verificó su correcta implementación. No se observaron comportamientos anómalos en el sistema del PREP 2012, sino incidencias inherentes al desarrollo y mantenimiento de software asociadas a la complejidad de la aplicación y a las características del proceso electoral, que fueron corregidas por el IFE; por lo que se puede concluir que el sistema del PREP 2012 auditado está libre de todo algoritmo que pueda distorsionar los datos capturados en los CEDAT.

¹ Una inspección de software es un análisis sistemático para detectar de forma oportuna, defectos en los elementos de software para asegurar la calidad de los mismos, tomando en cuenta los aspectos aplicables en cuanto a funcionalidad, fiabilidad, eficiencia, mantenibilidad, portabilidad y usabilidad.

² En el contexto computacional, se denomina "caja negra" al elemento que es analizado desde el punto de vista de las entradas que recibe y las salidas que produce. En este sentido, las pruebas funcionales de caja negra se refieren a un método para validar la funcionalidad de un sistema informático a través de la introducción de datos en los dispositivos de captura y la revisión de los resultados de salida que se presentan al usuario en las pantallas finales.



**INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA
REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS
FUNCIONALES DE CAJA NEGRA DEL PREP 2012**

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



Esta es la segunda auditoría de software realizada por la UNAM al sistema del PREP. La anterior se llevó a cabo en 2009 para la elección de diputados federales y en la auditoría de 2012 que comprende la elección federal de presidente, senadores y diputados, el IFE agregó algunas funcionalidades al PREP que fueron auditadas:

- a) La digitalización de la imagen de las actas que estarán disponibles para su consulta a partir de las 20 horas del lunes 2 de julio, y cuyos datos son capturados en los CEDAT. La UNAM auditó los programas que permiten la organización y publicación de estas imágenes.
- b) La publicación de un resumen de los resultados electorales preliminares a través de páginas Web diseñadas para su despliegue en dispositivos móviles. En este caso, la UNAM verificó el código fuente así como la consistencia de los resultados presentados, como parte de las pruebas de caja negra realizadas en la validación final.

Adicionalmente el PREP 2012 contempla otros mecanismos de difusión que no fueron incluidos en el alcance de la auditoría, debido a que no estaban considerados a la firma del convenio de colaboración.

Se concluye que el software del PREP 2012 es funcionalmente apropiado para cumplir con lo establecido en el Código Federal de Instituciones y Procedimientos Electorales (COFIPE) vigente. El sistema auditado brinda la funcionalidad necesaria para realizar la captura, el registro y la publicación de los datos e imágenes digitalizadas de las Actas de Escrutinio y Cómputo del Proceso Electoral 2011-2012, de manera íntegra conforme son captados en las Terminales de Captura Remota y en los dispositivos de digitalización utilizados en los CEDAT, permitiendo la difusión inmediata a través de Internet de los resultados preliminares de la elección federal de presidente, diputados y senadores de 2012.

Antes de que el PREP 2012 inicie operaciones el primero de julio, la UNAM comprobará ante notario público que los programas que fueron revisados por la DGTIC, sean los mismos que el IFE operará en esta elección federal. El notario público resguardará una relación de los programas auditados y sus firmas criptográficas.

Fecha: 25/Junio/2012	Página: 5 de 23
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO	INSTITUTO FEDERAL ELECTORAL



**INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA
REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS
FUNCIONALES DE CAJA NEGRA DEL PREP 2012**

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



El Convenio Específico de Colaboración establece disposiciones puntuales para ambas instituciones respecto al manejo de la información para cumplir con el objeto del instrumento legal. En razón de lo anterior, con fecha 25 de junio de 2012, en la quinta sesión de la Comisión de Evaluación y Seguimiento y Comunicación Social Conjunta, ambas instituciones acuerdan hacer público el presente documento junto con un boletín informativo e información complementaria, disponible en el sitio Web <http://www.auditoriaPREP2012.unam.mx>



**INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA
REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS
FUNCIONALES DE CAJA NEGRA DEL PREP 2012**

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



Introducción

En noviembre del 2011, el Instituto Federal Electoral (IFE) y la Universidad Nacional Autónoma de México (UNAM) suscribieron un Convenio Específico de Colaboración, con el objeto de desarrollar las siguientes actividades:

- a) Auditoría de software al Sistema del Programa de Resultados Electorales Preliminares (PREP) 2012, de la cual se desprende este informe.
- b) Auditoría en materia de seguridad informática a la infraestructura de la RedIFE y del PREP 2012, así como monitoreo y respuesta a incidentes durante la jornada electoral del 1° de julio de 2012, cuyos trabajos concluyen el día 2 de julio y son independientes a lo señalado en este informe. En el anexo 2 se incluye mayor información respecto a esta línea de trabajo.

Para la realización de estas auditorías, participó por parte del IFE el personal técnico de la Unidad de Servicios de Informática (UNICOM) y por parte de la UNAM, personal de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC).

En este documento se presentan exclusivamente las conclusiones relativas a la auditoría de software al sistema del Programa de Resultados Electorales Preliminares 2012 (PREP), la cual comprende la **revisión de código fuente** y la realización de **pruebas funcionales de caja negra** que se llevaron a cabo con la finalidad de verificar la integridad en el procesamiento de la información, desde su captura hasta la presentación de los resultados preliminares conforme a las especificaciones técnicas y normativas.

El alcance de la auditoría al sistema del PREP 2012 comprendió las siguientes actividades:

1. Planeación y preparación. Previo a las actividades de revisión de código fuente y pruebas funcionales, se revisó la documentación (técnica y normativa) del PREP para comprender la arquitectura y características del sistema informático, y así contar con los elementos suficientes de información que permitieran generar un plan de trabajo específico, detallando la metodología y criterios a seguir en la revisión del código de los programas y la preparación de los datos, casos y escenarios de pruebas necesarios para cumplir con el objetivo de esta auditoría.



INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS FUNCIONALES DE CAJA NEGRA DEL PREP 2012

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



2. Revisión del código fuente. Consistió en el análisis estático del código fuente³ que integra cada uno de los módulos de la aplicación mencionados en el anexo 1, conformados por líneas de texto plano. Lo anterior, con la finalidad de evaluar la lógica de los programas relacionada con el flujo de la información, desde su captura hasta su despliegue, así como los cálculos efectuados para la emisión de los resultados preliminares, con el fin de determinar si el tratamiento de la información es adecuado y conforme con las especificaciones indicadas en la documentación técnica y la normatividad aplicable.

3. Pruebas funcionales. Comprendió la realización de pruebas de caja negra para verificar si el software cumplía con las especificaciones funcionales señaladas en la documentación técnica, así como determinar la integridad de la información procesada y la generación de resultados conforme a la normatividad aplicable.

De cada módulo auditado y al concluir los ciclos de revisión, la UNAM emitió un informe con las observaciones detectadas y las recomendaciones sugeridas, jerarquizadas por su nivel de impacto. Las observaciones fueron informadas al personal técnico del IFE, con la finalidad de asegurar su comprensión y pertinencia. El Instituto tuvo un período de tiempo para implementar las recomendaciones, especialmente aquellas de importancia crítica, y posteriormente la UNAM validó su atención.

Las actividades mencionadas fueron realizadas del 30 de noviembre de 2011 al 25 de junio de 2012. Asimismo como parte del alcance de la auditoría, se contempla realizar las siguientes actividades:

Validación de software auditado. Consiste en la compilación y firma de los programas auditados para validar que el software que será instalado y utilizado en la jornada electoral, es el mismo que fue auditado por la UNAM. Como resultado de esta validación, se emitirán constancias de hechos que describen las actividades realizadas. El protocolo del proceso de validación del software auditado comprende lo siguiente:

a) Compilación de los programas (27 de junio de 2012). Comprende la generación de los paquetes y programas ejecutables a partir de la versión del código fuente auditado por la UNAM, la cual se realizará

³ Revisión del contenido de las instrucciones de los programas sin que éstos se encuentren en ejecución.



**INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA
REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS
FUNCIONALES DE CAJA NEGRA DEL PREP 2012**

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



en presencia del personal técnico del IFE y de la Universidad. Al finalizar, se grabará un disco compacto con la información obtenida, que será entregado a la UNAM para la realización del siguiente paso.

b) Obtención de las firmas criptográficas (27 de junio de 2012). En presencia del personal directivo y jurídico del IFE, de directivos de la UNAM y de un notario público, la UNAM generará las firmas criptográficas correspondientes a los archivos binarios contenidos en el disco compacto entregado en el paso anterior, mediante la aplicación del algoritmo SHA1 (Secure Hash Algorithm).

c) Al finalizar la obtención de firmas criptográficas, también el 27 de junio de 2012, la UNAM generará tres copias del disco compacto que contengan el resultado de dichas firmas, las cuales serán distribuidas al IFE, a la UNAM, y al notario público. Además se proporcionará al notario público un listado con las firmas criptográficas resultantes para que dé fe de las actividades realizadas.

d) Recolección de archivos y programas en los Centros Nacionales de Recepción de Resultados Electorales Preliminares (CENARREP) el día 30 de junio de 2012. Consiste en recolectar en medios de almacenamiento portátil, los archivos y programas binarios del sistema informático del PREP 2012 instalados en cada servidor y en las consolas del ambiente de producción del CENARREP primario y secundario. Para ello, en presencia del personal técnico de la UNAM, el personal técnico del IFE obtiene de los servidores, una copia de los archivos binarios que conforman el sistema informático del PREP 2012, los cuales son copiados a un dispositivo portátil nuevo, que es resguardado en un sobre cerrado y firmado por ambas partes, ante notario público.

e) Validación de la inicialización de la base de datos (1° de julio de 2012). El día de la jornada electoral se constatará que la base de datos se encuentre debidamente inicializada, es decir, que las tablas contengan sólo la información que deben tener y que no exista evidencia de actas con resultados. Para esto, personal técnico especializado del IFE, en presencia de autoridades de la UNAM, del Instituto y de un notario público, ejecutarán un script⁴, que contiene las consultas necesarias para verificar el contenido de las principales tablas; los resultados presentados por el script son contrastados contra un listado con los resultados esperados. Dicho script es previamente revisado por la UNAM.

⁴ Programa con una secuencia de comandos validados.



**INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA
REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS
FUNCIONALES DE CAJA NEGRA DEL PREP 2012**

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



f) Validación final de las firmas criptográficas de los programas (1° de julio de 2012). El día de la jornada electoral en presencia de autoridades del IFE, de la UNAM y de notario público, se realiza la comparación de las firmas criptográficas de los programas recolectados en los CENARREP, contra las firmas criptográficas de los programas compilados a partir del código fuente auditado por la UNAM.

La auditoría se realizó a solicitud expresa del IFE a la UNAM y en las actividades de planeación, ambas instituciones acordaron:

- a. Que la finalidad de la auditoría sería constatar la integridad del software del Programa de Resultados Electorales Preliminares 2012, en relación con el tratamiento lógico de la información que se captura a partir del contenido de las Actas de Escrutinio y Cómputo que serán recibidas en los Centros de Acopio y Transmisión de Datos (CEDAT), al término de la jornada electoral federal del 1° de julio de 2012.
- b. Que el propósito específico de la auditoría fuera verificar que la entrada, el procesamiento y la salida de información se implementaran en el software conforme a las especificaciones técnicas y normativas⁵ sin sufrir adición, omisión o alteración, accidental o dolosa, que afectara los resultados presentados.
- c. Que se auditaran los programas que integran el sistema PREP 2012 a través de técnicas como la revisión estática de código fuente y la realización de pruebas funcionales de caja negra.

⁵Las especificaciones técnicas comprenden la documentación generada por el IFE a lo largo del ciclo de desarrollo de la aplicación (requerimientos, análisis, diseño, construcción y pruebas). Las especificaciones normativas se refieren al Código Federal de Instituciones y Procedimientos Electorales (COFIPE), publicado el 14 de enero de 2008 en el Diario Oficial de la Federación, y las resoluciones posteriores que respecto al COFIPE haya emitido el Poder Judicial de la Federación. Asimismo se tomó como referencia el prototipo de los 11 formatos de las Actas de Escrutinio y Cómputo del Proceso Electoral Federal 2011-2012 y la relación de partidos políticos, coaliciones y distritos proporcionados por el IFE.



INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS FUNCIONALES DE CAJA NEGRA DEL PREP 2012

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



Actividades realizadas

La revisión del código fuente consistió en la inspección de los programas de cómputo⁶ del PREP, a través del análisis de cada una de sus instrucciones, con la finalidad de evaluar su estructura y lógica interna en relación con el tratamiento de la información, así como las prácticas de programación utilizadas. Las pruebas funcionales de caja negra⁷ por su parte, consistieron en la introducción de conjuntos de datos en el sistema, que se puso en funcionamiento en un entorno tecnológico similar al de la jornada electoral, para de esta forma verificar el flujo de información desde su captura hasta su despliegue en los diferentes reportes de resultados electorales preliminares que emite el PREP. La combinación de estos dos métodos, permitió obtener una conclusión desde la perspectiva interna (código fuente) y externa (funcionalidad visible al usuario) del software.

El software del PREP 2012 consta de los módulos y submódulos mencionados a continuación, los cuales comprenden 1,501 archivos, con un total de 262,540 líneas de código, que en su conjunto conforman la materia auditada⁸:

A. PREP DE DATOS.

1. Módulo de Captura.
 - a) Generación de la información de tarjetas magnéticas.
 - b) Terminales de Captura Remota (TCR).
 - c) Monitor CEDAT.
2. Módulo de Aplicativo Central⁹.
 - a) Registro central.
 - b) Consola de administración.

⁶ Una inspección de software es un análisis sistemático para detectar de forma oportuna, defectos en los elementos de software para asegurar la calidad de los mismos, tomando en cuenta los aspectos aplicables en cuanto a funcionalidad, fiabilidad, eficiencia, mantenibilidad, portabilidad y usabilidad.

⁷ En el contexto computacional, se denomina "caja negra" al elemento que es analizado desde el punto de vista de las entradas que recibe y las salidas que produce. En este sentido, las pruebas funcionales de caja negra se refieren a un método para validar la funcionalidad de un sistema informático a través de la introducción de datos en los dispositivos de captura y la revisión de los resultados de salida que se presentan al usuario en las pantallas finales.

⁸ Ver el Anexo 1: Cuadro resumen de las líneas de código del PREP.

⁹ En el Convenio Específico de Colaboración se especificaron los siguientes submódulos del Módulo de Aplicativo Central: a) Comunicación y Registro, b) Consola y c) Download (descarga), sin embargo se consideró conveniente agruparlo de manera distinta para especificar una delimitación más precisa entre cada uno de los submódulos. No obstante la funcionalidad es equivalente.

Fecha: 25/Junio/2012	Página: 11 de 23
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO	INSTITUTO FEDERAL ELECTORAL



**INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA
REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS
FUNCIONALES DE CAJA NEGRA DEL PREP 2012**



CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12

3. Módulo de Extracción-Publicación.
 - a) Extracción.
 - b) Publicación.
 - c) Logística.

B. PREP DE ACTAS DIGITALIZADAS ¹⁰

1. Módulo de Captura de Actas Digitalizadas.
 - a)MCAD.
 - b)Administración de llaves.
2. Módulo de Aplicativo Central.
 - a)Registro central.
 - b)Consola de administración.
3. Módulo de Publicación-Logística.
 - a)Publicación.
 - b)Logística.

El software del PREP 2012 auditado, está diseñado para realizar la captura de información a través de las TCR que serán habilitadas en cada uno de los 300 CEDAT, así como la digitalización de la imagen de las Actas de Escrutinio y Cómputo, lo cual es enviado al CENARREP¹¹ para el registro y publicación de los resultados preliminares a través de páginas Web en Internet.

Es importante señalar que si bien el PREP comprende todo un conjunto de procesos y de infraestructura tecnológica, y tomando en cuenta el alcance del convenio signado por el IFE y la UNAM, el proceso logístico asociado a la jornada electoral -que es de donde proviene la información que alimenta el sistema del PREP 2012-, no fue revisado por la UNAM, sin embargo sí se inspeccionó el software que opera en los CEDAT para la captura de los datos y de la imagen de las Actas de Escrutinio y Cómputo.

¹⁰ En el Convenio Específico de Colaboración este componente se denominó como *Submódulo de Digitalización* ya que aún no estaba completamente diseñado y desarrollado por el Instituto, sin embargo una vez que fue terminado, resultó ser un sistema con módulos similares al PREP de datos.

¹¹ Centro Nacional de Recepción de Resultados Electorales Preliminares



**INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA
REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS
FUNCIONALES DE CAJA NEGRA DEL PREP 2012**

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



Otra fuente de información que alimenta al sistema del PREP, son los resultados de los votos de los mexicanos residentes en el extranjero, que se ingresan a través de un procedimiento de carga en la base de datos por personal técnico de la UNICOM, en el cual la UNAM no participa. De acuerdo con lo señalado por el IFE, el tratamiento de esta información es como sigue:

“El conteo de los votos se realizará en las mesas de escrutinio y cómputo de la votación de los electores residentes en el extranjero. Éstas deben instalarse en un local único en el Distrito Federal, el cual estará ubicado en este proceso electoral en las instalaciones del Instituto Tecnológico y Estudios Superiores de Monterrey, Campus Ciudad de México (ITESM CCM). (Artículo 329, párrafos 2 y 3 del COFIPE)...Una vez contabilizados los votos emitidos en el extranjero, el Secretario Ejecutivo del IFE rendirá un informe preliminar al Consejo General sobre el número de votos emitidos por ciudadanos residentes en el extranjero, clasificado por país de residencia de los electores. Posteriormente, dicho funcionario hará entrega a los integrantes del Consejo General del informe que contendrá los resultados por distrito electoral uninominal de la votación recibida en el extranjero y ordenará su inclusión por distrito electoral y mesa de escrutinio y cómputo en el Programa de Resultados Electorales Preliminares (PREP). (Artículo 328, párrafo 3 y Artículo 333, párrafo 2 del COFIPE).”¹²

¹² Fuente: Sitio de Internet www.votoextranjero.mx, habilitado por el IFE.



**INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA
REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS
FUNCIONALES DE CAJA NEGRA DEL PREP 2012**

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



Revisión de código fuente

En relación con el análisis del código fuente, el Instituto realizó la entrega de los archivos fuente y la documentación técnica en forma modular y de conformidad con el protocolo señalado en el Convenio Específico de Colaboración, es decir, en formato electrónico y firmado con el algoritmo criptográfico SHA-1¹³, en las fechas indicadas a continuación:

	Módulo	Submódulo	Primera entrega por parte del IFE para revisión de la UNAM	Entrega por parte del IFE con las recomendaciones implementadas para verificación por parte de la UNAM	Entrega del software final por parte del IFE para la validación final de la UNAM ¹⁴	Entrega de la versión final del software que será utilizada el 1 de julio
PREP DE DATOS	Módulo de Captura	Generación de la información de tarjetas magnéticas	1/mar/2012	23/abr/2012	14/may/2012 ¹⁵	----
		TCR	1/mar/2012	23/abr/2012	18/jun/2012	25/jun/2012
		Monitor CEDAT	1/mar/2012	23/abr/2012	18/jun/2012	25/jun/2012
	Módulo de Aplicativo Central	Registro central	1/mar/2012	23/abr/2012	18/jun/2012	25/jun/2012
		Consola de administración	1/mar/2012	23/abr/2012	18/jun/2012	25/jun/2012
	Módulo de Extracción-Publicación	Extracción	7/may/2012	4/jun/2012	18/jun/2012	25/jun/2012
		Publicación	9/abr/2012	4/jun/2012	18/jun/2012	25/jun/2012
		Logística	9/abr/2012	4/jun/2012	18/jun/2012	25/jun/2012
	PREP DE ACTAS DIGITALIZADAS	Módulo de Captura de Actas Digitalizadas	MCAD	23/abr/2012	31/may/2012	18/jun/2012
Administración de llaves			23/abr/2012	31/may/2012	18/jun/2012 ¹⁶	----
Módulo de Aplicativo Central		Registro central	23/abr/2012	31/may/2012	18/jun/2012	25/jun/2012
		Consola de administración	23/abr/2012	31/may/2012	18/jun/2012	25/jun/2012
Módulo de Publicación-Logística		Publicación	9/abr/2012	4/jun/2012	18/jun/2012	25/jun/2012
		Logística	23/abr/2012	31/may/2012	18/jun/2012	25/jun/2012

¹³ *Secure Hash Algorithm*, función criptográfica que se calcula sobre cada uno de los archivos, y que genera como resultado una firma del archivo (cadena de 40 caracteres alfanuméricos que identifica de forma unívoca al archivo). Cualquier cambio en el contenido del archivo, por mínimo que sea, genera una firma totalmente diferente, por lo cual es un mecanismo útil para comprobar la integridad de la información.

¹⁴ Entrega de la versión final, una vez que el IFE implementó las recomendaciones de la UNAM y en su caso, atendió las observaciones resultantes de sus simulacros y las nuevas solicitudes por parte del COTAPREP o de los representantes de los partidos políticos.

¹⁵ Este submódulo funciona de forma independiente al software central del PREP 2012 por lo que una vez auditado, fue compilado conjuntamente el día 16 de mayo de 2012 y ejecutado en presencia de representantes del Instituto y del COTAPREP el día 8 de junio de 2012.

¹⁶ Este submódulo es utilizado de manera independiente y en fechas anteriores a la jornada electoral, por lo que no se requirió entregarlo nuevamente.



INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS FUNCIONALES DE CAJA NEGRA DEL PREP 2012

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



El código fuente fue revisado en las instalaciones de la UNAM por especialistas en cada una de las tecnologías utilizadas en su desarrollo. La revisión consistió en la inspección visual del código con la ayuda de herramientas de análisis, para verificar que las instrucciones de los métodos y funciones, así como las variables contenidas en cada uno de los programas, implementaran la funcionalidad indicada en la documentación técnica y que el procesamiento de la información fuera íntegro.

De forma complementaria y no exhaustiva, se verificó que no existieran vulnerabilidades de seguridad, código redundante o en desuso, empleo ineficiente de recursos de cómputo, así como que el código cumpliera con los estándares de codificación y documentación generalmente aceptados en el desarrollo de software.

Los archivos revisados fueron todos aquellos con contenido en texto plano con las siguientes extensiones: .bat, .c, .cfg, .cpp, .css, .dat, .dl, .DocumentBuilderFactory, .DTMManager, .err, .form, .h, .html, .java, .js, .MF, .policy, .pro, .properties, .sgn, .sh, .sp, .sql, .txt, .ui, .xml.

De cada uno de los módulos auditados, la UNAM emitió los siguientes informes preliminares con las observaciones detectadas y las recomendaciones sugeridas, las cuales fueron previamente presentadas al personal técnico del Instituto con la finalidad de asegurar su comprensión y pertinencia:

Entregable	Fecha
Informe de resultados de la revisión de código fuente del software del PREP 2012, Módulo de <i>Captura</i> .	12/Abril/2012
Informe de resultados de la revisión de código fuente del software del PREP 2012, Módulo <i>Aplicativo Central</i> .	12/Abril/2012
Informe de resultados de la revisión de código fuente del software del PREP 2012, Submódulo de <i>Digitalización de Actas</i> .	23/Mayo/2012
Informe de resultados de la revisión de código fuente del software del PREP 2012, Módulo de <i>Extracción-Publicación</i> .	28/Mayo/2012 ¹⁷
Minuta y disco compacto con el estado de las observaciones de código fuente en su versión entregada el 4 de junio de 2012.	11/Junio/2012

¹⁷ Fecha acordada en la tercera sesión ordinaria de la Comisión de Evaluación y Seguimiento y Comunicación Social Conjunta.



INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS FUNCIONALES DE CAJA NEGRA DEL PREP 2012

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



Una vez entregadas las observaciones, el IFE contó con un periodo para implementar las recomendaciones y posteriormente entregar a la UNAM los programas corregidos para su verificación. En cada nueva entrega que el Instituto llevó a cabo, la UNAM verificó que las observaciones fueran debidamente atendidas, además de que no hubiera cambios injustificados, todo ello con el objetivo de asegurar la integridad del código revisado inicialmente. La comprobación de la UNAM sobre las actualizaciones de software hechas por el personal del IFE se realizó de manera sucesiva hasta llegar a la versión final del sistema del PREP 2012, el 25 de junio de 2012.

Pruebas funcionales

Las pruebas funcionales de caja negra fueron efectuadas en las instalaciones del IFE, en un ambiente tecnológico con características similares al ambiente de operación de la jornada electoral. Este tipo de pruebas comprenden la definición de escenarios y datos de pruebas preparados por la UNAM, con la finalidad de verificar el funcionamiento y comportamiento del sistema en diferentes situaciones, así como la integridad y precisión de los datos ingresados desde su captura en el sistema hasta su despliegue en Internet.

Se realizaron tres ciclos de pruebas y una verificación final como se indica a continuación¹⁸:

- a) Primer ciclo, del 12 al 23 de marzo de 2012, incluyó las pruebas a los módulos de Captura y Aplicativo Central del PREP.
- b) Segundo ciclo, del 2 al 18 de mayo de 2012, contempló la revisión sistémica de todos los módulos del PREP, en lo relativo a la captura, registro y publicación de datos y de las actas digitalizadas.
- c) Tercer ciclo, del 4 al 10 de junio de 2012, comprendió una revisión integral de todos los módulos del PREP en una nueva versión en la que se esperaba la implementación de las recomendaciones emitidas en el primer y segundo ciclos de prueba, así como los cambios

¹⁸ En el Convenio Específico de Colaboración originalmente se consideraba la realización de dos ciclos de pruebas y una verificación final a partir del 4 de junio, sin embargo debido a replanteamientos en el calendario de trabajo originados por nuevos requerimientos en el software que fueron solicitados a la UNICOM por parte del COTAPREP y de los representantes de los partidos políticos, fue necesario realizar un tercer ciclo adicional, así como la validación final de la implementación de las recomendaciones emitidas por la UNAM. Lo anterior fue acordado en la cuarta sesión de la Comisión de Evaluación y Seguimiento y Comunicación Social Conjunta encargada de dar seguimiento al convenio de colaboración para el adecuado desarrollo y supervisión de actividades.



**INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA
REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS
FUNCIONALES DE CAJA NEGRA DEL PREP 2012**

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



recientes solicitados por el COTAPREP¹⁹ y los representantes de los partidos políticos a la UNICOM.

- d) Validación final, del 19 al 23 de junio de 2012, consistió en la última verificación de la implementación de las recomendaciones sugeridas por la UNAM en los ciclos anteriores, en la versión final del software, para dar por concluidas las actividades de pruebas.

Cabe señalar que debido a la complejidad que implica para el IFE el despliegue de la infraestructura tecnológica que requiere el PREP 2012 para su puesta en operación en un entorno seguro y de alta disponibilidad similar al de la jornada electoral, durante el segundo y tercer ciclos, así como en la fase de validación final, se redujeron los plazos para la realización de las pruebas conforme a lo planeado originalmente por la UNAM. Sin embargo, se corroboró la funcionalidad de todos los módulos del sistema del PREP 2012 con un grado de certeza aceptable.

Al concluir las pruebas funcionales, la UNAM entregó al IFE los siguientes documentos:

Entregable	Fecha
Informe de resultados de las pruebas funcionales de caja negra del software del PREP 2012.	28/mayo/2012 ²⁰
Minuta y disco compacto con las observaciones del tercer ciclo de pruebas.	11/junio/2012

¹⁹ Comité Técnico Asesor del PREP, el cual está conformado por personal experto en materia de desarrollo de sistemas y software, y en los aspectos relacionados con la Internet y de difusión, planeación, administración y desarrollo de proyectos, y se encarga de apoyar y asesorar al Instituto sobre los aspectos relativos al PREP.

²⁰ Fecha acordada en la tercera sesión ordinaria de la Comisión de Evaluación y Seguimiento y Comunicación Social Conjunta.



INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS FUNCIONALES DE CAJA NEGRA DEL PREP 2012

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



Resultados de la aplicación de recomendaciones

Como resultado de la revisión de código y la realización de pruebas funcionales, se detectaron diversas observaciones, que por su importancia fueron catalogadas en tres categorías:

Alto impacto. Afecta gravemente las características del software y/o la integridad de la información, lo que podría poner en riesgo el funcionamiento del sistema del PREP 2012.

Medio impacto. Afecta características importantes del software, sin poner el riesgo el funcionamiento del sistema del PREP 2012.

Bajo impacto. Afecta características que disminuyen la calidad global software, pero no afectan su funcionamiento u operación.

Todas las observaciones de alto impacto que requirieron ser atendidas de manera prioritaria, fueron subsanadas por el IFE, y la UNAM verificó su correcta implementación a través de sucesivas revisiones del código fuente y de pruebas de caja negra, que permitieron validar la incorporación de las recomendaciones.

También fueron atendidas en su mayoría, las observaciones de medio y bajo impacto, que si bien no afectan el funcionamiento del sistema del PREP 2012, contribuyen a incrementar las características de calidad como fiabilidad²¹, eficiencia²², mantenibilidad²³, portabilidad²⁴ y usabilidad²⁵ del software. Algunas observaciones ya no fue necesario atenderlas debido a que las mismas actualizaciones en otros elementos del software las anulaban, o bien no eran prioritarias. En todos los casos, la UNAM validó la pertinencia de la acción tomada.

²¹ Capacidad del software de mantener su nivel de servicio, bajo condiciones establecidas, durante un período determinado.

²² Nivel de desempeño del software y la cantidad de recursos requeridos bajo condiciones establecidas.

²³ Facilidad de extender, modificar o corregir errores en un sistema software.

²⁴ Capacidad de un sistema software para transferirlo desde una plataforma tecnológica a otra.

²⁵ Esfuerzo requerido para su uso y comprensión desde la perspectiva del usuario.



**INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA
REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS
FUNCIONALES DE CAJA NEGRA DEL PREP 2012**

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



En las observaciones identificadas por la UNAM, no se detectaron comportamientos anómalos en el software, sólo casos inherentes al desarrollo y mantenimiento de software, que fueron atendidos por el IFE y que estuvieron asociados a factores como:

- La complejidad de las reglas para la publicación de resultados electorales preliminares en una elección federal de presidente, diputados y senadores, que no se encuentran expresamente definidas en la documentación normativa.
- El caso de una coalición total de tres partidos que no se había presentado con anterioridad en una elección federal, así como una coalición parcial de dos partidos.
- Una solución tecnológica que implica una arquitectura compleja para soportar la operación a nivel nacional en un entorno seguro de alta disponibilidad.
- Los componentes del software que son reutilizados de elecciones anteriores y se adaptan para soportar la elección federal de 2012.
- La implementación de un nuevo sistema para la digitalización y publicación de actas, el cual tuvo que ser diseñado y desarrollado en poco tiempo por el personal técnico del IFE.
- Los cambios solicitados en las últimas fases del desarrollo por parte del COTAPREP y los representantes de los partidos políticos.

El IFE concluyó una versión estable y funcional con las recomendaciones prioritarias sugeridas por la UNAM y debidamente implementadas, el día 25 de junio de 2012.



**INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA
REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS
FUNCIONALES DE CAJA NEGRA DEL PREP 2012**

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



Conclusiones

Como resultado de la auditoría técnica realizada al software del Programa de Resultados Electorales Preliminares desarrollado por el Instituto Federal Electoral, y una vez que éste atendió las observaciones y recomendaciones emitidas por la UNAM derivadas de la revisión de código fuente y las pruebas funcionales de caja negra, bajo el alcance señalado en este documento, se concluye que:

El software es funcionalmente apropiado para cumplir con lo establecido en el Código Federal de Instituciones y Procedimientos Electorales vigente, en relación con *“Establecer un mecanismo para la difusión inmediata en el Consejo General, de los **resultados preliminares** de las elecciones de diputados, senadores y Presidente de los Estados Unidos Mexicanos; para este efecto se dispondrá de un sistema de informática para recabar los **resultados preliminares**... Al sistema que se establezca tendrán acceso en forma permanente los consejeros y representantes de los partidos políticos acreditados ante el Consejo General”*.²⁶

El sistema auditado brinda la funcionalidad necesaria para realizar la captura, el registro y la publicación de los datos y de la imagen digitalizada de las Actas de Escrutinio y Cómputo del Proceso Electoral Federal 2011-2012, de manera íntegra conforme son captados en las Terminales de Captura Remota y en los dispositivos de digitalización utilizados en los Centros de Acopio y Transmisión de Datos (CEDAT), permitiendo la difusión inmediata a través de Internet de los resultados preliminares de la elección federal de presidente, diputados y senadores del 2012. El sistema del PREP 2012 auditado está libre de todo algoritmo que pueda distorsionar los datos capturados en los CEDAT.

No obstante, es importante señalar que como en todos los sistemas informáticos, la calidad de los datos dependerá de sus entradas, que en este caso provienen de lo asentado en las Actas de Escrutinio y Cómputo que son llenadas en las casillas, y de la captura realizada en los CEDAT ubicados en cada uno de los 300 distritos electorales; en relación con la captura de los CEDAT, el software sí considera un mecanismo de doble captura para reducir la probabilidad de error en este procedimiento.

²⁶ Inciso L, párrafo 1 del artículo 125 del Código Federal de Instituciones y Procedimientos Electorales (COFIPE), publicado el 14 de enero de 2008 en el Diario Oficial de la Federación.



**INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA
REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS
FUNCIONALES DE CAJA NEGRA DEL PREP 2012**

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



Para concluir este proceso de auditoría, el 1° de julio de 2012 la UNAM verificará ante notario público que los programas revisados por la DGTIC, sean los mismos que el IFE operará en esta elección federal.

Complementario a las conclusiones señaladas, la UNAM considera importante reiterar las siguientes recomendaciones para futuros procesos electorales:

La normatividad no indica que se pongan a disposición de la ciudadanía los resultados preliminares de la elección, sin embargo el PREP se ha convertido en una fuente de información oportuna que los usuarios pudieran interpretar de forma indebida si no se comprenden los elementos normativos de una elección federal. Por ello, se sugiere que el IFE mejore de manera continua los mecanismos de información a la ciudadanía sobre las reglas acordadas entre los involucrados para la publicación preliminar de los resultados, así como los elementos de ayuda del sistema que faciliten la comprensión de la información presentada.

Complementario a lo señalado en el *Código Federal de Instituciones y Procedimientos Electorales* y en la documentación técnica especializada, se observa la falta de una especificación que puntualice los criterios para la publicación de resultados preliminares, que pudiera tomarse como una referencia pública de las reglas y excepciones que deben considerarse para la presentación de la información.

Se sugiere considerar la opinión de expertos en usabilidad y realizar grupos de enfoque con personas que tengan diversidad de: edad, nivel académico, cultura política, habilidades informáticas, entre otras características, con la finalidad de recabar opiniones para detectar oportunidades de mejora relacionadas con la distribución y cantidad de la información mostrada en el sistema del PREP.

Uno de los aspectos medulares en cualquier sistema informático es tener como entrada un conjunto de datos preciso y confiable. En este sentido, son vitales las acciones orientadas a promover un adecuado llenado de las Actas de Escrutinio y Cómputo, a través del fortalecimiento de los elementos logísticos y de capacitación necesarios en la ciudadanía.

Fecha: 25/Junio/2012	Página: 21 de 23
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO	INSTITUTO FEDERAL ELECTORAL



**INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA
REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS
FUNCIONALES DE CAJA NEGRA DEL PREP 2012**

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



Anexo 1. Cuadro resumen de las líneas de código del PREP

	Módulo	Submódulo	Cantidad de archivos totales	Cantidad de líneas de código
PREP DE DATOS	Módulo de Captura	Generación de la información de tarjetas magnéticas	17	5,395
		TCR	77	18,939
		Monitor CEDAT	30	6,062
	Módulo de Aplicativo Central	Registro central	262	49,702
		Consola de administración		
	Módulo de Extracción-Publicación	Extracción	267	49,269
		Publicación	42	10,646
		Logística	91	18,918
	PREP DE ACTAS DIGITALIZADAS	Módulo de Captura de Actas Digitalizadas	MCAD	279
Administración de llaves			4	618
Módulo de Aplicativo Central		Registro central	339	50,897
		Consola de administración		
Módulo de Publicación-Logística		Publicación ²⁷	42	10,646
		Logística	93	19,402
TOTAL			1,501	262,540

²⁷ El código fuente del submódulo de *Publicación* del PREP de actas digitalizadas es exactamente el mismo que se utiliza en el PREP de datos, por lo que se indica la cantidad de archivos y líneas de código pero sólo se contabilizan una vez en el total.



**INFORME DE LA APLICACIÓN DE RECOMENDACIONES DE LA
REVISIÓN DE CÓDIGO FUENTE Y DE LAS PRUEBAS
FUNCIONALES DE CAJA NEGRA DEL PREP 2012**

CONVENIO DE COLABORACIÓN NÚM. 30863-87-16-I-12



Anexo 2. Sobre la línea de colaboración en seguridad informática

De manera independiente a la auditoría de software y con el objetivo de identificar vulnerabilidades de seguridad informática asociados a la infraestructura tecnológica de la RedIFE y la del PREP 2012, se estableció la línea de colaboración denominada Auditoría de Seguridad Informática, a fin de auditar, evaluar y monitorear los elementos que componen ambas redes, antes y durante la jornada electoral del 1° de julio de 2012.

Dentro del alcance de esta línea de colaboración, el convenio establece las siguientes actividades:

1. Auditoría de seguridad a la infraestructura de la red de datos del IFE (Pentest a RedIFE) y del Programa de Resultados Electorales Preliminares (Pentest al PREP).

Se llevaron a cabo pruebas de penetración a la infraestructura de red de datos del Instituto (RedIFE) y del PREP, en las que se consideraron los elementos más significativos de la infraestructura, especificados por el IFE, a fin de determinar las amenazas a las que se enfrentan los activos tanto interna como externamente. El servicio contempló la revisión no exhaustiva de sus segmentos de red, con la finalidad de recabar la mayor información sensible para el IFE.

Asimismo, se llevaron a cabo actividades enfocadas a identificar las debilidades de programación en el código de los aplicativos involucrados en el flujo de información del PREP, y se evaluaron características de disponibilidad, confidencialidad, integridad y control de acceso de los aplicativos.

Los resultados y las recomendaciones derivadas de dichas revisiones fueron entregados al IFE para su evaluación. El IFE determinó las acciones aplicables para fortalecer la infraestructura de la red de datos del Instituto y del PREP. En una fase posterior a la revisión inicial, la Universidad revisó las recomendaciones atendidas por el Instituto.

2. Monitoreo de la jornada electoral y respuesta a incidentes técnicos.

Los trabajos de colaboración sobre seguridad informática concluirán el 2 de julio de 2012.

Fecha: 25/Junio/2012	Página: 23 de 23
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO	INSTITUTO FEDERAL ELECTORAL