Universidad Nacional Autónoma de México
Facultad de Estudios Superiores Aragón.
Centro Tecnológico Aragón.
Laboratorio de Cómputo.

Auditoría Informática al Programa de Resultados Electorales Preliminares PREP 2017 para el IEEM.

Informe Final de la auditoría de software.

Bitácora de modificaciones

Historia de versiones

Versión	Fecha	Descripción del cambio	Autor
0.0.1	30/abril/2017	Creación del formato.	Marcelo Pérez
0.1.0	1/mayo/2017	Revisión de infraestructura y caja negra PREP	Marcelo Pérez Jesús Hernández Guillermo Villafuerte Ángel Moreno
0.1.1	6/mayo/2017	Resultados parciales de las pruebas de caja negra.	Marcelo Pérez Jesús Hernández Guillermo Villafuerte Ángel Moreno
0.1.5	7/mayo/2017	Evaluación y resultados parciales de los casos de prueba PREP	Jesús Hernández Edgar Morales Eduardo Bolaños
1.2.0	12/mayo/2017	Resultados de las revisiones y pruebas durante el primero y segundo simulacro.	Marcelo Pérez. Jesús Hernández Edgar Morales Eduardo Bolaños Guillermo Villafuerte Ángel Moreno
1.3.0	15/mayo/2017	Resultados de las pruebas de caja gris y caja negra.	Marcelo Pérez. Jesús Hernández Guillermo Villafuerte Ángel Moreno
1.4.0	20/mayo/2017	Evaluación de la funcionalidad del sistema PREP	Marcelo Pérez. Jesús Hernández Edgar Morales Eduardo Bolaños
1.5.0	22/mayo/2017	Resultados de las revisiones y pruebas durante el tercer simulacro.	Marcelo Pérez. Jesús Hernández Edgar Morales Eduardo Bolaños Guillermo Villafuerte Ángel Moreno
1.5.1	29/mayo/2017	Revisión del documento	Jesús Hernández
1.5.2	31/mayo/2017	Revisión del documento	Marcelo Pérez
1.6.0	31/mayo/2017	Revisión del documento	Jesús Hernández Edgar Morales.

Contenido

Antecedentes

El 2 de febrero de 2017 el Instituto Electoral del Estado de México aprobó los "LINEAMIENTOS DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES" como consta en el oficio IEEM/CG/36/2017 [1], En dichos lineamientos en el Título VI "De la Auditoría, en su Capítulo único "Auditorias del programa" menciona:

"Artículo 74. Para verificar y analizar los sistemas informáticos utilizados en la implementación del PREP se aplicará una auditoria con la finalidad de evaluar la integridad en el procesamiento de la información y la generación de los resultados. Dicha auditoría incluye los sistemas y la infraestructura informática y de telecomunicaciones (red de cómputo, equipos servidores y de telecomunicaciones) que se utilizará en el desarrollo del PREP. Esta actividad se llevará a cabo tanto en los órganos centrales, como en una muestra de diez oficinas de los órganos desconcentrados. "

1. OBJETIVO GENERAL

Realizar una auditoría informática al Programa de Resultados Electorales Preliminares 2017 (PREP), del Instituto Electoral del Estado de México. Conforme al Acuerdo del Consejo General del IEEM No. IEEM/CG/36/2017.

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

Realizar una auditoría al PREP del IEEM, que permita identificar vulnerabilidades en el

[1] Tomado de http://www.ieem.org.mx/consejo_general/cg/2017/acu_17/a036_17.pdf

sistema principal, la infraestructura que lo mantiene y los sitios web allegados al Instituto Electoral del Estado de México (IEEM), con lo que se podrán realizar sugerencias para el control o erradicación en el mejor de los casos de las mismas.

2. OBJETIVOS ESPECÍFICOS

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

B. Probar todos los aplicativos desarrollados específicamente para el PREP, en términos de funcionalidad.

C. Analizar las posibles vulnerabilidades de la infraestructura tecnológica del PREP.

D. Ejecutar pruebas de denegación de servicios, de inyección de código malicioso y de acceso a los diversos recursos del sistema informático.

3. ALCANCES

A. La auditoría se realizó del 21 de marzo al 1 de junio de 2017.

B. La auditoría consistió en dos partes: La primera, corresponde a revisión de la funcionalidad e inspección de código fuente; la segunda, identifica posibles vulnerabilidades que tenga el sistema.

C. Se realizó una planificación de la auditoría, identificando claramente los recursos materiales y técnicos necesarios para llevarla a cabo; dicha planificación se encuentra en poder de la Unidad de Informática y Estadística.

D. La auditoría se realizó con base a los requerimientos establecidos en el anexo técnico del convenio de colaboración UNAM – IEEM y en la metodología IEEE Std 1028™-2008 "IEEE Standard for Software Reviews and Audits" la cual es una metodología estandarizada internacionalmente.

4. METODOLOGÍA

La metodología utilizada para la realización de esta auditoría es la IEEE Std 1028™-2008 "IEEE Standard for Software Reviews and Audits" la cual es una metodología estandarizada internacionalmente y se utilizó para las realización de las pruebas OSSTM, que es un estándar para la realización de pruebas y métricas de seguridad desarrollado por un grupo de profesionales especialistas en seguridad informática y agrupados bajo una organización denominada ISECOM (Institute for Security and Open Methodologies), OSSTMM, hace referencia al manual o documento guía de OSSTM, OSSTM Manual (en inglés). Los casos de pruebas del OSSTM se agrupan en cinco (5) diferentes áreas que en conjunto prueban:

A. Robustez de los controles implementados para la seguridad de la información y de datos.

B. Los controles implementados para la infraestructura de cómputo y de comunicaciones, de redes inalámbricas y dispositivos móviles.

C. Los controles para la detección de intentos de ataques de ingeniería social.

D. Los niveles de concientización en relación a los temas de seguridad informática en el personal de una organización.

E. Los controles de seguridad física de una organización.

En este servicio la metodología OSSTM v3 se usará exclusivamente para delinear las actividades técnicas de los diferentes elementos a ser probados y las acciones a realizar antes, durante y después de cada una de las pruebas. La

metodología OSSTM contempla de manera general las siguientes fases de estudio:

- Definición de Objetivos.
- Exploración.
- Enumeración.
- Explotación.
- Escalación y Finalización de prueba.

Otro estándar utilizado fue OWASP (www.owasp.org), el cual es una metodología que contiene información de cómo construir un ambiente de pruebas y del tipo de técnicas de verificación que se deben usar en los desarrollos de aplicaciones WEB. Teniendo como objetivo principal el desarrollo de aplicaciones seguras. Basándonos en lo que se consideran las mejores prácticas de programación haremos sugerencias para buscar que los cambios sean los menos posibles si es que se necesitan.

En este documento se mencionan cada una de las pruebas que exige la metodología OWASP como parte de un Checklist de las tareas a llevar a cabo aplicado esta metodología. El objetivo es tener una matriz de pruebas/evaluaciones para determinar el grado de seguridad que presentan las aplicaciones desarrolladas. Las pruebas/evaluaciones pueden ser realizadas y/o complementadas a través de una serie de entrevistas con esto se determina de manera adecuada el grado de madurez y la seguridad implícita en las aplicaciones desarrolladas internamente.

En resumen lo que se debe hacer es lo siguiente:

- Recopilar información de las aplicaciones, infraestructura y entorno web.
- Examinar cada fase del proceso para probar vulnerabilidades.
- Identificar puntos críticos y atacarlos para determinar puntos de falla.
- Probar con diferentes métodos de ataque, de acuerdo al checklist.
- Generar resultados.

El checklist o lista de verificación correspondiente a OWASP, se encuentra en el apartado de resultados de la auditoría.

5. Resultados de la auditoría

Al ser este informe final de naturaleza pública, se omiten datos específicos tales como direcciones de Internet (IP), versiones del software sobre el que corren las aplicaciones y otros datos técnicos que por ser información que pudiese comprometer la seguridad de la infraestructura y aplicaciones que sobre ella se ejecutan no se presentan en este documento, dichos detalles técnicos se describen en los informes parciales ya en posesión del Instituto Electoral del Estado de México.

Para esta auditoría las pruebas se realizaron en dos periodos de tiempo:

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

Si bien las pruebas se realizaron en dos periodos de tiempo distintos, los resultados se estructuran para este informe, por infraestructura y seguridad y por funcionalidad; los resultados de la auditoría se estructuran de la siguiente forma: en primer lugar se presentan los resultados de la revisión de la infraestructura. Posteriormente se presentan los resultados de pruebas realizadas sobre el sistema Programa de Resultados Electorales Parciales (PREP), el estado de la verificación de las medidas de remediación y por último el dictamen de la auditoría.

Durante la realización de la auditoría, el equipo auditor se abstuvo de:

- instalar cualquier tipo de puerta trasera o aplicación que permita acceso remoto encubierto y reiterado.
- instalar cualquier tipo de keylogger, boot, troyano, rootkit o tecnología similar.
- instalar aplicaciones de acceso remoto que sean claramente identificables como procesos activos y cuyos puertos, y conexiones sean visibles.

- borrar, alterar o apagar el uso de las bitácoras (logs) en cualquier dispositivo, estación de trabajo o servidor.
- modificar la configuración de un servidor, estación de trabajo o dispositivo de red.

Una vez concluida la auditoría el equipo auditor no dejó ninguna modificación o rastro en la infraestructura del IEEM originado a raíz de las pruebas realizadas.

A) Resultados de la revisión de la infraestructura del PREP

Respecto al uso de equipo por parte del auditor:

Todo equipo de cómputo propiedad del auditor que fue conectado a la infraestructura de red del IEEM, estuvo protegido y actualizado contra código malicioso, virus, troyanos, etc., y cumplió con las políticas de seguridad para equipos de terceros.

Los aspectos que se revisaron fueron los siguientes:

Resguardar con seguridad el área destinada a los servidores:

Respecto a los servidores del PREP 2017

En las inspecciones se constató que los servidores que albergan el servidor de aplicaciones y los servidores de bases de datos se encontraban correctamente confinadas en el *site* propio del Instituto. Se verificó que el control de acceso estuviera bien implementado y físicamente se pudiera restringir el acceso a personas ajenas al instituto; En ambos casos la inspección resultó satisfactoria.

Respecto a los equipos de digitalización y captura.

Se realizó la inspección de los 211 equipos de captura en los centros de captura 1 y 2 ("auditorio" y "carpa") y se encontró lo siguiente:

1. La instalación de Red de datos y eléctrica, están hechas de acuerdo a los diagramas de infraestructura; La red de datos tienen conexión directa al Site del instituto por medio de fibra óptica instalada exclusivamente para ambos centros y por ductos protegidos en todo su trayecto hacia los servidores del PREP.
2. Todos los equipos contaban con el mismo tipo y la misma distribución de Sistema Operativo.
3. Todos los equipos estaban protegidos para encendido con contraseña de BootLoader, contraseña en control de personal limitado y de confianza del propio instituto.
4. Además de la contraseña de BootLoader, los equipos contaban con una contraseña del sistema operativo, también bajo control y resguardo del personal del instituto.
5. El equipo auditor realizó pruebas detalladas sobre el sistema operativo y se encontró que la instalación era idéntica en todas las computadoras, lo cual es una ventaja en cuanto a mantenimiento y reducción del tiempo de configuración.
6. Se realizó un escaneo de puertos y servicios, se comprobó que sólo los relacionados al sistema PREP fueran los que estaban activos. La única excepción fue un servicio de administración remota, contemplada por la Unidad de Informática y Estadística. Se recomendó que se cerrará y la Unidad de Informática y Estadística se comprometió a cerrarlo para el día de las elecciones.
7. Se inspeccionó la existencia de equipo de respaldo de energía en los dos centros de captura.
8. Durante los simulacros se verificó la existencia de pruebas de corte de energía. En estas pruebas se detectaron fallas en algunas unidades de respaldo, lo cual para el tercer simulacro el Instituto reportó que ya habían sido remplazadas.
9. Se realizó la inspección de 30 equipos de digitalización producto de la visita a 10 distritos electorales tomados como muestra. En donde se encontró lo siguiente:

Respecto a los equipos en los Centros de Acopio y Transmisión de Datos.

1. La instalación de Red de datos y eléctrica, están hechas de acuerdo a los diagramas de infraestructura; La interconexión con el CEsCo es por medio de enlaces privados punto a punto y una VPN como respaldo.
2. Todos los equipos contaban con el mismo tipo y la misma distribución de Sistema Operativo.
3. Todos los equipos estaban protegidos para encendido con contraseña de BootLoader, contraseña en control de personal limitado y de confianza del propio instituto.
4. Además de la contraseña de BootLoader, los equipos contaban con una contraseña del sistema operativo, también bajo control y resguardo del personal del instituto.
5. El equipo auditor realizó pruebas detalladas sobre el sistema operativo y se encontró que la instalación era idéntica en todas las computadoras, lo cual es una ventaja en cuanto a mantenimiento y reducción del tiempo de configuración.
6. Se realizó un escaneo de puertos y servicios, se comprobó que sólo los relacionados al sistema PREP fueran los que estaban activos. La única excepción fue un servicio de administración remota, contemplada por la Unidad de Informática y Estadística. Se recomendó que se cerrará y la Unidad de Informática y Estadística se comprometió a cerrarlo para el día de las elecciones.
7. Se verificó el aislamiento de los equipos a Internet; el acceso estaba permitido. De igual forma la Unidad de Informática y Estadística tenía el conocimiento y se comprometió a cerrarlo para el día de las elecciones.
8. Se inspeccionó la existencia de equipo de respaldo de energía.
9. Durante los simulacros se verificó la existencia de pruebas de corte de energía. En estas pruebas se detectaron fallas en algunas unidades de respaldo, lo cual para el tercer simulacro el Instituto reportó que ya habían sido remplazadas.

Comprobar que la arquitectura de la infraestructura de cómputo y comunicaciones corresponda a las necesidades del sistema PREP:

Se verificó que la infraestructura planteada en la solución del sistema fuera la adecuada y que además estuviera implementada según el diseño de la misma.
Los enlaces de telecomunicaciones previstos para la operación del PREP son los adecuados, un primer enlace de 150Mb y uno segundo de 50Mb, ambos enlaces filtrados por un firewall y un clúster fortinet respectivamente.
Internamente la red del IEEM, la red de aplicaciones del sistema PREP y la red de captura se encuentra adecuadamente segmentada, se comprobó por medio de una inspección y realizando pruebas con herramientas de red sobre el sistema operativo Linux.
En cuanto a los distritos electorales, se implementó en cada uno de ellos dos redes VPN uno para el Centro de Acopio y transmisión de Datos (CATD) y una para la red interna de la junta distrital. En resumen ambas redes están aisladas una de otra y tienen una conexión aislada con un encapsulamiento hacia la infraestructura del instituto.

Infraestructura para el módulo de publicación.

Se observó que los responsables de la toma de decisiones realizaron un análisis de riesgo y establecieron el nivel de apetito de riesgo, ambos conceptos forman parte de las buenas prácticas de gobierno de TI, que dio como resultado la transferencia del riesgo del módulo de publicación del PREP a un tercero. En este sentido fue a través de un convenio con la empresa Telmex para que la misma se encargue de la implementación tecnológica de la publicación de resultados y el almacenamiento de las actas digitales. Esta implementación resulta adecuada en varios sentidos:

1. En primer lugar por el hecho que el día de la jornada electoral las peticiones de los usuarios domésticos (ciudadanía) se hará sobre la

infraestructura Telmex y no sobre la infraestructura IEEM. Con lo cual se evita tráfico excesivo en la infraestructura del instituto.

2. Debido a la naturaleza de las actas de escrutinio y cómputo digitalizadas que cuentan con un tamaño de archivo digital de 500kb (en promedio) y que el número total de actas es de 18,606, da como resultado de 8.9 GB de almacenamiento, este almacenamiento estará a cargo de este servicio.
3. La consulta a las actas digitalizadas estará disponible al público en general, y será la empresa Telmex quien absorberá el tráfico generado sobre esta parte del servicio y no el IEEM.
4. La infraestructura de la empresa Telmex está preparada para ajustar los recursos de la infraestructura interna, según la demanda o ataques informáticos que se podría llegar a presentar el día de la jornada.

Pruebas de caja negra (Black box):

Estas pruebas se realizaron desde la red externa (Internet) y sin contar con información del Instituto (por ello la denominación de caja negra). Debido a la criticidad de las pruebas, estás se realizaron en horarios acordados con el personal de la Unidad de Informática y Estadística.

Para definir los objetivos de las pruebas, se recurrió a un motor de búsqueda en el cual se observó que el sitio *.ieem.org.mx cuenta con 8 subdominios en operación, los cuales fueron analizados en diversas etapas.

A) Enumeración

La fase de enumeración inicia con la indagación manual a través del sitio y de la información pública en cada uno de los sitios, para recabar todos los detalles de contacto (nombre completo, correo electrónico, teléfonos y extensiones, redes sociales, etcétera) que se encuentren tras terminar la revisión, debido a que es un factor que un atacante considera a la hora de intentar un ataque al Instituto.

Posteriormente, se ejecutaron herramientas automatizadas de exploración de sitios web y motores de búsqueda con la finalidad de encontrar todos los recursos web servidos en cada uno de los sitios, y obtener los metadatos de los documentos descargados desde ahí, donde es muy común encontrar información del personal que realiza los documentos o de las máquinas en las que se procesa la información.

Los hallazgos fueron reportados con el Instituto en forma de matrices de reconocimiento, las cuales fueron entregadas como anexo de los informes parciales.

B) Identificación de vulnerabilidades

En esta etapa se realizó un análisis de vulnerabilidades automatizado a los servidores del Instituto y al de difusión del sistema PREP para revisar la existencia de posibles vulnerabilidades debido a configuración deficiente del sistema o al uso de componentes antiguos o sin los parches de seguridad correspondientes.

Durante esta fase no se encontró ninguna vulnerabilidad de alta criticidad, y las que se encontraron correspondían a configuración o recursos encontrados por defecto en el servidor, por lo que se pueden solucionar rápidamente.

C) Escaneo de puertos

Se revisaron los puertos y servicios que cada uno de los subdominios del Instituto y del sitio difusor de los resultados preliminares tenían abiertos con la finalidad de revisar si alguno de los servicios es vulnerable a algún ataque conocido y asimismo checar si alguno de los puertos abiertos no es necesario para el servicio que preste el servidor.

En los servidores de disponibilidad pública no se encontró nada fuera de lo

ordinario ni versiones demasiado anticuadas de los programas utilizados en los servidores.

Pruebas de caja gris (Gray Box):

Las pruebas de caja gris son aquellas en las que se nos dio acceso y autorización a la infraestructura que el Instituto ocupa en las juntas distritales a las cuales se acudió a revisión; dichas juntas fueron detalladas en el informe parcial correspondiente. Esto con la finalidad de revisar si la red y las máquinas del Instituto se encuentran configuradas de acuerdo a lo esperado.

A) Arquitectura de red

Tras solicitar acceso a cada una de las redes de las juntas distritales correspondientes se realizó un análisis de red de cada segmento utilizado para garantizar la existencia de únicamente los dispositivos necesarios para realizar la captura o digitalización de los datos utilizados en el sistema PREP, como las terminales de captura, impresoras, y el dispositivo que da acceso a la red. No se encontraron dispositivos ajenos a este propósito.

B) Acceso únicamente a red interna del CEsCo

Se revisó que las redes utilizadas para capturar y digitalizar las actas, respectivamente en el CEsCo y en las juntas distritales visitadas, no contaran con acceso a Internet, sino solamente a la red interna del Instituto.

En los Centros de Captura y Verificación (CCapV) ubicados físicamente en el Instituto se comprobó que desde el inicio no se contaba con acceso a Internet, y así se mantuvo a lo largo de las pruebas.

Sin embargo, en todas las juntas distritales se la siguiente situación: que todas las redes de los distritos contaban con acceso libre a Internet, siendo esto inadecuado debido a que no se puede garantizar la confidencialidad de las actas que vayan a ser transmitidas al CEsCo. Este problema fue informado en varias

ocasiones y se nos dijo que el acceso iba a ser cerrado para el día de la elección, lo cual será comprobado y reportado en el informe de evaluación.

C) Escaneo de puertos

Se revisaron los puertos y servicios correspondientes a las máquinas de captura del Centro Estatal de Cómputo (CEsCo) y las máquinas de digitalización de las juntas distritales visitadas. Esto con la finalidad de revisar si alguno de los servicios es vulnerable a algún ataque conocido y asimismo checar si alguno de los puertos abiertos no es necesario para el servicio que preste el servidor.

Respecto a las máquinas de captura y digitalización se encontró abierto el puerto SSH en todas, lo cual se nos justificó diciendo que ayudaba a la administración remota del sistema, lo cual es un vector de ataque para usuarios con acceso a la red interna, por lo que se recomendó desactivar a la brevedad, recomendación que fue acatada.

D) Análisis de tráfico de red

Para analizar el tráfico transmitido en las redes de captura y digitalización del sistema PREP se procedió a realizar una prueba man-in-the-middle en el CCapV1 ubicado en el Instituto, durante los ejercicios previos al simulacro de actividades del sistema, para corroborar que la información de las actas iba debidamente cifrada para asegurar su integridad y confidencialidad. En este caso se pudo verificar exitosamente que el sistema transmite la información, del centro al site, cifrada utilizando una suite de cifrado TLS robusta. El centro de captura y el servidor que recibe los datos se encuentran ambos en el mismo inmueble.

Pruebas sobre la red inalámbrica dentro de las instalaciones de la UIE:

Es conveniente recordar que la seguridad de las redes inalámbricas radica en el cifrado utilizado y en la contraseña utilizada para cifrar dicha información. Esta negociación se realiza cada cierto tiempo y al inicio de cada conexión

inalámbrica. Nos dimos a la tarea de capturar una de estas negociaciones para la red utilizada en el Instituto.

Tras obtener la negociación hay que probar con los patrones de clave más comunes y con un software específico encargado de realizar el "cracking" de dicha contraseña. A la fecha no se pudo obtener la contraseña, lo cual indica que no es lo suficientemente común para ser adivinada con rapidez.

Pruebas de denegación de servicio (DoS):

Para estas pruebas se diseñó un ataque simulado con el cual se simularían cientos o miles de peticiones consecutivas al servidor de difusión de resultados del sistema PREP para obtener parte del tráfico usual del día de la elección.

Tras iniciar la prueba, a las 5:26 PM, se comenzó a monitorear el sitio web para observar su comportamiento. Aproximadamente un minuto después de iniciado el ataque se observó que el sitio dejó de responder peticiones por espacio de un minuto, tras lo cual, al parecer, el balanceador de carga entró en acción, permitiendo nuevamente la navegación (si bien más lenta de lo usual) a través del difusor PREP.

Tras mantener este nivel de peticiones por unos diez minutos, se procedió a aumentar el volumen de las peticiones, dejando pasar unos minutos entre el primer y el segundo ataque, para intentar dejar sin servicio nuevamente al difusor. Sin embargo, esta vez no logró saturar al servidor.

Esto demuestra que la infraestructura utilizada para el difusor soporta ataques de denegación de servicio de baja o mediana intensidad, aunque cabe mencionar que ninguna plataforma está exenta de riesgo cuando el ataque se realiza con una gran cantidad de computadoras, que pueden llegar a varios miles de equipos. En resumen podemos afirmar que la infraestructura de publicación está razonablemente protegida contra ataques de denegación de servicio.

Escaneo de puertos - identificando así los sockets del sistema PREP; los cuales deberán ser exclusivamente los necesarios para atender los servicios solicitados.

Resultado de la revisión: Las revisiones y escaneos ejecutados sobre el sistema PREP en sus secciones CCapV, y difusores facilitaron la identificación de los puertos y servicios, tanto abiertos, como cerrados en los dispositivos de captura, digitalización y difusión. Respecto a los dispositivos de captura se puede indicar que la mayoría de los puertos y servicios se encuentran cerrados o filtrados, a excepción de un servicio en un puerto determinado, el cual fue identificado en todos los dispositivos dentro de los CCapV 1 y 2. En cuanto a los dispositivos de digitalización ubicados en los CATD, se informa que de los puertos escaneados, únicamente uno con un servicio que se encuentra abierto, además de que existe la posibilidad de establecer conexiones a través de internet con elementos ajenos al sistema PREP. Se nos informó por parte de la Unidad de Informática y Estadística que dicho puerto estará cerrado el día de la elección, esto se verificará y se reportará en el informe de evaluación. Por otra parte en los dispositivos de difusión, los puertos que se encontraron abiertos, estaban controlados bajo la configuración de un balanceador de cargas que permite distribuir las peticiones entrantes al puerto correspondiente a WEB.

Resultados de la revisión del sistema del Programa de Resultados Electorales Preliminares (PREP)

Metodología

La auditoría La auditoría en términos de funcionalidad se llevó a cabo por medio del diseño de casos de prueba tomando como base la documentación proporcionada por los equipos de desarrollo del sistema. El formato de casos de prueba se muestra en la figura 1.1

	Proyecto:	Auditoria PREP 2017 IEEM	
	Institución:	Universidad Nacional Autónoma de México Facultad de Estudios Superiores Aragón Centro tecnológico aragón	UNAM FES Aragón
No. Caso de prueba:	15	Nombre:	Captura de Acta correcta

*Casilla capturada.
*Re-captura.
*Leyenda casilla capturada.
*Apartado de verificación marca errores

	Pasos a seguir	Check
1	Verificar en BD en la tabla de conteos que no exista la información correspondiente al conteo del acta seleccionada.	✓
2	Acceder a la captura de acta por medio del Menú principal.	✓
3	Verificar los datos obtenidos correspondientes al acta que se captura (sección, casilla, Observaciones)	✓
4	Verificar que el Total inicie en 0	✓
5	Verificar que los votos de los partidos participantes inicien en cero	✓
6	Si los datos son ilegibles bloquer campo de captura y se pone en cero	✓
7	Si en el acta el partido no tiene datos se pone S/D se bloquea el campo de captura y se queda vacio.	✓
8	El conteo de votos, se realiza de forma automática al ingresar datos en el campo de captura. -"Guardar >>". Verificar que el sistema muestre aviso que ~~<Primer conteo guardado>~~ casilla capturada -"Regresar" Verificar que no se haya guardado la información en BD tabla de conteo y siga disponible el acta	✓
9	Ingresar nuevamente los datos del conteo pulsar -"Guardar". Verificar que el sistema muestre mensaje ~~<Segundo conteo guardado>~~ casilla recapturada -"Regresar" Verificar que no se haya guardado la información en BD tabla de conteo y siga disponible el acta para su captura	✓

*Casilla verificada

Auditor **Representante IEEM**

Nombre y Firma Nombre y cargo
Firma

Figura 1.1 Ejemplo de caso de prueba ejecutado.

Requerimientos definidos en el anexo técnico:

Adicionalmente a las funcionalidades determinadas por los casos de uso, se revisó que el sistema cumpla con requerimientos adicionales, los cuales se encuentran mencionados en el anexo técnico del convenio de colaboración UNAM – IEEM para la elaboración de esta auditoría.

Se revisó que:

Las pantallas de captura de datos estén diseñadas en forma consistente con los documentos fuente:

Resultado de la revisión: Las pantallas de capturas de datos se encuentran definidas conforme a los requerimientos emanados de los documentos de creación y los lineamientos de IEEM respecto al sistema PREP.

En el ingreso de los datos, la aplicación tenga mensajes de ayuda, con el fin de facilitar su captura.

Resultado de la revisión: Las ventanas de captura poseen suficiente ayuda explicita para continuar con el proceso.

Restringir el acceso de los usuarios a las diferentes opciones de la aplicación.

Resultado de la revisión: Los usuarios tienen acceso solamente a las opciones que corresponden a su perfil de acceso.

Verificar los procedimientos de asignación de permisos a usuarios de la base de datos.

Resultado de la revisión: La asignación de permisos de la base de datos se realiza por medio del administrador del sistema, pero hasta el momento de la revisión si existía la funcionalidad en el sistema para que el usuario pudiera cambiar su contraseña. Se le informó al responsable para que eliminara esta funcionalidad del sistema, situación que fue corregida.

Verificar en cada pantalla de captura, que los campos de los datos importantes sean de obligatoria digitación.

Resultado de la revisión: Se verificó que los campos de datos importantes son requeridos de forma obligatoria, en caso de no ser digitados el sistema no permite avanzar en el proceso.

En toda la aplicación, cada campo tenga el formato de datos apropiado.
Resultado de la revisión: Se verificó que cada campo tuviera el tipo y formato de dato apropiado.

Para los campos numéricos y campos fecha, tengan controles de límite.
Resultado de la revisión: Se verificó que los campos numéricos y de tipo fecha aceptarán solamente datos válidos dentro de un cierto rango.

En la captura o modificación de datos críticos tengan una pista (log o bitácora) donde se identifique lo siguiente: nombre del usuario, fecha y hora, valor del campo y donde se realizó la transacción así como qué tipo de operación realizó ese cambio.
Resultado de la revisión: En las operaciónes sustantivas del sistema PREP como lo es la Captura, recaptura y validación comprobamos que si quedan registrados tanto la hora y el usuario que realiza la operación. Pero no se registran bitácoras de acceso al sistema. No se registra en bitácoras el número de intentos fallidos.

Verificar que los log´s de la aplicación puedan ser revisados por los responsables para investigar accesos y manipulaciones no autorizadas.
Resultado de la revisión: Las bitácoras que existen están implementadas por base de datos y están distribuidas en diferentes tablas del sistema y sólo las personas con privilegios suficientes pueden consultar esta información.

En la captura numérica, se controle la correcta digitación de cantidades.
Resultado de la revisión: Se verificó la correcta digitación de cantidades en la captura numérica, impidiendo digitar caracteres no numéricos, también se verifican los límites de las cantidades para evitar cantidades inválidas, tales como números no enteros.

Existen mecanismos para realizar un monitoreo del avance de digitalización y captura.

Resultado de la revisión: La unidad de sistemas cuanta con un sistema interno para al monitoreo en tiempo real de la digitalización y captura de actas. Reportando tiempos en el proceso, avances y faltantes.

El módulo de digitalización cuenta con una funcionalidad para consultar el avance de actas digitalizadas. Por otro lado en el CEsCo se encuentra un equipo de personas monitoreando el avance de digitalización de los distritos.

Los datos ingresados no puedan ser re-ingresados para el procesamiento más de una vez.

Resultado de la revisión: Se realizó la comprobación de que no puedan ser ingresados más de una vez al sistema los datos cuyos identificadores ya hayan sido ingresados. Para la implementación de este control el instituto lleva el registro del estado (por base de datos) de una acta desde que se digitaliza hasta la captura, segunda captura y validación. También se controla la integridad de transmisión de datos con el uso de firma electrónica sobre las actas digitalizadas.

Si en el ingreso de los datos hay un rechazo por el sistema; que ese dato sea analizado y corregido por los usuarios.

Resultado de la revisión: En el módulo de digitalización el sistema comprobaba la integridad de las actas, en caso de no coincidir no permitía avanzar el proceso. En el caso de la captura, las actas pasan por 3 procesos para realizar la captura, re-captura y la validación.

Validar los procedimientos de excepciones tales como: una acta tenga problemas de origen, Como datos ilegibles, etcétera.

Resultado de la revisión: Si el número es ilegible, el capturista tiene la responsabilidad de escribir el número que está escrito con texto. Si la acta no es legible por errores de digitalización, esto es, la imagen no es lo suficientemente clara para determinar los números, es responsabilidad del capturista marcarla como acta ilegible y se regresa el acta para que se digitalice nuevamente en el CATD correspondiente.

Revisar el funcionamiento del procedimiento del validador al momento que se detecte que un error de captura.

Resultado de la revisión: El sistema es capaz de detectar inconsistencias de la captura y la re-captura, incluso las resalta en color rojo y azul. De esta forma el proceso de verificación es muy rápido. El capturista se guía con estos colores para validar y no lo realiza revisando los valores del acta.

Deterioros o degradación a la base de datos.

Resultado de la revisión: Se comprobó que la base de datos no sufre de deterioros o degradación del rendimiento, al realizar un estudio volumétrico de la base de datos se detectó que el tamaño máximo de la base de datos no degrada el rendimiento del sistema, aunado a esto, se encontró que emplean manejadores de bases de datos confiables y manejan un adecuado mecanismo de respaldos.

Asegurar la consistencia de los datos de las transacciones en la base de datos local y en las bases de datos de replicación.

Resultado de la revisión: Se realizaron pruebas de funcionalidad en donde se verificó que la información capturada por el sistema se almacenara de forma congruente en la base de datos, se contaba con un ambiente controlado de pruebas para este fin.

Durante los simulacros se verificó el entorno de base de datos y la replicación a dos bases de datos, una en sitio y otra fuera del instituto, se realizaron consultas para verificar la consistencia de las replicas de información.

Asegurar que existan mecanismos de detección de errores y de prácticas de corrección de los mismos.

Resultado de la revisión: El equipo de desarrollo realiza pruebas unitarias sobre módulos que les corresponde a los desarrolladores.

Durante los simulacros se observó que el personal de supervisión de captura llevaba registro de los errores detectados en el sistema y posteriormente se reportaban al equipo de desarrollo para su atención.

Mantener continuidad en el procedimiento en línea en caso de in-operatividad de alguna terminal.

Resultado de la revisión:

Se observó que durante el primer y segundo simulacros se pusiera a prueba el plan de contingencia en los Centros de Acopio y transmisión de Datos, cubriendo el 100% de los distritos en esta prueba.

En los dos centros de captura está preparada para responder a contingencias, al tener dos redes separadas una de otra e independientes en soporte de energía; además se cuenta con un tercer centro emergente para continuar con la captura en caso que se requiera.

Verificar la existencia de manuales y procedimientos de entrenamiento.

Resultado de la revisión: La forma de capacitar a su personal de captura y digitalización es por medio de videos realizados por el equipo de desarrollo. Además la capacitación fue continua, realizando prácticas diarias, además de los simulacros oficiales, en donde se mejoraron los tiempos de captura y disminuyeron las dudas sobre las inconsistencia en las actas.

Verificar que el sistema cuente con los siguientes controles:

Minimizar la posibilidad de que se cometan errores humanos durante la captura de datos.

Resultado de la revisión: Se verificó que el sistema no permite que se introduzcan datos erróneos dentro de ciertos parámetros, minimizando de esta forma que se cometan errores humanos durante la captura de estos. Los campos de captura, los botones y otros elementos de la interfaz de las aplicaciones tienen el tamaño suficiente, así como una distribución adecuada.

Restringir la posibilidad de ingresos de datos, consulta y actualización de archivos a personas exclusivamente autorizadas e identificadas.

Resultado de la revisión: Se verificó que sólo usuarios con las credenciales permitidas pueden hacer uso de consulta, actualización de archivos e ingresos de datos: esto se logra por medio de manejo de contraseñas y por medio de control de acceso tanto físico como lógico a los equipos y sistemas. De esta manera ninguna persona ajena tiene acceso a datos y/o archivos importantes del sistema PREP 2017.

Asegurar el mantenimiento confidencial de las claves de cifrado de datos y contraseñas.

Resultado de la revisión: Se verifico este aspecto y las contraseñas no se encuentran cifradas en la Base de datos, sin embargo la red se encuentra bien resguardada disminuyendo el riesgo.

Facilitar y simplificar la tarea del operador.

Resultado de la revisión: En el módulo de digitalización se observó que la operación del sistema es sencilla, el proceso requiere de pocos pasos y muy claros, con la posibilidad de llevarlos a cabo en lotes de 5 o 10 actas por lote.

En el módulo de captura se observó durante los 3 simulacros qué el módulo de captura es de facil uso y que permitió a los capturistas optimizar los tiempos de captura y la disminución de errores.

Utilizar opciones limitadas en los módulos del sistema.

Resultado de la revisión: Se verificó que los módulos sólo pueden ser accedidos por los usuarios bajo las condiciones previstas para ello.

Efectuar control de duplicación.

Resultado de la revisión: Se verificó en base de datos el mecanismo para evitar que se duplicarán actas, el mecanismo es congruente a las especificaciones.

Asegurar, que el sistema sea utilizado por operadores autorizados y desde lugares autorizados.

Resultado de la revisión: Se controlan los accesos de forma centralizada desde el Instituto, de tal forma que sólo si la terminal se encuentra dentro de la red del PREP se le permite el acceso al sistema.

Asegurar la autenticidad del operador/usuario

Resultado de la revisión: Se controlan los accesos de forma centralizada desde el Instituto, adicionalmente los nombres de usuario y contraseñas para los distritos son generados dentro de la UIE, y se entregan en los distritos electorales a través de procedimientos definidos por el IEEM.

Evitar que personas no autorizadas puedan obtener información confidencial.

Resultado de la revisión: Se verificó que cada usuario debe autenticarse con las credenciales adecuadas para el acceso a la información confidencial de sistema.

Respecto a verificar que el desarrollo del PREP cumpla por lo menos un proceso estándar de Ingeniería de Software.

Resultado de la revisión: El desarrollo del sistema fue con base a un ciclo de vida en cascada y cumpliendo con las etapas establecidas en los lineamientos.

Verificar que existan procedimientos para el control de cambios y de versiones del PREP.

Se verificó que el instituto contara con un mecanismo de control de cambios de funcionalidad del sistema, se nos proporcionó el formato con el cual realizarían dicho control y se nos informó que se aplicaría dicho mecanismo una vez que el sistema se encontrara en una versión estable final.

Comprobar que el PREP tenga el licenciamiento requerido para su operación.

El sistema PREP al ser un desarrollo propio de la Unidad de Informática y Estadística (UIE) del IEEM no requiere licenciamiento.

Pruebas de estrés a las aplicaciones que se utilicen en el PREP identificando así los siguientes umbrales de riesgo: alto, moderado, menor, bajo.

Se realizaron diversas pruebas de estrés y se detectó que el promedio de error es de 2.81%, lo cual es considerado un nivel bajo de riesgo ya que el sistema tarda sólo segundos en responder, pero sigue en línea.

6. Dictamen de la auditoría

Como resultado de las pruebas y revisiones a los sistemas del "Programa de Resultados Electorales Preliminares" (PREP) 2017 del Instituto Electoral del Estado de México, manifestamos que:

- Los servidores e infraestructura asociada a los procesos del PREP 2017 son razonablemente seguros, su nivel de riesgo es muy bajo para la operación del servicio mencionado.
- El sistema "PREP 2017" del Instituto Electoral del Estado de México es seguro: robusto, confiable, y cumple con los requerimientos funcionales del sistema, realizan el 100% de las funcionalidades para las que fue creado y no realiza ninguna actividad fuera de las que están descritas en la documentación del sistema.

El sistema "PREP 2017" del Instituto Electoral del Estado de México está en condiciones adecuadas para operar en la jornada del día 4 de junio de 2017.

M. en C. MARCELO PÉREZ MEDEL
Responsable de la auditoría

M. en C. JESÚS HERNÁNDEZ CABRERA
Corresponsable de la auditoría