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

Auditoría Informática al Programa de Resultados Preliminares PREP 2018 para el IECM

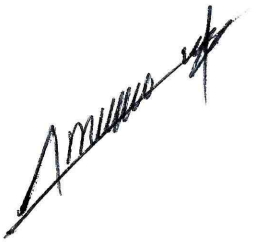
Informe final de la Auditoría

Periodo de evaluación:
Del 14 de mayo al 26 de junio de 2018

Bitácora de modificaciones

Historia de versiones

Versión	Fecha	Descripción del cambio	Autor
0.0.1	02/abril/2018	Creación del formato.	Marcelo Pérez
0.1.0	25/mayo/2018	Estructuración Rubros	Angel Moreno
0.2.1	12/junio/2018	Pruebas funcionales de caja negra	Eduardo Bolaños, Axel Pantoja, Diego Rocha, Paulett Toledo, Yazmin Santiago
0.3.0	20/junio/2018	Análisis de vulnerabilidades a la infraestructura tecnológica	Edgar Portillo
0.4.0	20/junio/2018	Pruebas de negación de servicio	Jesús Cabrera, Rafael Hernández
0.5.0	20/junio/2018	Validación del sistema informático del PREP y de sus bases de datos	Angel Moreno, Jesús Cabrera
1.0.0	21/junio/2018	1era Revisión	Gabriel Ortiz
1.0.1	22/junio/2018	2da Revisión	Jesús Cabrera
1.0.2	25/junio/2018	Revisión final	Marcelo Pérez



1. OBJETIVO GENERAL

Realizar una auditoría informática al Programa de Resultados Electorales Preliminares (PREP) 2018, del Instituto Electoral de la Ciudad de México conforme al reglamento de elecciones aprobado mediante acuerdo del Consejo General del Instituto Nacional Electoral. No. INE/CG661/2016.

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

2. OBJETIVOS ESPECÍFICOS

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

Dentro de los aspectos a revisar en el rubro de calidad del sistema se incluyen:

- Verificación de la arquitectura del sistema.
- Controles adecuados en la entrada de datos.
- Almacenamiento y restauración de datos.
- Implementación de bitácoras en el procesamiento de datos sensibles.

- Cumplimiento en buenas prácticas de codificación basado en estándares en donde se protejan los componentes por medio de encapsulamiento, niveles de acceso y buena implementación de estructuras de control.
- Manejo de errores.
- Evaluación de desempeño y ausencia de leaks de memoria y recursos.

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 (DoS) para comprobar la robustez y disponibilidad del servicio.

E. Diseñar y ejecutar pruebas de Penetración (PenTest) al sistema e infraestructura que soporta al sistema PREP.

3. ALCANCES

A. La auditoría se realiza del 18 de mayo al 5 de julio de 2018.

B. La auditoría consiste 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 Técnica de Servicios Informáticos.

D. La auditoría se realizó con base a los requerimientos establecidos en el anexo técnico del convenio de colaboración UNAM – IECM 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 OSSTMM, OSSTMM Manual (en inglés). Los casos de pruebas del OSSTMM 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 OSSTMM 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 OSSTMM 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 una lista de verificación de las tareas a llevar a cabo aplicando 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.

5. Resultados 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 IECM originado a raíz de las pruebas realizadas.

Durante nuestra participación en la auditoría aparte de realizar todas las revisiones y pruebas que se presentan en las siguientes secciones, visitamos distritos electorales para realizar revisiones y tuvimos presencia en el Instituto durante todos los simulacros y monitoreamos estos desde fuera.

Los resultados se presentan a continuación:

A) Pruebas funcionales de caja negra al sistema informático del PREP.

Introducción

Esta sección contiene los resultados de las pruebas funcionales de caja negra, los cuales se obtuvieron al verificar el proceso técnico operativo mediante el PREP y PREP Casilla. Para lo cual, se considera lo descrito en el Anexo 13 de los Lineamientos Operativos del Programa de Resultados Electorales Preliminares 2018; de dicho documento se toman en cuenta:

- Título II, Capítulo II, numeral 4.
- Título II, Capítulo III, numeral 8.II, 8.III, 9 y 10.I.

De acuerdo al plan de pruebas funcionales de caja negra, se verifica el ciclo de vida del sistema PREP y PREP Casilla. Estos deben cumplir mínimo con las etapas: Análisis, Diseño, Construcción y Pruebas.

De acuerdo con el plan de pruebas funcionales de caja negra, la ejecución de casos de prueba se realizó del 25 al 31 de mayo de 2018.

Metodología

Se hace uso de OWASP (www.owasp.org), la cual es una metodología que contiene información de cómo construir un ambiente de pruebas y del tipo de técnicas de verificación que se deben usar en los desarrollos de aplicaciones WEB teniendo como objetivo principal el desarrollo de aplicaciones seguras y en la metodología IEEE Std 1028™-2008 "IEEE Standard for Software Reviews and Audits".

La metodología empleada para la ejecución de las pruebas funcionales de caja negra está fundamentada en el diseño de casos de prueba para los diferentes casos de uso relacionados con el sistema, tomando como base la documentación proporcionada por los equipos de desarrollo del sistema PREP.

El formato utilizado para registrar los casos de uso se muestra en la Ilustración 1.

	Proyecto:	Auditoría SCR 2018 IECM	
	Institución:	Universidad Nacional Autónoma de México Facultad de Estudios Superiores Aragón Centro Tecnológico Aragón	
No. Caso de prueba:	26	Nombre:	Supervisión de casillas

Diseñado por:	Jesús Hernández Cabrera.
Probado por:	
Fecha de la prueba:	
Tipo de prueba:	Software.
Precondiciones:	Haber ejecutado el caso de prueba de pantalla de inicio del módulo de supervisión del sistema.
Descripción de la prueba:	Se verificarán los flujos principales del caso de uso para visualizar la información del módulo de supervisores.

Elemento (s) a ser probado		
1		Verificación de la información del usuario mostrada en la parte superior de la pantalla.
2		Verificación del funcionamiento del menú superior "Avance en la captura de las casillas de la muestra" y de sus botones.
3		Verificación de cada una de las tablas y gráficos mostrados en las diferentes pantallas.
4		Verificación de los datos mostrados en las gráficas.

Configuración de la prueba (hardware, software, base de datos, tiempo)

Hardware: Computadora en Distrito validado por el IECM con acceso a la red del sistema SCR.

Software: Navegador con acceso a la ruta del sistema.

Base de datos: Se requiere un usuario con privilegios de sólo lectura sobre las tablas de administración

Especificaciones		
Entrada	**Resultado esperado**	**Resultado obtenido**
-Uso del botón "Mapas":	-Se muestra un mapa de una demarcación territorial (inicial por defecto es Azcapotzalco) dividida por estratos, cada estrato tiene un color según su avance de casillas.	-El mapa se mostró correctamente.

Ilustración 1.- Formato de casos de uso

Basándonos en lo que se consideran las mejores prácticas de programación se realizaron sugerencias buscando que los cambios fueran los menos posibles en caso de ser necesarios.

Criterios utilizados para la auditoría

Los hallazgos encontrados durante la prueba se agregan a una matriz y posteriormente se clasifican de acuerdo con nivel de criticidad que presenten en relación con el impacto que se genere. Los niveles de criticidad que se utilizarán son informativo, baja, media y alta, siendo el primero el de menor importancia y el último el de mayor; por otra parte, el instituto debe atender con prioridad los hallazgos de nivel alto.

Nivel de criticidad	Descripción	Prioridad para ser atendido
Alto	El sistema no cubre con la funcionalidad señalada en los lineamientos, convenio o documentos de análisis.	Alta
Medio	El sistema cubre parcialmente la funcionalidad, el sistema puede operar en capacidad mínima.	Media
Bajo	El sistema cubre con la funcionalidad, sin embargo, se encuentran detalles de diseño, información al usuario, entre otras.	Baja

Resultados

Las pruebas de funcionalidad se realizaron a través de 25 casos de prueba, en ellos se establece el funcionamiento técnico operativo del sistema PREP y PREP Casilla. Cada caso de prueba contiene un número de pasos que a ser revisados, para dichas pruebas se estableció un total de 461 pasos, los cuales resultan en un status:

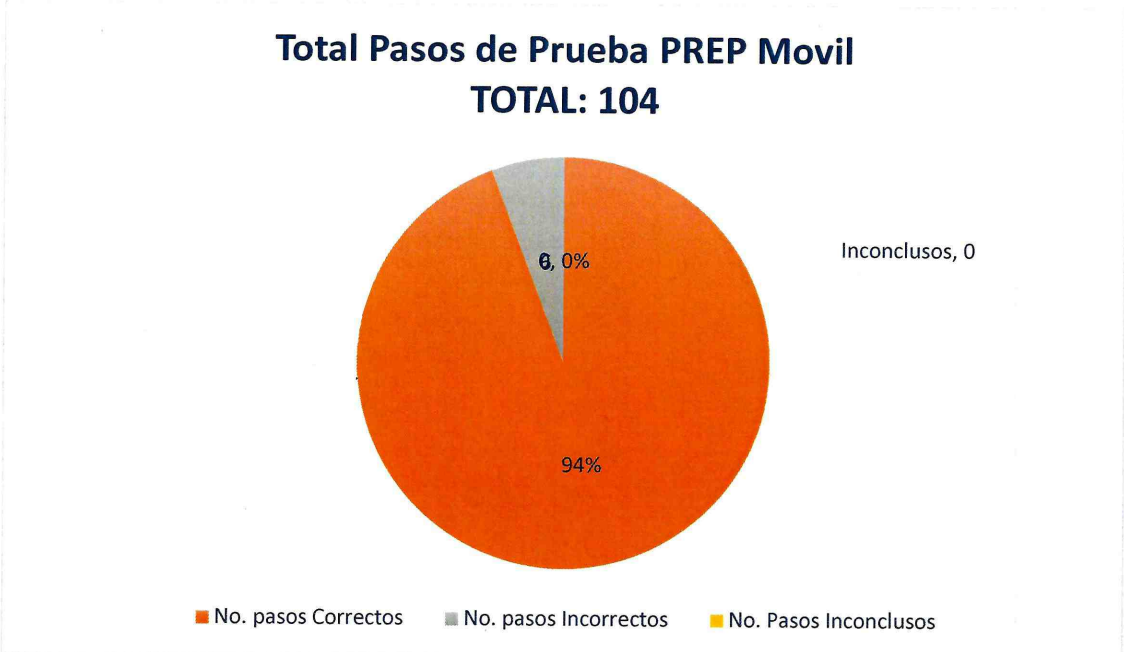
- Correcto. - Al ejecutar el paso, el resultado esperado es igual al resultado obtenido.
- Incorrecto. - Se ejecuta el paso y el resultado obtenido es distinto al esperado.
- Inconcluso. -Se ejecuta el paso, sin embargo, por falta de información en base de datos no se puede observar el resultado para compararlo con lo esperado.

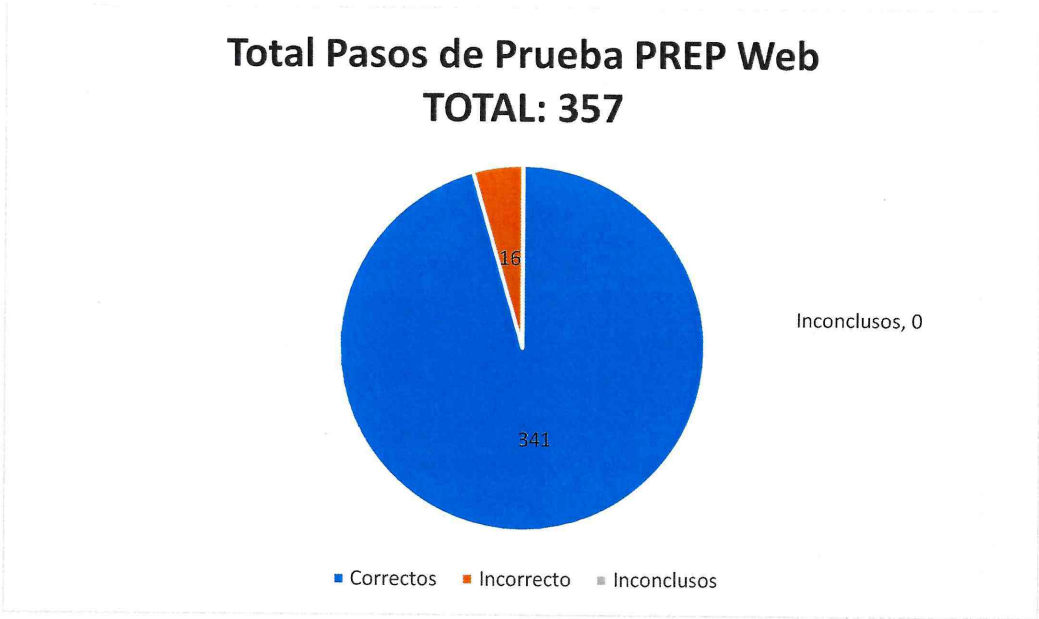
Se presenta la información obtenida al ejecutar los casos de prueba para PREP y PREP Casilla durante las etapas de revisión preliminar y final, posteriormente se presentan los hallazgos encontrados, los solventados y los no solventados.
Resultados de la revisión preliminar.

Resultados de la revisión preliminar:

Al momento de la primera revisión el flujo de operación estándar funcionaba adecuadamente, pero aún faltaban detalles de la operación de flujos alternos, es decir, cuando la operación trata con excepciones.

	Pasos a probar	Correctos	Incorrectos	Inconclusos
PREP	357	341	16	0
PREP Casilla	104	98	6	0
Total	461	439	22	0

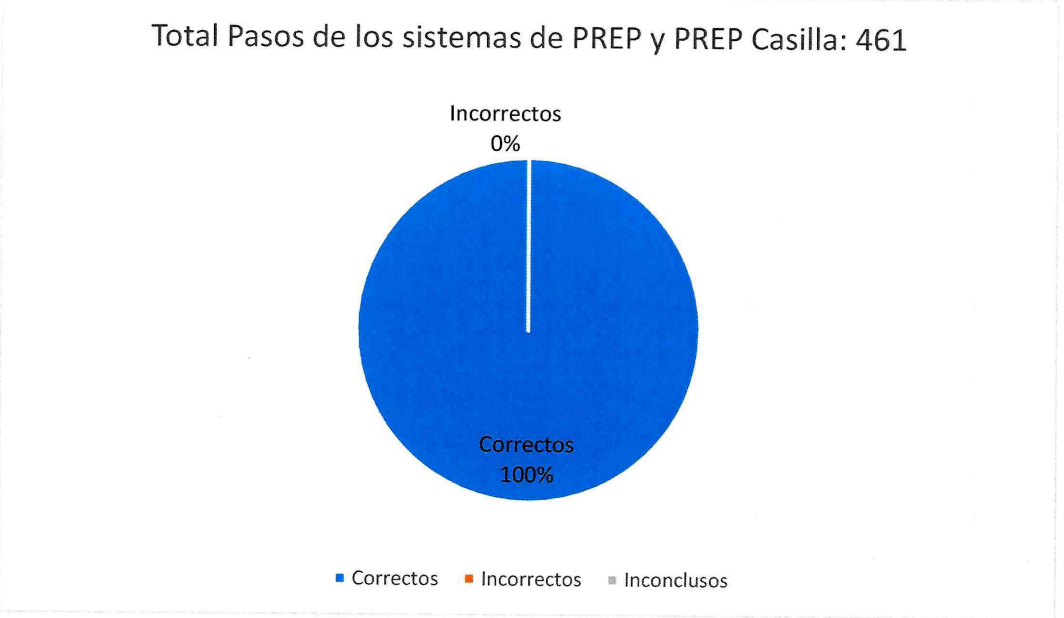




Resultados de la revisión final:

Durante la revisión final se pudo corroborar que todos los hallazgos habían sido subsanados y el manejo de flujos alternos estaba completamente implementado.

	Pasos a probar	Correctos	Incorrectos	Inconclusos
PREP	357	357	0	0
PREP Casilla	104	104	0	0
Total	461	461	0	0



B) Validación del sistema informático del PREP y de sus bases de datos.

Objetivo

Validar que el sistema informático del PREP que operará el día de la Jornada Electoral, corresponda al software auditado, así como que la base de datos se encuentre sin registros adicionales a los necesarios para que el sistema opere. La validación respecto a la correspondencia del software auditado y el utilizado en la operación del PREP, se tendrá que realizar al inicio, durante y al final de la operación del sistema informático del PREP.

Alcance

Llevar a cabo un procedimiento técnico para verificar que los programas auditados se encuentren operando desde el inicio y hasta el cierre de operación del sistema informático del PREP, así como que la base de datos se encuentre debidamente inicializada.

Procedimiento técnico

Núm.	Actividad	Área responsable	Documento empleado
1	Entrega al Titular de la UTSI el disco compacto con los archivos binarios del PREP 2018.	Auditor externo.	No aplica
2	Rompe los lacres del disco compacto con los archivos binarios del PREP 2018 y los entrega al personal técnico.	Titular de la UTSI	No aplica
3	Realiza la copia de los archivos del disco compacto a la computadora portátil de firma.	Jefe de Departamento de Web, Seguridad y Nuevas Tecnologías	No aplica
4	Genera el HASH de los archivos copiados.	Jefe de Departamento de Web, Seguridad y Nuevas Tecnologías	No aplica
5	Abre el programa "Seguridoc" y selecciona el certificado del Secretario Ejecutivo.	Jefe de Departamento de Web, Seguridad y Nuevas Tecnologías	No aplica
6	Selecciona los archivos binarios del disco compacto y se aseguran los mismos con la firma del Secretario Ejecutivo.	Jefe de Departamento de Web, Seguridad y Nuevas	No aplica

Núm.	Actividad	Área responsable	Documento empleado
		Tecnologías	
7	El Secretario Ejecutivo ingresa su contraseña para firmar el código fuente del PREP 2018.	Secretario Ejecutivo	No aplica
8	Retira el disco compacto de la computadora portátil de firma y lo entrega al Titular de la UTSI. (Este disco se utilizará para su instalación en los servidores centrales del PREP 2018).	Jefe de Departamento de Web, Seguridad y Nuevas Tecnologías	No aplica
9	Graba en un disco compacto los archivos firmados por el Secretario Ejecutivo.	Jefe de Departamento de Web, Seguridad y Nuevas Tecnologías	No aplica
10	Coloca los sellos al disco compacto y lo entrega al Titular de la UTSI.	Jefe de Departamento de Web, Seguridad y Nuevas Tecnologías	No aplica
11	Realizan el lacrado del disco compacto Entrega al Secretario Ejecutivo el disco compacto con los archivos firmados y el disco compacto con los archivos originales para sus respectivos resguardos.	Consejero Presidente de la COREPRE, Secretario Técnico de la COREPRE Secretario Ejecutivo y Titular de la UTSI.	No aplica
12	Conserva una copia de los archivos binarios.	Titular de la UTSI.	No aplica
13	Coloca el disco lacrado bajo su resguardo en la caja fuerte de la Secretaría Ejecutiva.	Secretario Ejecutivo.	No aplica

Núm.	Actividad	Área responsable	Documento empleado
14	Copia la carpeta con la versión firmada en el servidor central, en el directorio virtual y replica la nueva versión a las sedes distritales.	Subdirector de Sistemas de Información	No aplica
15	Verifica que la versión firmada se ejecute en las direcciones distritales a través de la bitácora de acceso a la base de datos.	Subdirector de Sistemas de Información	Bitácora del PREP
FIN DEL PROCEDIMIENTO			

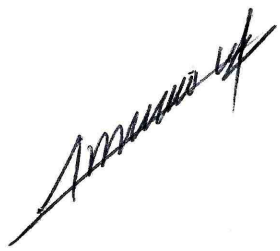
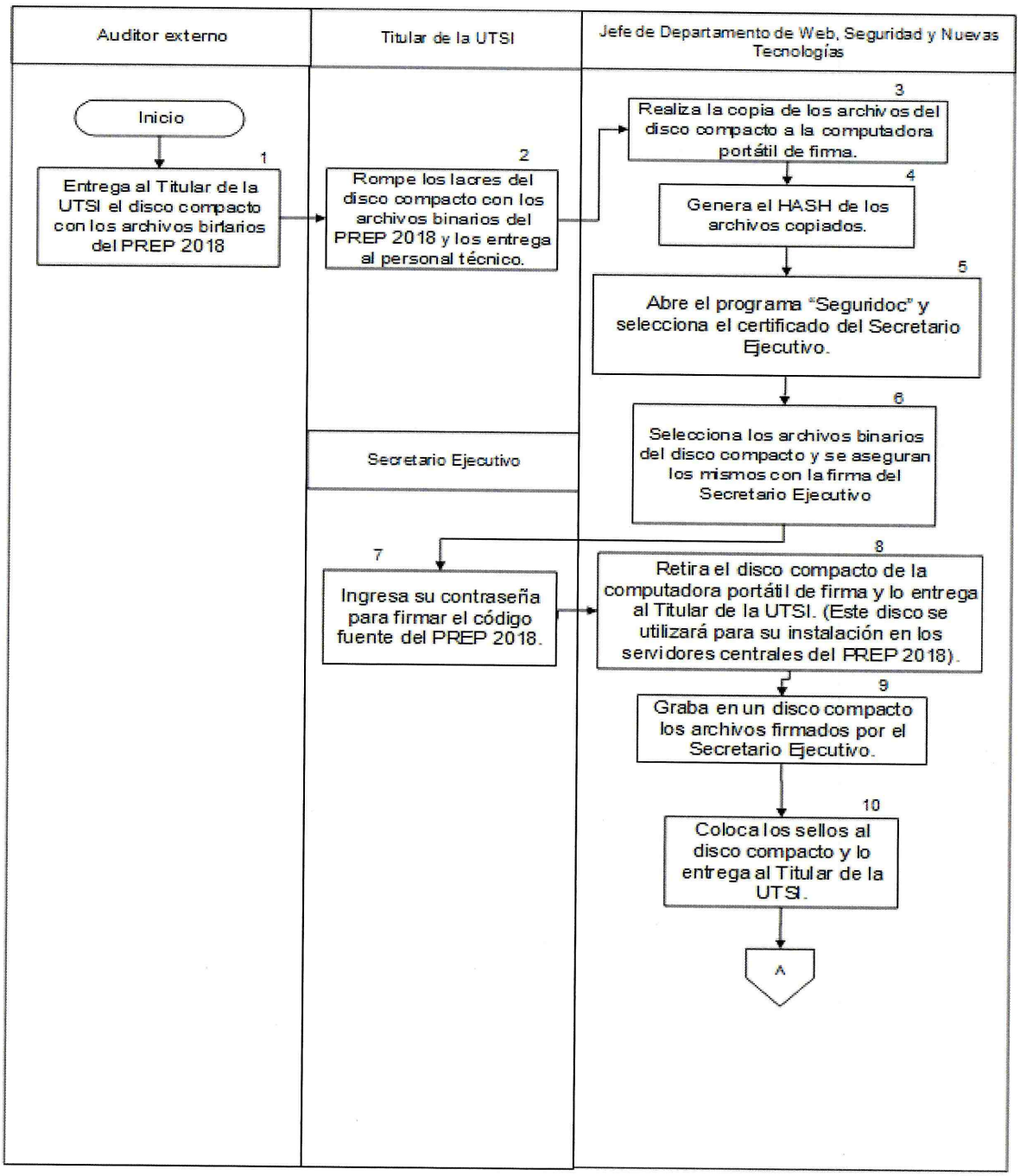
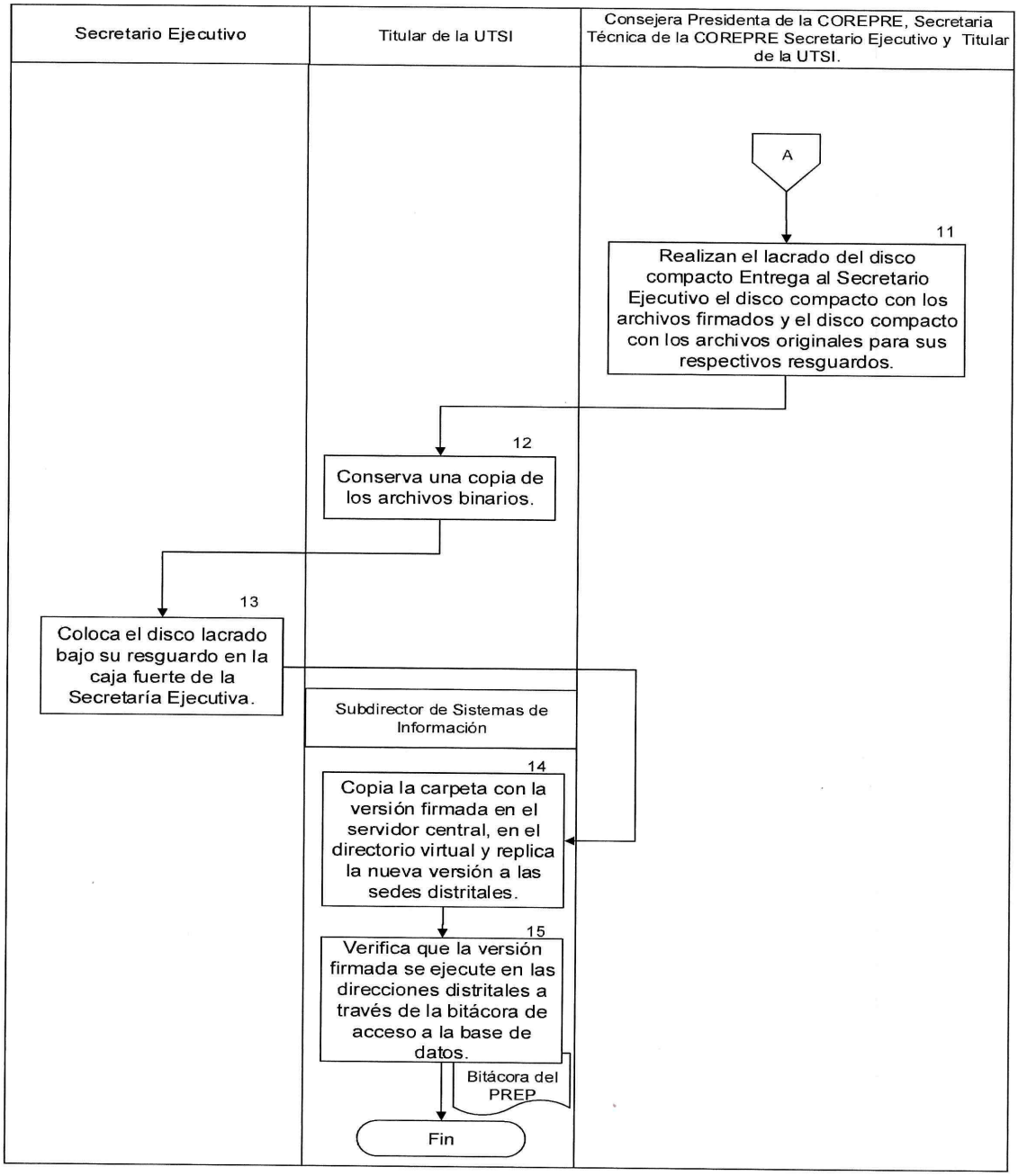


Diagrama de flujo




Secretario Ejecutivo
Titular de la UTSI
Consejera Presidenta de la COREPRE, Secretaria Técnica de la COREPRE Secretario Ejecutivo y Titular de la UTSI.
A
11
Realizan el lacrado del disco compacto Entrega al Secretario Ejecutivo el disco compacto con los archivos firmados y el disco compacto con los archivos originales para sus respectivos resguardos.
12
Conserva una copia de los archivos binarios.
13
Coloca el disco lacrado bajo su resguardo en la caja fuerte de la Secretaría Ejecutiva.
Subdirector de Sistemas de Información
14
Copia la carpeta con la versión firmada en el servidor central, en el directorio virtual y replica la nueva versión a las sedes distritales.
15
Verifica que la versión firmada se ejecute en las direcciones distritales a través de la bitácora de acceso a la base de datos.
Bitácora del PREP
Fin

C) Análisis de vulnerabilidades a la infraestructura tecnológica.

Objetivos

- Identificar debilidades de seguridad en la infraestructura tecnológica mediante la ejecución de pruebas de penetración y revisión de configuraciones de seguridad.

- Clasificar el impacto y documentar las vulnerabilidades identificadas con el propósito de recomendar al IECM las posibles medidas para la mitigación de las vulnerabilidades que previamente fueron identificadas y documentadas.

- Verificar que las medidas implementadas por el IECM hayan atendido adecuadamente las vulnerabilidades reportadas.

Alcance

El análisis de vulnerabilidades de la infraestructura tecnológica deberá realizarse con base en las etapas que se describen a continuación.

Pruebas de penetración (pentest). Las pruebas de penetración se deberán llevarán a cabo tanto desde el interior como desde el exterior de la red de datos a examinar y deberán enfocarse en:

- Servidores
- Aplicaciones web
- Equipos de telecomunicaciones
- Estaciones de trabajo

I. Presentación de hallazgos. El ente auditor deberá presentar un informe preliminar con los hallazgos encontrados, así como la recomendación para atender los mismos.

Para la presentación de hallazgos se utilizará un registro de datos en el que, de forma

conjunta el ente auditor y el IECM, puedan dar seguimiento a los mismos.

II. Validación de reporte de hallazgos. El IECM presentará al ente auditor la retroalimentación acerca de los hallazgos encontrados con el fin de descartar falsos positivos (hallazgos que indican incorrectamente sobre la presencia de una vulnerabilidad) y homologar criterios de interpretación de dichos hallazgos.

III. Atención de hallazgos. Una vez validados los hallazgos, el IECM aplicará los diferentes controles necesarios para mitigarlos y atenderlos. Cabe señalar que el ente auditor deberá considerar dentro de su plan de trabajo, otorgar al menos 10 días hábiles para que el IECM pueda atender los hallazgos.

IV. Validación de la atención de los hallazgos. El ente auditor validará que el IECM haya aplicado los controles necesarios para atender a los hallazgos reportados.

Pruebas de penetración (pentest)

1. *Introducción*

Las pruebas ejecutadas previo al primer simulacro del sistema PREP tuvieron como objetivo, la identificación anticipada de posibles vulnerabilidades que expongan al sistema y/o sus activos durante la ejecución del mismo. En esta primera etapa se realizó únicamente el descubrimiento y enumeración de recursos dentro de la infraestructura perteneciente al sistema.

2. *Alcance*

Este documento integra la información recuperada durante el proceso de auditoría, e incluye lo siguiente:

- Pruebas de penetración (pentest)
- Revisión de configuraciones de seguridad

Aplicándose los puntos anteriores a elementos de la infraestructura como son, equipos de redes y telecomunicaciones, servidores y las aplicaciones web que en ellos residen, así como las estaciones de trabajo que capturan y envían información.

Se presentarán evidencias que validen los hallazgos obtenidos al realizar las pruebas, de tal forma que el instituto pueda identificar y mitigar (apoyado en las recomendaciones) los riesgos provocados por la existencia de ciertas vulnerabilidades.

3. Clasificación de vulnerabilidades

Como resultado de las actividades descritas anteriormente, se obtendrán ciertos hallazgos provenientes de las pruebas que hayan sido ejecutadas durante el análisis de vulnerabilidades, las pruebas de penetración y la revisión de las configuraciones. Dichos hallazgos deberán ser evaluados con base en un criterio de impactos que se muestra a continuación:

Criterio de impacto a los procesos

Nivel	Impacto	Descripción
1	Menor	No se detiene ni afecta ningún proceso.
2	Medio	Procesos de baja prioridad se ven afectados, pero no detenidos.
3	Alto	Procesos de alta prioridad se ven afectados, pero no detenidos.
4	Crítico	Procesos de alta prioridad se ven afectados y pueden ser detenidos.

4. Técnicas y vectores de ataque

Durante las pruebas ejecutadas previo al primer simulacro se utilizaron técnicas de descubrimiento y escaneo basadas en diferentes protocolos para obtener información sobre el sistema que nos permita generar vectores de ataque con altas probabilidades de efectividad.

Entre las técnicas utilizadas se encuentran:

- Escaneos de protocolos basados en modelo TCP/IP de acuerdo con el puerto estándar
- Escaneos de protocolo ICMP
- Trazados de ruta entre IP origen e IP destino
- Escaneos de protocolo ARP
- Pruebas de aislamiento de segmentos de red

5. Resultado de la verificación de la aplicación de las recomendaciones

De acuerdo al carácter de la fase de pruebas (descubrimiento), los hallazgos no corresponden a vulnerabilidades críticas del sistema, sin embargo, todos los hallazgos deben ser analizados y evaluados para su posterior mitigación o aceptación. Durante la ejecución de las pruebas se obtuvieron los resultados que se muestran a continuación.

Se ejecutaron pruebas de escaneo de puertos, pruebas de vulnerabilidades, se revisó la configuración de la red, y el aislamiento de la red.

Se encontraron dos hallazgos de impacto bajo y dos de impacto medio, los cuales fueron reportados al Instituto, mismos que fueron subsanados adecuadamente.

Revisión de configuraciones

1. *Objetivos*

El objetivo es analizar las configuraciones de los dispositivos que conforman la infraestructura tecnológica con base en mejores prácticas de seguridad informática para identificar oportunidades y emitir recomendaciones orientadas al fortalecimiento de ésta.

2. *Alcance*

La auditoría se realiza del 24 de mayo al 11 de junio de 2018.

Los alcances de este documento están establecidos en el Anexo 13, del Reglamento de Elecciones de los cuales se consideran:

Capitulo IV, numeral 12 sección II donde se identifican los activos críticos.

Capitulo VII, numeral 15 sección I, II, II, IV donde se determina el espacio físico del CATD y las facilidades con que cuentan sus integrantes

3. *Hallazgos*

Se realizaron dos recomendaciones respecto a cambiar parámetros de configuración en servidores, los cuales fueron atendidos por el Instituto.

4. *Conclusiones de la revisión de las configuraciones*

La revisión de las configuraciones encontró servidores con parches de software actualizados, con una correcta configuración de seguridad, salvo dos hallazgos menores acerca de configuraciones de bajo riesgo, los cuales fueron reportados y subsanados.

D) Pruebas de negación de servicios.

Objetivo

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 del IECM, durante el periodo de operación del PREP.

Alcance

Generar tráfico de red desde la infraestructura del ente auditor, o en su caso la que éste determine, hacia los servicios web que se publican dentro del dominio del OPL, ya sea en su propia infraestructura o en la que provea un tercero.

Las pruebas de negación de servicio deberán considerar dos apartados:

- Tráfico no malintencionado que consiste en transacciones sintéticas que simulen el tráfico legítimo que se espera el día de la jornada.
- Tráfico de red malintencionado, consistente en paquetes de red malformados.

Las pruebas mencionadas anteriormente deberán realizarse de manera concurrente. Los ataques de negación de servicio deben contemplar, al menos, tráfico de red malintencionado con las siguientes características:

- Ataques volumétricos por protocolo TCP
  - Al menos de 400 Mbps de throughput
  - Al menos realizar SYN FLOOD

- Ataques volumétricos por protocolo UDP
  - Al menos de 400 Mbps de throughput
  - Al menos realizar DNS AMPLIFICATION

- Ataques volumétricos por protocolo ICMP
  - Al menos de 400 Mbps de throughput
  - Al menos realizar ICMP FLOOD

- Ataques en la capa de aplicación (HTTP)
  - Al menos realizar SLOWRIS ATACK

Las pruebas mencionadas anteriormente deberán realizarse de manera concurrente; considerando la generación de tráfico malintencionado (SYN FLOOD, DNS AMPLIFICATION, ICMP FLOOD, SLOWRIS ATACK) en un volumen que represente las condiciones de un ataque.

Durante las pruebas, cada simulación de ataque deberá apegarse a las condiciones de un ataque para hacer que el sitio web que se esté probando quede fuera de línea (no disponible) por, al menos 2 minutos, previo a que el OPL efectué la contramedida para la mitigación.

Tipos de ataque

Se realizaron ataque de tipo: SYN FLOOD, DNS AMPLIFICATION, ICMP FLOOD y de CAPA DE APLICACIÓN, los cuales se perpetraron a través de los protocolos TCP, UDP, ICMP y HTTP.

TIPO DE ATAQUE	PROTOCOLO
SYN FLOOD	TCP/IP
DNS AMPLIFICATION	UDP
ICMP FLOOD	ICMP
CAPA DE APLICACIÓN	HTTP

Resultados

Generando un tráfico de al menos 400 Mbps/s y alcanzando un pico máximo de 3 Gbps/s. provocó que el sitio web del IECM quedara fuera de línea y dejara de responder peticiones legítimas. Este evento comenzó a las 22:06 hrs del día 12 de junio y finalizó a las 02:01 hrs del día 13 de junio dado como resultado 3 horas y 54 minutos como tiempo de ataque DoS.

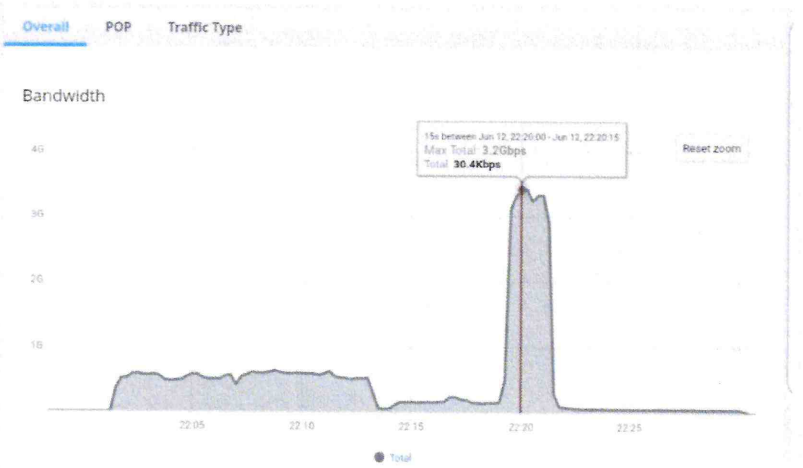
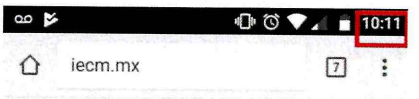
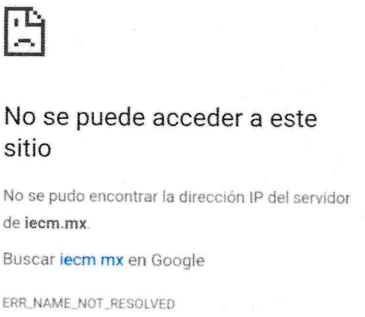


Imagen 3. Monitoreo Ancho de banda a la 22:06 hrs

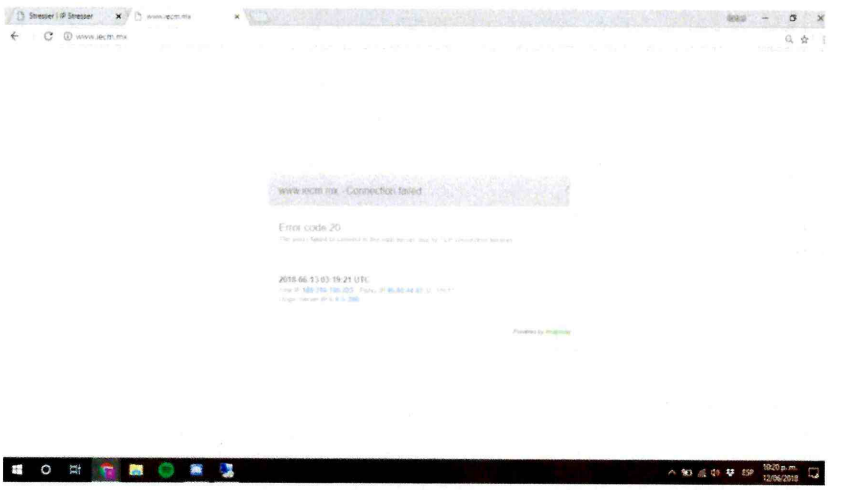
Se alcanzó un máximo de 3.2 Gbps de tráfico de red entrante para la infraestructura del IECM, haciendo uso de las herramientas pertinentes, permitiendo así, identificar las debilidades de la página web.

No obstante, no se necesitó el ancho de banda antes mencionado para que el sitio web dejara de dar servicio, ya que en las siguientes imágenes antes de que se alcanzara el pico máximo de 3Gb el sitio ya presentaba el mensaje de error 20.



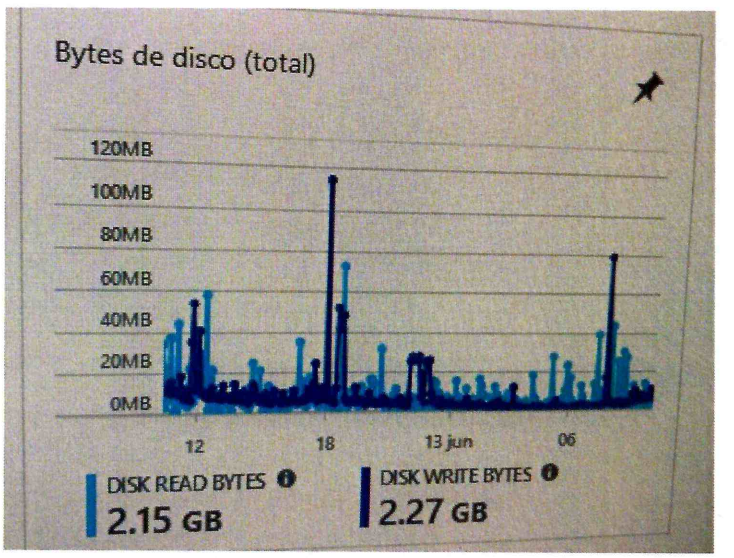


En estas imágenes se puede apreciar como antes de llegar al pico de solicitudes de 3 Gb la página dejó de dar servicio.

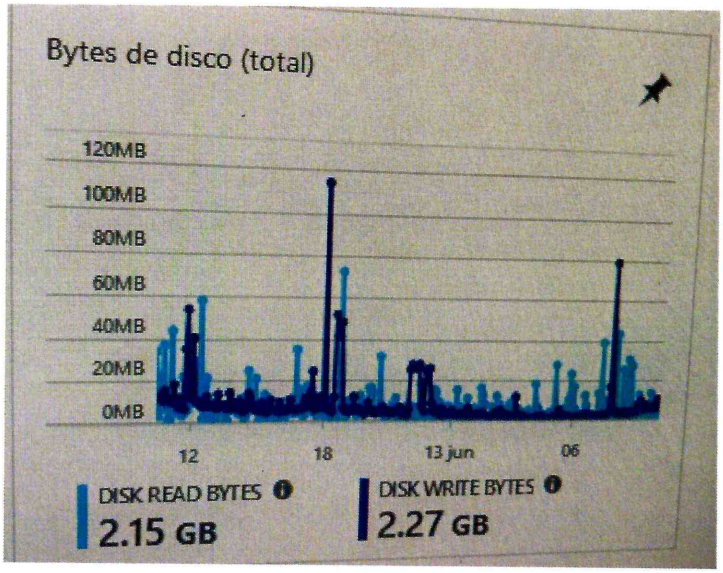


Una vez terminada la prueba la página siguió sin responder peticiones durante al menos un minuto.

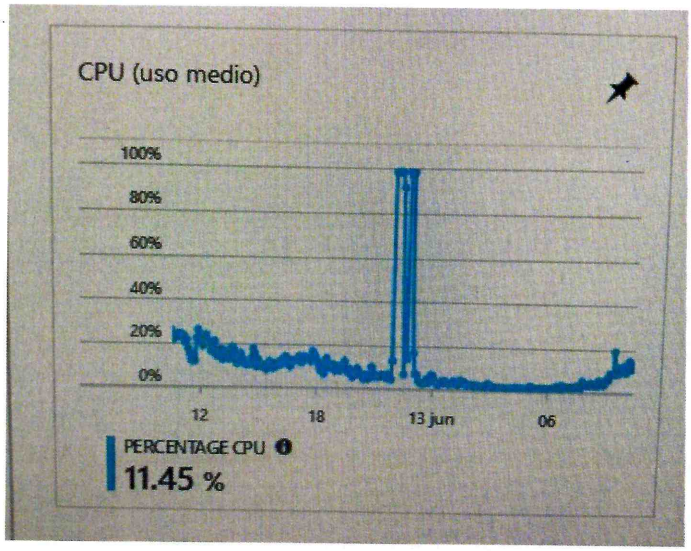
Se revisaron los registros de monitoreo encontrándose que el recurso que se saturó fue el procesador, mientras que el disco duro permaneció dentro de parámetros normales.



Carga del disco duro



Cantidad de bytes manejados por el disco duro



Porcentaje de utilización del CPU.

Como se puede observar en las imágenes anteriores el recurso saturado fue el CPU.

A partir de todo lo anterior podemos afirmar que el sistema dejó de funcionar debido a dos situaciones, pocos recursos en el servidor y que el sistema de protección dejó pasar muchas peticiones no legítimas, como si lo fueran.

Hallazgo	Nivel de impacto	Recomendación
El sistema de protección permitió el paso de muchas peticiones no legitimas	Alto	Se recomienda configurar correctamente y aumentar los niveles de protección de la herramienta utilizada.
El servidor cuenta con recursos muy limitados	Alto	Se recomienda incrementar los recursos del servidor.

Posteriormente a la prueba se informó al instituto acerca de los hallazgos y recomendaciones.

Hallazgo	Nivel de impacto	Atendido
El sistema de protección permitió el paso de muchas peticiones no legítimas.	Alto	SI
El servidor cuenta con recursos muy limitados.	Alto	SI

Hallazgo: El sistema de protección permitió el paso de muchas peticiones no legítimas.

Respuesta del Instituto: Se incrementó el nivel de protección de la herramienta, lo cual mejoró notablemente el número de peticiones filtradas.

Hallazgo: El servidor cuenta con recursos muy limitados

Respuesta del Instituto: Se incrementó considerablemente los recursos indicados durante las pruebas.

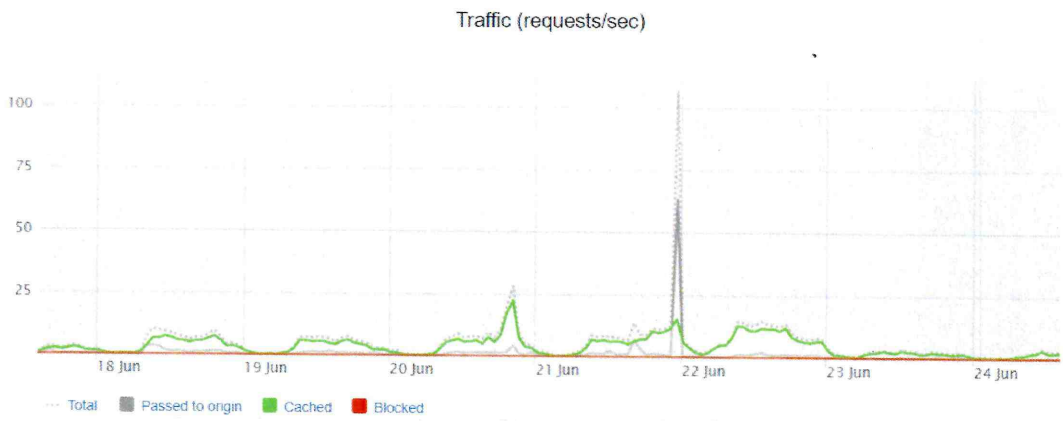


Figura 1 Tráfico durante la prueba

En la figura 1 se puede ver el ataque realizado el 22 de junio en donde sobresale un pico considerable en el número de peticiones realizadas al servidor.

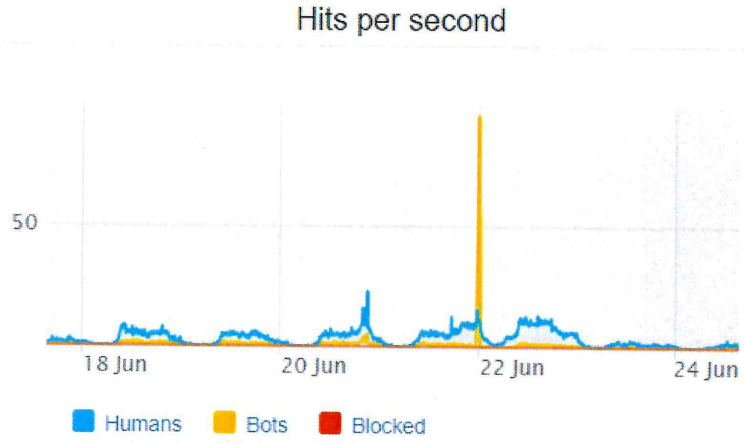


Figura 2 Hits por segundo

En la figura n°. 2 puede verse la diferencia entre las peticiones realizadas por humanos en comparación con las realizadas por procesos automatizados, lo cual demuestra que la herramienta discrimina adecuadamente las peticiones legítimas de las que no lo son.

Conclusiones del ataque DoS

Una vez identificadas las vulnerabilidades presentadas durante la primera prueba de Negación de Servicio y ataque de Negación de Servicio Distribuido, el instituto realizó las medidas correspondientes para contrarrestarlas. Durante un segundo ataque el sistema se encontró, en todo momento en línea garantizando una correcta configuración del sistema, por lo que es posible afirmar que tanto el sistema PREP como el portal principal del IECM se encuentran adecuadamente protegidos contra este tipo de ataques para el día de la jornada electoral del 1ero de julio de 2018.

E) Revisión del Código fuente del sistema PREP.

Introducción

Este informe contiene los resultados de la revisión del código fuente de los sistemas del PREP, del sistema de captura y validación de actas así como de la página web de visualización de las fotografías de las actas por capturar o validar.
La revisión del código del sistema de captura y validación se llevó a cabo manualmente analizando los archivos contenidos en este. En cuanto al sitio web de las imágenes, su código fue revisado tanto manualmente como utilizando una herramienta que realiza el análisis de manera automática:

SonarQube:
SonarQube es una herramienta de análisis de código que nos permite identificar errores y vulnerabilidades en proyectos de diferentes lenguajes de programación.

Objetivo general

Revisar el código fuente de los sistemas del Programa de Resultados Electorales Preliminares 2018 (PREP) del Instituto Electoral de la Ciudad de México, para verificar que no existan vicios ocultos en éste. De este modo se puede verificar que no existan

errores que puedan provocar un funcionamiento no deseado de los sistemas ni que existan vulnerabilidades de seguridad.

Revisión del código fuente

Métricas de calidad

Deuda Técnica: Es el tiempo que se tendría que invertir para corregir una carencia, ya sea porque es un mal código o porque es una deuda técnica asumida previamente.

Puntuación	Descripción
A	Deuda Técnica menor al 10%. Se considera un proyecto estable y no requiere modificaciones.
B	Deuda Técnica entre el 10% y el 20%. Se considera que está en unos parámetros aceptables, pero es recomendable realizar un chequeo periódico para vigilar que no empeore.
C	Deuda Técnica entre el 21% y el 50%. Valores en los que el proyecto requiere algunas modificaciones. Es necesario revisar si estos errores obtenidos son falsos positivos y que estos no afecten el funcionamiento del sistema.
D	Deuda Técnica entre el 51% y el 100%. Es necesario que se tomen medidas correctivas para hacer más fiable el sistema. Se recomienda revisar si estos errores obtenidos son falsos positivos y que estos no afecten el funcionamiento.
E	Deuda Técnica" superior al 100%. Se requieren correcciones mayores tanto de seguridad como de buenas prácticas en la programación. Es necesario revisar si estos errores obtenidos son falsos positivos y que estos no afecten el funcionamiento del sistema.

Evidencias: Número de "malas prácticas" (violaciones) en el código. Por ejemplo, números mágicos, llamar a un método que no es un constructor con el mismo nombre que una clase etc.

Bloqueante	Errores con una alta probabilidad de impactar en el comportamiento de las aplicaciones en producción: pérdida de memoria, conexión a BD no cerrada.
Critica	Errores con una baja probabilidad de impacto en el comportamiento del sistema o un tema que representa un fallo de seguridad: bloque catch vacío, inyección SQL, etc. El código debe ser revisado.
Mayor	Defecto de calidad que puede tener un alto impacto en la productividad de los desarrolladores: trozo de código no cubierto, bloques duplicados, parámetros no utilizados.
Menor	Defecto de calidad con un leve impacto en la productividad de los desarrolladores: líneas que no deberían ser tan largas, las sentencias "switch" deben tener al menos tres casos.
Info	Ni un error, ni un defecto de calidad, sólo un hallazgo.

Resultados de la revisión de código

Página web de visualización de actas por capturar o validar

Fiabilidad: Incluye las evidencias de tipo bug y vulnerabilidades. Un bug representa algo que está mal en el código.

Numero de Bugs	Evaluación de fiabilidad	Esfuerzo de corrección
12	C	2 h 50 min

Seguridad: Incluye las evidencias de tipo vulnerabilidad, que representan una potencial para atacantes.

Vulnerabilidades	Evaluación de seguridad	Esfuerzo de corrección en seguridad
1	D	5 min

A 0 Vulnerabilidades B Al menos 1 vulnerabilidad C Al menos 1 vulnerabilidad mayor D Al menos 1 vulnerabilidad crítica E Al menos 1 bloqueador de vulnerabilidad

Mantenibilidad: Incluye las evidencias de tipo code smells, que son todas esas malas prácticas que a la larga van a provocar que cada vez sea más difícil hacer cambios en el código.

Code Smells	Evaluación de mantenibilidad	Deuda Técnica	Relación de la deuda Técnica	Esfuerzo para Alcanzar la Capacidad de Mantenimiento
35	A	2 h 44 min	0.1 %	0

A 0 Vulnerabilidades B Al menos 1 vulnerabilidad C Al menos 1 vulnerabilidad mayor D Al menos 1 vulnerabilidad crítica E Al menos 1 bloqueador de vulnerabilidad

Duplicado: Incluye información sobre líneas de código, bloques y archivos duplicados.

0.0 %	Bloques duplicados	0
	Líneas duplicadas	0
	Archivos duplicados	0

Tamaño: Número total de líneas de código, sentencias, funciones clases, etc.

Líneas totales	11,347
Sentencias	3,873
Funciones	644
Clases	0
Archivos	15

Directorios	4
Líneas comentadas	1,658
Porcentaje de líneas comentadas	18.1 %

Complejidad: Análisis del código para calcular la complejidad ciclomática. Cuando el flujo de una función se altera, es decir, se produce un salto, este contador incrementa.

Complejidad	2,961
Complejidad / Función	4.6
Complejidad / Archivos	269.2
Complejidad /Clases	0.4
Archivos	15
Directorios	4
Líneas comentadas	1,658
Porcentaje de líneas comentadas	18.1 %

Evidencias: Malas prácticas (violaciones de código).

Evidencias Encontradas	48
Evidencias confirmadas	0
Falsos positivos	0

Observaciones:

Se encontraron doce bugs en el código, sin embargo, fueron falsos positivos ya que se encuentran en el archivo jquery.js que contiene código de librerías.

Con respecto a las vulnerabilidades, se encontró una, sin embargo, también fue un falso positivo porque se encuentra en el archivo jquery.js.

Sobre los code smells se encontraron algunos detalles sobre convenciones de programación que no se siguieron, de este modo, no afectan al funcionamiento del sistema, pero se recomienda seguir las convenciones para que el mantenimiento del software sea más sencillo.

Sistema de captura y validación PREP 2018

El código del sistema de captura y validación PREP 2018 fue revisado manualmente en busca de posibles bugs y vulnerabilidades de seguridad, habiendo encontrado cuatro de las últimas, las cuales fueron reportadas y atendidas.

F) Revisión del Código fuente del sistema PREP Casilla.

Introducción

Este informe contiene los resultados de la revisión del código fuente y del archivo de aplicación (apk) de la aplicación móvil PREP-Casilla.
La revisión del código de la aplicación móvil y del archivo APK fue realizada utilizando dos herramientas que analizan el código y los archivos de la aplicación de manera automática y los hallazgos verificados manualmente.

Objetivo general

Revisar el código fuente de la aplicación móvil del Programa de Resultados Electorales Preliminares 2018 (PREP) del Instituto Electoral de la Ciudad de México, para verificar que no existan vicios ocultos en éste. De este modo se puede verificar que no existan errores que puedan provocar un funcionamiento no deseado de la aplicación ni que existan vulnerabilidades de seguridad.

Revisión del código fuente

1. *Métricas de calidad*

Deuda Técnica: Es el tiempo que se tendría que invertir para corregir una carencia, ya sea porque es un mal código o porque es una deuda técnica asumida previamente.

Puntuación	Descripción
A	**Deuda Técnica menor al 10%**. Se considera un proyecto estable y no requiere modificaciones.
B	**Deuda Técnica entre el 10% y el 20%.** Se considera que está en unos parámetros aceptables, pero es recomendable realizar un chequeo periódico para vigilar que no empeore.
C	**Deuda Técnica entre el 21% y el 50%.** Valores en los que el proyecto requiere algunas modificaciones. Es necesario revisar si estos errores obtenidos son falsos positivos y que estos no afecten el funcionamiento del sistema.
D	**Deuda Técnica entre el 51% y el 100%**. Es necesario que se tomen medidas correctivas para hacer más fiable el sistema. Se recomienda revisar si estos errores obtenidos son falsos positivos y que estos no afecten el funcionamiento.
E	**Deuda Técnica" superior al 100%**. Se requieren correcciones mayores tanto de seguridad como de buenas prácticas en la programación. Es necesario revisar si estos errores obtenidos son falsos positivos y que estos no afecten el funcionamiento del sistema.

Evidencias: Número de "malas prácticas" (violaciones) en el código. Por ejemplo, números mágicos, llamar a un método que no es un constructor con el mismo nombre que una clase etc.

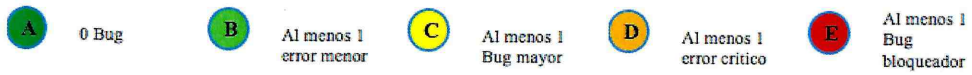
Bloqueante	Errores con una alta probabilidad de impactar en el comportamiento de las aplicaciones en producción: pérdida de memoria, conexión a BD no cerrada.
Critica	Errores con una baja probabilidad de impacto en el comportamiento del sistema o un tema que representa un fallo de seguridad: bloque catch vacío, inyección SQL, etc. El código debe ser revisado.
Mayor	Defecto de calidad que puede tener un alto impacto en la productividad de los desarrolladores: trozo de código no cubierto, bloques duplicados, parámetros no utilizados.

Menor	Defecto de calidad con un leve impacto en la productividad de los desarrolladores: líneas que no deberían ser tan largas, las sentencias "switch" deben tener al menos tres casos.
Info	Ni un error, ni un defecto de calidad, sólo un hallazgo.

2. ***Resultados de la revisión de código***

Fiabilidad: Incluye las evidencias de tipo bug y vulnerabilidades. Un bug representa algo que está mal en el código.

Numero de Bugs	Evaluación de fiabilidad	Esfuerzo de corrección
2	C	25 min



Seguridad: Incluye las evidencias de tipo vulnerabilidad, que representan una potencial para atacantes.

Vulnerabilidades	Evaluación de seguridad	Esfuerzo de corrección en seguridad
358	E	11 d

Mantenibilidad: Incluye las evidencias de tipo code smells, que son todas esas malas

prácticas que a la larga van a provocar que cada vez sea más difícil hacer cambios en el código.

Code Smells	Evaluación de mantenibilidad	Deuda Técnica	Relación de la deuda Técnica	Esfuerzo para Alcanzar la Capacidad de Mantenimiento
14,329	B	95 d	5.0 %	1 h 32 min

A 0 Vulnerabilidades B Al menos 1 vulnerabilidad C Al menos 1 vulnerabilidad mayor D Al menos 1 vulnerabilidad crítica E Al menos 1 bloqueador de vulnerabilidad

Duplicado: Incluye información sobre líneas de código, bloques y archivos duplicados.

69.1 %	**Bloques duplicados**	644
	Líneas duplicadas	39,383
	Archivos duplicados	32

Tamaño: Número total de líneas de código, sentencias, funciones clases, etc.

Líneas totales	56,981
Sentencias	530
Funciones	46
Clases	351
Archivos	291
Directorios	272
Líneas comentadas	17,670
Porcentaje de líneas comentadas	36.6%

Complejidad: Análisis del código para calcular la complejidad ciclomática. Cuando el flujo de una función se altera, es decir, se produce un salto, este contador incrementa.

Complejidad	143
Complejidad / Función	2.0
Complejidad / Archivos	3.3
Complejidad /Clases	0.4
Archivos	291
Directorios	272
Líneas comentadas	17,670
Porcentaje de líneas comentadas	36.6%

Evidencias: Malas prácticas (violaciones de código).

Evidencias Encontradas	14,689
Evidencias confirmadas	0
Falsos positivos	0

Observaciones: Se encontraron dos bugs en el código, sin embargo, estos eran falsos positivos porque las excepciones a las que el sistema era propenso fueron evitadas en líneas previas. Con respecto a las vulnerabilidades, se encontraron 358, de las cuales 352 fueron falsos positivos, ya que se encontraron variables públicas en los archivos R.java, los cuales son generados automáticamente. El resto de las observaciones fueron atendidas por el Instituto.

Conclusiones de la revisión de la aplicación móvil

La aplicación móvil es adecuada para su uso el día de la jornada electoral del 1ero de julio de 2018, el sistema es seguro, hace lo que debe hacer y nada más.

G) verificación a la infraestructura de cómputo y de comunicaciones.

Objetivo

Revisar tanto la infraestructura de cómputo como la de comunicaciones del Instituto para comprobar que son adecuados para la ejecución del sistema PREP 2018.

Respecto a la energía eléctrica se realizaron las siguientes verificaciones:

Criterios a evaluar	Cumple	Observacion
Cuentan con planta de energía	si	Una planta para el Site y otras para el Instituto en general
Tiempo de funcionamiento necesario de la planta desde su activación	si	75 horas de duración
La planta cuenta con tierra física	si	
Se cuenta con fusibles de repuesto	si	Solo uno
El Site cuenta con UPS	si	80 Kv (aproximadamente una hora de respaldo), son dos y están en redundancia
Documentos probatorios presentados		Protocolo para situación de emergencia, mantenimiento cada tres meses y compra de fusibles

También se corroboró que:

- El instituto cuenta con dos proveedores de Internet.
- Cuenta con sistemas redundantes de comunicaciones.
- Sus equipos principales cuentan con doble fuente de poder.
- El Instituto posee su Site en instalaciones propias.
- Cuentan con acceso a un site alterno.

En general se pudo comprobar que las instalaciones de cómputo y comunicaciones son adecuadas para soportar la ejecución del sistema PREP 2018.

6. Dictamen de la auditoría

Como resultado de las pruebas y revisiones a la infraestructura y el desarrollo del sistema del "Programa de Resultados Preliminares" (**PREP**) 2018 del Instituto Electoral de la Ciudad de México, manifestamos que:

- Los servidores e infraestructura asociada a los procesos del **"PREP"** son razonablemente seguros, su nivel de riesgo es muy bajo para la operación del servicio mencionado.
- El **"PREP"** del Instituto Electoral de la Ciudad de México es robusto, confiable, y cumple con los requerimientos funcionales del sistema, realiza 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 y no contiene vicios ocultos.

El sistema **"PREP"** del Instituto Electoral de la Ciudad de México está en condiciones adecuadas para operar durante la jornada electoral del 1ero de julio de 2018.

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