Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA
Unidad Iztapalapa

Servicio de Auditoría al Sistema Informático y a la Infraestructura Tecnológica del Programa de Resultados Electorales Preliminares (PREP) para las Elecciones 2024

Informe Final de la Auditoría

31 de mayo de 2024

Aprobación del Documento

Línea de Trabajo	Responsable	Firma
Coordinador General del Convenio	Ing. Luis Fernando Castro Careaga	

31 de mayo de 2024

Historia de versiones

Fecha	Versión	Autor	Descripción
31/05/2024	1.0	RMR, ERF, JMCV y LFCC	Versión Final

Tabla de Contenido

1 Resumen Ejecutivo

El 16 de febrero del 2024, la UAM I y el INE firmaron un convenio específico de colaboración para la Auditoría al sistema informático y a la infraestructura tecnológica del Programa de Resultados Electorales Preliminares 2024 teniendo como objetivo final validar ante la sociedad que el sistema informático del PREP 2024 es confiable y seguro.

La auditoría se realizó a través de 4 líneas de trabajo.

Pruebas funcionales de caja negra (PFCN)

> Las PFCN consisten en usar de una manera estructurada las funciones del sistema informático y validar que su comportamiento es como se espera de acuerdo con sus especificaciones, sin tomar en cuenta la forma en que está construido.
>
> Se realizaron 2 ciclos de prueba aplicándose pruebas para verificar que el sistema funciona como se espera. Los hallazgos encontrados por el equipo de la UAM I fueron notificados al equipo del INE, el cual los atendió y el equipo de la UAM I verifico su correcta resolución.
>
> De los resultados de las PFCN puede afirmarse que el sistema informático del PREP 2024 funciona como se espera y no tiene funciones que no estén dentro de sus especificaciones.

Auditoría y pruebas de seguridad informática (APSI)

> El objetivo de la Auditoría y las Pruebas de Seguridad Informática es evaluar el nivel de seguridad de los aplicativos que conforman los módulos y submódulos del sistema informático del PREP 2024 desarrollado por el Instituto Nacional Electoral (INE), mediante la ejecución de pruebas de seguridad para identificar y minimizar los riesgos de seguridad.
>
> Se realizaron análisis de vulnerabilidades, se revisaron las configuraciones del sistema informático y de su infraestructura tecnológica del PREP 2024, se hicieron pruebas de penetración.
>
> Los hallazgos encontrados por el equipo de la UAM I fueron notificados al equipo del INE, el cuál los atendió y el equipo de la UAM I verifico su correcta resolución.
>
> De los resultados de la APSI se puede afirmar que el sistema informático del PREP 2021 es seguro y es capaz de resistir ataques informáticos.

Validación del sistema informático y de su base de datos (VSIBD)

La VSIBD tiene como objetivo asegurar que el sistema informático usado para el PREP 2024 es el mismo que fue auditado, así como asegurar que al iniciar la operación del PREP 2024, este inicializado correctamente y no existan actas precargadas.

Para hacer la validación se desarrolló un módulo de validación que permite hacer las validaciones previo al inicio de operaciones, durante la operación y al cierre de operaciones del PREP 2024.

Este módulo será utilizado los días de 2 y 3 de junio de 2024 para las actividades de la VSIBD.

Acompañamiento para las Pruebas de Negación de Servicio

Consistió en realizar el acompañamiento al personal del Instituto durante la realización de pruebas de negación de servicio. Lo anterior con la finalidad de medir la efectividad de los controles de protección contra ataques informáticos de volumen.

Del acompañamiento a estas pruebas y los resultados de las mismas, se concluye que la infraestructura asociada al sitio del PREP es capaz de manejar de manera segura estas amenazas y podrá dar el servicio esperado durante la operación del PREP.

En la realización de Auditoría participaron activamente Profesores (6) y profesionales (2), ambos especialistas en Desarrollo de Sistemas de Información e Ingeniería de Software, así como 8 especialistas en seguridad informática y 30 alumnos de trimestres avanzados de las licenciaturas en Computación, Ing. Electrónica, Matemáticas y Química y de la Maestría y Doctorado en Matemáticas.

2 Introducción

La auditoría al sistema informático del PREP 2024 es una actividad para aumentar la confianza en el PREP 2024 y los resultados que publique.

La realización de la auditoría implicó gran esfuerzo de los equipos de la UAM I y del INE con un número grande de participantes (cerca de 50 personas), durante 3 meses calendario.

Este documento presenta el Informe final de la Auditoría al sistema informático del PREP 2024.

El reporte consta de un Resumen ejecutivo describiendo en términos generales las actividades realizadas y los resultados obtenidos.

A continuación de esta introducción se presentan los resultados de cada línea de trabajo de la auditoría.

3 Resultados

3.1. Resultados de las Pruebas Funcionales de Caja Negra

La estrategia de las PFCN consideró 2 ciclos de prueba los cuales fueron reportados en dos informes preliminares y uno final de esta línea de trabajo.

Se muestran los resultados obtenidos en cada ciclo de pruebas.

3.1.1. Resultados del 1er ciclo de pruebas

En el primer ciclo de pruebas de auditoría se llevó a cabo el reconocimiento al ambiente de auditoría, la resolución de temas de configuración, acceso y estabilidad del ambiente del sistema informático, pruebas de captura de campos (tipos y longitud), validación de reglas de negocio entre los diferentes valores capturados, así como pruebas de flujo completo considerando flujos alternos y pruebas limitadas de volumen para validación de cálculos en el módulo de publicación para el mayor tipo de actas posible.

Las primeras versiones que se pusieron a disposición del Ente Auditor presentaron problemas de estabilidad que impidieron la realización de las pruebas de auditoría. Fue hasta la versión de software y ambiente que se proporcionó al Ente Auditor el 20 de marzo que se reunieron los requisitos de estabilidad y la no presencia de errores graves, lo que permitió continuar con el segundo ciclo de pruebas.

3.1.2. Resultados del 2º ciclo de pruebas

En el segundo ciclo de pruebas de auditoría se llevó acabo la aplicación de pruebas de ciclo completo realizando todas las actividades y flujos de proceso técnico operativo que considera el sistema informático, así como las pruebas de volumen para validar cálculos en el módulo de publicación para todos los tipos de actas que maneja el PREP.

Durante el segundo ciclo de PFCN se realizaron cuatro tipos de pruebas:

- De volumen medio.
- De alto volumen.
- De regresión.
- Otras modalidades de voto (voto en el extranjero, anticipado y prisión preventiva).

Al cierre del segundo ciclo la aplicación se comportó de manera adecuada, las pruebas de regresión, cálculos y actas de otros tipos de votación fueron exitosas, sin que se presentaran hallazgos graves.

Por lo que al final del segundo ciclo de pruebas se concluyó que el Sistema Informático del PREP no presentaba problemas funcionales graves que impidieran su adecuada y correcta operación durante la jornada electoral.

3.2. Resultados de la Auditoria y Pruebas de Seguridad informática

Se realizó una evaluación exhaustiva del sistema informático del PREP con el objetivo de detectar posibles vulnerabilidades que pudieran ser explotadas por personas malintencionadas.

Para ello, se llevó a cabo la identificación de equipos visibles en la red utilizando técnicas de evasión de protección perimetral. El objetivo principal de esta actividad fue obtener una visión inicial de los servicios, plataformas y versiones que se encuentran dentro del alcance, así como evaluar las políticas de seguridad implementadas. Para lograrlo, se realizó una exploración exhaustiva, recorriendo e identificando los puertos y servicios relacionados con el proyecto. Se utilizaron tanto herramientas automatizadas como pruebas manuales para detectar, según su huella, banner y versión, cuáles de ellos presentan vulnerabilidades documentadas en fuentes públicas.

Además, se emplearon herramientas automatizadas de detección de vulnerabilidades y se analizaron los resultados obtenidos. Se examinó minuciosamente la configuración de los sistemas y aplicaciones para identificar posibles debilidades. Esto incluyó aspectos como permisos, controles de acceso, cifrado de datos, configuración de elementos de infraestructura de software y servicios de red.

Con la información recopilada previamente, se llevó a cabo una explotación controlada sin causar daño ni impacto negativo en los sistemas y datos. Se utilizaron técnicas de hacking ético para intentar aprovechar las vulnerabilidades identificadas y obtener acceso no autorizado a sistemas o datos.

Los resultados generados por las pruebas anteriores fueron comparados con respecto a vulnerabilidades conocidas, así como con relación a desviaciones de estándares y buenas prácticas.

Las pruebas se realizaron en dos ciclos y estuvieron alineadas con metodologías estándares ampliamente reconocidas. Después del primer ciclo de pruebas, los hallazgos identificados fueron informados al equipo del INE mediante un sistema automático de control de defectos para su tratamiento.

Luego de su atención por parte del INE, se realizó un segundo ciclo de pruebas para comprobar que los hallazgos se hubieran solucionado correctamente.

La conclusión de esta línea de trabajo es que, el Sistema Informático del PREP y la infraestructura tecnológica relacionada es lo suficientemente segura para resistir amenazas y ataques tales como los que fueron aplicados durante la auditoría. Por lo mismo la opinión es que, será capaz de manejar estas amenazas durante su operación.

3.3. Resultados de la Validación del Sistema Informático y de su base de datos

Esta línea de trabajo plantea asegurar que el sistema informático del PREP en operación el 2 y 3 de junio sea el mismo que fue auditado y por lo mismo todas las conclusiones de la auditoría le son aplicables. Adicionalmente plantea una validación que no existan actas precargadas antes de que el sistema informático inicie sus operaciones.

Las validaciones tienen que hacerse previo a la operación del PREP, durante la operación del PREP y al cierre de operaciones del PREP, estas validaciones deben hacerse ante un notario público.

Para validar que el sistema informático en operación es el mismo que el que fue auditado, se comparan los elementos del sistema informático contra los del sistema auditado. La comparación de elementos se hace mediante la obtención de la firma criptográfica de cada elemento, la cual es única. Si dos elementos son iguales, sus firmas criptográficas son idénticas, si hay una variación por pequeña que sea, las firmas son diferentes.

Las firmas se obtienen mediante un algoritmo que procesa cada byte de un archivo y genera como resultado la firma criptográfica.

Para poder hacer la validación es necesario desarrollar programas que lean los archivos de los componentes del sistema informático, generen sus firmas criptográficas, hagan lo mismo con el sistema auditado y compare las firmas.

Para validar que no hay actas precargadas, es necesario desarrollar programas que consulten la base de datos.

Para poder realizar la VSIBD se elaboró un Procedimiento de Validación que indica la forma en que se harán las distintas actividades de la VSIBD y se incluyó un Módulo de Validación para poder centralizar los programas de validación.

Se desarrollo un Módulo de Validación que sigue el Procedimiento de Validación y realiza las consultas, generaciones de firmas criptográficas y comparaciones que se requieren.

Este módulo permite visualizar de manera sencilla cada una de las actividades relacionadas con la VSIBD.

El Procedimiento de Validación se llevará a cabo los días 2 y 3 de junio utilizando el Módulo de Validación.

El resultado de la validación se dará a través de las Constancias de Hechos para los siguientes puntos del Proceso de Validación:

- Toma de huellas criptográficas del ambiente de auditoría
- Validación del sistema informático previo al inicio de operaciones del PREP 2024.
- Validación del sistema informático durante la operación del PREP 2024.

- Validación del sistema informático al cierre de la operación del PREP 2024.

3.4. Resultados del Acompañamiento a las Pruebas de Negación de Servicio del Sitio del PREP 2024.

Esta línea de trabajo consistió en realizar el acompañamiento al personal del Instituto durante la realización de pruebas de negación de servicio. Lo anterior con la finalidad de medir la efectividad de los controles de protección contra ataques informáticos de volumen.

El acompañamiento se proporcionó en todas las fases de las pruebas de negación de servicio:

- Diseño de las pruebas de negación de servicio
  Apoyando en el diseño de las pruebas, revisando y haciendo sugerencias sobre las direcciones a donde dirigir las pruebas, los tipos de prueba, la volumetría y la duración de estas, así como los resultados esperados, para generar pruebas más efectivas para validar la seguridad ante ataques de negación de servicio.
- Planeación de las pruebas de negación de servicio
  Acompañamiento al personal del INE sobre la revisión de los pasos a seguir y la planeación de las pruebas de negación de servicio.
- Ejecución de las pruebas de negación de servicio
  Acompañamiento al personal de INE durante la ejecución de las pruebas de negación de servicio con respecto a seguir el plan de pruebas y los flujos esperados.
- Análisis de los resultados de las pruebas de negación de servicio
  Apoyo al personal de INE en el análisis de los datos recolectados durante las pruebas para determinar las conclusiones pertinentes y sugerir los ajustes necesarios para remediar cualquier hallazgo que surja.

Del acompañamiento a estas pruebas y los resultados de las mismas, se concluye que la infraestructura asociada al sitio del PREP es capaz de manejar de manera segura estas amenazas y podrá dar el servicio esperado durante la operación del PREP.

4. Recomendaciones

Dado el proceso de desarrollo seguido por el INE, se han generado varias versiones, las últimas cercanas al proceso electoral del 2 de junio.

Aunque no es objetivo de esta auditoría la verificación del proceso del software, sus efectos se ven reflejados en los resultados que se obtuvieron. Se recomienda que el INE modifique sus procesos de desarrollo para tener una versión estable auditable con mayor antelación y una liberación más espaciada de nuevas versiones.

5. Conclusiones

Después de realizar todas las actividades planteadas en el Anexo Técnico, la auditoría al sistema informático del PREP emite las siguientes conclusiones:

- El sistema informático del PREP realiza las funciones de su especificación y las que le marca el Proceso Técnico Operativo.
- El sistema informático del PREP no tiene vulnerabilidades de seguridad significativas que pongan en riesgo su operación.
- El sitio de publicación de resultados del pueden resistir ataques de negación de servicio.

Adicionalmente, se cuenta con un mecanismo que valida que el sistema informático del PREP el día de la elección es equivalente al sistema informático que fue utilizado durante la auditoría y por lo mismo las afirmaciones hechas por la auditoría le son aplicables.