



Informe que rinde la Unidad Técnica de
Cómputo sobre el avance en las actividades del
Departamento de Sistemas y Computación del
Instituto Tecnológico de Durango, respecto a la
auditoría del Sistema Informático del Programa
de Resultados Electorales Preliminares en el
Estado de Durango

Proceso Electoral Ordinario 2017-2018

Unidad Técnica de Cómputo

25-ABR-2018

Contenido

Contenido	2
Definición de actividades e informes de la auditoría al sistema informático del PREP	3
• Definición de metodología propuesta de la auditoría.	3
• Pruebas funcionales de caja negra al sistema informático del PREP.	3
• Validación del sistema informático del PREP y de sus bases de datos (previo a la jornada electoral).	3
• Análisis de vulnerabilidades de la infraestructura tecnológica.	4
• Pruebas de negación de servicio a sitios web del PREP y al sitio principal del IEPC.	5
Avances en las actividades de auditoría	6
• Reuniones de trabajo del grupo de auditores.	6
• Complementación de la documentación del equipo auditor de acuerdo a las observaciones emitidas por el INE.	6
• Definición de roles del equipo de trabajo de acuerdo a las observaciones emitidas por el INE.	6
• Definición de metodologías de la auditoría.	6
• Cronograma de Actividades.	7
• Determinación de los sitios a auditar.	7
Cronograma de actividades del Ente Auditor	8

Definición de actividades e informes de la auditoría al sistema informático del PREP

- **Definición de metodología propuesta de la auditoría.**

Entregable:

1. Documento que describe la metodología empleada, sitios por auditar, descripción de la elección de los sitios a auditar, personal que asiste a las visitas de auditoría, roles del equipo de trabajo y definición de funciones.

Fecha de entrega: abril 2018

- **Pruebas funcionales de caja negra al sistema informático del PREP.**

-Módulo de digitalización, captura y validación
-Módulo de publicación de resultados

Entregable:

1. Plan de pruebas funcionales de caja negra del sistema informático
Fecha de entrega: Abril del 2018
2. Informe preliminar de las pruebas funcionales de caja negra
Fecha de entrega: Primera quincena de mayo del 2018
3. Informe final de las pruebas funcionales de caja negra del sistema informático.
4. Fecha de entrega: 27 de junio del 2018
5. Calendario de trabajo para auditoría de software y pruebas de calidad del sistema informático.
Fecha de entrega: abril del 2018

- **Validación del sistema informático del PREP y de sus bases de datos (previo a la jornada electoral).**

Entregable:

1. Plan de trabajo que cuente con el desglose de actividades, entregables, duración, fecha de inicio y fin, así como responsables de las actividades.
Fecha de entrega: abril del 2018
2. Procedimiento técnico con el esquema de validación de los programas y la base de datos del sistema informático, etapas de validación, generación de diagramas y descripciones.
Fecha de entrega: abril del 2018

3. Constancia de hechos previa a la jornada electoral de la generación de huellas criptográficas de los programas probados del sistema informático PREP. (Tercero con fe pública). Esta constancia deberá describir el protocolo de la actividad, fecha, lugar, hora de inicio y termino, objetivo, actividades realizadas, resultados obtenidos y las firmas autógrafas del personal participante.

Fecha de entrega: Cuarta semana de mayo 2018

4. Constancia de hechos de la validación de los programas y la base de datos del sistema informático del PREP previo al inicio, durante y posterior al cierre de operaciones del PREP (Tercero con fe pública). Esta constancia deberá describir el protocolo de la actividad, fecha, lugar, hora de inicio y termino, objetivo, actividades realizadas, resultados obtenidos y las firmas autógrafas del personal participante.

Fecha de entrega: 1 de julio del 2018

5. Calendario de actividades

Fecha de entrega: abril del 2018

- **Análisis de vulnerabilidades de la infraestructura tecnológica.**

Entregable:

Pentest

1. Documentación de la junta de inicio, donde la instancia interna proporciona una lista de activos críticos y define espacios y ventanas de tiempo para la ejecución de la auditoría (este entregable lo elabora el IEPC).

Fecha de entrega: abril del 2018

2. Plan de pruebas de penetración a la infraestructura tecnológica.

Fecha de entrega: abril del 2018

3. Informe preliminar de las pruebas de penetración a la infraestructura tecnológica.

Fecha de entrega: Primera quincena de mayo del 2018

4. Validación de reporte de hallazgos (este entregable lo elabora el IEPC).

Fecha de entrega: Tercera semana de mayo del 2018

5. Atención de hallazgos (este entregable lo elabora el IEPC).

Fecha de entrega: Tercera semana de mayo del 2018

6. Informe de la aplicación de recomendaciones de las pruebas de penetración a la infraestructura tecnológica.

Fecha de entrega: Cuarta semana de mayo del 2018

Revisión de configuraciones

7. Plan de revisión de configuraciones de la infraestructura.

Fecha de entrega: abril del 2018

8. Informe preliminar de la revisión de las configuraciones de infraestructura.

Fecha de entrega: Primera quincena de mayo del 2018

9. Validación de reporte de hallazgos (este entregable lo elabora el IEPC).

Fecha de entrega: Tercera semana de mayo del 2018

10. Atención de hallazgos (este entregable lo elabora el IEPC).

Fecha de entrega: Tercera semana de mayo del 2018

11. Informe de la aplicación de las recomendaciones de la revisión de configuraciones de la infraestructura.

Fecha de entrega: Cuarta semana de mayo del 2018

12. Informe final de análisis de vulnerabilidades a la infraestructura tecnológica.

Fecha de entrega: 27 de junio del 2018

13. Calendario de actividades.

Fecha de entrega: abril del 2018

- **Pruebas de negación de servicio a sitios web del PREP y al sitio principal del IEPC.**

Entregable:

1. Plan de trabajo detallado que cuente como mínimo con el desglose de actividades, entregables, duración fecha de inicio y termino, así como responsables de las actividades.

Fecha de entrega: abril del 2018

2. Plan de ataques de negación de servicio

Fecha de entrega: abril del 2018

3. Informe de resultados

Fecha de entrega: 13 de junio del 2018, 20 de junio del 2018

4. Estadísticas del tráfico de red generado.

Fecha de entrega: 13 de junio del 2018, 20 de junio del 2018

5. Calendario de actividades.

Fecha de entrega: abril del 2018

Avances en las actividades de auditoría

- **Reuniones de trabajo del grupo de auditores.**

Se realizaron 5 reuniones de trabajo, en las cuales se realizaron los análisis de requerimientos, selección de sitios de auditoría, definición del equipo de trabajo, así como calendarización de las actividades de auditoría.

- **Complementación de la documentación del equipo auditor de acuerdo a las observaciones emitidas por el INE.**

- Sergio Valdez Hernández – Entregado
- José Roberto López Quiñones – Entregado
- Marco Antonio Rodríguez Zúñiga – Entregado
- Salvador Ramos Collins – Entregado
- José Antonio Gutiérrez Reyes – Entregado

- **Definición de roles del equipo de trabajo de acuerdo a las observaciones emitidas por el INE.**

Con base en la experiencia de trabajo y previo análisis de los requerimientos de la auditoría se definieron los siguientes roles del equipo de trabajo.

- Administrador del proyecto: **Sergio Valdez Hernández**
- Auditores de software y Calidad: **Marco Antonio Rodríguez Zúñiga y Salvador Ramos Collins**
- Auditores de Seguridad: **José Roberto López Quiñones y José Antonio Gutiérrez Reyes**
- Auxiliares: Alumnos de las especialidades de Tecnologías de la Información del Instituto Tecnológico de Durango como parte de sus actividades integradoras.

- **Definición de metodologías de la auditoría.**

Con base en los requerimientos de la auditoría se eligió la metodología OSSTMM ya que cubre las necesidades solicitadas para la presente auditoría.

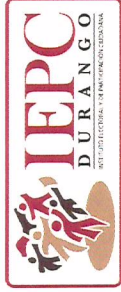
- **Cronograma de Actividades.**

Se definió el cronograma de actividades, mismo que se presenta el siguiente apartado.

- **Determinación de los sitios a auditar.**

Se seleccionaron como muestra representativa los siguientes puntos a visitar:

- CATD Durango (primera visita)
- CATD Nombre de Dios (primera visita)
- CATD Gómez Palacio (segunda visita)



Cronograma de actividades del Ente Auditor

Actividad	Mes											
	Abril			Mayo			Junio			Julio		
Definición de metodología	X											
Selección de sitios a auditar	X											
Definición de roles de equipo auditor	X											
Primera visita a CATDs												
• Pruebas funcionales de caja negra												
• Análisis de vulnerabilidades de la Infraestructura Tecnológica												
Entrega de reporte de resultados de la primera visita				X								
Segunda visita a CATDs												
• Pruebas funcionales de caja negra						X						
• Análisis de vulnerabilidades de la Infraestructura Tecnológica												
Entrega de reporte de resultados de la segunda visita							X					
Tercera visita a CV									X			
• Simulacro 1 de sistema PREP												
Entrega de resultados de la tercera visita										X		
Cuarta visita a CV										X		
• Simulacro 2 de sistema PREP												
Entrega de reporte final										X		
• Pruebas funcionales de caja negra.												
• Análisis de vulnerabilidades de la Infraestructura Tecnológica.												
• Validación del sistema informático del PREP y sus bases de datos.												
• Análisis de vulnerabilidades de la infraestructura tecnológica.												
• Pruebas de negación de servicio a sitios web del PREP y al sitio principal del IEPC												