



2 Propuesta Técnica

Los entregables a la OPL serán los resultados y evidencias del análisis hecho previo al evento de la elección del 6de Junio y una revisión posterior al evento de elecciones. Los siguientes entregables se entregarán los siguientes documentos descritos en las siguientes secciones.

Página | 5

2.1 Análisis de Vulnerabilidades

En esta sección se identificará las debilidades de seguridad en la infraestructura de la OPL y se procederá a ejecutar análisis de vulnerabilidades. Para esta etapa, se entregará los siguientes documentos

1. **Informe final de vulnerabilidades** – Este sería el documento por entregar como resultado de los análisis previos al evento y el proceso de remediación y corrección por la parte de la OPL para mitigar los riesgos presentados por la entidad auditora.
2. **Informe de desempeño de la operación el sistema** – Este reporte sería un resumen de alto nivel sobre los resultados del proceso del análisis de vulnerabilidades.

IMPORTANTE:

- a) Se requiere tener acceso vía VPN para escanear la red de activos de la OPL
- b) Se requiere conocer, previo a la entrega de los reportes finales, las acciones a tomar en caso de que los reportes finales arrojen resultados en donde no se hayan tomado en consideración las recomendaciones, riesgos y acciones de mitigación de las vulnerabilidades encontradas.

2.2 Revisión de configuraciones

El objetivo es analizar las configuraciones de los dispositivos que conforman la infraestructura tecnológica con base a mejores prácticas de seguridad e identificar oportunidades para emitir recomendaciones para su fortalecimiento. Para esta etapa se entregarán los siguientes documentos:

1. **Plan de revisión de configuraciones** – Se efectuará el análisis de configuraciones de la infraestructura tecnológica para recomendaciones que aminoren riesgos a los que pueda estar expuesta la OPL.
2. **Informe preliminar de revisión** – El reporte de la revisión de configuraciones con las recomendaciones y acciones de mitigación que hayan surgido del plan de revisión.
3. **Informe de la aplicación de recomendaciones** – Reporte que contiene el resultado final de la revisión posterior a las acciones de remediación que la OPL haya tomado en función de las recomendaciones que se hayan hecho por parte de la entidad auditora.

Chur



2.3 Pruebas de penetración (pentest)

En esta sección se analizarán configuraciones para emitir recomendaciones basadas en mejores prácticas para el fortalecimiento de esta. Para esta etapa se entregarán los siguientes documentos:

1. **Plan de pruebas** – En este documento se informará el procedimiento a ejecutar, así como el calendario de pruebas en que se realizarán los análisis
2. **Informe preliminar** – el informe preliminar contiene el resultado de las pruebas realizadas sobre los activos.
3. **Informe del estado de seguridad** – Este es el reporte que se hará cuando se hayan aplicado las recomendaciones dadas por la auditoría

Página | 6

2.4 Pruebas de Negación de Servicio

La realización de pruebas de negación de servicio tiene como objetivo el identificar las debilidades, que en los sistemas pueda haber, para evitar una caída de servicio en caso de un flujo de tráfico de tal magnitud que llegue a afectar el servicio de presentar los resultados a los ciudadanos.

1. **Plan de Trabajo** – Se presentará un calendario con las actividades y metodología a seguir para las pruebas a ejecutar por parte de la entidad auditora.
2. **Plan de ataques de DOS** – Este documento describe los pasos y metodología a utilizar para realizar los 4 tipos de ataque que se están solicitando por parte de la OPL:
 - Ataque volumétrico por TCP @400Mbps SYN FLOOD
 - Ataque volumétrico por UDP @400Mbps DNS Amplification
 - Ataque volumétrico por TCP @400Mbps ICMP FLOOD
 - Ataque a nivel aplicación (HTTP) mediante un ataque de bajo ancho de banda (SLOWLORIS)
3. **Informe de resultados** – En este informe se detallará el resultado de las pruebas de ejecución de los ataques de DOS requeridos y los impactos que este tuvieron sobre la aplicación de HTTP y de los sitios sobre los que se harán.
4. **Estadísticas del tráfico generado** – Este será el reporte de tráfico documentado que se tenga por parte de las herramientas de tráfico de la OPL para revisar de qué forma se recibió este tipo de ataques.

Quir

NOTAS IMPORTANTES:

- Los ataques de tipo DOS pueden afectar otros servicios distintos a los que se quiere probar de la OPL, por lo que se requiere tener la autorización firmada del representante técnico y administrativo de la OPL para realizar dicho ataque. (carta anexa en este documento).
- Durante el curso de las pruebas de DOS puede haber afectación a otros servicios y comunicaciones de la OPL por lo que la entidad auditora dará aviso, previa firma de carta de autorización, a la OPL



para realizar dicha prueba eximiendo a la entidad auditora de cualquier afectación en tráfico y otras aplicaciones durante la duración de esta prueba

- Es importante recalcar que las pruebas de DOS solamente se realizarán sobre infraestructura bajo la responsabilidad de la OPL, de ninguna manera se efectuará sobre algún tipo de servicios compartidos o ubicados en nubes públicas, privadas o híbridas donde estén estos servicios

2.5 Pruebas Caja Negra PREP

Mediante el análisis de pruebas funcionales de caja negra, se evaluará la integridad del procesamiento de la información y generación de resultados preliminares. Para tener los entregables correctos, se requerirá que la OPL entregue la lista de los programas y funcionalidades atribuidas a estos para poder probarlos bajo ambientes de prueba (simulacros) y validar los resultados esperados. Los documentos que entregar de esta sección serán:

1. **Documento de Plan de Pruebas** – Los escenarios y pruebas a realizar para validar las funcionalidades de los programas de software a utilizar en las elecciones
2. **Documento de Informe preliminar** – Este serán los resultados de las pruebas realizadas y acordadas con la OPL para ver el SW en funcionamiento y validar los resultados esperados. Documentando hallazgos para ser corregidos, de ser necesario, posteriormente por la OPL
3. **Informa final de pruebas del PREP** – Este reporte se realizará posterior a la remediación de los hallazgos del Documento de Informe Preliminar, donde se esperaría que los hallazgos encontrados sean resueltos por el equipo de la OPL antes del evento del 1º de julio.
4. **Informe de desempeño de la operación del sistema informático** – Este documento describirá el resultado de la operación del sistema

NOTAS IMPORTANTES:

- Las pruebas de caja negra solamente tienen que ver con las funcionalidades a revisar del programa.
- En dichas pruebas no se hará ingeniería en reversa ni verificación de líneas código durante las actividades de validación

2.6 Validación Sistema informático

Mediante la validación del sistema informático, se garantiza que el sistema auditado, sea el que estará en operación el día de las elecciones, garantizando la integridad de este durante su análisis y auditoría.

1. **Documento de Plan de Trabajo** – Se documentará el plan de trabajo a seguir y actividades a realizar para generar la evidencia necesaria.



2. Procedimiento Técnico – Descripción del proceso técnico mediante el cual se realizará la obtención de firmas digitales de los programas en operación en base a una huella criptográfica usando la función criptográfica basada en SHA256
3. Constancia de hechos de generación de huellas de programas probados - deberá describir el protocolo de la actividad, fecha y lugar, hora de inicio y término, objetivo, actividades realizadas, resultados obtenidos y las firmas autógrafas del personal participante por parte de la OPL y del ente auditor Página | 8
4. Constancia de hechos de la validación de programas y Base de Datos - Estas validaciones se deberán realizar previo al inicio, durante y posterior al cierre de operaciones del PREP y deberán describir el protocolo de validación en el ambiente de producción del sistema informático del PREP. Además, deberán incluir la fecha y lugar, hora de inicio y término, objetivo, actividades realizadas, resultados y las firmas autógrafas del personal participante por parte de la OPL y el ente auditor.
5. Informes parciales referentes a los resultados emitidos durante el proceso de auditoría, los cuales tendrán calidad de reservados en términos de las disposiciones aplicables en materia de transparencia y acceso a la información.
6. Informe final: correspondiente a los resultados finales de la auditoría.
7. Informe de evaluación de la operación, considerando el cierre de operaciones del PREP, así como la etapa de evaluación del mismo.

NOTAS IMPORTANTES:

- De haber modificaciones al programa, debido a correcciones hechas por hallazgos durante la auditoría del programa de SW (Sección 4.2), corrección de funcionalidades de éste o cualquier otra razón; la OPL deberá notificar a la entidad auditora previo a la obtención del HASH para notificar a las autoridades de esta modificación, ya que, de haber cambios en el programa, no habrá integridad en el programa al comparar las firmas obtenidas previamente.



4 Plan de Trabajo

Las actividades del plan de trabajo están hechas para realizarse en cierto orden en base a la metodología descrita en la sección 6 de este documento y aprovechar de la mejor manera los resultados obtenidos en cada actividad.

Página | 11

- **Reconocimiento y análisis** – Para iniciar se requiere tener conocimiento de la infraestructura, de ahí que se inicie con las actividades de análisis de vulnerabilidades y luego con la revisión de configuraciones
- **Ejecución Ataques y Sondeos** – Teniendo la información del reconocimiento y análisis se pasa a efectuar las pruebas de penetración (Pentesting). En el mismo tiempo se efectúan las pruebas de DOS aprovechando las vulnerabilidades encontradas en el análisis.
- **Pruebas de Caja Negra** – Estas pruebas se ejecutarán posterior a las revisiones de infraestructura tecnológica, pentest, ataque de DOS, pero es crítico para esta actividad tener los alcances, así como descripción de funcionalidades del sistema informático PREP desde el inicio de los trabajos para construir los casos de prueba y documentación de los criterios de aceptación de estas actividades.
- **Validación de aplicación** – Esta actividad se documentará como procedimiento previo al inicio de los simulacros en el IEES, la constancia se obtendrá una semana antes de la jornada electoral, durante el último ensayo y posteriormente la prueba de firma se obtendrá previo al inicio de arranque del PREP el día de la jornada. La comprobación de la BD se documentará su proceso previo al último simulacro de actividades de IEES y el día de la jornada electoral se ejecutará para probar la Re inicialización de la Base de datos y probar que esta se encuentra vacía.

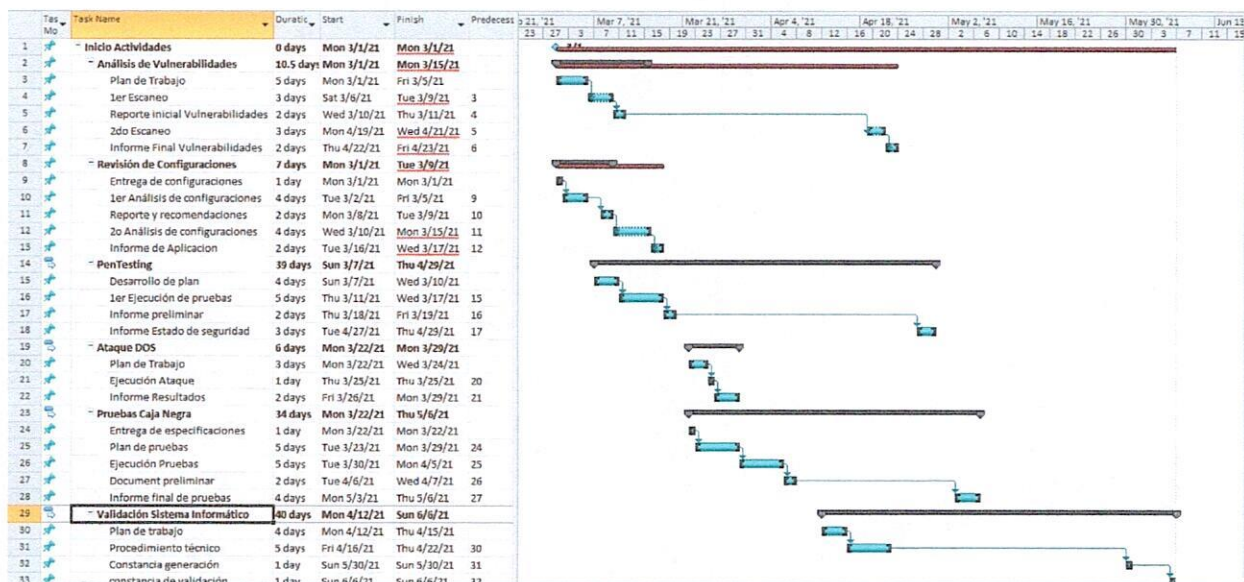
Quir



5 Cronograma (NOTA: Este es un EJEMPLO del plan de trabajo que se desarrollará una vez que esté autorizado el proyecto)

El cronograma comprende actividades y tareas que debe iniciarse desde el 1º de Marzo para finalizar el 6 de junio, el día de la jornada electoral.

Página | 12



El plan se hizo para evitar hacer actividades la semana previa a las elecciones, de modo que inicia un mes antes las actividades. Esto asegura evitar problemas antes de las elecciones.

Todas las actividades de los entregables requeridos se realizarán durante las primeras 5 semanas para tener referencia y dejar tiempo para corrección y/o implementación de medidas correctivas. La revisión de estas se hará durante las últimas semanas de abril y la primera de mayo, justo antes de los simulacros de las elecciones.

Handwritten signature