TECNOLÓGICO DE MONTERREY®

Dictamen final sobre Auditoría de Seguridad Información

Análisis de Riesgos

Descripción breve

Este documento es un reporte sobre el proceso de reconocimiento de la infraestructura del IEC sobre la cual se efectuó las pruebas y los análisis descritos en otras secciones de todo el trabajo.

Jesús R. González / Juan Arturo Nolazco

jrgonza@gmail.com jnolazco@itesm.mx

Índice

1 Resumen Requerimientos 3
2 Alcance 3
3 Estructura del proyecto 4
3.1 Excepciones 5
4 Esquema operativo 6
4.1 Centro de acopio Central 6
4.2 Centro de acopio con escanner digital 6
4.3 Centro de acopio con teléfono celular 7

Tabla de Ilustraciones

Ilustración 1 Nivel de análisis 4
Ilustración 2 Plan de proyecto para el análisis 5
Ilustración 3 Conexión desde el Centro de Acopio con Escanner 7
Ilustración 4 Conexión desde el Centro de Acopio con Celular 7

Versión	Fecha	Descripción
1.0	18 – Mayo – 2017	Resultados del descubrimiento de infraestructura tanto interna como externa del IEC. Análisis de vulnerabilidades inicial (no determinante)

Dictamen elaborado por MsC. Jesús Raúl González Hernández en coordinación con Dr. Juan Arturo Nolazco.

1 Resumen Requerimientos

El Instituto Electoral de Coahuila (IEC) requiere de un análisis de vulnerabilidades así como pruebas de penetración en la infraestructura de red y 5 aplicaciones que desarrollaron para el uso durante las elecciones estatales del 2017.

Se requiere tener una revisión de seguridad de los sistemas y de toda la red como parte de los requerimientos que el INE tiene previo a las elecciones y que lo requiere para el instituto electoral de Coahuila (IEC)

La descripción detallada se presenta en la sección del documento referente al descubrimiento y análisis de vulnerabilidadades.

2 Alcance

El alcance de la auditoría es sobre la infraestructura del IEC. Particularmente se solicita pruebas de vulnerabilidaes a 5 desarrollos internos efectuados por el equipo del IEC. Las características de estos desarrollos son:

- Programadas por el equipo del IEC
- La programación se hizo en PHP, Python, MongoDB.
- Los 5 sistemas corren en containers, sobre el sistema operativo ubuntu linux 16.04; tanto en el host como en los contenendores
- Los programas son aplicaciones basadas en WEB haciendo uso de Bases de datos en mysql

También se requiere tener un análisis de la infraestructura de la red para validar permisos, flujos, infraestructura así como los riesgos de todo el sistema (redes y aplicaciones) en conjunto.

Los entregables de este proyecto serán el resultado de un Análisis Táctico enfocado solamente a los sistemas informáticos.

Ilustración 1 Nivel de análisis

El entregable de este trabajo se dará contemplando estos requerimientos y enfocado a los sistemas informáticos. La estructura del entregable estará basado en la estructura descrita en la sección 2 de este documento.

3 Estructura del proyecto

Este dictamen está estructurado en 6 partes que comprenden los requerimientos dados por el IEC para la auditoría de seguridad. Cada uno de estas partes es un documento por separado que en conjunto es el dictamen final de la auditoría de seguridad de las plataformas del IEC. Los documentos y su descripción son:

1. **Descripción de entregables** – Este es el presente documento el cual describe las partes que comprenden el dictamen final así como los requerimientos y el alcance de los requerimientos dados por el IEC
2. **Reporte de reconocimiento** – Este es un reporte sobre el proceso de reconocimiento de la infraestructura del IEC sobre la cual se efectuó las pruebas y los análisis descritos en otras secciones de todo el trabajo.
3. **Reporte de escaneo de vulnerabilidades** – El reporte de escaneo de vulnerabilidades detalla el resultado del análisis de los activos encontrados en el reporte de reconocimiento.
4. **Reporte de Pentesting** – En este reporte se describe a que plataformas de las requeridas se pudo tener acceso, bajo qué condiciones y con qué herramientas se hizo dicha prueba. Así también se detalla el método, plataforma y escenario bajo el cual se pudo penetrar a las plataformas.

5. **Reporte de modelado de riesgos** – Esta sección detalla el modelado de riesgos siguiendo la metodología NIST300-80. El reporte describe de forma cualitativa los impactos de riesgo de las plataformas involucradas.
6. **Recomendaciones Finales** – En este documento se hacen recomendaciones sobre lo que encontró en las plataformas y análisis que se les hizo durante este trabajo.

Las partes se estructuran en base a como se definió el proyecto inicialmente y que consta en un plan presentado previamente de dos semanas

Actividad	Fecha Inicio	Fecha Final	27	28	29	30	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Auditoría de Seguridad del IEC	**27/04/2017**	**15/05/2017**																			
Alcances																					
Descubrimiento Infraestructura	27/04/2017	03/05/2017																			
Preparación ambiente	27/04/2017	29/04/2017																			
Ejecución de descubrimiento	29/04/2017	30/04/2017																			
Revisión	30/04/2017	30/04/2017																			
Documentación	30/04/2017	03/05/2017																			
Análisis de Vulnerabilidades	**29/04/2017**	**07/05/2017**																			
Preparación ambiente	29/04/2017	30/04/2017																			
Ejecución del escaneo	01/05/2017	03/05/2017																			
Análisis de resultados	03/05/2017	04/05/2017																			
Documentación	05/05/2017	07/05/2017																			
Pentesting	**29/04/2017**	**11/05/2017**																			
Preparación ambiente	29/04/2017	03/05/2017																			
Ejecución del escaneo	03/05/2017	06/05/2017																			
Análisis de resultados	07/05/2017	08/05/2017																			
Documentación	09/05/2017	11/05/2017																			
Perfil de Riesgos	**04/05/2017**	**13/05/2017**																			
Ponderación y definiciones	04/05/2017	06/05/2017																			
Entrevistas	07/05/2017	08/05/2017																			
Análisis y clasificación	09/05/2017	10/05/2017																			
Documentación	11/05/2017	13/05/2017																			
Recomendaciones	**13/05/2016**	**15/05/2017**																			
Evaluación	13/05/2017	15/05/2017																			
Documentación	14/05/2017	15/05/2017																			

Ilustración 2 Plan de proyecto para el análisis

Solo se podrá incluir observaciones del primer simulacro que el IEC tenga en sus instalaciones, dado que este se dará el día 14/Mayo/2017.

3.1 Excepciones

Todas las pruebas a ejecutarse pueden encontrar situaciones y/o condiciones bajo las cuales no sea posible efectuarse. Estas pruebas pudieran representar riesgo operativo de la organización o a las aplicaciones.

Cuando esto sea así, será notificado en el reporte de no poderse llevar acabo dichas pruebas así como la justificación de esto.

4 Esquema operativo

En el estado de Coahuila hay 38 municipios distribuyendo 38 distritos electorales que cuentan con casi 3,500 casillas donde votarán aproximadamente 2, 000,000 de votantes en el padrón.

El IEC cuenta con un centro de captura central ubicado en Saltillo el cual recibe de los distintos centros de acopio en el estado de Coahuila las actas que contabilizan los votos de las casillas que agrupa dicho centro de acopio.

Puede haber tres tipos de centros de acopio en todo el estado:

- El centro de acopio central que se encuentra en saltillo en donde llegan todas las actas digitalizadas y se capturan para alimentar la información de manera centralizada y pueda publicarse directamente o mediante replicadores (entidades, sitios-web o empresas que en línea replican la información del conteo preliminar) en el estado.
- El que cuenta con escáner digitalizadores donde se escanea el acta y se envía de forma digital hacia el centro de acopio central en Saltillo
- El que requiere que mediante teléfono celular con cámara se digitalice el acta para enviarse al centro de acopio en Saltillo

4.1 Centro de acopio Central

El centro de acopio central ubicado en Saltillo es donde reciben las actas validadas desde los sitios remotos desde donde son escaneadas y enviadas al sitio central para su contabilidad total.

Las actas son escaneadas en los centros de acopio remotos ya sea vía un escáner o por medio de un teléfono. Más detalle en las secciones 4.2 y 4.3. Los archivos digitales son enviados al centro de acopio central para su contabilidad

El centro de acopio central se compone de una operación de 40 personas con estaciones de trabajo para capturar los resultados enviados.

4.2 Centro de acopio con escáner digital

El centro de acopio con escáner digital se justifica dependiendo del número de casillas existentes en la cercanía. Esto dado el costo del escáner para hojas de doble carta.

En estos centros de acopio al terminar los conteos, las actas son escaneadas y enviadas al centro de acopio central. La arquitectura bajo la cual funciona un centro de estos utiliza un una conexión de ADSL la cual conecta un firewall en el sitio conectando en una red a los escáneres.

Los firewalls inician una conexión segura hacia los servidores en el centro de acopio central donde se cargan las actas digitalizadas para su integración y conteo.

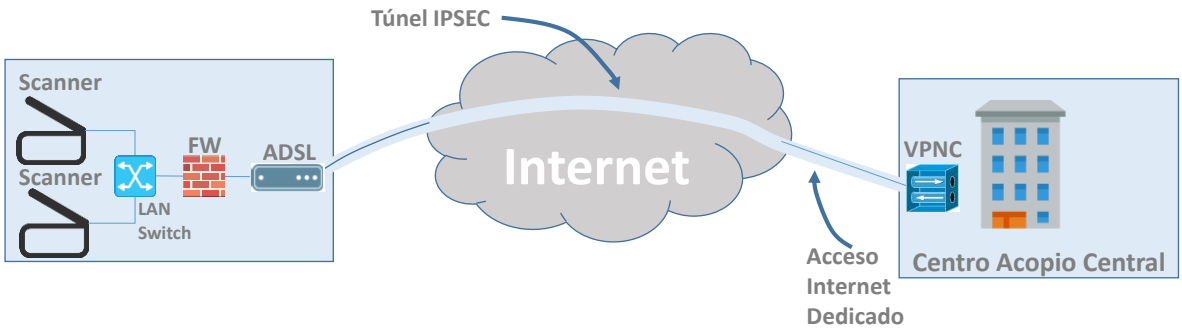

Ilustración 3 Conexión desde el Centro de Acopio con Escáner

4.3 Centro de acopio con teléfono celular

Los centros de acopio con teléfono celular son aquellos en donde debido a su concentración de casillas no justifica la adquisición de escáneres digitales. Para propósitos de digitalizar las actas se utiliza un teléfono celular, propiedad del IEC con doble chip con un armazón que permite ubicar el teléfono a distancia para tomar la foto del acta cubriendo la totalidad del documento.

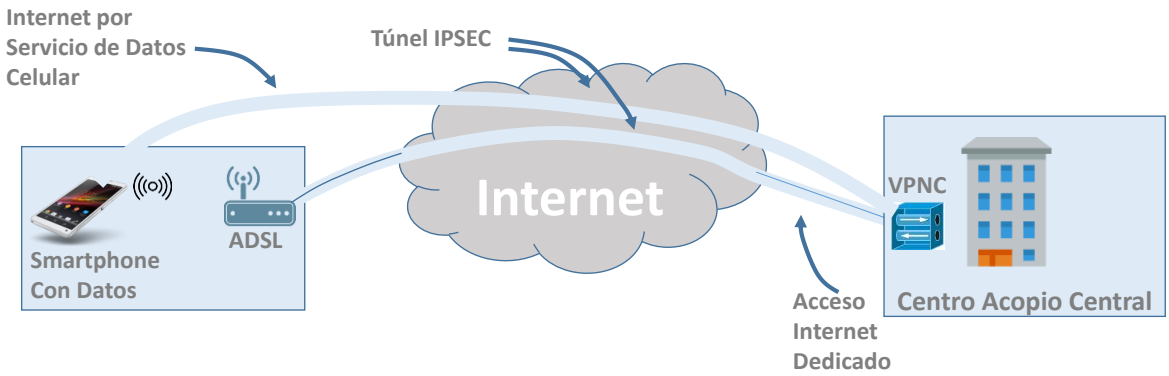

Ilustración 4 Conexión desde el Centro de Acopio con Celular

La aplicación en el teléfono permite aislar el fondo sobre el que se toma la foto para que esta solo incluya el acta.

La transmisión de la imagen digitalizada del centro se puede llevar acabo de dos maneras:

- Vía WiFi – Si en el centro hay facilidades de WiFi por medio de acceso de ADSL, entonces el teléfono usa el medio inalámbrico para gestionar un túnel de IPSEC y conectarse al servidor para transmitir la imagen.
- Vía Celular – Si en el centro no hay facilidades de WiFi, entonces la aplicación del teléfono utilizará los servicios de datos de cualquiera de los dos chips de celular en caso de que alguno de ellos no tenga cobertura.