Plan de Pruebas para la empresa QuantumMovil, S.A de C.V.

Hardware:

- 1 laptop con enchufe de red o usb a rj45
- 2 cables de red de 5 metros
- 1 cable cruzado
- 1 cable para consola
- escáner, etc.

Software:

- Netlog
- ISS (Internet Security Scanner)
- Wireshark
- Office
- Kali Linux con herramientas como nmap preinstaladas
- Licencia Adobe Acrobat para convertir a PDF
- Argus

Soporte:

- Datos 4G

Plan de Pruebas Funcionales

1. Técnicas de revisión

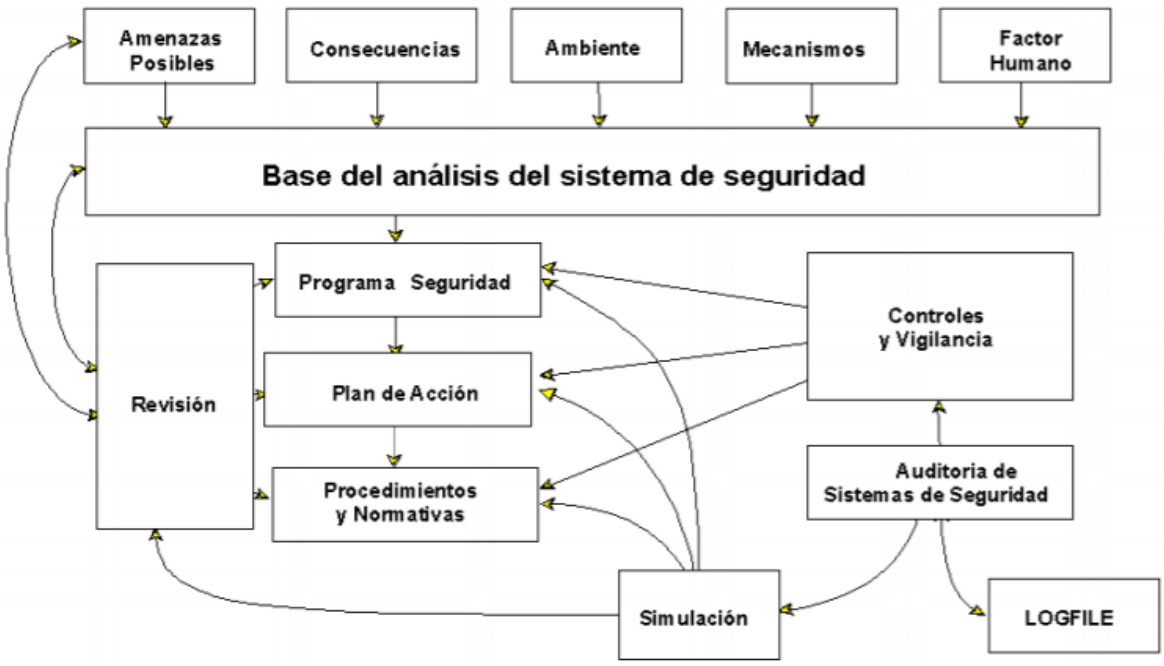
- Revisión de políticas, procedimientos y documentación
- Revisión de bitácoras
- Revisión de la configuración
- Análisis de la red (network sniffing)
- Revisión de la integridad de archivos (checksum)
- Identificación de objetivos de evaluación
- Descubrimiento de la red
- Identificación de puertos y servicios
- Escaneo de vulnerabilidades

- Escaneo en redes inalámbricas

2. Validación de vulnerabilidades

- Descifrado de contraseñas
- Prueba de intrusión
- Ingeniería Social

Plan de Pruebas de Seguridad



Speech de apertura

Con este speech de apertura, nuestro propósito es confirmar el acuerdo de todas las partes sobre el plan de auditoria que se realizará a la empresa antes mencionada, así como presentar al equipo auditor, que es conformado por Bernardo Aceves y Omar Ramos.

De igual forma, tenemos que asegurarnos de que se puedan realizar todas las actividades de auditoría planificadas; las cuales son mencionadas en el plan de auditoria.

Siéntanse libres de hacer cualquier pregunta o aclaración para dejar todo claro, ya que es de nuestra mayor intención el que la comunicación se dé de una manera satisfactoria. Para nosotros el grado de detalle es una prioridad, por lo que les pedimos que se explayen de ser necesario.

Informe de auditoría.

El trabajo presentado surge de la identificación de la logística como un factor crucial para las empresas. El objetivo fue el de realizar un seguimiento, evaluación y verificación de la gestión de logística y abastecimiento para asegurar que la empresa QuantumMovil, S.A de C.V. cumple con los requerimientos para acreditar o poder tener la certificación ISO 27001(Information technology — Security techniques — Guidelines for the assessment of information security controls).

Un punto que nos pareció importante del caso de estudio fue que el auditor entró sin saber el nombre completo del auditado, dando solo su apellido. En este punto nos hubiera gustado saber si al auditor le pidieron algún documento que corroborara su identidad o si solo con dar su nombre se le permitió el ingreso, ya que esto representaría un gran riesgo de seguridad.

Dentro de las instalaciones se observó que la recepción de la señal inalámbrica de la red no cumple con la cobertura adecuada de las instalaciones por lo que para resolver dicho problema dejan las puertas de las oficinas abiertas, lo que resulta en un riesgo de acceso no autorizado a dichas zonas, además de que no se cuenta con la ventilación adecuada lo que puede causar que los dispositivos electrónicos se sobrecalienten, ocasionando mal funcionamiento o fallas.

En cuanto a la administración de la red se encontró que se cuenta con bitácoras del tráfico de red lo que es bueno para el análisis de este, pero no se cuenta con un proceso de seguimiento de incidentes, perdiendo valiosa información recabada de las bitácoras. Los servidores se encuentran en sitio y se observó que el diagrama de red que se proporcionó ya no está actualizado de acuerdo a su infraestructura lo que requiere una verificación de dicho diagrama para su posterior actualización. Evitando de esta manera tener accesos indeseados a la red.

Por ultimo se detectó que no se cuenta con un procedimiento establecido para la actualización o instalación de software, ya que no han podido darle una actualizacion debido

Speech de cierre

De acuerdo con el resultado del proceso auditor, se evidencian las siguientes debilidades:

- Posible brecha de seguridad al ingresar al plantel.
- Falla de seguridad ya que las oficinas puedes ser accesadas por personas que no tienen permitido estar ahí, lo que conlleva al riesgo de pérdida de información.
- No se aplican sanciones a los infractores que utilizan los recursos de red para fines personales, por lo que no consideramos que ciertos empleados vayan a dejar de infringir.
- El diagrama de red no está actualizado, lo que puede suponer una configuración de red no adecuada que puede conllevar a puertos abiertos u otros posibles vectores de ataque.

Al incumplir los puntos 6.1 (Acciones para tratar los riesgos y oportunidades) y 6.1.3 (Tratamiento de los riesgos de seguridad de la información) consideramos que la empresa QuantumMovil, S.A de C.V. no puede ser acreedora del certificado iso 27001.

Tomada esta decisión, recomendamos a la empresa antes mencionada, tomar las medidas necesarias para cumplir cada uno de estos puntos y así conseguir la certificación, ya que de otra forma su negocio puede verse gravemente afectado.