LA AUDITORIA EN LA PRÁCTICA

AUTOR: JAVIER CHINCHILLA MORALES

NOVIEMBRE: 2020

San Marcos

INTRODUCCIÓN

- Una vez terminado el plan de auditoria es importante saber como se debe llevar a cabo y cuales son los pasos a la hora de ponerlo en pracica, esto por que se debe hacer una planeación con todo el equipo de trabajo ya que no es solo de iniciar las obras y hacer por hacer sino debe de coordinarse y asignarse con cada miembro del equipo sus funciones, alcances, responsabilidades y limitaciones.

La auditoría en la práctica

El auditor externo o interno revisa que cada uno de los diferentes controles implantados siempre funcionen como se espera que funcionen y, sobre todo, que cumplan con las normas internas y externas, de acuerdo con el nivel de riesgo detectado y conforme a los objetivos de seguridad dictados por la dirección general y el director de sistemas o área de informática de la organización, El auditor externo o interno revisa que cada uno de los diferentes controles implantados siempre funcionen como se espera que funcionen y, sobre todo, que cumplan con las normas internas y externas, de acuerdo con el nivel de riesgo detectado y conforme a los objetivos de seguridad dictados por la dirección general y el director de sistemas o área de informática de la organización.

Modelo de Bell-Lapadula

Creado por William Elliot Bell y Len Lapadula para el ejército de Estados Unidos de América, el modelo divide el permiso de acceso de los usuarios de la información con base en etiquetas de seguridad que tienen cuatro categorías: no clasificado, confidencial, secreto y top secret (ultra secreto). Como se observa, el modelo hace énfasis en la confidencialidad más que en la integridad, definiendo los estados seguro e inseguro. Si un estado es seguro, la única forma de que una persona tenga acceso a cierta información es si la forma de acceso está en concordancia con la política de seguridad, lo cual se comprueba comparando los papeles de acreditación que tiene la persona que solicita acceso con la clasificación que tiene la información.

El modelo define dos reglas: control de acceso requeridas por ley (MAC, por sus siglas en inglés; Mandatory Access Control) y una regla de control de acceso discrecional (DAC, por sus siglas en inglés; Discretionary Access Control), cada una con tres propiedades:

1. Propiedad de seguridad simple. Se refiere a que una persona de determinado nivel de seguridad no puede tener acceso a consultar información de un nivel superior al suyo.
2. Propiedad de restricción. Se refiere a que una persona de determinado nivel de seguridad está restringida para escribir un documento que pertenece a un nivel de seguridad más bajo.
3. Propiedad discrecional. Se refiere a que una persona puede crear contenido sólo en su nivel de acceso o superior, pero para consultar información, sólo puede hacerlo para su nivel o un nivel inferior.

Modelo de Brewer-Nash

Desarrollado en 1989 por David Brewer y Michael Nash, también conocido como modelo de la Muralla china. El enfoque de este modelo fue concebi do para proponer controles que minimicen los conflictos de intereses en organizaciones comerciales, construido sobre un modelo de flujo de información. Se le llama modelo de la Muralla china porque crea una barrera lógica entre el usuario y la información a la cual no tiene acceso, y aunque dos usuarios tengan el mismo nivel de acceso, no necesariamente podrán consultar la misma información. El modelo hace énfasis en la confidencialidad, porque los datos que se manejan no pueden leerse por solicitantes distintos a los interesados, pero si esto llegara a ocurrir, el modelo garantiza que la información obtenida por los solicitantes no pueda ser difundida en otros medios de comunicación.

Este modelo es muy utilizado entre consultores comerciales, quienes tienen acceso a datos confidenciales de las empresas a las cuales asesoran; sin embargo, no podrían utilizar estos datos para beneficio de otra

empresa, (lo cual crearía un conflicto de intereses) aplicando de manera adecuada la política de este modelo, con lo que se garantiza la confidencialidad de los datos.

En general, existe una clasificación jerárquica de datos del negocio en todos los modelos de seguridad reconocidos, en la que suelen considerarse tres niveles:

- Nivel inferior. Formada por partes individuales de información, cada una de las cuales sólo pertenece a una empresa. A este tipo de información se le considera como un objeto.
- Nivel intermedio. Todos los objetos pertenecientes a la misma empresa se agrupan y se les denomina datos de la empresa.
- Nivel superior. Todos los datos de las empresas que están en competencia se agrupan en las llamadas clases de conflictos de interés.

La política de seguridad se establece con base en los objetos relacionados con el conjunto de datos de la empresa y el nombre de la clase de conflicto de interés al cual pertenece. Luego, se establecen las reglas de acceso a la información, las cuales se explican a continuación.

- Cuando una persona haya accedido a un objeto en particular, sólo podrá accesar a otros objetos que se encuentren dentro del mismo conjunto de datos de la empresa o que se hallen en un conflicto de intereses diferente.
- Una persona sólo puede tener acceso a un conjunto de datos de empresas por cada clase de conflicto de intereses.

Modelo HRU

Llamado así en honor de sus creadores, de quienes se toma la primera inicial de su nombre, Harrison, Ruzzo y Ullman. Es un modelo de seguridad en una computadora, a nivel del sistema operativo, enfocado a la integridad de los derechos de acceso en el sistema. Se considera una extensión del modelo Graham-Denning, que se basa en la idea de un conjunto finito de procedimientos que están disponibles para editar los derechos de acceso de una persona sobre un objeto; en general el objeto es determinada información. Es uno de los pocos modelos que se basa en un algoritmo para determinar derechos de acceso a la información.

El modelo define un sistema de protección que consta de un conjunto de derechos genéricos y de un conjunto de comandos u órdenes, los cuales se forman con operaciones básicas y tienen una lista de precondiciones que requieren ciertos derechos que se presentan por pares persona-objeto. Los requisitos originales pueden modificar la matriz de acceso agregando o suprimiendo derechos de acceso para cada par persona-objeto. La creación de nuevos pares persona-objeto requiere que ambos no tengan un registro previo en la configuración que está activa, en tanto que para suprimir un derecho, se necesita que la persona y el objeto tengan un registro previo en la configuración active (ver página 318-325 del libro de lectura)

CONCLUSIONES y RECOMENDACIONES

En la práctica los auditores deben de realizar una planeación de como llevar a cabo lo planeado para la empresa donde van a aplicar la revision de todos los diferentes controles con el fin de detector anomalias en su funcionamiento, y una vez que se hallan trabajado todos los procesos involucrados es importante que los auditores recaben las pruebas necesarias de la incidencia detectada, y al final se debe generar un informe final, el cual debe ser presentado y discutido con los encargados a nivel de jefarutas de TI y gerencia.

REFERENCIAS BIBLIOGRÁFICAS

- Baca, G. (2016). *Introducción a la Seguridad informática* (1a. ed.). Grupo editorial Patria.

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica