Anexo 2 – Unidad 1

Niveles de Seguridad Informatica

El estándar más utilizado es el TCSEC. Los niveles describen diferentes tipos de seguridad del S.O. Estos niveles fueron la base de las ISO/IEC.

Nivel D: Contiene solo la división y esta reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad.

Nivel C1 - Protección Discrecional: Requiere identificación de usuarios que permite el acceso a distinta información. Hace distinción de roles y cada uno maneja su propia información. Debe cumplir dos requerimientos:

- Acceso de Control Discrecional: Distinción de usuarios y recursos.
- Identificación y Autenticación.

Nivel C2 – Protección de Acceso Controlado: Mayor cantidad de restricciones que C1. Capacidad de restringir que los usuarios ejecuten y/o tengan acceso a ciertas funciones del S.O. Requiere auditoria, la cual lleva registro de todas las actividades relacionadas con la seguridad.

Nivel B1 – Seguridad Etiquetada: Soporta seguridad multinivel. El dueño del archivo no puede modificar los permisos de un objeto que esta bajo control de acceso obligatorio. A dicho objeto se le asigna una etiqueta y cada usuario deberá posee el permiso expreso para poder acceder al mismo y/o viceversa.

Nivel B2 – Protección Estructurada: Existe una estructura de objeto en la cual el objeto de nivel superior debe estar etiquetado por ser el padre del objeto inferior. Si no se accede al padre, no se puede acceder al hijo.
El sistema es capaz de alertar a los usuarios si sus condiciones de seguridad y accesibilidad son modificadas.

Nivel B3 – Dominios de Seguridad: Refuerza los dominios con la instalación de hardware. Por medio de un monitor de referencia, se reciben las peticiones de acceso de cada usuario y las permite o deniega según las políticas de acceso definidas. Requiere que la terminal del usuario este conectada mediante una conexión segura.

Nivel A – Protección Verificada: Nivel de seguridad mas alto. Incluye un proceso de diseño, control y verificación, mediante métodos matemáticos para asegurar todos los procesos que realiza un usuario sobre el sistema. El software y hardware se encuentran protegidos para evitar infiltraciones ante traslados o movimientos de equipos.