14-9-2015

[nombre de la empresa]

[Título del documento]

[Subtítulo del documento]

**1.4.2.- CONTABILIDAD**

Se encarga del conteo del tiempo de conexión y terminación, número de mensajes transmitidos y recibidos, nombre del punto de acceso al servicio, razón por la que terminó la conexión y el control de Inventarios.   
  
Este servicio provee datos concernientes al cargo por uso de la red. Entre los datos proporcionados están los siguientes:

* Número de mensajes transmitidos y recibidos.
* Tiempo de conexión y terminación.
* Nombre del punto de acceso al servicio.
* Razón por la que terminó la conexión.

 Se encarga también de las mediciones, control de costes y facturación de los clientes.

La estadística de red es de gran importancia, ya que esta permite el manejo de la contabilidad, la resolución de problemas, la realización de pronósticos a largo plazo, la planificación de la capacidad entre otras.

Ejemplo:

* Las facilidades de comunicación: LAN, WAN, líneas modem, PBX
* Hardware: Servidores, estaciones de trabajo
* Software: Aplicaciones Instaladas

Un PBX o PABX (siglas en inglés de Private Branch Exchange y Private Automatic Branch Exchange para PABX) cuya traducción al español sería Ramal privado de conmutación automática, o más bien Central Secundaria Privada Automática; es en realidad cualquier central telefónica conectada directamente a la red pública de telefonía por medio de líneas troncales para gestionar además de las llamadas internas, las entrantes y salientes con autonomía sobre cualquier otra central telefónica. Este dispositivo generalmente pertenece a la empresa que lo tiene instalado y no a la compañía telefónica, de aquí el adjetivo Privado a su denominación.

**1.4.3.- SEGURIDAD**

Se encarga de controlar el acceso de los clientes a la red de datos y a los recursos.

La estructura administrativa de la red debe tener mecanismos de seguridad buenos para lo siguiente: Identificación y autentificación del usuario, una clave de acceso y un password, autorización de acceso a los recursos, es decir, solo personal autorizado, Confidencialidad, entre otros.

Tiene como objetivo controlar el acceso a los recursos de la red de acuerdo a lo establecido localmente de modo que la red no pueda ser saboteada y que no pueda accederse a información importante sin la debida autorización. Estos sistemas trabajan subdividiendo los recursos de la red en áreas autorizadas y áreas no autorizadas.

Generalmente involucra los siguientes pasos:

* Identificación de la información a proteger y dónde se encuentra.
* Identificación de los puntos de acceso a la información.
* Protección de los puntos de acceso.
* Mantenimiento de los puntos de acceso protegidos.

Los tipos de amenaza que se pueden dar son:

Internas: Usuarios que conocen la red, que estas son más serias que las externas ya que pueden lograr robar información personal y utilizarlas para perjudicar al prójimo.

Externas: Se originan fuera de la red y son más fáciles de prevenir por el administrador como son los virus.

Una de las técnicas que se pueden realizar para asegurar nuestro sistema es en restringir el acceso a los programas y archivos, asegurar que los operadores pueden trabajar pero que no puedan modificar los programas ni los archivos que correspondan y más que nada cerciorarse que se utilicen los datos, archivos y programas correctos, también hay que asegurarse que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.