TEORIA DE COMPONENTES PARA SISTEMAS DE MONITOREO

Durante el diseño de un sistema de monitoreo resultan esenciales componentes tales como: sensores, unidades terminales remotas, sistemas de transmisión y el software de recepción de señales de campo; adicionalmente encontramos que podemos desear obtener un sistema óptimo que permita el manejo de la información procesada en campo tiempo atrás, para lo cual es indispensable la creación de una base de datos con sus interfaces de manejo y administración, por otra parte, puede ser de gran utilidad para la comunidad la visualización de toda o parte de la información mediante Internet, para lo cual se requerirá la configuración de un servidor WEB y la generación de script´s que faciliten una navegación dinámica por parte del usuario en Internet.

Por lo tanto, es de gran importancia el manejo de la teoría referente a estos componentes; el presente anexo a sido orientado a esa parte, aquí usted encontrará la teoría básica de los componentes de un sistemas de monitoreo.

1. Sensores y Acondicionadores de señal

En todo proceso de automatización es necesario captar las magnitudes del medio, para poder así saber el estado del proceso que estamos observando. Para ello empleamos los sensores y transductores. En general, la estructura de un transductor completo se compone de lo siguiente:

- Elemento sensor o captador elemental.
  Convierte las variaciones de una magnitud física en variaciones de una magnitud eléctrica (señal).

- Acondicionamiento de la señal.
  Si existe, realiza la función de modificar la señal entregada por el sensor para obtener una señal adecuada (amplificación, linealización, etc.).

Un transductor es, en general, un dispositivo que convierte una señal de una forma física en una señal correspondiente pero de otra forma física distinta. Es decir, convierte un tipo de energía en otro. En la transducción siempre se extrae una cierta energía del sistema donde se mide, por lo que es importante garantizar que esto no lo perturba.

Dado que hay seis tipos de señales: mecánicas, térmicas, magnéticas, eléctricas, ópticas y moleculares (químicas), cualquier dispositivo que convierta una señal de un tipo en una señal de otro tipo debería considerarse un transductor, y la señal de salida podría ser de cualquier forma física "útil".

En la práctica, generalmente los transductores ofrecen una señal de salida eléctrica, debido al interés de este tipo de señales en la mayoría de procesos de medida. Los sistemas de medida electrónicos ofrecen, entre otras, las siguientes ventajas:

- Debido a la estructura electrónica de la materia, cualquier variación de un parámetro no eléctrico de un material viene acompañada por la variación de un parámetro eléctrico. Eligiendo el material adecuado, esto permite realizar transductores con salida eléctrica para cualquier magnitud física no eléctrica.
- Dado que en el proceso de medida no conviene extraer energía del sistema donde se mide, lo mejor es amplificar la señal de salida del transductor. Con amplificadores electrónicos se pueden obtener fácilmente ganancias de potencia de 10^{10} en una sola etapa, a baja frecuencia.
- Además de la amplificación, hay una gran variedad de recursos, en forma de circuitos integrados, para acondicionar o modificar las señales eléctricas. Incluso hay

transductores que incorporan físicamente en un mismo encapsulado parte de estos recursos.

- Existen también numerosos recursos para presentar o registrar información si se hace electrónicamente, pudiéndose manejar no sólo datos numéricos, sino también textos, gráficos y diagramas.
- La transmisión de señales eléctricas es más versátil que la de señales mecánicas, hidráulicas o neumáticas, y si bien no hay que olvidar que éstas pueden ser más convenientes en determinadas circunstancias.

Un sensor es un dispositivo que, a partir de la energía del medio donde se mide, da una señal de salida transducible que es función de la variable medida. Sensor y transductor se emplean a veces como sinónimos, pero sensor sugiere un significado más extenso: la ampliación de los sentidos para adquirir un conocimiento de cantidades físicas que, por su naturaleza o tamaño, no pueden ser percibidas directamente por los sentidos. Por otro lado, transductor sugiere que la señal de entrada y la de salida no deben ser homogéneas. Para el caso en que lo fueran se propuso el término "modificador", pero no ha encontrado aceptación.

La distinción entre transductor de entrada (señal física/señal eléctrica) y transductor de salida (señal eléctrica/presentación) está prácticamente en desuso. La tendencia actual, particularmente en robótica, es emplear el término sensor (o captador en bibliografía francesa) para designar el transductor de entrada, y el término actuador o accionamiento para designar el transductor de salida. Los primeros pretenden la obtención de información, mientras que los segundos buscan la conversión de energía.

A partir de ahora, se usará el término sensor para hacer referencia a los transductores de entrada. A veces, sobre todo en el caso de la medida de magnitudes mecánicas, puede existir un elemento llamado sensor primario, que convierte la variable de medida en una señal de medida, siendo el sensor electrónico quien la convierte en una señal eléctrica. Un

método para medir una diferencia de presiones, por ejemplo, consiste en emplear un diafragma cuya deformación se mide mediante una galga extensométrica. En este caso el diafragma es el sensor primario y la galga hace la transducción. No obstante, se denomina sensor al conjunto de ambos elementos junto con su encapsulado y sus conexiones.

1.1. Tipos de sensores

El número de sensores disponibles para las distintas magnitudes físicas es tan elevado que no se puede proceder racionalmente a su estudio sin clasificarlos previamente de acuerdo con algún criterio. Existen diversos criterios adicionales a los que se expondrán aquí.

En el cuadro 1.1 se recogen varios criterios de clasificación y se dan ejemplos de sensores de cada clase. Cualquiera de estas clasificaciones es exhaustiva, y cada una tiene interés particular para diferentes situaciones de medida.

Clasificación atendiendo al aporte de energía.

Según el aporte de energía, los sensores se pueden dividir en moduladores y generadores. En los sensores moduladores o activos, la energía de la señal de salida procede, en su mayor parte, de una fuente de energía auxiliar. La entrada sólo controla la salida. En los sensores generadores o pasivos, en cambio, la energía de salida es suministrada por la entrada.

Los sensores moduladores requieren en general más hilos que los generadores, ya que la energía de alimentación suele suministrarse mediante hilos distintos a los empleados para la señal. Además, esta presencia de energía auxiliar puede crear un peligro de explosiones en algunos ambientes. Por contra, su sensibilidad se puede modificar a través de la señal de alimentación, lo que no permiten los sensores generadores.

La designación de activos y pasivos es empleada con significado opuesto al aquí dado, en algunos textos.

Criterio	Clases	Ejemplos
Aporte de energía	Moduladores	Termistor
	Generadores	Termopar
Señal de salida	Analógicos	Potenciómetro
	Digitales	Codificador de posición
	Todo o nada	Célula fotoeléctrica
Modo de operación	De deflexión	Acelerómetro de deflexión
	De comparación	Servoacelerómetro
Magnitud física a medir	Posición lineal o angular	Resolvers
	Desplazamiento o deformación	Condensador diferencial
	Velocidad lineal o angular	Tacogenerador, encoders
	Aceleración	Galga + masa resorte
	Fuerza y par	Galga extensiométrica
	Presión	Tubo Bourdon + Potenciómetro
	Caudal	Anemómetro
	Temperatura	Resistencias NTC, PTC
	Presencia o proximidad	Ultrasonidos
	Táctiles	Matriz de contactos
	Intensidad lumínica	Fotodiodo, fototransistor
	Sistemas de visión artificial	Cámaras CCD
Parámetro variable	Resistivos	Galga
	Capacitivos	Dieléctrico variable
	Inductivos y electromagnéticos	LVT
	Generadores	Piroeléctricos
	Digitales	Vórtices
	Uniones p-n	Fotoeléctricos
	Ultrasonidos	Efecto Doppler

Cuadro 1.1 Clasificaciones de los sensores

Clasificación según la señal de salida.

Según la señal de salida, los sensores se clasifican en analógicos, digitales y todo-nada. En los analógicos la salida varía, a nivel macroscópico, de forma continua. La información está en la amplitud, si bien se suelen incluir en este grupo los sensores con salida en el dominio temporal. Si es en forma de frecuencia, se denominan, a veces, "casidigitales", por la facilidad con que se puede convertir en una salida digital.

En los sensores digitales, la salida varía en forma de saltos o pasos discretos. No requieren conversión A/D y la transmisión de su salida es más fácil. Tienen también mayor fidelidad y mayor fiabilidad, y muchas veces mayor exactitud, pero lamentablemente no hay modelos digitales para muchas de las magnitudes físicas de mayor interés. Los sensores todo-nada son aquellos que únicamente poseen dos estados, los cuales están separados por un valor umbral de la variable detectada.

Clasificación atendiendo al modo de funcionamiento.

Atendiendo al modo de funcionamiento, los sensores pueden ser de deflexión o de comparación. En los sensores que funcionan por deflexión, la magnitud medida produce algún efecto físico, que engendra algún efecto similar, pero opuesto, en alguna parte del instrumento, y que está relacionado con alguna variable útil. Un dinamómetro para la medida de fuerzas es un sensor de este tipo, en el que la fuerza aplicada deforma un muelle hasta que la fuerza de recuperación de éste, proporcional a su longitud, iguala la fuerza aplicada.

En los sensores que funcionan por comparación, se intenta mantener nula la deflexión mediante la aplicación de un efecto bien conocido, opuesto al generado por la magnitud a medir. Hay un detector del desequilibrio y un medio para restablecerlo. En una balanza

manual, por ejemplo, la colocación de una masa en un platillo provoca un desequilibrio, indicado por una aguja sobre una escala. El operario coloca entonces una o varias masas en el otro platillo hasta alcanzar el equilibrio, que se juzga por la posición de la aguja.
Las medidas por comparación suelen ser más exactas porque el efecto conocido opuesto se puede calibrar con un patrón o magnitud de referencia de calidad.

El detector de desequilibrio sólo mide alrededor de cero y, por lo tanto, puede ser muy sensible y no necesita estar calibrado. Por contra, tienen en principio menor respuesta dinámica y, si bien se pueden automatizar mediante un servomecanismo, no se logra normalmente una respuesta tan rápida como en los de deflexión.

Clasificación según el tipo de relación E/S

Según el tipo de relación entrada-salida, los sensores pueden ser de orden cero, de primer orden, de segundo orden o de orden superior. El orden está relacionado con el número de elementos almacenadores de energía independientes que incluye el sensor, y repercute en su exactitud y velocidad de respuesta. Esta clasificación es de gran importancia cuando el sensor forma parte de un sistema de control en lazo cerrado.

Clasificación atendiendo al parámetro variable

Para el estudio de un gran número de sensores se suele acudir a su clasificación de acuerdo con la magnitud medida. Se habla, en consecuencia, de sensores de temperatura, presión, caudal, humedad, posición, velocidad, aceleración, fuerza, par, etc. Sin embargo, esta clasificación difícilmente puede ser exhaustiva ya que la cantidad de magnitudes que se pueden medir es prácticamente inagotable. Piénsese, por ejemplo, en la variedad de

contaminantes químicos en el aire o en el agua, o en la cantidad de proteínas diferentes que hay en el cuerpo humano y que interesa detectar.

Desde el punto de vista de la ingeniería electrónica, es más atractiva la clasificación de los sensores de acuerdo con el parámetro variable: resistencia, capacidad, inductancia, añadiendo luego los sensores generadores de tensión, carga o corriente, y otros tipos no incluidos en los anteriores grupos. Si bien este tipo de clasificación es poco frecuente, permite reducir el número de grupos a unos pocos y se presta bien al estudio de los acondicionadores de señal asociados. En el cuadro 1.2 se recogen los sensores y métodos de detección ordinarios para las magnitudes más frecuentes.

	Magnitudes								
Sensores	Posición Distancia Desplazamiento	Velocidad	Aceleración Vibración	Temperatura	Presión	Caudal Flujo	Nivel	Fuerza	Humedad
Resistivos	Potenciómetros Galgas Magnetoresistencias		Galgas + masa-resorte	RTD Termistores	Potencióme-Tros + tubo Bourdon	Anemómetros de hilo caliente Galgas + Voladizo Termistores	Potenciómetr o + flotador	Galgas	Humistor
Capacitivos	Condensador Diferencial				Condensado r variable + diafragma		Condensado r Variable	Galgas capacitivas	Dieléctrico variable
Inductivos y Electro-Magnéticos	LVDT Corrientes Foucault Resolver Efecto Hall	Ley Faraday LVT Efecto Hall Corrientes Foucault	LVDT + masa-resorte		LVDT + diafragma Reluctancia variable + diafragma	LVDT + rotá-Metro Ley Faraday	LVDT + flo-Tador Corrientes Foucault	Magneto-elástico LVDT + célula carga	
Generadores			Piezoeléc-tricos + masa resorte	Termopares Piroeléc-Tricos	Piezoeléc-Tricos			Piezoeléc-tricos	
Digitales	Codificadores in-Crementales y Absolutos	Codificado-res incre-mentales		Osciladores De cuarzo	Codificador + tubo Bourdon	Vórtices			SAW
Uniones p-n	Fotoeléctricos			Diodo Transistor Convertido-Res T/I			Fotoeléctri-Cos		
Ultrasonidos	Reflexión	Efecto Doppler				Efecto Doppler Tiempo trán-Sito Vórtices	Reflexión Absorción		

Cuadro 1.2. Sensores y métodos de detección ordinarios para las magnitudes más frecuentes

1.2. Exactitud, fidelidad y sensibilidad

La exactitud (en inglés, "accuracy") es la cualidad que caracteriza la capacidad de un instrumento de medida de dar indicaciones que se aproximen al verdadero valor de la magnitud medida. En castellano se emplea como sinónimo de exactitud el término precisión, pero en inglés americano "accuracy" y "precisión" no siempre se emplean como sinónimos.

El valor "exacto", "verdadero" o "ideal", es el que se obtendría si la magnitud se midiera con un método "ejemplar". Se considera como tal aquel método de medida en el que los expertos coinciden que es suficientemente exacto para la finalidad pretendida con los resultados que se obtengan.

La exactitud de un sensor se determina mediante la denominada calibración estática. Consiste ésta en mantener todas las entradas excepto una a un valor constante. La entrada en estudio se varía entonces lentamente, tomando sucesivamente valores "constantes" dentro del margen de medida, y se van anotando los valores que toma la salida. La representación de estos valores en función de los de la entrada define la curva de calibración. Para poder conocer el valor de la magnitud de entrada, ésta debe tener un valor bien conocido, constituyendo lo que se denomina un "patrón" de referencia. Su valor debe conocerse con una exactitud al menos diez veces mayor que la del sensor que se calibra.

La discrepancia entre la indicación del instrumento y el verdadero valor de la magnitud medida se denomina "error". La diferencia entre la indicación del instrumento y el verdadero valor se denomina error absoluto. A veces se da como porcentaje respecto al máximo valor que puede medir el instrumento (valor de fondo de escala) o con respecto a la diferencia entre el valor máximo y el valor mínimo medibles. Así pues,

$$Error\ absoluto = Resultado - Verdadero\ valor$$

Sin embargo, lo más común es especificar el error como cociente entre el error absoluto y el verdadero valor de la magnitud medida, cociente que se denomina error relativo. Éste suele tener dos términos: uno dado como porcentaje (tanto por ciento) de la lectura, y otro constante, que puede estar especificado como porcentaje del fondo de escala o un umbral, o un número de "cuentas" en el caso de instrumentos digitales,

$$Error\ relativo = \frac{Error\ absoluto}{Verdaderovalor}$$

Para algunos sensores puede que se especifique un error relativo como porcentaje del fondo de escala, sin más, o bien como porcentaje de la lectura exclusivamente. Si el margen de medida incluye valores pequeños, lo primero implica que en dicha zona del margen se tendrá un error muy grande, mientras que lo segundo da lugar a errores increíblemente pequeños.

La fidelidad (en inglés americano designada a veces como "precisión") es la cualidad que caracteriza la capacidad de un instrumento de medida de dar el mismo valor de la magnitud medida, al medir varias veces en unas mismas condiciones determinadas (ambientales, operador, etc.), prescindiendo de su concordancia o discrepancia con el valor real de dicha magnitud. La fidelidad implica que se tenga simultáneamente una conformidad en las sucesivas lecturas y un número alto de cifras significativas y es, por tanto, una condición necesaria pero no suficiente para la exactitud.

La sensibilidad o factor de escala es la pendiente de la curva de calibración, que puede ser o no constante a lo largo de la escala de medida. Para un sensor cuya salida esté relacionada con la entrada *x* mediante la ecuación *y = f(x)*, la sensibilidad en el punto x_a , $S(x_a)$, es

$$S(X_a) = \left.\frac{dy}{dx}\right|_{x=x_a}$$

En los sensores interesa tener una sensibilidad alta y, si es posible, constante. Para un sensor con respuesta

$$y = kx + b$$

la sensibilidad es $S = k$, para todo el margen de valores de *x* aplicables. Para uno cuya respuesta sea

$$y = kx^2 + b$$

la sensibilidad es $S = 2\,kx$, y varía a lo largo de todo el margen de medida.

2. SCADA (Control y adquisición de datos de supervisión)

SCADA es un acrónimo por Supervisory Control And Data Adquisition (control y adquisición de datos de supervisión). Los sistemas SCADA utilizan la computadora y tecnologías de comunicación para automatizar el monitoreo y control de procesos industriales. Estos sistemas son partes integrales de la mayoría de los ambientes industriales complejos o muy geográficamente dispersos ya que pueden recoger la información de una gran cantidad de fuentes muy rápidamente, y la presentan a un operador en una forma amigable. Los sistemas SCADA mejoran la eficacia del proceso de monitoreo y control proporcionando la información oportuna para poder tomar decisiones operacionales apropiadas.

Los primeros SCADA eran simplemente sistemas de telemetría que proporcionaban reportes periódicos de las condiciones de campo vigilando las señales que representaban medidas y/o condiciones de estado en ubicaciones de campo remotas. Estos sistemas ofrecían capacidades muy simples de monitoreo y control, sin proveer funciones de aplicación alguna. La visión del operador en el proceso estaba basada en los contadores y las lámparas detrás de paneles llenos de indicadores. Mientras la tecnología se desarrollaba, los ordenadores asumieron el papel de manejar la recolección de datos, disponiendo comandos de control, y una nueva función - presentación de la información sobre una pantalla de CRT. Los ordenadores agregaron la capacidad de programar el sistema para realizar funciones de control más complejas.

Los primeros sistemas automatizados SCADA fueron altamente modificados con programas de aplicación específicos para atender a requisitos de algún proyecto particular. Como ingenieros de varias industrias asistieron al diseño de estos sistemas, su percepción de SCADA adquirió las características de su propia industria. Proveedores de sistemas de software SCADA, deseando reutilizar su trabajo previo sobre los nuevos proyectos,

perpetuaron esta imagen de industria-específicos por su propia visión de los ambientes de control con los cuales tenían experiencia. Solamente cuando nuevos proyectos requirieron funciones y aplicaciones adicionales, hizo que los desarrolladores de sistemas SCADA tuvieran la oportunidad de desarrollar experiencia en otras industrias.

Hoy, los proveedores de SCADA están diseñando sistemas que son pensados para resolver las necesidades de muchas industrias con módulos de software industria-específicos disponibles para proporcionar las capacidades requeridas comúnmente. No es inusual encontrar software SCADA comercialmente disponible adaptado para procesamiento de papel y celulosa, industrias de aceite y gas, hidroeléctricas, gerenciamiento y provisión de agua, control de fluidos, etc. Puesto que los proveedores de SCADA aún tienen tendencia en favor de algunas industria sobre otras, los compradores de estos sistemas a menudo dependen del proveedor para una comprensiva solución a su requisito, y generalmente procurar seleccionar un vendedor que pueda ofrecer una completa solución con un producto estándar que esté apuntado hacia las necesidades específicas del usuario final.

La mayoría de los sistemas SCADA que son instalados hoy se está convirtiendo en una parte integral de la estructura de gerenciamiento de la información corporativa. Estos sistemas ya no son vistos por la gerencia simplemente como herramientas operacionales, sino como un recurso importante de información. En este papel continúan sirviendo como centro de responsabilidad operacional, pero también proporcionan datos a los sistemas y usuarios fuera del ambiente del centro de control que dependen de la información oportuna en la cual basan sus decisiones económicas cotidianas. La mayoría de los vendedores principales de SCADA han reconocido esta tendencia, y están desarrollando rápidamente métodos eficientes para hacer disponibles los datos, mientras protegen la seguridad y funcionamiento del sistema SCADA. La arquitectura de los sistemas de hoy integra a menudo muchos ambientes de control diferentes, tales como tuberías de gas y aceite, en un solo centro de control.

Para alcanzar un nivel aceptable de tolerancia de fallas con estos sistemas, es común tener ordenadores SCADA redundantes operando en paralelo en el centro primario del control, y un sistema de reserva del mismo situado en un área geográficamente distante. Esta arquitectura proporciona la transferencia automática de la responsabilidad del control de cualquier ordenador que pueda llegar a ser inasequible por cualquier razón, a una computadora de reserva en línea, sin interrupción significativa de las operaciones.

Supongamos tener un circuito eléctrico simple que consiste en un interruptor y una luz. Similar a este:

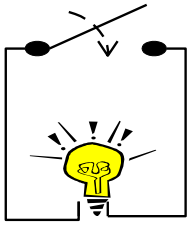

Figura No.1 Circuito simple

Este circuito permite que un operador mire la luz y sepa si el interruptor está abierto o cerrado. El interruptor puede indicar que un motor está trabajando o parado, o si una puerta está abierta o cerrada, o aún si ha habido un incidente o el equipo está trabajando.

Hasta ahora no hay nada especial sobre esto. Pero ahora imagínese que el interruptor y la lámpara están separados 100 kilómetros. Obviamente no podríamos tener un circuito eléctrico tan grande, y ahora será un problema que involucrará equipamiento de comunicaciones.

Ahora complique un poco más el problema. Imagínese que tengamos 2000 de tales circuitos. No podríamos producir 2000 circuitos de comunicación. Sin embargo alguien encontró que podríamos utilizar un solo circuito de comunicación compartiéndolo. Primero enviamos el estado (abierto | cerrado o 0/1) del primer circuito. Luego enviamos el estado

del segundo circuito, etcétera. Necesitamos entonces, indicar a qué circuito se aplica el estado cuando enviamos los datos.

El operador en el otro extremo todavía tiene un problema: tiene que monitorear los 2000 circuitos. Para simplificar su tarea podríamos utilizar una computadora. La computadora vigilaría todos los circuitos, y le diría al operador cuándo necesita prestarle atención a un circuito determinado. La computadora será informada cuál es el estado normal del circuito y cuál es un estado de "alarma" de esta manera ella vigila todos los circuitos, e informa al operador cuando cualquier circuito entra en alarma.

Algunos circuitos pueden contener datos "analógicos", por ejemplo, un número que representa el nivel de agua en un tanque. En estos casos la computadora será informada de los valores de niveles máximo y mínimo que deban ser considerados normales. Cuando el valor cae fuera de este rango, la computadora considerará esto como una alarma, y el operador será informado.

Podríamos también utilizar la computadora para presentar la información de una manera gráfica (un cuadro vale mil palabras). Podría mostrar una válvula en color rojo cuando está cerrada, o verde cuando está abierta, etcétera.

Un sistema SCADA real es aún más complejo. Hay más de un sitio a supervisar, algunos tienen de 30.000 a 50.000 "puntos" que normalmente proporcionan tanto información "analógica" como digital o de estado (por ejemplo, números tales como el nivel del líquido en un tanque). Pueden enviar un valor de estado (por ejemplo, encender una bomba) ó recibir un valor de estado (por ejemplo, bomba encendida). Es aquí donde la potencia de la computadora se puede utilizar para realizar un complejo secuenciamiento de operaciones, por ejemplo: ABRA una válvula, después ENCIENDA una bomba, pero solamente si la presión es mayor de 50.

La computadora se puede utilizar para resumir y visualizar los datos que está procesando. Las tendencias (gráficos) de valores analógicos en un cierto plazo son muy comunes, recoger los datos y resumirlos en informes para los operadores y la gerencia son características normales de un sistema SCADA.

2.1. Definición General

SCADA (supervisory control and data acquisition): Un sistema industrial de mediciones y control que consiste en una computadora principal o master (generalmente llamada Estación Principal, Master Terminal Unit o MTU); una o más unidades obteniendo datos de campo (generalmente llamadas estaciones remotas, Remote Terminal Units, o RTU's); y una colección de software estándar y/o a medida, usado para monitorear y controlar remotamente dispositivos de campo. Los sistemas SCADA contemporáneos exhiben predominantemente características de control a lazo abierto y utilizan comunicaciones generalmente interurbanas, aunque algunos elementos de control a lazo cerrado y/o de comunicaciones de larga distancia pueden también estar presentes.

Sistemas similares a SCADA son vistos rutinariamente en fábricas, plantas de tratamiento, etc. Éstos son llamados a menudo como Sistemas de Control Distribuidos (DCS - Distributed Control Systems). Tienen funciones similares a los sistemas SCADA, pero las unidades de colección o de control de datos de campo se establecen generalmente dentro de un área confinada. Las comunicaciones pueden ser vía una red de área local (LAN), y serán normalmente confiables y de alta velocidad. Un sistema DCS emplea generalmente cantidades significativas de control a lazo cerrado.

Un sistema SCADA por otra parte, generalmente cubre áreas geográficas más grandes, y normalmente depende de una variedad de sistemas de comunicación menos confiables que una LAN. El control a lazo cerrado en esta situación será menos deseable. El control

puede ser automático, o iniciado por comandos de operador. La adquisición de datos es lograda en primer lugar por los RTU's que exploran las entradas de información de campo conectadas con ellos (pueden también ser usados PLC's - Programmable Logic Controllers). Esto se hace generalmente a intervalos muy cortos. La MTU entonces explorará los RTU's generalmente con una frecuencia menor. Los datos se procesarán para detectar condiciones de alarma, y si una alarma estuviera presente, sería catalogada y visualizada en listas especiales de alarmas.

Los datos pueden ser de tres tipos principales:

- Datos analógicos (por ejemplo números reales) que quizás sean presentados en gráficos.
- Datos digitales (on/off) que pueden tener alarmas asociadas a un estado o al otro.
- Datos de pulsos (por ejemplo contéo de revoluciones de un medidor) que serán normalmente contabilizados o acumulados.

La interfaz primaria al operador es un display que muestra una representación de la planta o del equipamiento en forma gráfica. Los datos vivos (dispositivos) se muestran como dibujos o esquemas en primer plano (foreground) sobre un fondo estático (background). Mientras los datos cambian en campo, el foreground es actualizado (una válvula se puede mostrar como abierta o cerrada, etc.). Los datos analógicos se pueden mostrar como números, o gráficamente (esquema de un tanque con su nivel de líquido almacenado). El sistema puede tener muchos de tales displays, y el operador puede seleccionar los más relevantes en cualquier momento.

2.2. La telemetría de radio como tecnología base de SCADA

La velocidad de transmisión de datos sobre radio estaba en su momento limitada al rango 300 baudios a 1200 baudios, pero las radios de datos modernas soportan hasta 9600 baudios

(e incluso hasta 64k). Una red de radio que funciona en la banda de 900 Mhz es autorizada normalmente para utilizar 12,5 o 25 kHz de ancho de banda. En 25 kHz, las velocidades de 9600 baudios pueden ser alcanzadas, pero en 12,5 kHz solamente 4800 baudios son posibles con el equipamiento actual.

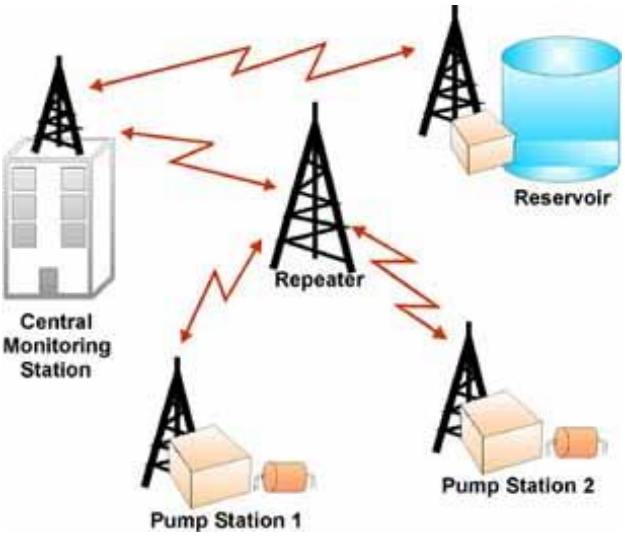

Figura No. 2 Esquema de red de radio

Una red de radio típica consiste en una conversación a través del repetidor situado en algún punto elevado, y un número de RTU's (PLC´s) que comparten la red. Todos los RTU's "hablan" sobre una frecuencia (F1) y escuchan en una segunda frecuencia (F2). El repetidor escucha en F1, y retransmite esto en F2. Los mensajes del Master viajan sobre un enlace de comunicación dedicado hacia el repetidor y son difundidos desde el repetidor en F2 a todos los RTU's. Si el protocolo de comunicaciones usado entre el Master y el repetidor es diferente al usado en la red de radio, entonces debe haber un "Gateway" en el sitio del repetidor. Este hecho permitiría utilizar los protocolos apropiados para cada uno de los medios.

El número de RTU's que puede compartir un repetidor depende de un número de factores. En primer lugar el tipo de equipo de radio puede afectar esto, teniendo en cuenta el retardo en alcanzar una señal estable. La aplicación también es un factor importante, ya que de ella depende el tiempo de respuesta requerido. Las características del protocolo (la

interrogación, informe por excepción, las transmisiones iniciadas por el RTU ó PLC) también pueden ser significativas. La velocidad tiene obviamente un impacto también.

2.3. Computadora Principal ó MTU - Master Terminal Unit

La parte más visible de un sistema SCADA es la estación central o MTU. Éste es el "centro neurálgico" del sistema, y es el componente del cual el personal de operaciones se valdrá para ver la mayoría del sistema. Una MTU a veces se llama HMI -Human Machine Interface, interfaz hombre/máquina .

Las funciones principales de una MTU de SCADA son:

- Adquisición de datos. Recolección de datos de los RTU's.
- Trending. Salvar los datos en una base de datos, y ponerlos a disposición de los operadores en forma de gráficos.
- Procesamiento de Alarmas. Analizar los datos recogidos de los RTU's para ver si han ocurrido condiciones anormales, y alertar a personal de operaciones sobre las mismas.
- Control. Control a Lazo Cerrado, e iniciados por operador.
- Visualizaciones. Gráficos del equipamiento actualizado para reflejar datos del campo.
- Informes. La mayoría de los sistemas SCADA tienen un ordenador dedicado a la producción de reportes conectado en red (LAN o similar) con el principal.
- Mantenimiento del Sistema Mirror, es decir, mantener un sistema idéntico con la capacidad segura de asumir el control inmediatamente si el principal falla.
- Interfaces con otros sistemas. Transferencia de datos hacia y desde otros sistemas corporativos para, por ejemplo, el procesamiento de órdenes de trabajo, de compra, la actualización de bases de datos, etc.
- Seguridad. Control de acceso a los distintos componentes del sistema.
- Administración de la red. Monitoreo de la red de comunicaciones.

- Administración de la Base de datos. Agregar nuevas estaciones, puntos, gráficos, puntos de cambio de alarmas, y en general, reconfigurar el sistema.
- Aplicaciones especiales. Casi todos los sistemas SCADA tendrá cierto software de aplicación especial, asociado generalmente al monitoreo y al control de la planta.
- Sistemas expertos, sistemas de modelado. Los más avanzados pueden incluir sistemas expertos incorporados, o capacidad de modelado de datos.

2.4. Remote Terminal Units - RTU's

La RTU es una pequeña y robusta computadora que proporciona inteligencia en el campo para permitir que el Master se comunique con los instrumentos. Es una unidad stand-alone (independiente) de adquisición y control de datos. Su función es controlar el equipamiento de proceso en el sitio remoto, adquirir datos del mismo, y transferirlos al sistema central SCADA.

Hay dos tipos básicos de RTU's- "single boards" (de un solo módulo), compactos, que contienen todas las entradas de datos en una sola tarjeta, y "modulares" que tienen un modulo CPU separado, y pueden tener otros módulos agregados, normalmente enchufándolos en una placa común (similar a una PC con una placa madre donde se montan procesador y periféricos).

Todos los RTU's requieren la siguiente funcionalidad. En muchos RTU's éstas se pueden mezclar y no necesariamente ser identificables como módulos separados.

- Sistema operativo en tiempo real.
- Driver para el sistema de comunicaciones, es decir la conexión con el Master.
- Drivers de dispositivo para el sistema de entrada-salida a los dispositivos de campo.

- Aplicación SCADA para exploración de entradas de información, procesamiento y el grabado de datos, respondiendo a las peticiones del Master sobre la red de comunicaciones.
- Algún método para permitir que las aplicaciones de usuario sean configuradas en el RTU. Ésta puede ser una simple configuración de parámetros, habilitando o deshabilitando entradas-salidas específicas que invalidan o puede representar un ambiente de programación completo para el usuario.
- Diagnóstico.
- Algunos RTU's pueden tener un sistema de archivos con soporte para descarga de archivo, tanto programas de usuario como archivos de configuración.

2.5. Controladores Lógicos Programables PLC's contra RTU's

Un PLC (Programmable Logic Controller) es un ordenador industrial que substituyó originalmente la lógica de los relais. Tenía entradas de información y salidas similares a las de un RTU. Contenía un programa que ejecutaba un bucle, explorando las entradas de información y tomando las acciones basadas en estas entradas de información. El PLC no tenía originalmente ninguna capacidad de comunicaciones, sino que comenzaron a ser utilizadas en situaciones donde las comunicaciones eran una característica deseable. Los módulos de comunicaciones fueron desarrollados así para PLC's, utilizando Ethernet (para el uso en DCS) y el protocolo de comunicaciones modbus para el uso sobre conexiones dedicadas (cables). Con el correr del tiempo los PLC's han sido desarrollados para soportar protocolos de comunicación más sofisticados logrando así superar en muchos casos el nivel de una RTU

El PLC cumple las mismas funcionalidades software de las RTU´s y tiene los siguientes componentes hardware:

- CPU y memoria volátil (RAM).
- Memoria no volátil para grabar programas y datos.
- Capacidad de comunicaciones a través de puertos seriales o a veces con módem incorporado.
- Fuente de alimentación segura (con salvaguardia de batería) y protección eléctrica contra fluctuaciones en la tensión..
- Watchdog timer (que asegure reiniciar el RTU si algo falla).
- Interfaces de entrada-salida a DI/DO/AI/AO's.
- Reloj de tiempo real.

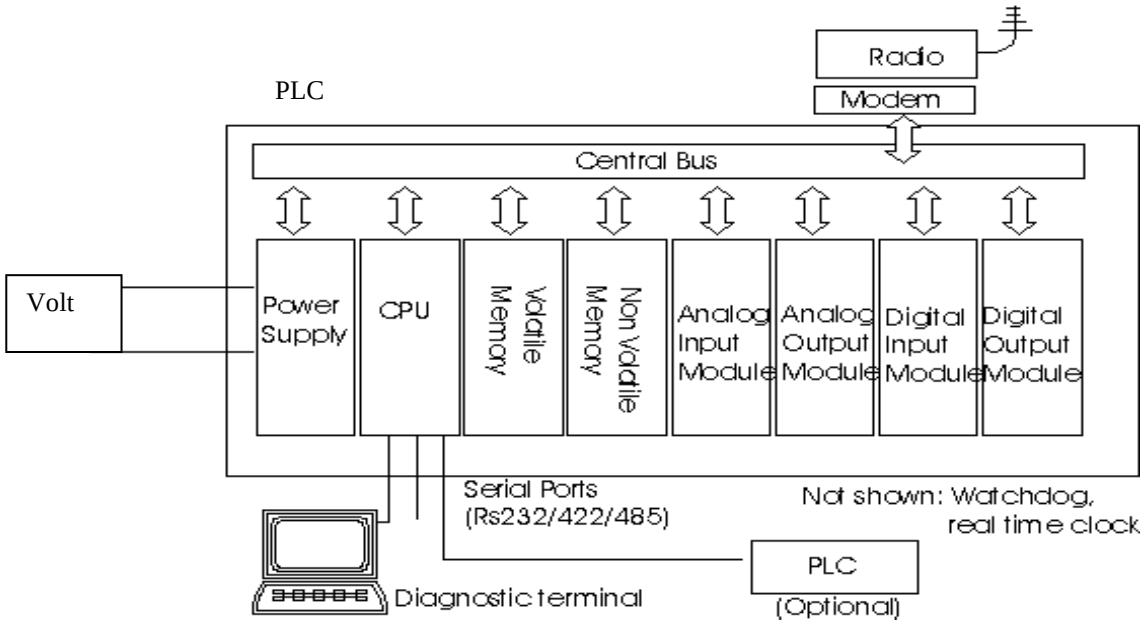

Figura No. 3 Estructura de un controlador lógico programable

3. Interfaces de Usuario

Los Avances de la Ciencia y la Tecnología han puesto al hombre en un plano intermedio entre lo tangible e intangible computacionalmente hablando, es ahora tan común el convivir con un computador diariamente que cada vez se hace más imperativo la mejor interacción hombre-máquina a través de una adecuada interfaz (Interfaz de Usuario), que le brinde tanto comodidad como eficiencia.

Lewis y Rieman [1993] definen las interfaces hombre computadora como:

“Las interfaces básicas de usuario son aquellas que incluyen cosas como menús, ventanas, teclado, ratón, los "beeps" y algunos otros sonidos que la computadora hace, en general, todos aquellos canales por los cuales se permite la comunicación entre el hombre y la computadora”.

La idea fundamental en el concepto de interfaz es el de mediación, entre hombre y máquina. La interfaz es lo que "media", lo que facilita la comunicación, la interacción, entre dos sistemas de diferente naturaleza, típicamente el ser humano y una máquina como el computador. Esto implica, además, que se trata de un sistema de traducción, ya que los dos "hablan" lenguajes diferentes: verbal-icónico en el caso del hombre y binario en el caso del procesador electrónico.

De una manera más técnica se define la Interfaz de usuario, como conjunto de componentes empleados por los usuarios para comunicarse con las computadoras. El usuario dirige el funcionamiento de la máquina mediante instrucciones, denominadas genéricamente entradas. Las entradas se introducen mediante diversos dispositivos, por ejemplo un teclado, y se convierten en señales electrónicas que pueden ser procesadas por la computadora. Estas señales se transmiten a través de circuitos conocidos como bus, y son

coordinadas y controladas por la unidad de proceso central y por un soporte lógico conocido como sistema operativo. Una vez que la CPU ha ejecutado las instrucciones indicadas por el usuario, puede comunicar los resultados mediante señales electrónicas, o salidas, que se transmiten por el bus a uno o más dispositivos de salida, por ejemplo una impresora o un monitor.

Resumiendo entonces podemos decir que, una interfaz de software es la parte de una aplicación que el usuario ve y con la cual interactúa. Está relacionada con la subyacente estructura, la arquitectura, y el código que hace el trabajo del software, pero no se confunde con ellos. La interfaz incluye las pantallas, ventanas, controles, menús, la ayuda en línea, la documentación y el entrenamiento. Cualquier cosa que el usuario ve y con lo cual interactúa es parte de la interfaz.

Dentro de las Interfaces de Usuario se distinguir básicamente dos tipos :

- Una interfaz de hardware, a nivel de los dispositivos utilizados para ingresar, procesar y entregar los datos: teclado, ratón y pantalla visualizadora; y
- Una interfaz de software, destinada a entregar información acerca de los procesos y herramientas de control, a través de lo que el usuario observa habitualmente en la pantalla.

3.1. Interfaces gráficas de usuario (Graphical user interfaces – GUIs)

Un GUI es una representación gráfica en la pantalla del ordenador de los programas, datos y objetos, así como de la interacción con ellos. Un GUI proporciona al usuario las herramientas para realizar sus operaciones, más que una lista de las posibles operaciones que el ordenador es capaz de hacer.

Una característica importante es que el GUI permite manipular los objetos e información de la pantalla, no sólo presentarla.

Para usar un GUI, los usuarios deben conocer (o aprender) una serie de conceptos: organización del sistema (ficheros, directorios), diferentes tipos de iconos y efecto de las acciones sobre ellos, elementos básicos de una ventana, uso de los controles del GUI, uso del ratón.

Los GUI usan el estilo objeto-acción, en contraposición al acción-objeto de los CUI o las interfaces de menú. El usuario selecciona un objeto, y después la acción a realizar sobre dicho objeto. Los objetos son el principal foco de atención del usuario, lo cual resulta más natural y próximo a su modelo mental.

3.2. Interfaces de usuario orientadas a objetos (object oriented user interfaces, OOUIs).

Su aspecto es similar al de las GUIs. La diferencia estriba en el modelo subyacente: las GUIs son interfaces orientadas a la aplicación, mientras que las OOUIs están orientadas al objeto.

El objetivo de la OOUI es que el usuario se concentre en sus tareas en lugar de en el ordenador y cómo utilizar las aplicaciones y ficheros necesarios para cumplir sus objetivos. Por ello se esconde la organización del sistema al usuario.

El estilo de interacción de los OOUIs es el de objeto-acción (también se da en los GUIs, aunque mezclado con el estilo acción-objeto). La ventana es un objeto ventana, no una ventana de aplicación; desaparecen pues los menús de barra y ganan terreno los contextuales.

La tabla siguiente muestra las principales diferencias entre ambos estilos de interfaz:

Interfaces orientadas a la aplicación	Interfaces orientadas a objetos
La aplicación consiste en un icono, una ventana principal y varias secundarias	El producto consiste en una colección de objetos que cooperan y vistas de dichos objetos
Los iconos representan aplicaciones o ventanas abiertas	Los iconos representan objetos que se pueden manipular directamente
Los usuarios deben abrir una aplicación antes de trabajar con objetos	Los usuarios abren objetos como vistas en el escritorio
Proporciona al usuario las funciones necesarias para realizar las tareas	Proporciona al usuario los materiales necesarios para realizar las tareas
Se centra en la tarea principal determinada por la aplicación	Se centra en las entradas y salidas de los objetos y tareas
Las tareas relacionadas son soportadas por otras aplicaciones	Las tareas relacionadas son soportadas por el uso de otros objetos
Estructura rígida: función	Estructura flexible: objeto
Los usuarios pueden quedar atrapados en una tarea	Los usuarios no deben quedar atrapados en una tarea
Los usuarios deben seguir la estructura de la aplicación	Los usuarios pueden realizar tareas a su propio gusto
Se requieren muchas aplicaciones: una por tarea	Se requieren pocos objetos, que se reutilizan en muchas tareas

Cuadro 1.3 Diferenciación entre los estilos de interfaz

3.3. Características humanas del diseño de interfaz

Al diseñar interfaces de usuario deben tenerse en cuenta las habilidades cognitivas y de percepción de las personas, y adaptar el programa a ellas.

Así, una de las cosas más importantes que una interfaz puede hacer es reducir la dependencia de las personas de su propia memoria, no forzándoles a recordar cosas

innecesariamente (por ejemplo, información que apareció en una pantalla anterior) o a repetir operaciones ya realizadas. Algunos puntos a tener en cuenta son:

- Demasiada simetría puede hacer las pantallas difíciles de leer.
- Si se ponen objetos sin alinear, hacerlo drásticamente.
- Asimetría=activo, simetría=sereno.
- Elementos de tamaño y color similares se perciben como pertenecientes a un grupo.
- Asumir errores en la entrada del usuario.
- Diseñar para el usuario, no para demostrar los propios conocimientos tecnológicos.
- Unos gráficos espectaculares no salvarán a una mala interfaz.

3.4. Pasos para el diseño de interfaz

En el proceso de diseño de una interfaz de usuario se pueden distinguir cuatro fases o pasos fundamentales:

- Reunir y analizar la información del usuario:

Es decir concretar a través de técnicas de requerimentación, qué tipo de usuarios van a utilizar el programa, qué tareas van a realizar los usuarios y cómo las van a realizar, qué exigen los usuarios del programa, en qué entorno se desenvuelven los usuarios (físico, social, cultural).

- Diseñar la interfaz de usuario.

Es importante dedicar tiempo y recursos a esta fase, antes de entrar en la codificación. En esta fase se definen los objetivos de usabilidad del programa, las tareas del usuario, los objetos y acciones de la interfaz, los iconos, vistas y representaciones visuales de los

objetos, los menús de los objetos y ventanas. Todos los elementos visuales se pueden hacer primero a mano y luego refinar con las herramientas adecuadas.

- Construir la interfaz de usuario.

Es interesante realizar un prototipo previo, una primera versión del programa que se realice rápidamente y permita visualizar el producto para poderlo probar antes de codificarlo definitivamente

- Validar la interfaz de usuario.

Se deben realizar pruebas de usabilidad del producto, a ser posible con los propios usuarios finales del mismo.

4. Bases de datos

Un archivo es un elemento de información conformado por un conjunto de registros. Estos registros a su vez están compuestos por una serie de caracteres o bytes. Las formas en las cuales pueden organizarse los archivos, son archivos secuenciales o archivos directos.

En los archivos secuenciales los registros están almacenados en una secuencia que depende de algún criterio definido. El uso de archivos secuenciales presenta algunas desventajas en el proceso de actualización, consulta o registro de información cuando se maneja gran volumen de datos.

La otra forma de organizar los archivos es a través de archivos directos, con los cuales se eliminan las desventajas mencionadas en los archivos secuenciales, ya que los archivos directos dan mayor flexibilidad en su manejo. Esta forma de organización es la que hace posible que existan las bases de datos. Los archivos directos permiten accesar directamente un registro de información sin tener que buscar uno a uno por todos los registros del archivo, utilizando una llave de acceso dentro del archivo.

Una Base de Datos es pues, un conjunto de datos estructurados, relacionados y almacenados en un soporte físico. Su objetivo es el de automatizar la manipulación, uso y mantenimiento de la información. Las bases de datos proporcionan la infraestructura requerida para los Sistemas de Apoyo a la Toma de Decisiones y para los Sistemas de Información Estratégicos, ya que estos sistemas explotan la información contenida en las bases de datos de la organización para apoyar el proceso de toma de decisiones o para lograr ventajas competitivas.

4.1. Historia de las Bases de Datos

Tuvieron sus orígenes en 1960 – 1962, cuando se empezaron a usar las maquinas que codificaban la información en tarjetas perforadas por medio de agujeros. Las bases de datos se crean con el objetivo de almacenar grandes cantidades de datos que antes se almacenaba en libros, lo que era lento, costoso y complejo(cualquier actualización a realizar, había que hacerla en cada uno de los libros en los que apareciera dicha información a modificar).

Las primeras bases de datos manejaban ficheros que eran almacenados en tarjetas o soportes magnéticos. Cuando los ordenadores evolucionan, aparecen las cintas y los discos, a la vez que las maquinas son dotadas de mucha mas potencia y facilidad de manipulación, es por tanto en ese momento cuando las bases de datos comienzan a ser realmente utiles.

En 1970 se convoca una Conferencia de Lenguajes de Programación y se establece un modelo llamado CODASYL - Modelo para el tratamiento de bases de datos que fue publicado por E. Cod en 1970. Cod, propuso una forma de organizar las bases de datos mediante un modelo matemático lógico.

4.2. Ventajas en el uso de bases de datos

La utilización de bases de datos como plataforma para el desarrollo de Sistemas de Información en las Organizaciones se ha incrementado notablemente en los últimos años, se debe a las ventajas que ofrece su utilización, algunas de las cuales se comentarán a continuación:

- Globalización de la información: permite a los diferentes usuarios considerar la información como un recurso corporativo que carece de dueños específicos.

- Eliminación de información inconsistente: si existen dos o más archivos con la misma información, los cambios que se hagan a éstos deberán hacerse a todas las copias del archivo, lo que permite mantener la integridad en la información.
- Permite compartir información.
- Independencia de datos: el concepto de independencia de datos es quizás el que más ha ayudado a la rápida proliferación del desarrollo de Sistemas de Bases de Datos. La independencia de datos implica un divorcio entre programas y datos.
- Posibilidada de aplicar Restricciones de Seguridad: Para mantener la seguridad a cerca del mantenimiento de los datos, los administradores de la Base de Datos, crean una jerarquía de acceso, que permitirá o prohibirá a los usuarios hacer una u otra acción sobre dicha base de datos.

4.3. Tipos de bases de datos

Las bases de datos se pueden dividir en cuatro tipos básicos:

- Bases de datos de fichero plano (o ficheros por bloques)
- Bases de datos relacionales
- Bases de datos orientadas a objetos
- Bases de datos híbridas

Las bases de datos de fichero plano consisten en ficheros de texto divididos en filas y columnas. Estas bases de datos son las más primitivas y quizás ni tan siquiera merezcan considerarse como tales. Pueden ser útiles para aplicaciones muy simples, pero no para aplicaciones medianas o complejas, debido a sus grandes limitaciones en cuanto a manejo y acceso de la información.

Las bases de datos relacionales son las más populares actualmente. Su nombre proviene de su gran ventaja sobre las bases de datos de fichero plano: la posibilidad de relacionar varias tablas de datos entre sí, compartiendo información y evitando la duplicidad y los problemas que ello conlleva (espacio de almacenamiento y redundancia). Existen numerosas bases de datos relacionales para distintas plataformas (Access, Paradox, Oracle, Sybase, PostGreat, Informix, MiniSQL, Interbase, SQLServer, MySQL y otras) y son ampliamente utilizadas.

Las bases de datos orientadas a objetos incorporan el paradigma de la Orientación a Objetos (OO) a las bases de datos. La base de datos está constituida por objetos, que pueden ser de muy diversos tipos, y sobre los cuales se encuentran definidas unas operaciones. Actualmente no existe una base de datos puramente orientada o objetos.

Las bases de datos híbridas combinan características de las bases de datos relacionales y las bases de datos orientadas a objetos. Manejan datos textuales y datos binarios, a los cuales se extienden las posibilidades de consulta. Es una tecnología reciente y aún existen pocas en el mercado.

4.4. Tipos de modelos de datos

Los modelos siempre han sido aceptados por ingenieros, científicos, artistas y gestores como una técnica inestimable para presentar ideas, ayudar a la comprensión e incluso predecir nuevas formas de hacer cosas.

Discutiblemente, nuestra propia percepción del mundo es un modelo elaborado que se crea en nuestro cerebro a partir de la información que se utiliza para desarrollar un modelo de datos de alta calidad. El modelo de datos ofrece una forma estándar de definir los datos y las relaciones entre éstos para todos los sistemas de información. Esto mejora enormemente la calidad del sistema e incrementa la productividad del software.

Los diferentes modelos de datos propuestos se clasifican en tres grupos diferentes: modelos lógicos basados en objetos, modelos lógicos basados en registros y modelos físicos.

Los *modelos lógicos basados en objetos* se usan para describir datos en los niveles lógicos y de vistas. Se caracterizan por el hecho de que proporcionan capacidades estructurales muy flexibles y permiten que las ligaduras de datos sean especificadas explícitamente. Algunos de los más ampliamente conocidos son:

- El modelo de datos semántico
- El modelo de datos funcional
- El modelo de datos entidad-relación (E-R) está basado en una percepción del mundo real que consta de un colección de objetos básicos, llamados entidades y de relaciones entre estas entidades. Una entidad es una "cosa" u "objeto" en el mundo real que es distinguible de otros. Las entidades se describen en una base de datos mediante un conjunto de atributos. Una relación es una asociación entre varias entidades. La totalidad de estructuras lógicas de una base de datos se puede expresar gráficamente mediante un diagrama E-R (entidad-relación).
- El modelo orientado a objetos está basado en una colección de objetos. Un objeto contiene valores almacenados en variables de ejemplares (instance variables) dentro de ese objeto. Un objeto tambien posee métodos que operan sobre él. Los objetos que contienen los mismos tipos de valores se agrupan en clases.

Los *modelos lógicos basados en registros* se usan para describir datos en los niveles lógicos y de vistas. En contraste con el modelo lógico basado en objetos, se usan tanto para especificar la estructura lógica completa de la base de datos como para proporcionar una descripción de alto nivel de la implementación.

Los modelos lógicos basados en registros se llaman así debido a que la base de datos se estructura en registros de formato fijo de diferentes tipos. En cada tipo de registro se define un número fijo de campos o atributos, y cada campo tiene normalmente una longitud fija. El uso de registros de longitud fija simplifica la implementación en el nivel físico de la base de datos.

Los tres modelos basados en registros más ampliamente manejados son:

- El modelo relacional en donde se usa una colección de tablas para representar tanto los datos como las relaciones entre estos datos. Se diferencia de los modelos de red y jerárquico en que no usa punteros o enlaces, esta liberación del uso de punteros permite que se defina la estructura mediante un fundamento matemático formal.
- El modelo de red en el cual los datos se representan mediante colecciones de registros y las relaciones entre los datos se representan mediante enlaces, que se pueden ver como punteros. Los registros de la base de datos se organizan como una colección de grafos dirigidos.
- El modelo Jerárquico, el cual es muy similar al modelo de redes, en el sentido es que los datos y las relaciones entre los datos se representan mediante registros y enlaces respectivamente. La diferencia radica en que en el modelo jerárquico los registros se organizan como colecciones de árboles en lugar de grafos dirigidos.

El *modelo de datos físico* se usa para describir datos en un nivel más bajo. Dos de los más conocidos son:

- El modelo de unificación y
- El modelo de memoria por marcos

4.4. Lenguajes de bases de datos

Un sistema de bases de datos relacional proporciona dos tipos de lenguajes diferentes: uno para especificar el esquema de la base de datos (DDL) y otro para expresar las consultas y actualizaciones de la base de datos (MDL), estas dos partes se unen en el SQL sigla de Structured Query Lenguage (lenguaje de consulta estructurado) estandarizado en 1992 (última actualización del estándar 1995).

4.5. Sistemas de administración de bases de datos

Un sistema manejador de bases de datos (DBMS) es el software de computadora que administra el acceso a las bases de datos. Un típico DBMS multiusuario realiza las siguientes tareas: da un medio de definición de datos al sistema, usa los recursos de la computadora de forma que permite que multiples usuarios realicen sus trabajos con buenos tiempos de respuesta, protege la información de la base de datos. Más alla de esas funciones principales, un DBMS puede tambien brindar seguridad contra accesos no autorizados, recuperación en casos de falla del sistema, chequeo de integridad para que los datos en diferentes partes de la base de datos permanezcan consistentes.

Manejadores de bases de datos relacionales

El modelo de bases de datos relacionales iniciado teóricamente por E. F Codd de IBM entre 1969-1970 estableció un sistema formal para el almacenamiento de datos que separa la representación interna de los datos, de su representación lógica y acceso, las primeras bases de datos en este concepto aparecieron al inicio de la década de los 80´s para cambiar la jerarquía dominante y los modelos de bases de datos en red, a finales de los 80´s los RDBMS (Relational Database Management System), manejador de bases de datos relacionales prevalecen sobre las viejas tecnologías y entran a formar parte integral en el paradigma cliente/servidor.

La potencialidad de las RDBMS yace en su habilidad de ocultar los detalles de almacenamiento y recuperación al usuario de la base de datos. Las bases de datos no son solo más accesibles para los desarrolladores de aplicaciones – quienes pueden concentrar más sus esfuerzos en el código de la aplicación -, sino también para los negocios y los usuarios finales, quienes pueden ahora escoger de entre una gran cantidad de herraminetas visuales para formular consultas y recuperar datos de las bases de datos.

5. Seguridad

Daremos inicio a esta sección realizando un distinción entre seguridad y protección. El problema de la seguridad consiste en lograr que los recursos de un sistema sean, bajo toda circunstancia, utilizados para los fines previstos. Para eso se utilizan mecanismos de protección tales como encriptación, firewall y otros.

La seguridad ha sido el principal concerniente a tratar cuando una organización desea conectar su red privada al Internet. Sin tomar en cuenta el tipo de negocios, se ha incrementado el numero de usuarios de redes privadas por la demanda del acceso a los servicios de Internet tal es el caso del World Wide Web (WWW), Internet Mail (e-mail), File Transfer Protocol (FTP) y muchos otros. Adicionalmente los corporativos buscan las ventajas que ofrecen las paginas en el WWW y los servidores FTP de acceso publico en el Internet.

Los administradores de red tienen que incrementar todo lo concerniente a la seguridad de sus sistemas, debido a que se expone la organización privada de sus datos así como la infraestructura de sus red a los Expertos de Internet (*Internet Crakers*). Algunas de las amenazas y ataques posibles son:

- Virus. Un virus es parecido a un gusano, en cuanto se reproduce, pero la diferencia es que no es un programa por sí sólo, si no que es un trozo de código que se adosa a un programa legítimo, contaminándolo. Cuando un programa contaminado se ejecuta, ejecutará también el código del virus, lo que permitirá nuevas reproducciones, además de alguna acción (desde un simple mensaje inocuo hasta la destrucción de todos los archivos).
- Caballo de troya. Un caballo de troya es un programa aparentemente útil que contiene un trozo de código que hace algo no deseado.

- Puerta trasera. Una puerta trasera es un punto de entrada secreto, dejado por los implementadores del sistema para saltarse los procedimientos normales de seguridad. La puerta trasera puede haberse dejado con fines maliciosos o como parte del diseño; en cualquier caso, son un riesgo.
- Caza claves. Dejar corriendo en un terminal un programa que pida "login:" y luego "password:", para engañar a los usuarios de modo que estos revelen su clave.
- Solicitar recursos como páginas de memoria o bloques de disco, y ver qué información contienen; muchos sistemas no los borran cuando se liberan, de modo que se puede encontrar información "interesante".

Para superar estos temores y proveer el nivel de protección requerida, la organización necesita seguir una política de seguridad para prevenir el acceso no-autorizado de usuarios a los recursos propios de la red privada, y protegerse contra la exportación privada de información. Todavía, aun si una organización no esta conectada al Internet, esta debería establecer una política de seguridad interna para administrar el acceso de usuarios a porciones de red y proteger sensitivamente la información secreta.

5.1. Qué debe tener una política de seguridad

Esta es una labor bastante complicada y depende en gran medida del tipo de empresa al que se le aplique la política, pero un buen administrador de red debe lograr la comunicación entre usuarios y gerentes de forma que puedan tomar las políticas de seguridad acertadas para la empresa. Algunos puntos a tener en cuenta son:

- Aclaraciones: Explicar claramente el porqué de las instrucciones.
- Responsabilidades: Plasmar por escrito las responsabilidades en todos los niveles de la empresa frente a las políticas de seguridad.

- Lenguaje común: la pregunta es ¿como explicarle a los distintos usuarios para entiendan la importancia del tema pero no se convierta en una amenaza?.
- Revisiones: Determinación de formas y tiempos para revisar las políticas de seguridad.
- Asuntos de seguridad: Debido a las diferentes empresas es difícil ser específico pero algunas de las preguntas a resolver son: ¿quién debe tener una cuenta?, ¿qué tipo de cuenta debe tener?, ¿Ofrecer cuentas a personas no pertenecientes a la empresa?, ¿Pueden las cuentas ser compartidas?, ¿Qué pasa si el empleado es despedido o se le niega el acceso?, ¿Quién puede instalar conexiones a redes exteriores, autorizaciones y formatos?, ¿Qué métodos de protección de datos habrá?, ¿Qué clase de contraseña debe implementarse?, ¿Qué uso se requiere de Internet?, ¿Cómo prevenir virus?.

Después de haber definido una política de seguridad se puede realizar un estudio para especificar la necesidad de mecanismos hardware y software de protección tales como algoritmos, encriptación, firewalls, etc.

5.2. Mecanismos de protección

Algoritmos

En la literatura académica se han descrito numerosos algoritmos de firma digital. En la práctica, destacan tres de ellos: *la firma de comprobación aleatoria (hash), el Digital Signature Standard (DSS)* del gobierno de EE.UU. y la *signatura RSA*, que utiliza el algoritmo clásico desarrollado por Roven Rivest, Adi Shamir y Len Adlemn. Los tres algoritmos tienen usos y requisitos distintos.

Encriptación

¿ Por qué es importante la criptografía en Internet ?. La razón, como la explican los mexicanos Daniel Germán y Alejandro López Ortiz en su artículo “¿ Es la red lo

suficientemente confiable ?", es que "desde sus inicios se decidió que la seguridad de la información que se transmitía no era una prioridad, lo más valioso en ese momento era interconectar computadoras de forma tal que pudiera resistir fallas severas, posiblemente resultado de un ataque nuclear contra los Estados Unidos".

El protocolo principal por el cual se transmite la información que viaja por la red (TCP/IP, Transfer Control Protocol/Internet Protocol) no ha variado en su esencia desde la creación de Internet. Esta información se divide en paquetes más pequeños a los cuales se llama datagramas. Estos datagramas son enviados por la red sin ningún orden específico. Así cuando enviamos un mensaje que contenga, por ejemplo, las letras ABCD, éste se dividirá en cuatro datagramas, cada uno con una letra. Estos datagramas vijarán de modo independiente, para luego recomponerse en la computadora de destino, sin que el receptor final pueda saber qué ruta tomó cada uno de ellos. Sin embargo, ninguno de estos datagramas está encriptado y cualquiera que los tome en su recorrido puede leerlos sin problema.

Y aquí es donde entra la criptografía como aliada de la seguridad y del comercio en línea. La idea es encontrar un sistema en donde los datos puedan viajar de un modo seguro por la red. A ese sistema se le ha llamado SET (Secure Electronic Transaction

SET es un sistema de criptografía basado en el mecanismo de llave pública y en el cual participan las más importantes compañías de tarjetas de crédito a nivel mundial (Visa, Master Card y American Express) y varios colosos de la informática (Microsoft, IBM, Netscape, entre otros). SET cubre los tres principios básicos para asegurar la información en línea:

1. Que la información transmitida sea confidencial.
2. Transacciones que se lleven a cabo con total integridad, es decir sin pérdida de datos.
3. Autentificar a los tarjetahabientes y a los comerciantes.

En la actualidad, los ordenadores de la mayoría de usuarios sólo investigan un nivel de jerarquía de certificación. Si su navegador WEB está conectado a un servidor con capacidades *Secure Sockets Layer (SSL) o a un Secure HyperText Transfer Protocol (S-HTTP)*, el servidor establecerá su identidad expidiendo una copia de su clave pública encuadrada en un certificado. Lo más probable es que el certificado haya sido emitido por VeriSign , uno de los principales proveedores de certificados para servidores WEB que utilizan SSL para cifrar los datos que discurren entre el servidor y el navegador.

El **Protocolo SSL** fue desarrollado por Netscape para permitir confidencialidad y autenticación en Internet. SSL opera como una capa adicional entre Internet y las aplicaciones, esto permite que el protocolo sea independiente de la aplicación, siendo posible utilizar FTP, SSH y otras aplicaciones además de HTTP.
Para establecer una comunicación segura utilizando SSL se tienen que seguir una serie de pasos. Primero se debe hacer una solicitud de seguridad. Después de haberla hecho, se deben establecer los parámetros que se utilizarán para SSL. Esta parte se conoce como *SSL Handshake*. Una vez se haya establecido una comunicación segura, se deben hacer verificaciones periódicas para garantizar que la comunicación sigue siendo segura a medida que se transmiten datos. Luego que la transacción ha sido completada, se termina SSL.

En la siguiente figura se ilustra el proceso de handshake:

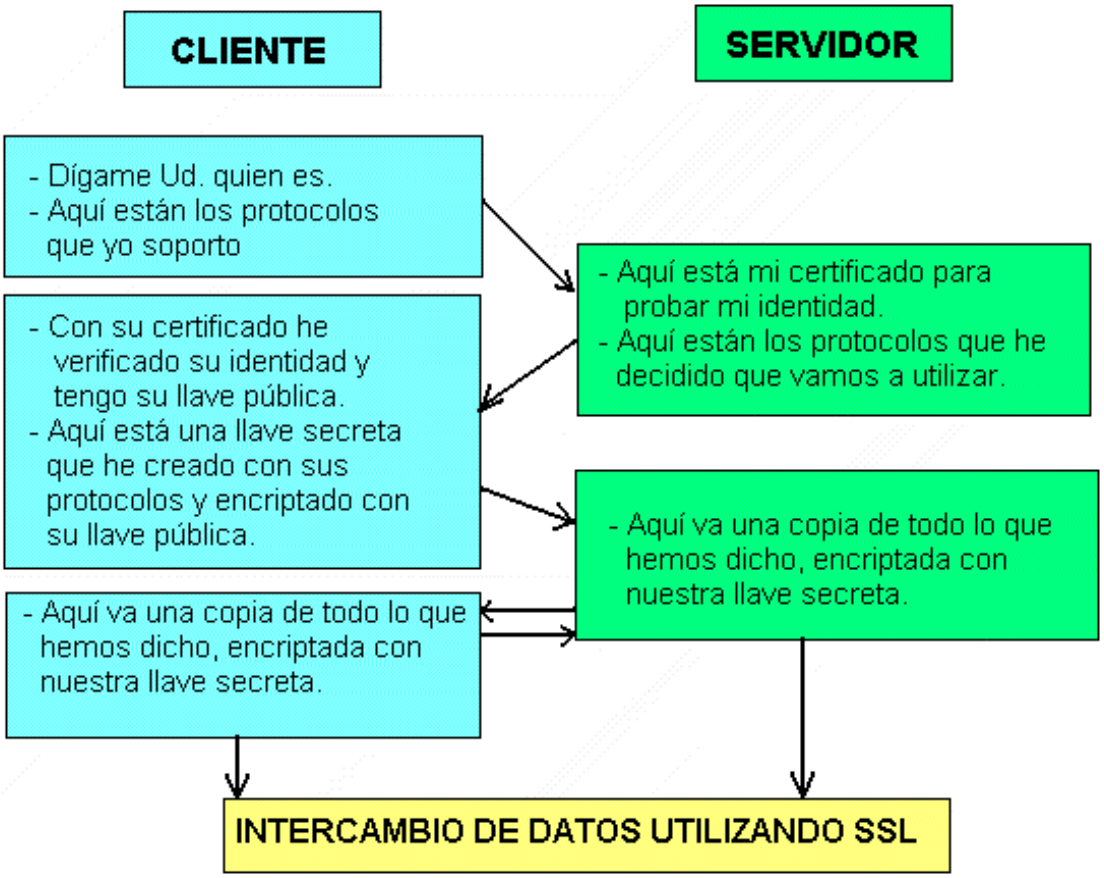

Figura No.4 Proceso de Handshake

El **Protocolo S-HTTP** fue desarrollado por Enterprise Integration Technologies (EIT). Al igual que SSL, permite tanto el cifrado como la autenticación digital. Sin embargo, a diferencia de SSL, S-HTTP es un protocolo de nivel de aplicación, es decir, que extiende el protocolo HTTP por debajo.

La propuesta de S-HTTP sugiere una nueva extensión para los documentos, `.shttp`, y el siguiente nuevo protocolo:

```
Secure * Secure-HTTP/1.1
```

Usando GET, un cliente solicita un documento, le dice al servidor qué tipo de cifrado puede manejar y le dice también dónde puede encontrar su clave pública. Si el usuario con esa clave está autorizado a acceder al documento, el servidor responde cifrando el documento y enviándoselo al cliente, que usará su clave secreta para descifrarlo y mostrárselo al usuario. Uno de los métodos de cifrado disponible en S-HTTP es el popular PGP

El PGP (Pretty Good Privacy ó Encriptación bastante buena) es un sistema de encriptación por llave pública escrito por Philip Zimmermann, y sirve para que nadie salvo uno mismo y el destinatario o destinatarios a los que vaya dirigido el mensaje puedan leerlo al ir los mensajes codificados, también puede usarse para comprobar la autenticidad del mensaje asegurándonos que lo ha escrito el remitente en realidad, realmente es muy bueno y es prácticamente indescifrable, esto mismo le ha llevado al autor del mismo Philip Zimmermann a tener bastantes quebraderos de cabeza con la ley en Estados Unidos, afortunadamente su caso ya se ha cerrado. La intimidad del correo personal tanto postal como electrónico esta amparada por la ley y la constitución de la mayoría de los países.

Firewalls

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo trafico de información a través del Internet deberá pasar a

través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del trafico, y el mismo podrá ser inmune a la penetración. desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

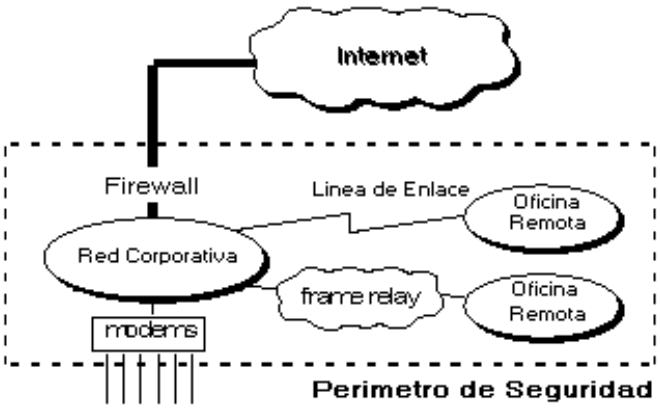

Figura No. 5 Perímetros de defensa.

La política de seguridad crea un perímetro de defensa lo cual es muy importante, ya que debemos de notar que un firewall de Internet no es justamente un ruteador, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información. Esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de dial-in y dial-out, reglas de enciptacion de datos y discos, normas de protección de virus, y entrenamiento. Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad. Un firewall de Internet sin una política de seguridad comprensiva es como poner una puerta de acero en una tienda.

Beneficios de un firewall en Internet

Los firewalls en Internet administran los accesos posibles del Internet a la red privada. Sin un firewall, cada uno de los servidores propios del sistema se exponen al ataque de otros servidores en el Internet. Esto significa que la seguridad en la red privada depende de la "Dureza" con que cada uno de los servidores cuenta y es únicamente seguro tanto como la seguridad en la fragilidad posible del sistema.

El firewall permite al administrador de la red definir un "choke point" (envudo), manteniendo al margen los usuarios no-autorizados (tal, como., hackers, crakers, vándalos, y espías) fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles. Uno de los beneficios clave de un firewall en Internet es que ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran nuestra red privada.

El firewall ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa , este generara una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el transito de los datos. Esto se podrá notar al acceder la organización al Internet, la pregunta general es "si" pero "cuando" ocurrirá el ataque. Esto es extremadamente importante para que el administrador audite y lleve una bitácora del trafico significativo a través del firewall. También, si el administrador de la red toma el tiempo para responder una alarma y examina regularmente los registros de base. Esto es innecesario para el firewall, desde que el administrador de red desconoce si ha sido exitosamente atacado!.

Concentra la seguridad Centraliza los accesos.
Genera alarmas de seguridad Traduce direcciones (NAT).
Monitorea y registra el uso de Servicios de WWW y FTP.

Gigura No.6 Beneficios De Un Firewall De Internet.

Con el paso de algunos años, el Internet ha experimentado una crisis en las direcciones, logrando que el direccionamiento IP sea menos generoso en los recursos que proporciona. Por este medio se organizan las compañías conectadas al Internet, debido a esto hoy no es posible obtener suficientes registros de direcciones IP para responder a la población de usuarios en demanda de los servicios. Un firewall es un lugar lógico para desplegar un Traductor de Direcciones de Red (NAT) esto puede ayudar aliviando el espacio de direccionamiento acortando y eliminando lo necesario para re-enumerar cuando la organización cambie del Proveedor de Servicios de Internet (ISPs) .

Un firewall de Internet es el punto perfecto para auditar o registrar el uso del Internet. Esto permite al administrador de red justificar el gasto que implica la coneccion al Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda, y promueve el método de cargo a los departamentos dentro del modelo de finanzas de la organización.

Un firewall de Internet ofrece un punto de reunión para la organización. Si una de sus metas es proporcionar y entregar servicios información a consumidores, el firewall de Internet es ideal para desplegar servidores WWW y FTP.

Finalmente, el firewall puede presentar los problemas que genera un punto de falla simple. Enfatizando si este punto de falla se presenta en la conexión al Internet, aun así la red interna de la organización puede seguir operando - únicamente el acceso al Internet esta perdido - .

La preocupación principal del administrador de red, son los múltiples accesos al Internet, que se pueden registrar con un monitor y un firewall en cada punto de acceso que posee la organización hacia el Internet. Estos dos puntos de acceso significa dos puntos potenciales de ataque a la red interna que tendrán que ser monitoreados regularmente!

Limitaciones de un firewall

Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.

Por ejemplo, si existe una coneccion dial-out sin restricciones que permita entrar a nuestra red protegida, el usuario puede hacer una coneccion SLIP o PPP al Internet. Los usuarios con sentido común suelen "irritarse" cuando se requiere una autenticación adicional requerida por un Firewall Proxy server (FPS) lo cual se puede ser provocado por un sistema de seguridad circunvecino que esta incluido en una conexión directa SLIP o PPP del ISP.

Este tipo de conexiones derivan la seguridad provista por firewall construido cuidadosamente, creando una puerta de ataque. Los usuarios pueden estar consientes de que este tipo de conexiones no son permitidas como parte de integral de la arquitectura de la seguridad en la organización.

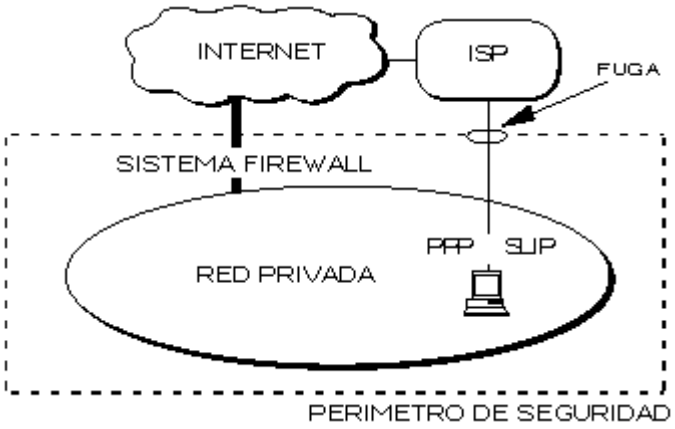

Figura No.7 Conexión Circunvecina Al Firewall De Internet.

El firewall no puede protegerse de las amenazas a que esta sometido por traidores o usuarios inconscientes. El firewall no puede prohibir que los traidores o espías corporativos copien datos sensitivos en disquettes o tarjetas PCMCIA y substraigan estas del edificio.

El firewall no puede proteger contra los ataques de la "Ingeniería Social", por ejemplo un Hacker que pretende ser un supervisor o un nuevo empleado despistado, persuade al menos sofisticado de los usuarios a que le permita usar su contraseña al servidor del corporativo o que le permita el acceso "temporal" a la red.

Para controlar estas situaciones, los empleados deberían ser educados acerca de los varios tipos de ataque social que pueden suceder, y a cambiar sus contraseñas si es necesario periódicamente.

El firewall no puede protegerse contra los ataques posibles a la red interna por virus informativos a través de archivos y software. Obtenidos del Internet por sistemas operativos al momento de comprimir o descomprimir archivos binarios, el firewall de Internet no puede contar con un sistema preciso de SCAN para cada tipo de virus que se puedan

presentar en los archivos que pasan a través de el. La solución real esta en que la organización debe ser consciente en instalar software anti-viral en cada despacho para protegerse de los virus que llegan por medio de disquettes o cualquier otra fuente.

Finalmente, el firewall de Internet no puede protegerse contra los ataques posibles en la transferencia de datos, estos ocurren cuando aparéntente datos inocuos son enviados o copiados a un servidor interno y son ejecutados despachando un ataque. Por ejemplo, una transferencia de datos podría causar que un servidor modificara los archivos relacionados a la seguridad haciendo mas fácil el acceso de un intruso al sistema.

Bases para el diseño decisivo del firewall

Cuando se diseña un firewall de Internet, se tiene que tomar algunas decisiones que pueden ser asignadas por el administrador de red:

- Posturas sobre la política del Firewall.
- La política interna propia de la organización para la seguridad total.
- El costo financiero del Proyecto "Firewall".
- Los componentes o la construcción de secciones del Firewall.

Un firewall típico se compone de uno, o una combinación, de los siguientes obstáculos.

- Ruteador Filtra-paquetes.
- Gateway a Nivel-aplicación.
- Gateway a Nivel-circuito.

Edificando obstáculos: ruteador filtra-paquetes

Este ruteador toma las decisiones de rehusar/permitir el paso de cada uno de los paquetes que son recibidos. El ruteador examina cada datagrama para determinar si este corresponde

a uno de sus paquetes filtrados y que a su vez haya sido aprobado por sus reglas. Las reglas de filtrado se basan en revisar la información que poseen los paquetes en su encabezado, lo que hace posible su desplazamiento en un proceso de IP. Esta información consiste en la dirección IP fuente, la dirección IP destino, el protocolo de encapsulado (TCP, UDP,ICMP, o IP tunnel), el puerto fuente TCP/UDP, el puerto destino TCP/UDP, el tipo de mensaje ICMP, la interface de entrada del paquete, y la interface de salida del paquete. Si se encuentra la correspondencia y las reglas permiten el paso del paquete, este será desplazado de acuerdo a la información a la tabla de ruteo, si se encuentra la correspondencia y las reglas niegan el paso, el paquete es descartado. Si estos no corresponden a las reglas, un parámetro configurable por incumplimiento determina descartar o desplazar el paquete.

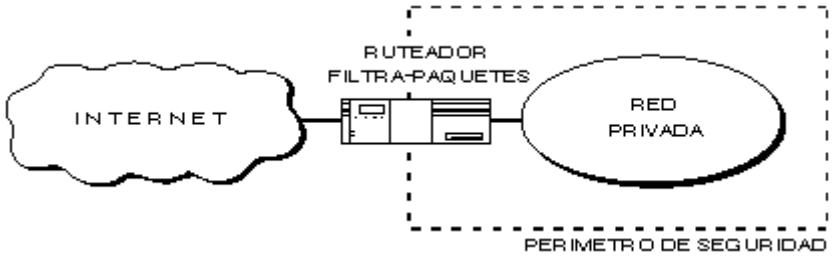

Figura No.8 Ruteador Filtra-Paquetes.

Beneficios del ruteador filtra-paquetes

La mayoría de sistemas firewall son desplegados usando únicamente ruteadores filtra-paquetes. Otros que tienen tiempo planean los filtros y configuran el ruteador, sea este pequeño o no , el costoso para implementar la filtración de paquetes no es cara; desde que los componentes básicos de los ruteadores incluyen revisiones estándar de software para dicho efecto. Desde entonces el acceso a Internet es generalmente provisto a través de interfaces WAN, optimando la operación del ruteador moderando el trafico y definiendo menos filtros. Finalmente, el ruteador de filtrado es por lo general transparente a los

usuarios finales y a las aplicaciones por lo que no se requiere de entrenamiento especializado o software especifico que tenga que ser instalado en cada uno de los servidores.

Limitaciones del ruteador filtra-paquetes

Definir el filtrado de paquetes puede ser una tarea compleja porque el administrador de redes necesita tener un detallado estudio de varios servicios de Internet, como los formatos del encabezado de los paquetes, y los valores específicos esperados a encontrase en cada campo. Si las necesidades de filtrado son muy complejas, se necesitara soporte adicional con lo cual el conjunto de reglas de filtrado puede empezar a complicar y alargar el sistema haciendo mas difícil su administración y comprensión. Finalmente, estas serán menos fáciles de verificar para las correcciones de las reglas de filtrado después de ser configuradas en el ruteador. Potencialmente se puede dejar una localidad abierta sin probar su vulnerabilidad.

Edificando obstáculos: gateways a nivel-aplicación

Los gateways nivel-aplicación permiten al administrador de red la implementación de una política de seguridad estricta que la que permite un ruteador filtra-paquetes. Mucho mejor que depender de una herramienta genérica de filtra-paquetes para administrar la circulación de los servicios de Internet a través del firewall, se instala en el gateway un código de proposito-especial (un servicio Proxy) para cada aplicación deseada. Si el administrador de red no instala el código Proxy para la aplicación particular, el servicio no es soportado y no podrán desplazarse a través del firewall.

Aun cuando, el código Proxy puede ser configurado para soportar únicamente las características especificas de una aplicación que el administrador de red considere aceptable mientras niega todas las otras.

Beneficios del gateway a nivel-aplicación

Son muchos los beneficios desplegados en un gateway a nivel-aplicación. Ellos dan a la administración de red un completo control de cada servicio desde aplicaciones proxy limitadas por un conjunto de comandos y la determinación del servidor interno donde se puede accesar a los servicios. Aun cuando, el administrador de la red tenga el completo control acerca de que servicios que son permitidos desde la carencia de un servicio proxy para uno en particular significa que el servicio esta completamente bloqueado. Los gateways a nivel-aplicación tienen la habilidad de soportar autenticaciones forzando al usuario para proveer información detallada de registro. Finalmente, las reglas de filtrado para un gateway de este tipo son mucho mas fáciles de configurar y probar que en un ruteador filtra-paquetes.

Limitaciones del gateway a nivel-aplicación

Probablemente una de las grandes limitaciones de un gateway a nivel-aplicación es que requiere de modificar la conducta del usuario o requiere de la instalación de software especializado en cada sistema que accese a los servicios Proxy.

Edificando obstáculos: gateway a nivel-circuito

Un Gateway a nivel-circuito es en si una función que puede ser perfeccionada en un Gateway a nivel-aplicación. A nivel-circuito simplemente trasmite las conexiones TCP sin cumplir cualquier proceso adicional en filtrado de paquetes.

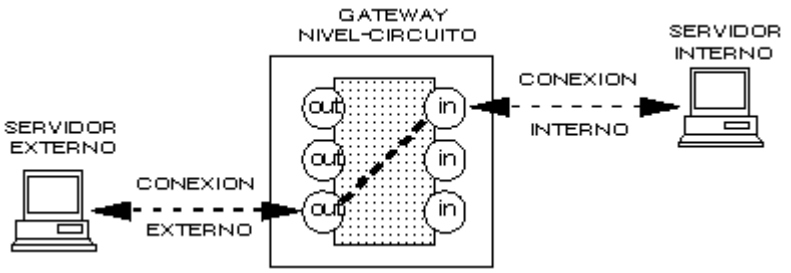

Figura No.9 Gateway Nivel-Circuito.

El gateway a nivel-circuito acciona como una cable copiando los bytes antes y después entre la conexión interna y la conexión externa. De cualquier modo, la conexión del sistema externo actúa como si fuera originada por el sistema de firewall tratando de beneficiar el encubrir la información sobre la protección de la red.

El Gateway a nivel-circuito se usa frecuentemente para las conexiones de salida donde el administrador de sistemas somete a los usuarios internos. La ventaja preponderante es que el servidor de defensa puede ser configurado como un Gateway "híbrido" soportando nivel-aplicación o servicios Proxy para conexiones de venida y funciones de nivel-circuito para conexiones de ida.

Esto hace que el sistema de firewall sea fácil de usar para los usuarios internos quienes desean tener acceso directo a los servicios de Internet mientras se proveen las funciones del firewall necesarias para proteger la organización de los ataques externos.

Como colocar el Servidor WEB en relación con el Firewall

Si una organización utiliza un firewall para proteger su red interna de ataques externos, tiene varias posibilidades respecto a dónde colocar el servidor WEB:

- Lo puede colocar fuera del firewall, como muestra la figura. No. 10, la ventaja de colocarlo así es que el servidor puede ser sujeto de ataques, en caso de que sea violado, el atacante no habrá ganado la batalla ya que para conseguir atacar los datos de la organización deberá pasar el firewall. La desventaja es que el servidor web no se beneficia de la protección proporcionada por el firewall.

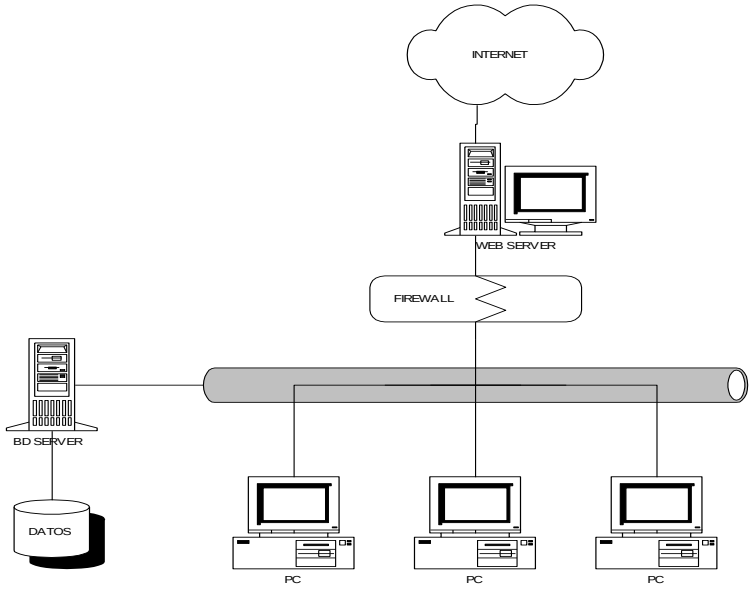

Figura No.10 Configuración de Servidor WEB fuera del firewall

- Lo puede colocar dentro del firewall, como muestra la figura No. 11, de esta forma es necesario configurar el firewall de forma que permita pasar transacciones en el puerto 80 de TCP/IP. La ventaja de esta configuración es que el firewall evita que los usuarios externos utilicen otros servicios distintos a Internet, tales como SSH ó FTP. Sin embargo, si el firwall es traspasado por un atacante, él tendrá acceso completo a la red interna.

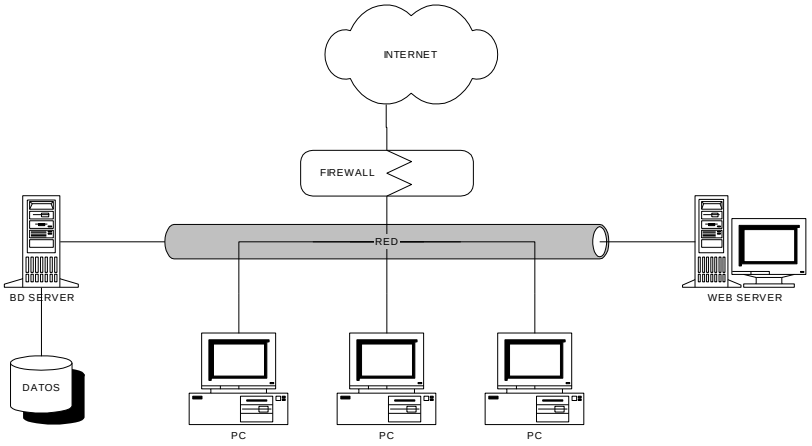

Figura No.11 Configuración de Servidor WEB dentro del Firewall

- La tercera opción es utilizar dos firewalls, como muestra la figura No. 12, el problema básico de esta configuración son los costos.

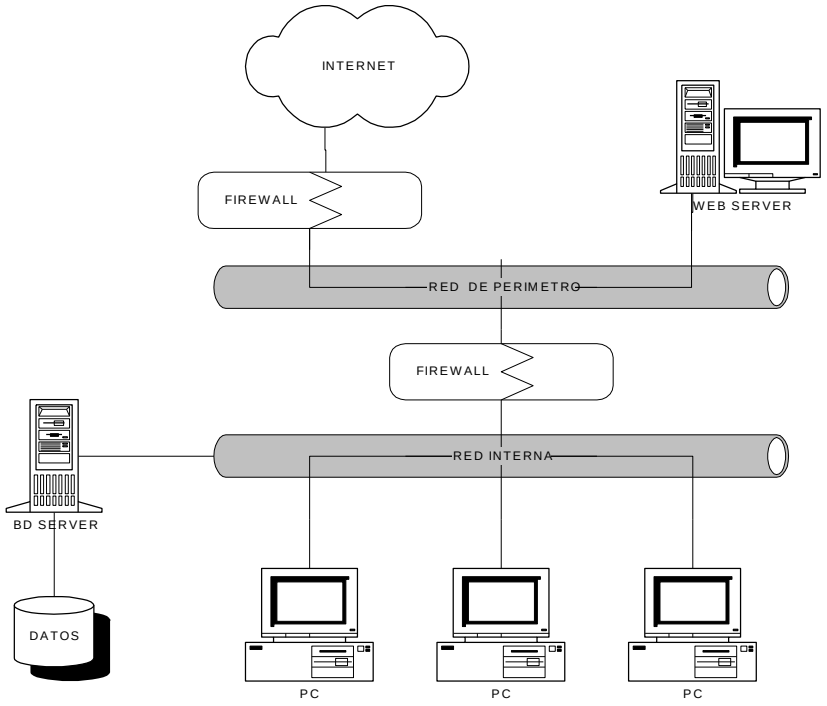

Figura No.12 Configuración de doble Firewall