# CAPITULO I

# GENERALIDADES DE LA RED DE COMPUTADORES

## 1.1 REDES DE COMPUTADORES.

### 1.1.1 INTRODUCCION A LAS REDES.

La evolución en las ultimas décadas de los sistemas de información constituyeron sistemas basados en servidores centralizados, conectados a un modo remoto que era común a todos, compartiendo el tiempo de proceso de la única unidad central. A sistemas corporativos de computación descentralizados, en los cuales los recursos de información y computadoras se encuentran distribuidos por toda la organizació n.

Por los años 70, aparece la microinformática y con ello los mini-ordenadores, facilitando una arquitectura ligera y flexible, asiendo posible la descentralización de los procesos mediante herramientas evolutivas adaptadas a tecnologías nuevas, los equipos inicialmente desarrollados, consistían en servidores de terminales que conectaban terminales no inteligentes mediante cable coaxial.

En los años 80, los usuarios fueron ganando importancia en la era de la información con la computadora personal almacenando grandes cantidades de información en sus propios ordenadores, apareciendo con esto las primeras redes de área local ( LAN ) constituyendo un sistema de comunicación integrado por distintos usuarios (terminales, servidores, etc.) permitiendo la transferencia en altas velocidades de los datos, en distancias cortas, surgiendo el problema de robo de datos, corrupción y escuchas que en cierta medida se incrementaba.

La sociedad a dedicado su esfuerzo, en lograr el desarrollo de medios que permitan la comunicación entre áreas geográficamente distantes, como: el espacio exterior, internacionales, nacionales, locales; iniciándose en la telefonía analógica, siguiendo una evolución hasta llegar en la actualidad a lo que se lo conoce como Internet, que es un ambiente de “red de redes”.

El acople o unión de redes se lo hace mediante dispositivos de interconexión. Las redes se diferencian ya sea, por su protocolo de comunicación, el medio de transmisión, la tecnología que aplica, el sistema operativo que maneja, entre otros.

### 1.1.2 CONCEPTO DE REDES.

Es un sistema de permite acceder a la comunicación de datos que enlaza dos o más computadoras y diferentes dispositivos, logrando así que estas puedan compartir el trabajo y la información, libre de su arquitectura, características físicas y lógicas, como topologías, sistemas de transmisión, acceso y conmutación, medios de transmisión y modelos matemáticos del comportamiento de la red para evaluar sus parámetros de calidad.

### 1.1.3 MEDIOS DE TRANSMISIÓN.

Se refiere al medio físico que transporta la información, de modo que puede condicionar la distancia, velocidad de transferencia, topología e incluso el método de acceso. Los principales medios de transmisión son:

**Cable Par Trenzado.** — Filamentos de cobre, cubiertos cada uno por plástico aislante y entrelazado el uno con el otro.

**Cable Coaxial.** — Cable en un ambiente completamente cerrado, una pantalla sólida, bajo una cubierta exterior.

| | |
|---|---|
| **Cable de Fibra Óptica** | Filamento de vidrio sumamente delgado diseñado para la transmisión de luz. |
| **Tecnología de Radio.** | Utilizada en redes inalámbricas. |

### 1.1.4 CLASIFICACIÓN DE LAS REDES.

Su clasificación se establece en función de dimensión, radio de acción, y localización geográfica, (distancia entre nodos).

| | |
|---|---|
| **Red de Área Local LAN.** | Se expande en un área relativamente pequeña. Éstas se encuentran comúnmente dentro de una edificación o un conjunto de edificaciones que estén contiguos, proporciona interconexión a una variedad de dispositivos. |
| **Red de Área Metropolitana MAN.** | De tamaño superior a una LAN, soliendo abarcar el tamaño de una ciudad. Es típica de empresas y organizaciones que poseen oficinas distintas repartidas en una misma área metropolitana, por lo que en su tamaño máximo comprenden un área de unos 10 kilómetros. |
| **Red de Área Extendida WAN** | Red de campus, metropolitana o extendida comprende un espacio geográfico mayor, debido a que las organizaciones grandes tienen la necesidad de interconectar sistemas en edificios distintos, en campus de universidades y empresas. |

| Características | Red de área local | Red de área extendida |
|---|---|---|
| Tipo de información transportada. | Datos primordialmente. | Voz, datos y video conjuntamente integrados. |
| Área geográfica de cobertura. | Localizado en un edificio, grupo de edificios o campus. | Ocupa un área que varía en tamaño desde una ciudad a todo el planeta. |
| Taza de transmisión de datos. | Desde 4 Mbps a 16 Mbps, con redes de fibra óptica operando a 100Mbps. | Operan a tasas de transmisión de T1 y E1 o pro debajo de ellas de 1544 Mbps y 2.048 Mbps. |
| Taza de errores. | Desde un bit en $10^7$ hasta 1 en $10^8$ . | Desde un bit en $10^8$ hasta 1 en $10^7$. |
| Propietario. | Por lo regular el que la implementa. | Existe un dueño de las líneas de comunicación y otro de las computadoras conectadas. |
| Ruteo de datos. | Sigue una ruta fija. | La capacidad de switcheo de la red permite alteraciones dinámicas del flujo de datos. |
| Topología. | Limitada a bus, anillo, árbol o estrella. | Capacidad virtualmente ilimitada en el diseño. |

**Tabla 1: Comparando LAN's y WAN's.**

### 1.1.5 PRINCIPALES TOPOLOGÍAS DE RED.

La topología de una red define la distribución de cada estación en relación a la red y a las demás estaciones, todas ellas tienen sus ventajas e inconvenientes. La elección de una topología se encuentra en gran parte influenciada por el tipo de acceso al medio utilizado, número de host a interconectar, etc.

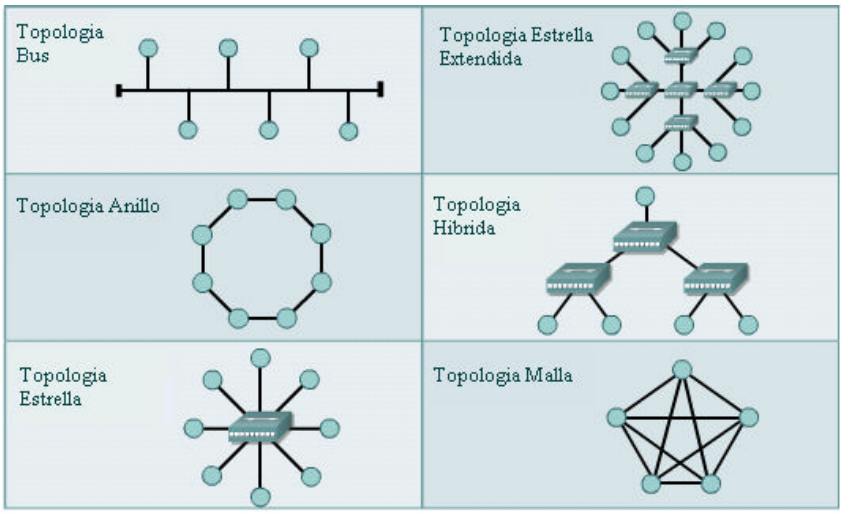


**Figura 1: Topologías de Red.**

### 1.1.6 TECNOLOGÍAS FUNDAMENTALES DE RED

#### 1.1.6.1 Tecnología Ethernet.

Esta tecnología ha tenido un crecimiento, desarrollo y una evolución formidable, con respecto a la velocidad de transmisión de datos,

medios de transmisión (coaxial, UTP, fibra óptica), en solución fácilmente los embotellamientos de conexiones de red, sus categorías son:

- Ethernet IEEE 802.3
- Fast Ethernet IEEE 802.3 u
- Gigabit Ethernet IEEE 802.3 z

| **TECNOLOGÍAS CARACTERÍSTICAS** | **ETHERNET (IEEE 802.3)** | **FAST ETHERNET (IEEE 802.3 u)** | **GIGABIT ETHERNET (IEEE 802.3 z)** |
|---|---|---|---|
| Solución Ethernet | 10 base - T | 100 base – T | 1000 base – T |
| Velocidad de transferencia | 10 Mbps | 100 Mbps | 1000 Mbps |
| Distancia máxima | 100 Metros | 100 Metros | 100 Metros |
| Medio | UTP(par trenzado) Categoría 3/4/5 | UTP Categoría 3/4/5 | UTP Categoría 4/5 |
| Topologías | Bus,Estrella, Árbol | Estrella | Estrella |

**Tabla 2: Comparación de tecnologías Ethernet.**

#### 1.1.6.2 100VG – AnyLAN.

Ante la necesidad de coexistencia con las redes locales tradicionales, Ethernet y Paso a Testigo (Token Ring), y las ventajas que implica el acceso controlado y el sistema de prioridades, surge este nuevo estándar para alta velocidad. Su acceso al medio lo realiza mediante un nuevo método llamado DPAM (Método de Acceso Prioritario por Demanda). Definida por la IEEE como el estándar 802.12.

#### 1.1.6.3 Token Ring.

Esta emplea una topología lógica de anillo pero físicamente utiliza una topología en estrella, tiene coordinación con el estándar IEEE 802.5, su velocidad de transmisión de datos es de 4Mbps – 16Mbps.

Token Ring, siempre tienen una estación que controla el buen funcionamiento de la red, mediante el token cada estación espera su turno, su desarrollo mejora en entornos de alta carga, utiliza enlaces punto a punto entre cada estación y la siguiente.

#### 1.1.6.4 Token Bus.

En el Token bus, las estaciones del bus forman un anillo lógico, es decir, cada estación tiene designada una posición lógica,

independientemente de la física, dentro de una secuencia ordenada y circular, en la que a la ultima estación le sigue la primera. Cada una de las estaciones conoce la dirección de su estación antecesora y de su estación sucesora.

#### 1.1.6.5 Tecnología FDDI: Fiber Distributed Data Interfase (Interfase de datos distribuida por fibra).

El funcionamiento de FDDI esta basado en un doble anillo que proporciona una conexión para el intercambio de información a alta velocidad (100 mbps), entre 500 estaciones como máximo, sobre distancias de hasta 100 Km. Es una tecnología usada tanto para LAN como MAN especialmente.

#### 1.1.6.6 Tecnología X.25

Diseñada para redes de área extensa, con baja fiabilidad y relativamente desciende capacidad de ancho de banda, creada para que los sistemas operen con enlaces muy cargados y con sofisticados métodos de control de error y control de flujo, mejorando la situación, reduciendo los procesos en los nodos de conmutación y permitiendo mayores velocidades de acceso.

#### 1.1.6.7 Tecnología Frame Relay.

Esta diseñada para delegar el control de flujo y errores a los terminales, mientras que la red es únicamente responsable de la transmisión y conmutación de datos. De ocurrir un error o la saturación de los nodos de la red, han de ser los terminales, de los usuarios que gestiones estas situaciones, reenviando las tramas erróneas o bien reduciendo la velocidad de transmisión para evitar las congestiones.

#### 1.1.6.8 Tecnología ATM, (Asynchronous Transfer Mode), Modo de Transferencia Asíncrono.

Las aplicaciones para diferentes servicios como voz, datos, imagen estática o video, tratan de encontrar la solución universal en todo tipo de ambientes como, LAN, MAN o WAN. Siendo ATM la tecnología mejor perfilada y opcionada para esta interoperación por su capacidad de integración de diferentes tipos de trafico, la asignación dinámica y flexible del ancho de banda, la optimización del compromiso entre caudal y latencia, su capacidad de optimizar la relación entre la suma de las velocidades de pico de las fuentes y la velocidad de enlace.

### 1.1.7 DISPOSITIVOS DE INTERCONEXIÓN.

Al experimentar las redes un crecimiento, es primordial que brinden una expansión que permita superar sus limites, como la longitud del cable y número de estaciones de trabajo. Con este fin se han desarrollado diferentes dispositivos, como:

| | |
|---|---|
| **Repetidores (Repeaters).** | Dispositivos encargados de regenerar y amplificar la señal circulante por la red. |
| **Puentes (bridges).** | Sus funciones básicas son las de autoaprendizaje, filtrado y reenvío de tramas. |
| **Encaminadores (Routers).** | Incorpora funciones de filtrado, además determina la ruta hacia el destino, empleándose tanto en redes de área local como de área extensa. |
| **Pasarelas (gateways)** | Realizan la traducción completa entre familias de protocolos, proporcionando conectividad extremo a extremo entre redes de distinta naturaleza, están definidas para un escenario de comunicaciones concreto. |

| Características | Repetidor | Puente | Encaminador | Pasarela |
|---|---|---|---|---|
| Nivel modelo OSI | Físico | Enlace | Red | Superiores |
| Gestión de | Bits | Tramas | Paquetes | Mensajes |
| Direccionamiento | Ninguno | MAC | Red | Aplicación |
| Gestión de tráfico | No | Si | Si | SI |
| Rendimiento | Alto | Alto | Medio | Bajo |
| Trafico de difusión | Todo | Alto | Bajo | Bajo |
| Coste | Bajo | Medio | Alto | Alto |
| Dependencia de protocolos | Ninguna | MAC | Red | Superiores |
| Segmentación de mensajes | No | No | Si | Si |

**Tabla 3: Características de los principales sistemas de expansión de red**

### 1.1.8 EQUIPOS DE GESTIÓN DE SERVICIOS (SERVIDORES).

El servidor es la máquina principal de la red, la que se encarga de administrar los recursos de la red y el flujo de la información.

Muchos de los servidores son "dedicados", es decir, están realizando tareas específicas, por ejemplo, un servidor de impresión sólo para imprimir; un servidor de comunicaciones, sólo para controlar el flujo de los datos, etc. Actualmente a los servidores se los consideran como “procesos” que proporcionan servicios, en lugar de equipos específicos.

Para que una máquina sea un servidor, es necesario que sea una computadora de alto rendimiento, en cuanto a velocidad y procesamiento, y gran capacidad en disco duro u otros medios de almacenamiento.

### 1.1.9 SERVICIOS QUE BRINDA UNA RED DE COMUNICACIÓN.

Las aplicaciones de computadoras requieren una combinación de datos, capacidad de procesamiento y recursos de entrada y salida para realizar sus tareas. Los servidores de red permiten a las computadoras compartir estos recursos utilizando aplicaciones de red especiales.

Las redes en general pueden ofrecer las siguientes categorías de servicios:

#### 1.1.9.1 Servicios Básicos de Transmisión – SBT.

Estos servicios son principalmente ofrecidos por los portadores o "carriers" de telecomunicaciones, son servicios en los cuales el objetivo principal es lograr conectividad entre dos o más entidades, resolviendo el problema de transporte de bits de información de un extremo a otro sin alterarlo o procesarlo. Algunos ejemplos de estas redes son: Sistema Telefónico, líneas dedicadas, N-ISDN, canales satélite o microondas, X.25, Frame Relay, SMDS entre otras.

#### 1.1.9.2 Servicios de Valor Agregado – SVA.

Son aquellos servicios que además de resolver posiblemente el problema de conectividad, procesan o alteran la información

transportada para el logro de algún objetivo, podemos nombrar entre estos servicios: archivos, impresoras, Internet, correo electrónico, software, aplicaciones distribuidas, teleconferencia, etc..

### 1.1.10 ARQUITECTURA Y MODELO DE REDES.

Al conjunto de todos los protocolos y niveles se les denomina "Arquitectura de Redes" y dan lugar a una solución completa en la implementación de sistemas telemáticos y teleinformáticos, algunas de estas arquitecturas o familias de protocolos son:

#### 1.1.10.1 Modelo de Arquitectura TCP/IP

Desarrollado por el Departamento de Defensa de EE.UU.. El Protocolo de Control de Transmisión y Protocolo de Internet (TCP/IP) es una familia de protocolos creados para permitir la comunicación entre cualquier par de computadores de cualquier fabricante respetando los protocolos de cada red individual. Protocolo de mayor crecimiento y ampliamente usado, compatible con el modelo OSI.

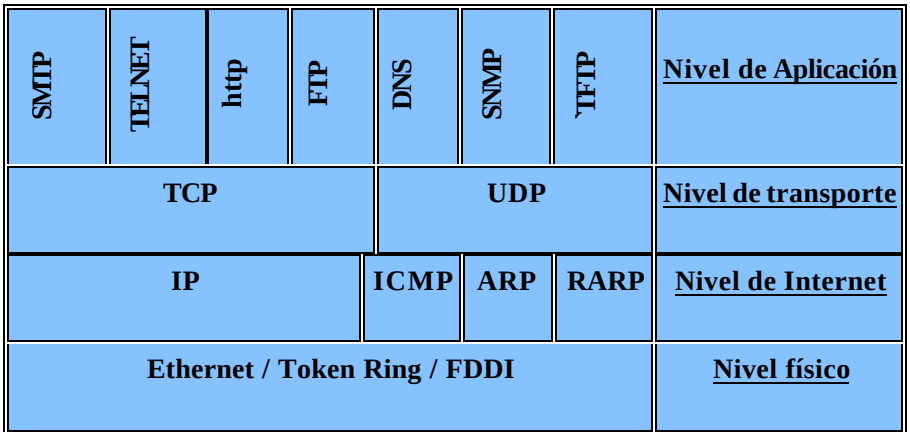


**Tabla 4: Suite de protocolos TCP/IP**

### 1.1.10.1.1 Sistema de Telecomunicaciones INTERNET.

El sistema de comunicaciones INTERNET esta formado por múltiples redes de paquetes interconectadas entre sí a través de elementos denominados gateway. Las direcciones Internet son las direcciones que utiliza el protocolo IP para identificar de forma única e inequívoca un nodo o host de la red, que en la mayoría de las ocasiones, será un computador, pero en otras pude ser un encaminador en la internet. Cada host en la internet tiene asignada una dirección, las dirección IP, que consta de dos partes que son:

| Dirección de Red | Dirección del host |
|---|---|

**Tabla 5: Estructura de la dirección Internet.**

Los protocolos más importantes del nivel Internet son los siguientes:

- IP (Protocolo Internet).
- ICPM (Protocolo de Mensajes de Control Internet).
- ARP (Protocolo de resolución de Direcciones).
- RARP (Protocolo Inverso de Resolución de Direcciones).

#### 1.1.10.1.2 Protocolo IP.

El protocolo IP siempre trabaja con entrega de datagramas (sin conexión previa) que viajan de extremo a extremo de la red. Los datagramas enviados por IP pueden perderse, llega desordenados o duplicados. IP no se responsabiliza de estas situaciones, que tendrán que ser contempladas por el nivel TCP. No obstante, la red realiza su mejor esfuerzo para intentar que los datagramas IP alcancen su destino.

##### 1.1.10.1.2.1 Mecanismo de Direcciones IP.

Cada host posee una dirección IP, que es la encargada de identificar la red y el host. Las direcciones IP son siempre

direcciones de 32 bits de longitud, representadas por decimales seguidas de un punto.

*123.003.002.008*

Cada dirección IP consta de dos direcciones lógicas:

*Dirección IP = <dirección de la red><dirección del host>*

En algunos sistemas también se puede identificar la subred en la que esta ubicado el host:

*Dirección IP = <dirección de la red><dirección de la subred><dirección del host>*

Esta segunda forma de direccionamiento surge como consecuencia del enorme crecimiento de Internet y a la realización de la división de la red en dos redes o más, de menor tamaño facilitando los cambios en las configuraciones de las redes.

#### 1.1.10.1.2.2 Formatos de las Direcciones IP.

Existen cinco tipos de formatos diferentes para las direcciones IP que las dividen en las siguientes clases:

**CLASE A:** Contiene 7 bits para direcciones de red (lo que permite un máximo de $2^7$=128 redes), cada una de las cuales puede tener $2^{24}$= 6.777.216 computadores. Se utiliza cuando se tiene muchos host.

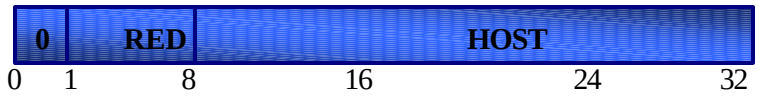


**Figura 2: IP clase A**

**CLASE B:** Tiene 14 bits para direcciones de red y 16 para direcciones de host. Esto permite un máximo de $2^{14}$-2=16.582 redes de cómo máximo $2^{16}$-2=65.534 host por red.

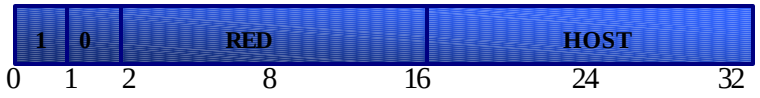


**Figura 3: IP clase B**

**CLASE C:** Posee 21 bits para direcciones de red y 8 bits para direcciones de host. Esto permite un máximo de $2^{21}$-2=2.097.150 redes de $2^8$-2=254 host.


**Figura 4: IP clase C**

**CLASE D:** Se reservan todas las direcciones para multidestino (multicasting), esto es, un computador transmite un mensaje a un grupo específico de computadores, entre computadores de la clase D.


**Figura 5: IP clase D**

**CLASE E:** esta clase se utiliza con fines experimentales, su formato es el siguiente.


**Figura 6: IP clase E**

### 1.1.10.1.2.3 Máscara en las Direcciones IP.

Para conseguir incrementar el número de computadores conectados se emplea una máscara en la dirección IP. La mascara es un mecanismo compuesto de “ceros” y de “unos” mediante el cual los “unos” indican la parte de dirección de red y subred, y los “ceros” se corresponden con las direcciones del host. Estos nuevos bits de red definen redes, denominadas subredes, dentro de grandes redes.

#### 1.1.10.2 Modelo de Sistemas Abiertos, OSI.

Desarrollado por la Organización Internacional de Estándares (International Organization for Standarization ), como una base para el desarrollo de estándares internacionales para soportar comunicaciones entre sistemas abiertos, es decir, permite comunicar múltiples computadores heterogéneos en un ambiente de aplicaciones distribuidas.

#### 1.1.10.3 Otras Arquitecturas.

A continuación otras arquitecturas de redes difundidas.

- XNS (Xerox Network System) de Xerox.
- SNA (System Network Architecture) de IBM.
- DNA (Digital Network Architecture) de DEC.
- IPX/SPX (Internet Packet eXchange / Sequenced Packet eXchange).de Novell.
- Algunas variaciones: Redes Microsoft, Novell y Banyan.

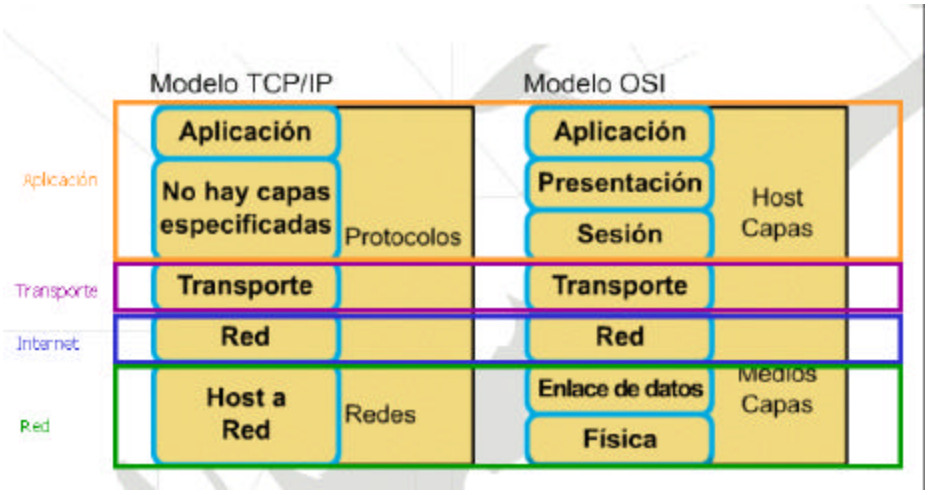


**Figura 7: Modelo OSI y la Arquitectura TCP/IP.**

### 1.1.11 CABLEADO ESTRUCTURADO.

Permite la administración flexible y eficiente para integrar y organizar las redes de información, otorgando una total independencia del tipo y marca de los dispositivos que la integren así como de las plataformas lógicas a utilizar.

Ofrecen una buena alternativa de seguridad física, a la vez una buena base para ahorrar costos futuros, permitiendo cambiar, identificar o mover equipos, periféricos de red con maleabilidad y sencillez, permitiendo el crecimiento no traumático de la red con modularidad y flexibilidad.

En si se trata de especificar una “estructura” o “sistema” de cableado para empresas y edificios que sean:

- Común y a la vez independiente de las aplicaciones.
- De gran ancho de banda.
- Documentada.
- Proyectada a largo plazo (más de 10 años).

#### 1.1.11.1 Elementos del Cableado Estructurado.

##### 1.1.11.1.1 Cableado Horizontal o de Planta.

El cableado horizontal incorpora el sistema de cableado que se extiende desde la salida de área de trabajo de telecomunicaciones (Work Area Outlet, WAO) hasta el cuarto de telecomunicaciones.

El término “horizontal” se utiliza porque típicamente este cableado se desplaza de una manera horizontal en el edificio. El cableado horizontal es típicamente el más difícil de mantener debido a la complejidad de trabajo en una oficina en producción. Es sumamente necesario que se tome en cuenta no solo las necesidades actuales sino las futuras para no causar molestias a los usuarios en el trabajo diario.

- **Topología:**

  - La topología del cableado siempre será de tipo estrella.
  - Un cable para cada salida en los puestos de trabajo.
  - Todos los cables de la corrida horizontal deben estar terminados en cajillas y paneles.

#### 1.1.11.1.2 Cableado Vertical o Backbone.

El propósito del cableado del backbone es proporcionar interconexiones entre cuartos de entrada de servicios del edificio, cuartos de equipo y cuartos de telecomunicaciones. Este incluye la conexión vertical entre pisos en edificios de varios pisos, así como también, medios de transmisión (cable), puntos principales e intermedios de conexión cruzada y terminaciones mecánicas. El cableado vertical es típicamente menos costoso de instalar y debe poder ser modificado con más flexibilidad.

- **Topología.**

  - La topología del cableado vertical debe ser típicamente una estrella.
  - En circunstancias donde los equipos y sistemas solicitados exijan un anillo, este debe ser lógico y no físico.

#### 1.1.11.1.3 Cuarto de Telecomunicaciones.

Es el área en un edificio utilizada para el uso exclusivo de equipo asociado con el sistema de cableado de telecomunicaciones. El espacio del cuarto de comunicaciones no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones. El cuarto de telecomunicaciones debe ser capaz de albergar equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado, el diseño de dicho cuarto debe considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable (CATV), alarmas, seguridad, audio y otros sistemas de telecomunicaciones.

#### 1.1.11.1.4 Cuarto de Equipos.

Es un espacio centralizado de uso específico para equipo de telecomunicaciones tal como central telefónica, equipo de cómputo y/o conmutador de video. Varias o todas las funciones de un cuarto de telecomunicaciones pueden ser proporcionadas por un cuarto de equipo. Los cuartos de equipo se consideran distintos de los cuartos de telecomunicaciones por la naturaleza, costo, tamaño y/o complejidad del equipo que contienen, estos cuartos incluyen

espacio de trabajo para personal de telecomunicaciones. Todo edificio debe contener un cuarto de telecomunicaciones o un cuarto de equipo.

Los requerimientos del cuarto de equipo se especifican en los estándares ANSI/TIA/EIA-568-A y ANSI/TIA/EIA-569.

#### 1.1.11.1.5 Cuarto de Entrada de Servicios.

Consiste en la entrada de los servicios de telecomunicaciones al edificio, incluyendo el punto de entrada a través de la pared y continuando hasta el cuarto o espacio de entrada. El cuarto de entrada puede incorporar el "backbone" que conecta a otros edificios en situaciones de campus.

Los requerimientos de los cuartos de entrada se especifican en los estándares ANSI/TIA/EIA-568-A y ANSI/TIA/EIA-569.

#### 1.1.11.1.6 Áreas de trabajo.

Son los espacios donde se ubican los escritorios, boxes, lugares habituales de trabajo, o sitios que requieran equipamiento de telecomunicaciones.

#### 1.1.11.1.7 Sistema de Puesta a Tierra y Punteado.

El sistema de puesta a tierra y puenteado establecido en el estándar ANSI/TIA/EIA-607 es un componente importante de cualquier sistema de cableado estructurado moderno.

## 1.2 SEGURIDADES EN LA RED DE COMPUTADORES.

### 1.2.1 INTRODUCCION A LA SEGURIDAD DE RED.

Seguridad de red informática es la combinación de lineamientos que una empresa o institución sigue para protegerse de amenazas tales como: naturales (producidas por la naturaleza), hacking (piratas informáticos), cracking (violadores de códigos), spoofing (falsificadores informáticos), sniffing (realizadores de escuchas), virus informáticos (Troyanos, gusanos, etc.) actividades realizadas por la sociedad de criminales, espías industriales y terroristas internacionales que quieren destruir los sistemas en su beneficio o por placer, comprometiendo de esta manera la integridad de la información.

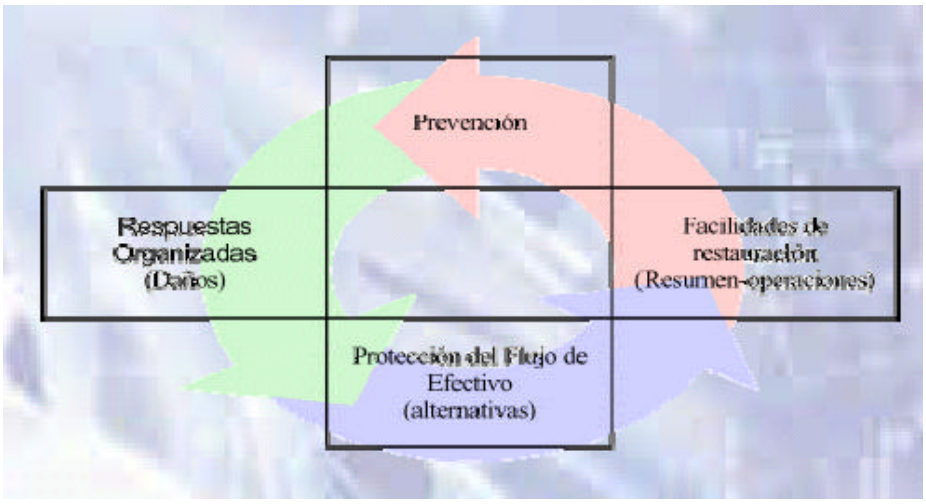


**Figura 8: Ciclo de vida de la seguridad**

### 1.2.2 PROBLEMAS DE SEGURIDAD.

Veremos algunas de las más comunes amenazas a la seguridad de los sistemas de computadores y de las redes informáticas.

- Amenazas Lógicos.
- Amenaza Físicas.

#### 1.2.2.1 Amenazas Lógicas.

Se refiere a datos de los sistemas que están vulnerables y son perpetrados por personas expertas en técnicas de seguridad, usan

herramientas y técnicas para asaltarlos, aprovechándose de estos puntos de entrada.

Entre las áreas vulnerables de las redes corporativas describimos algunas:

- Contraseñas Famosas (y fáciles de adivinar) o contraseñas débiles, que comprometen la identificación y el inicio de sesión del usuario.
- Inicios de sesión pobremente implementados, derechos de cuentas de usuario y permisos de acceso a archivos.
- Discos y correo electrónico que contengan virus.
- Puertas abiertas a redes internas creadas por usuarios que acceden a Internet o por cortafuegos Internet pobremente implementados.
- Computadoras móviles y remotas de acceso telefónico que han sido robadas junto a su información de inicio de sesión.
- Técnicas de encaminamiento inseguras e ineficientes que proporcionan caminos de acceso a los piratas informáticos a sus sistemas.
- Estrategias de duplicación de datos que duplican virus por la red.

- Errores de programas que aprovechan los piratas informáticos para acceder a sus sistemas.
- Puertas traseras que han sido dejadas abiertas en aplicaciones por sus programadores.
- Puertos de mantenimiento de equipos de red y PBX que son utilizados por personal de servicio para acceder a dispositivos en modo local o remoto.
- Módem conectados directamente en redes o en computadores de una red y colocados en modo de auto-respuesta.

#### 1.2.2.2 Amenazas Físicas y Ambientales.

No todas las amenazas a la integridad de la red provienen de la gente. Fallos en la alimentación eléctrica, fallos en los componentes, y otros problemas pueden arruinar el sistema y costar a la empresa millones de dólares.

En la siguiente lista se muestra la mayoría de amenazas naturales:

- La energía eléctrica puede perderse durante tormentas u otras causas. Las fuentes de alimentación para copias de seguridad son imprescindibles.

- Los fallos en el hardware pueden producir pérdidas en la disponibilidad de los datos. Los sistemas redundantes y las copias de seguridad son obligatorias.
- Los fuegos, las inundaciones, los temblores y otros desastres necesitan sistemas de copias de seguridad, centros alternativos de datos y plantas de recuperación ante catástrofes.

#### 1.2.2.3 Virus Informativos.

Son programas pequeños, que ejecutan alguna acción inmediata o esperan un momento especifico o a que el usuario ejecute una determinada instrucción para causar daño, una de sus características es duplicarse así mismo e irradiarse, por lo que son especialmente peligrosos en las redes, debido a que una vez que contaminan un sistema, se puede extender por toda la red, el método de infección ocurre por la falta de protección del sistema, información procedente de Internet, medios magnéticos infectados, etc.

| VIRUS | |
|---|---|
| **Virus del sector de arranque.** | Estos virus infectan el registro de arranque maestro de una computadora sobrescribiendo el código de arranque original. |
| **Virus de infección de archivos.** | Tipo de virus que infecta a archivos de disco, usualmente a archivos ejecutables con extensiones COM, EXE, OVL. Los archivos de sistema son también su objetivo. |
| **Virus Polimórficos.** | Este virus cambia su apariencia para evitar detecciones del software antivirus, se encripta así mismo con un algoritmo especial que cambia cada vez que se produce una infección. |
| **Virus ocultos.** | Estos intentan ocultarse así mismos del sistema operativo y del software antivirus, permanecen en memoria para interceptar los intentos de uso del sistema operativo y ocultan los cambios hechos en el tamaño de los archivos. |
| **Virus multi-formes.** | Infectan tanto a sectores de arranque como a archivos ejecutables. Son un problema real porque usan el polimorfismo y la ocultación para evitar ser detectados. |
| **Virus de macros.** | Es un nuevo tipo de virus, que atacan a los documentos creados en Microsoft Word y Excel. |
| **OTRAS AMENAZAS (programas destructivos no clasificados como virus)** | |
| **Gusanos.** | Suelen confundirse con un virus. Es un único programa destructivo de un solo sistema con frecuencia dejado allí por alguien que tiene acceso directo al sistema, no se replican así mismo como, los virus. |
| **Caballos de Troya** | Es un programa que puede aparentar ser otro. Un usuario que no sospeche ejecutara el programa sin saber su potencial de peligro. En algunos casos los caballos de troya no son destructivos, en su lugar recogen información como contraseñas de inicio o copian archivos sensibles a otro sistema o red sin que el usuario host sepa lo que pasa |
| **Bombas Lógicas.** | Una bomba lógica es básicamente un caballo de troya con n temporizador. Estalla en un momento determinado y hace su daño que puede ser, destruir datos en discos locales o diseminar virus. Un empleado descontento puede crear una bomba que estalle cuando se haya ido de la compania. |

**Tabla 6: Una de las pocas clasificaciones de virus resumidas por organizaciones como NCSA y CSI.**[2]

[2] Tom Sheldon; Manual de seguridades de Windows NT, Pagina 573,traducida de la primera edición en ingles; Editorial Osborne/McGraw Hill, España.

#### 1.2.2.4 Piratas Informáticos.

El pirateo es visto como un deporte electrónico para la gente que lo práctica**,** con frecuencia, estos intentan conseguir un beneficio u obtener servicios gratis, suelen vender información obtenida durante sus ataques a competidores o extranjeros.

Se los clasifica con diferentes términos, midiendo el efecto de sus ataques a los sistemas informáticos, como: **Hacker**, que acceden a un sistema protegido, pero como un reto personal, sin causar ningún tipo de daños, **Craker**, son aquellos que ingresan a los sistemas con el claro objetivo de producir daños en el mismo, **Spoofing**, realizan falsificaciones como cuentas de tarjetas de crédito, **Sniffing**, conocidos como los radio escuchas, **Phreaker**, personas que sacan ventaja del sistema de telecomunicaciones para hacer llamadas de larga distancia gratis, y un nuevo aspecto es la destrucción de códigos para romper claves de encriptación llevada a cabo por los llamados **Cypherpunks.**

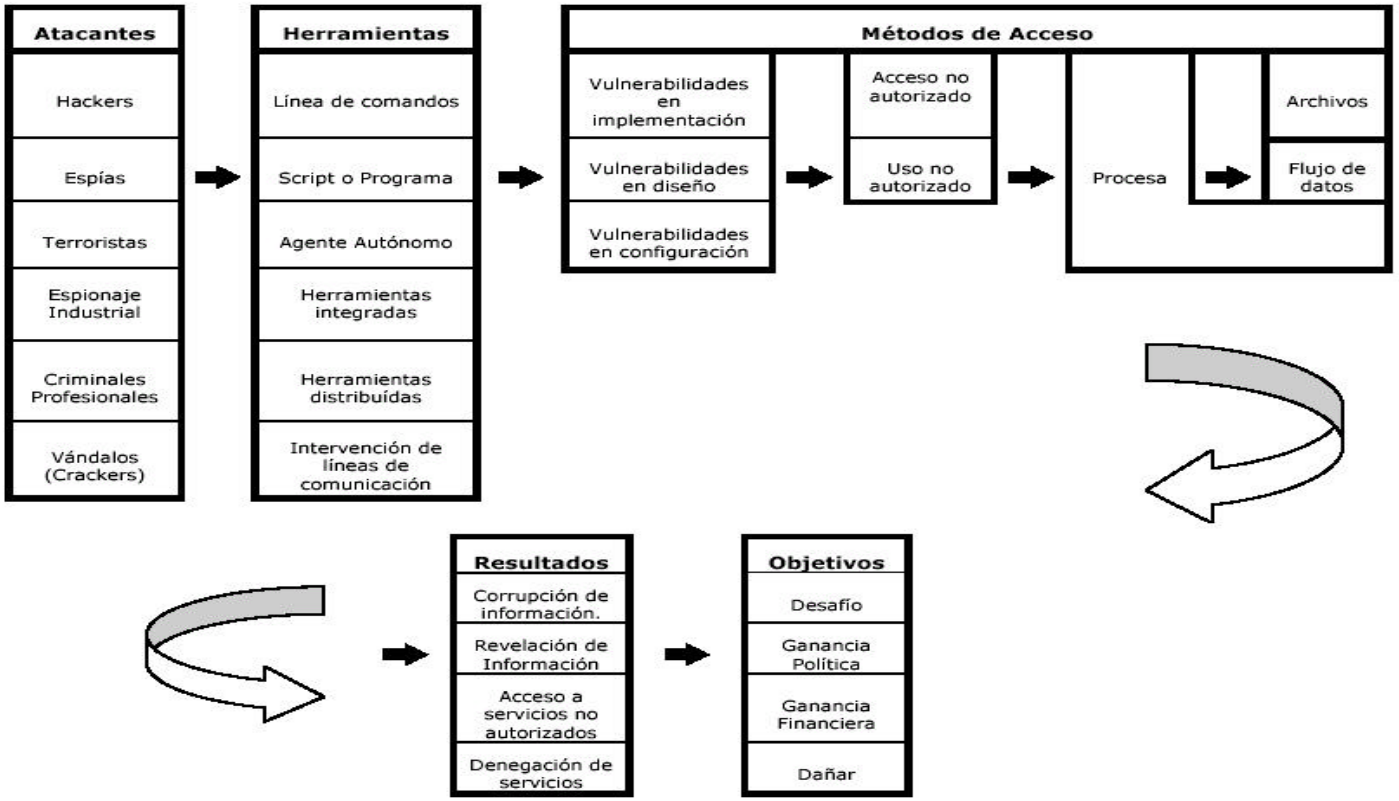


**Figura 9: Aquí se detalla el tipo de atacante, las herramientas utilizadas, en que fase se realiza el ataque, los tipos de procesos atacados, los resultados esperados y/u obtenidos y los objetivos perseguidos por los intrusos.**

En la tabla 7 se observa el tiempo de búsqueda de una clave de acuerdo a su longitud y tipo de caracteres utilizados. La velocidad de búsqueda se supone en 100.000 passwords por segundo, aunque este número suele ser mayor dependiendo del programa utilizado.

| Cantidad de caracteres | 26-Letras minúsculas | 36-Letras y dígitos | 52-Mayúsculas y minúsculas | 96-Todos los caracteres |
|---|---|---|---|---|
| 6 | 51 minutos | 6 horas | 2,3 días | 3 meses |
| 7 | 22,3 horas | 9 días | 4 meses | 24 años |
| 8 | 24 días | 10,5 meses | 17 años | 2,288 años |
| 9 | 21 meses | 32,6 años | 890 años | 219.601 años |
| 10 | 45 años | 1.160 años | 45.840 años | 21.081.705 años |

**Tabla 7: Tiempos de Búsqueda**

#### 1.2.2.5 Cortafuegos (Firewall).

Un cortafuegos es una máquina segura y confiable que se asienta entre una red privada y una red pública. El cortafuegos se configura con un conjunto de reglas que determinan a qué tráfico de red se le permitirá pasar y cuál será bloqueado o rechazado. En algunas organizaciones grandes, puede que encuentre un cortafuegos localizado dentro de la red corporativa para separar áreas sensibles de la organización de otros empleados. Algunos casos de

criminalidad informática acontecen dentro de la misma organización, no sólo provienen de fuera.

Actualmente existen dos tecnologías empleadas en los firewalls, filtrado de paquetes y nivel aplicativo. Dependiendo de las configuraciones utilizadas por os proveedores, éstos se pueden clasificar en: firewalls de filtrado de paquetes, firewalls de nivel aplicativo, híbridos y de nivel aplicativo de segunda generación.

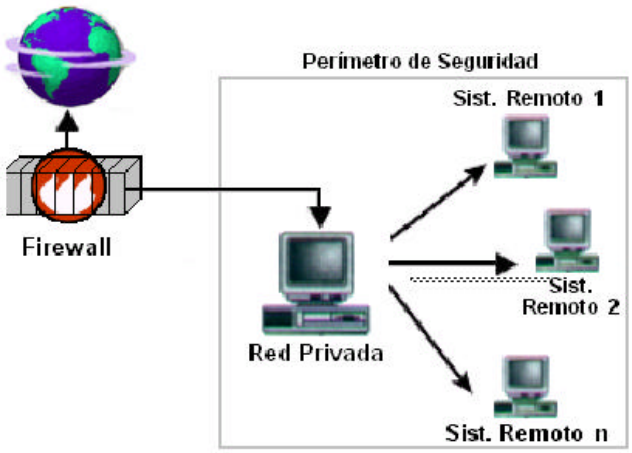


**Figura 10: FIREWALL.**

### 1.2.3 SEGURIDADES FÍSICAS Y AMBIENTALES.

Dentro de lo que es la seguridad física, se hace referencia a la protección de los sistemas (HARDWARE) y datos, de robos, corrupción y desastres naturales. Comienza con el reforzamiento de la

seguridad en sus localizaciones físicas. Guardias de seguridad, sistemas de acceso con clave y equipos de vigilancia, sistemas contra incendios, suministros de energía, son necesariamente requeridos si la ubicación de estos está abierta al público o si la información es extremadamente sensible, un claro ejemplo seria, si los piratas informáticos puede entrar en el edificio sin ser detectados, tendrán libre acceso a las computadoras, los sistemas de cableado, teléfonos y otros equipos, así como, archivos e información útil en las computadoras de sobremesa o listas de distribución, también pueden instalar virus o borrar un disco duro de un sistema por completo.

Otros puntos relacionados con la seguridad física están resumidos a continuación y se refiere tanto a computadoras de sobremesa como servidores.

- Configurar el arranque de la computadora en la memoria CMOS para que pregunte por contraseñas o configurar opciones especiales del sistema, bloquee la computadora para que nadie pueda borrar el CMOS quitando la pila.
- Activación de contraseñas de arranque y otras prioridades de seguridad en PC.

- Desactive o quite las unidades de disco flexible para prevenir que se puedan copiar archivos del disco y para prevenir que los usuarios puedan volcar virus a través de archivos.
- Si los usuarios deben tener acceso a la unidad de disco flexible, active el CMOS de modo que el sistema siempre arranque desde el disco C. Esto previene para que los intrusos no puedan arrancar un sistema con su propio disco de sistema operativo.
- Asegurar que los equipos y cables de red no puedan ser espiados. Controlar siempre las actividades del personal de servicio. No confiar en nadie que quiera acceder a los equipos.
- El cambio y las movilizaciones de equipos se realizaran a cargo del personal debidamente autorizado.
- Instalación de sistemas contra incendios, inundaciones, aire acondicionado, condiciones climatológicas.
- Controles de acceso como guardias de seguridad, utilización de detectores de metales, verificación de firmas, puertas electrónicas.

### 1.2.4 SEGURIDADES LÓGICAS.

Con respecto a las seguridades lógicas, implican la protección de la información mediante la implantación controles a través de mecanismos de programación (SOFTWARE), para fortalecer la protección de los

datos, procesos y programas, determinando el tipo de acceso de los usuarios y los niveles de autorización a la información.

Se define cinco servicios de seguridad:

- Autentificación.
- Control de acceso.
- Confidencialidad de los datos
- Integridad de los datos, y
- No-repudiación.

Estos servicios se proporcionan por un determinado nivel (N) a través de la apropiada aplicación de uno o más mecanismos de seguridad.

Se identifican ocho mecanismos de seguridad específicos:

- Cifrado
- Firma digital
- Control de acceso.
- Integridad de los datos.
- Intercambio de autentificación.
- Protección del trafico.(traffic padding).

- Control de encaminamiento
- Notarización.

Y cinco mecanismos de seguridad generales:

- Funcionalidad fiable
- Etiquetas de seguridad
- Detección de eventos
- Auditoría de seguridad
- Recuperación de la seguridad.

#### 1.2.4.1 Software de Escaneo.

Son paquetes de software de seguridad de contenidos y tráfico, que realizan un chequeo y exploración de los equipos. Ofrece así seguridad "en tiempo real" sin precedente en varios niveles en cualquier organización, como por ejemplo puede ser: directamente desde el Gateway de Internet a la máquina del empleado.

Este software, se sincroniza con Internet para proporcionar seguridad en tiempo real a la organización donde está implementado. Ofrecen administración centralizada de la seguridad del sistema, es decir, el

administrador de la red puede configurar las políticas globales de la seguridad para la compañía de una sola consola.

Están diseñados para entender diversos tipos de archivo, formatos de compresión y secuencias de datos. Puede ver dentro de las secuencias de datos e identificar configuraciones complejas.

Estos dan soporte en actualizaciones diarias como: parches de seguridad, corrección de instalaciones, puertos peligrosos y/o actualizaciones de sistemas; colaborando de esta forma a mantener nuestros sistemas con un cierto porcentaje de seguridad contra los atentados externos que hoy en día se vuelven más complejos y fuertemente destructivos con forme avanza la evolución en esta, nuestra era de la informativa.

### 1.2.5 NORMAS DE SEGURIDAD.

En esta categoría de normas, se consideran las relacionadas directamente con todo tipo de necesidades puntuales de seguridad para sistemas, protocolos de comunicación y herramientas de gestión concretas.

Las normas garantizan que los sistemas se ejecuten de acuerdo a ella, soportarán todas las aplicaciones de telecomunicaciones presentes y futuras por un lapso de al menos diez años.

Entre las más significativas de las actuales, se debe citar las normas IPSec, creadas por el IETF (Internet Engineering Task Force). Organismo de desarrollo y creación de normas de facto para el entorno de redes IP a nivel mundial.

Kerberos (Protocolo y sistema de autenticación en red ), PEM (Privacy Enhanced Mail), protocolo para la transmisión segura de correo electrónico, S-HTTP (Secure HyperText Transfer Protocol), protocolo para las transacciones de HTTP seguras por Internet, SOCKS, sistema de seguridad de los mensajes que pasan a través de cortafuegos.

También, dentro del mundo de las aplicaciones criptográficas son muy importantes las normas PKCS (Public Key Cryptographic Standards), NIST (National Institute of Standards and Technology) de Estados Unidos.

Una norma técnica importante en la actualidad por la constante aparición en sistemas de comercio en redes privadas virtuales es el protocolo SSL (Secure Sockets Layer).

Otras normas han sido desarrolladas por OASIS (Organization for the Advancement of Structured Information Standards), otra organización privada muy activa en el entorno del comercio electrónico basado en la Web.

### 1.2.6 ESTANDARES DE SEGURIDAD.

Se establecen como pautas a seguir, deben implementarse de acuerdo con una serie de pasos establecidos, pueden ser estos pasos, recomendaciones tecnológicas hechas por los fabricantes, o por asociaciones que agrupan industrias de electrónica y de telecomunicaciones, como por ejemplo:

Tres asociaciones, la Asociación de Industrias Electrónicas (EIA) y la Asociación de Industrias de Telecomunicaciones (TIA), y el Instituto de Estándares Nacionales Americanos (ANSI). ANSI/TIA/EIA.

La Organización Internacional para la Estandarización, (ISO), es la organización a nivel mundial, que formalmente tiene por misión la coordinación del desarrollo y aprobación de los estándares como estándares internacionales. El trabajo de ISO se estructura en un gran número de comités técnicos, cada uno de los cuales es responsable de

una determinada área de la tecnología. En el área tecnológica de la información, ISO conjuntamente con IEC, ha creado el JJC1 (Joint Technical Committee).

En el ámbito de las redes, las primeras tareas de estandarización han corrido a cargo del IEEE, cuyo proyecto 802 ofrece directrices orientadas a guiar la fabricación de componentes y software para las redes, algunas de las cuales han sido adoptadas como estándares de facto en el mundo de la industria.

Igualmente cabe hacer mención a organizaciones como ANSI, que a contribuido a la normalización de las redes, el Instituto Nacional de Estándares Norteamericano (ANSI), es la entidad normalizadora de los Estados Unidos, una organización no gubernamental constituida por más de un millar de organizaciones comerciales, sociales profesionales y corporativas, ANSI por sí misma no crea estándares, sino que se dedica a coordinar y sincronizar las actividades de otras organizaciones que si desarrollan estándares y asegurar que todos los intereses afectados tienen una oportunidad de participar en el proceso. Las entidades colaboradoras reciben el nombre de organizaciones acreditadas.

La Unión Internacional de Telecomunicaciones (UIT, International Telecommunication Union), es una organización mundial en la cual los gobiernos y el sector privado coordinan el establecimiento y operación de los servicios y redes de telecomunicaciones. Es el responsable de la regulación, normalización, coordinación y desarrollo de las telecomunicaciones internacionales, así como de la armonización de las políticas nacionales. UIT es una agencia de las Naciones Unidas.

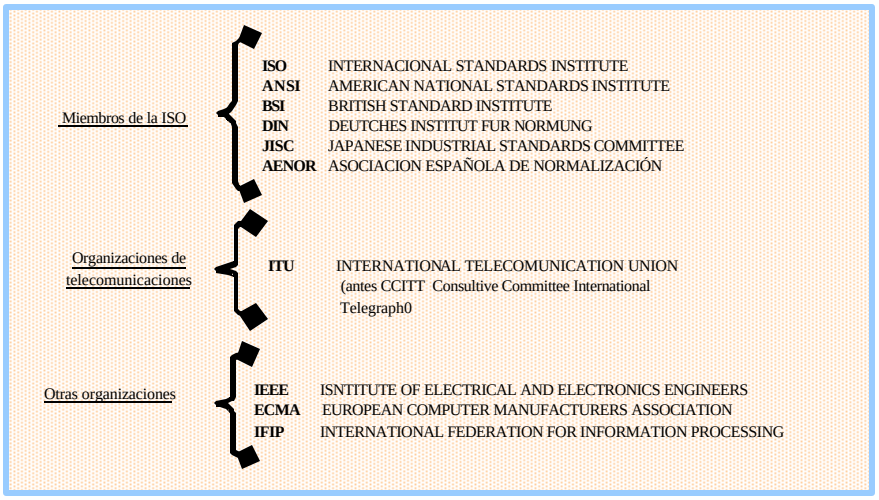


**Figura 11: Principales Organismos de Estandarización.**

### 1.2.7 POLITICAS DE SEGURIDAD.

El termino política de seguridad se suele definir como el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema o red que indica en términos generales qué esta y qué no esta

permitido en el área de seguridad durante la operación general de dicho sistema o servicios de la red. Al tratarse de términos generales, aplicables a situaciones o recursos muy diversos, suele ser necesario refinar los requisitos de la política para convertirlos en indicaciones precisas de qué es lo permitido y lo denegado en ciertas partes de las operaciones que esta realizan, lo que se denomina política de aplicación específica.

Las políticas de seguridad a establecerse en la empresa y en su red corporativa, estarán acordes a todos los niveles de la organización, ya sea por ejemplo, en cuanto a la función del personal, gestión de la red o administración los recursos y servicios informáticos que esta preste o brinde, con una descripción clara de sus objetivos que engloban a los elementos involucrados en su definición, y así sus respectivas sanciones para quienes lo incumplan o traten de hacerlo con la política establecida, seguridad que se reflejara cuando ocurra la amenaza o algún tipo de riesgo a la institución.

Una buena política de seguridad se beneficia del conocimiento de todos quienes conforman el departamento, muchas veces por desconocimiento, las políticas se implementan de forma inadecuada con

resultados mediocres. Es importante tener en claro quién o quienes administran las políticas, y sobre todo como se comunican las políticas.

#### 1.2.7.1 ETAPAS PARA LA DEFINICIÓN DE UNA POLÍTICA DE SEGURIDAD.

**Etapa 1: Planeación y Preparación.**

- Contar con el apoyo del cuerpo directivo.
- Conocer la postura institucional.
- Detectar la problemática de la organización (análisis de riesgos).
- Definir qué se debe proteger y contra qué.
- Informarse acerca de los aspectos informáticos.
- Legislados en el país o entidad donde se vayan a aplicar.

**Etapa 2: Desarrollo (Redacción y Edición).**

- Designar una persona responsable (coordinador, OSI).
- Definición de las políticas involucrando administradores de sistemas, representante del cuerpo directivo, asesor jurídico y usuarios informáticos.

**Etapa 3: Aprobación.**

- Revisiones por las autoridades de la institución.
- Esta etapa puede tomar meses, debido a que se depende, en cierta forma de la disposición, prioridad del documento ante los directivos. De allí que es indispensable vender la idea desde su planeación.

**Etapa 4: Difusión y Aplicación.**

- Difundir el documento (intranet, email, trípticos, Webpage oficial, revistas internas).
- Las políticas deben ser aplicadas por todos, directivos, administrativos, académicos y usuarios.
- La seguridad no depende de una sola persona sino de cada uno de los individuos que forman una organización.

**Etapa 5: Revisión y actualización**

- Al detectar una omisión, se define y se agrega, se revisa, se aprueba y se difunde.
- Etapa permanente debido a la naturaleza cambiante de las tecnologías de información.