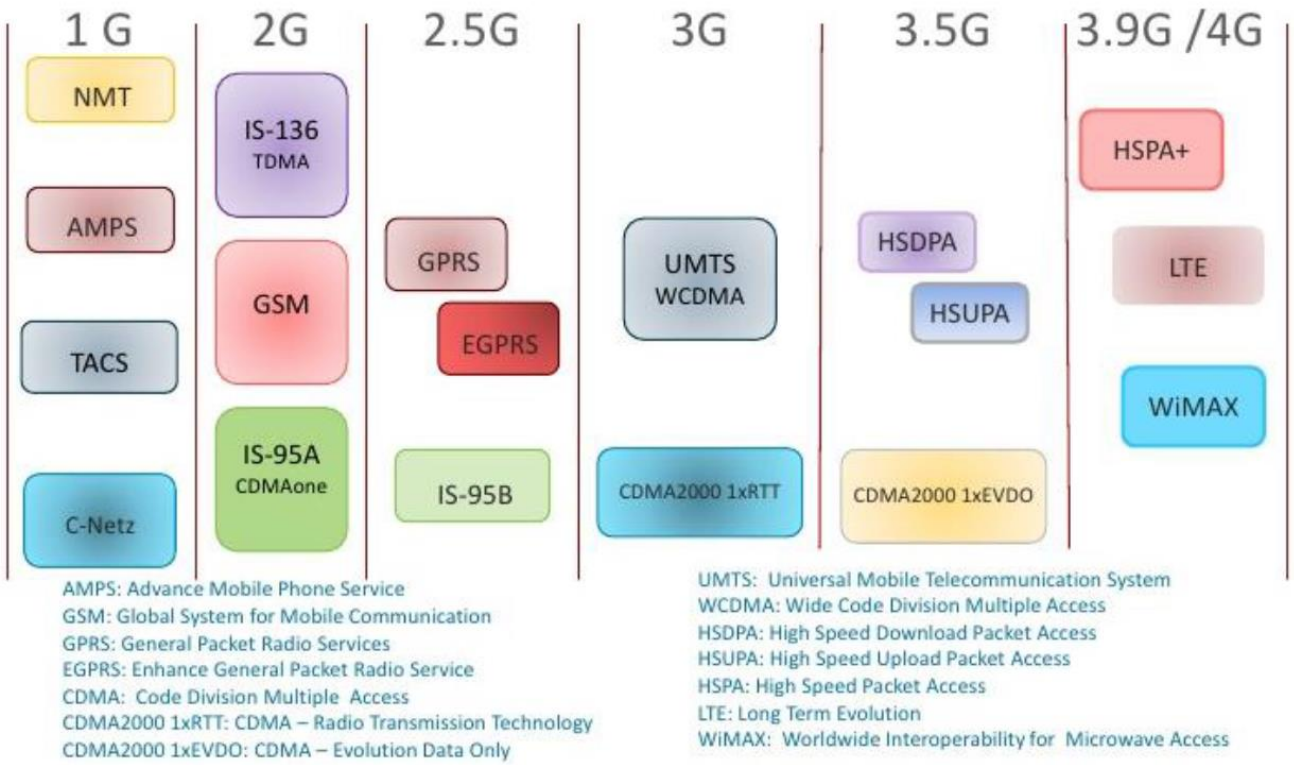
Conceptos y elementos Mobiles.

MS Movile Station. Estacion Movil

BTS Bse Transceiver Station. Estacion Movil de Transmision

BSC Base Station Controller. Controlador de Estación Base. Sección de red telefónica celular encargada del manejo del tráfico de voz y de datos, responsable de dirigir y conmutar la llamada.
PSTN Public Switched Telephone Network, Red de telefonía publica conmutada

ESTANDARES CELULARES



List of mobile phone generations		
0G (radio telephones)	MTS · MTA · MTB · MTC · MTD · IMTS · AMTS · OLT · Autoradiopuhelin · B-Netz	
1G	**AMPS family**	AMPS (TIA/EIA/IS-3, ANSI/TIA/EIA-553) · N-AMPS (TIA/EIA/IS-91) · TACS · ETACS
	Other	NMT · C-450 · Hicap · Mobitex · DataTAC
2G	**GSM/3GPP family**	GSM · CSD
	3GPP2 family	cdmaOne (TIA/EIA/IS-95 and ANSI-J-STD 008)
	AMPS family	D-AMPS (IS-54 and IS-136)
	Other	CDPD · iDEN · PDC · PHS
2G transitional (2.5G, 2.75G)	**GSM/3GPP family**	HSCSD · GPRS · EDGE/EGPRS (UWC-136)
	3GPP2 family	CDMA2000 1X (TIA/EIA/IS-2000) · 1X Advanced
	Other	WiDEN
3G (IMT-2000)	**3GPP family**	UMTS (UTRA-FDD / W-CDMA · UTRA-TDD LCR / TD-SCDMA · UTRA-TDD HCR / TD-CDMA)
	3GPP2 family	CDMA2000 1xEV-DO Release 0 (TIA/IS-856)
3G transitional (3.5G, 3.75G, 3.9G)	**3GPP family**	HSPA (HSDPA · HSUPA) · HSPA+ · LTE (E-UTRA)
	3GPP2 family	CDMA2000 1xEV-DO Revision A (TIA/EIA/IS-856-A) · EV-DO Revision B (TIA/EIA/IS-856-B) · DO Advanced
	IEEE family	Mobile WiMAX (IEEE 802.16e) · Flash-OFDM · iBurst (IEEE 802.20)
4G (IMT Advanced)	**3GPP family**	LTE Advanced (E-UTRA)
	IEEE family	WiMAX (IEEE 802.16m)
5G	conceptual (currently under formal research & development)	

1G – Redes Analógicas, Solo voz, 1era Generación. 70’ 80’. Introdujo la utilización de múltiples celdas y la capacidad de transferir llamadas de un lugar a otro. La torre de cobertura se enlazaba con los sitios de células cercanas para mantener la comunicación. La transmisión de estas celdas era inexacta.

- **Acceso Múltiple por División de Frecuencia (FDMA)**
- **Modulación Analogía (AM/FM)**
- Parcialmente Analógico y Digital (para Señalización)
- Baja capacidad de transmisión de datos. **Velocidades 2.4KBPS.**
- Sistema con baja confidencialidad en la comunicación

2G – Globalización digital. 2 Generacion. Los mensajes de texto SMS (Short Message Service), inicialmente. Luego el servicio de mensajes de texto estuvo disponible en todas las redes digitales.

- **Esquemas basados en sistemas digital TDMA (IS-136 y GSM/GPRS/EGPRS), la porción de tiempo asignada a cada frecuencia para realizar la comunicación se la denomina time slot.**
- Sistema GSM 2G Conmutacion de Circuito – Basado TDMA

3G – Alta transmisión. **3era Generarcion.** Diferencia básica es la conmutación de paquetes para transmisión de data. Transferir voz y datos en una simple comunicación telefónica o una videoconferencia. Datos -sin voz- descarga de programas, intercambio de correos electrónicos, mensajería instantánea, etc. 3G incremento el grado de seguridad al autenticar la red a la que se esta conectado. **Aparecen los Smarphone.**

- **Acceso Multiple por Division de Codigo CDMA.**
- Sistema CDMA/WCDMA

4G – Velocidad del futuro. Eliminacion de los circuitos de intercambio, para **emplear únicamente las redes IP**. Todos **los datos, serán transmitidos por medio de paquetes conmutados** con una velocidad que estará por encima de 1GBps. Con estos valores, a través de un teléfono móvil o celular **se puede obtener una perfecta recepción para la televisión** high definition o de alta resolución. **Su velocidad de transferencia puede superar 1GBPS.**

- **Esquemas 4G – Basados en OFDM (tecnología de modulación)**
- LTE – Long Term Evolution – 4G WIMAX – 4G
- OFM – Orthogonal Frequency Division Multiplexing. Multiples usuarios transmiten al mismo tiempo y son diferenciados por medio de la ortogonalidad de frecuencia.

5G – Conceptual

Celda: Cada una de las antenas de un emplazamiento cubre un sector circular denominado celda. Además, si en el mismo sector circular tenemos varias tecnologías (2G, 3G, LTE), cada una es una celda distinta, aunque coincidan en el espacio. **El área delimitada donde se realiza la comunicación efectiva con un teléfono celular en la cual se encaminan las comunicaciones en forma de ondas de radio desde y hasta los terminales de los usuarios**

MIMO es la abreviatura de "Multiple Input Multiple Output". También se denomina Spatial. Multiplexing o multiplexación espacial. La Tecnología Mimo que permite múltiples rutas de acceso a múltiples antenas que mejora considerable en cuanto a la velocidad de transferencia, una cobertura mayor, mayor capacidad de más usuarios conectados y una mayor estabilidad se aplica tanto en comunicaciones WI FI (802.11 AC) como en comunicaciones celulares (4G).

VoLTE: Es el sistema que nos permite realizar llamadas de voz sobre la tecnología 4G o LTE., que utiliza tecnologías para llamadas de voz en internet como el protocolo SIP

HetNet o "Heterogeneous Networks" es una red en la que conviven las celdas normales (denominadas macro) y small cells (denominadas micro o pico según el tamaño). Cada celda normal o macro conoce todas las celdas que están cerca denominadas "vecinas". Cuando un dispositivo cambia de una celda a otra este cambio está guiado y la red recomienda el mejor cambio. Esto no es así con las small cells que no tienen ningún conocimiento del resto de la

red. En este caso es el teléfono el que tiene que decidir la mejor celda a la que conectarse. Esto plantea una problemática adicional que se debe tener en cuenta en este tipo de redes.

Wifi Offload La idea está basada en que la inmensa mayoría de los teléfonos móviles permiten la conexión a redes Wifi.

Femtocelda es un dispositivo similar a nuestro router/Access Point wifi pero que emite en la banda de 3G. La cobertura es pequeña y su objetivo es simplemente dar una buena cobertura de 3G en el hogar donde está instalada.

El Canal de comunicaciones establecido de un teléfono celular a una torre de antenas de celulares es de tipo **analogico asincrónico y full dúplex.**

Simon: Primer teléfono celular prototipo fabricado por IBM en 1992 que podía hacer y recibir llamadas telefónicas, faxes, correos electrónicos, que poseía un procesador de 16-bits a una velocidad de 16 MHz compatible con computadores de arquitectura x86 y solo tenía 1 MB de memoria RAM y 1 MB de almacenamiento.

Red de Backhaul: El término "backhaul" se puede traducir por "soporte al transporte". En los comienzos de la telefonía móvil el enlace básico utilizado para comunicar los distintos elementos de una red eran los enlaces E1 que consistía en un enlace de 2 MBits/S dividido en 32 canales de 64 KBit/S. Con la llegada de GPRS comienzan a utilizarse enlaces TCP/IP similares a Internet: Los enlaces clásicos E1 seguían utilizandose para las conexiones de voz y estas redes TCP/IP se utilizaban para las conexiones de datos. Esto fue el comienzo de las redes de "backhaul". Son redes TCP/IP similares a Internet pero que su única función es comunicar los distintos elementos de la red móvil. Hoy en día se utiliza la tecnología VoIP para la voz y todas las conexiones (voz y datos) son TCP/IP. Todos los elementos de la red móvil tienen una dirección IP y se comunican entre ellos a través de la red de backhaul o backhaul network.

Tecnologías WAN Nº 1 Redes de Computadoras

Clasificación

(Tipos de Conexión)

- Conexión Directa (Punto a Punto)
- Múltiples Conexiones (Multipunto)

(Distribución Geográfica)

- PAN Personal Área Network
- LAN Local Área Network
- MAN Metropolitan Área Network
- WAN Wide Área Network

Topología

- Topología o Red en Bus
- Topología o Red en Estrella
- Topología o Red en Anillo
- Topología o Red en Malla + 100 km

Ejemplos

- Bus -> Ethernet
- Estrella -> ATM
- Anillo -> Token Ring /FDDI - token ring de IBM

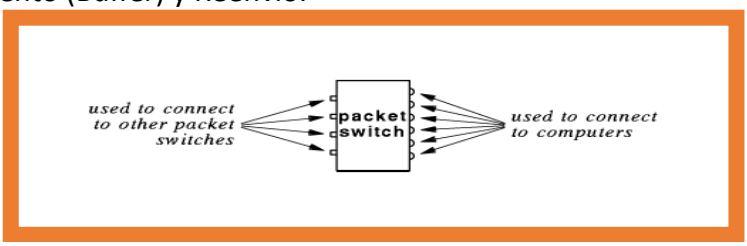
SIGLAS	ORGANIZACIÓN
ITU-T (ex CCITT)	International Telecommunication Union Telecommunication Standardization Sector (ex Consultative Committee for International Telegraph and Telephone)
ISO	International Organization for Standardization
IETF	Internet Engineering Task Force
EIA	Electronic Industries Association
TIA	Telecommunications Industries Association

WAN Red de Área Amplia

- También se las denomina Redes de larga distancia y cubren extensa Área geográfica.
- Se diferencia de Una LAN no solo de la Distribución Geográfica (Tamaño de La red) sino por la capacidad de crecimiento (Escalabilidad).
    - Tipo de Equipos Teleinformáticas.
    - Ancho de Banda de canal.
    - Gran capacidad de Comunicación Simultánea.
- Nodos de Conmutación con enlaces multiplexados (FDM -TDM).
    - Conmutación de Circuitos
    - Conmutación de paquetes
- Conmutación de Circuitos
    - Abonado
    - Bucle Local
    - Centrales
    - Líneas Principales Multiplexadas
- Conmutación de Circuitos -Fases
    - Establecimiento del Circuito
    - Transferencia de datos
    - Desconexión del Circuito

- Conmutador Digital
    - Interfaz de red

    - Unidad de Control
    - Conmutador Digital
- **Conmutación de Circuitos**
    - División en el Espacio
        - Matriz de Conexiones Simple.
        - Varias Matrices en Etapa.
    - División en el Tiempo
        - TDM Sincronía.
- **Conmutación de Paquetes**
    - No es necesario reservar recursos (Circuito).
    - Paquete de nodo de nodo siguiendo algún camino.
    - Nodo Almacena y Retransmite.
- Técnicas
    - Datagramas.
    - Circuitos Virtuales.
- Independencia de la fuente:
    - Los paquetes se encaminan independientemente de la fuente de origen o la trayectoria tomada antes en particular.
    - Aumenta la eficiencia porque todos los Switches utilizan el mismo principio.
- Los Nodos están interconectados por Switches (Conmutadores de paquetes) que hacen almacenamiento (Buffer) y Reenvío.



- Grupos de Conmutadores de Paquetes con varios conectores de Entrada/Salida

Direccionamiento Físico Jerárquico

Dirección {a,b} a=Conmutador b=Computadora

Tabla de Enrutamientos (Saltos)

- Estáticos: Las rutas son calculadas y quedan fijas.
- Dinámicos: Las rutas son calculadas y modificadas Dinámicamente.

Algoritmos

- Algoritmo de Dijkstra (Trayectoria con menores enlaces=menor peso).
- Calculo Distribuido de Rutas (Informar cálculo de rutas a vecinos=Adaptación permanente ante fallas) *uso del ICMP*
- Enrutamiento Vector-distancia (distancia de destino =suma de los Pesos).
- Enrutamiento por Estado de enlace (SPF)

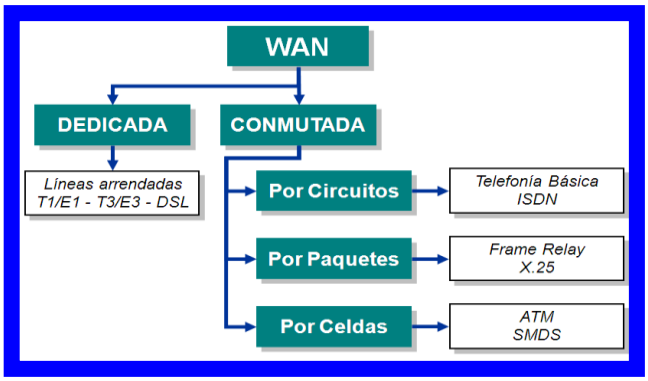
Arpanet

- Red de la Agencia de Investigación avanzada de proyectos (ARPA)
- Una de las primeras WAN de Conmutación de paquetes 1969 (30 Años).
- Red de Conmutación de paquetes.
- Dejo de funcionar en 1990 para convertirse en Internet.

Abilene

- Red de Servicios de conexión de alto rendimiento entre puntos de agregación regional de I2
- **Proyecto UCAID complementario a I2.**
- **Backbone de Red Primario para I2.**
- POS (Packet Over SONET)
- **Comenzó a prestar servicios en Enero de 1999**.
- IPv6 y QoS. (Calidad de Servicio)
- OC 48 (2,5 Gbps) 1999– OC 192 (10 Gbps) 2004

Enlaces - Opciones



X25

- Servicio Conmutador de Paquetes ofrecido por portadores públicos casado en la Norma CCITT X.25.
- Se utiliza para asistir a terminales remotos para conectar con sus Host.
- Comenzó con un ancho de banda de 64 KBPS y en 1992 paso a tener 2 MBPS.
- Argentina - Startel /Red Arpac.
- **Protocolo Normalizado que correspondía a los primeros tres niveles del modelo OSI (Física, Enlace y Red).**
- Trabaja bajo a una Topología que se la denomina Malla.
- Protocolo de Modo de transmisión Asincrónica.
- Aplica Detección y Corrección de Errores (Chequeo, Corrección, retransmisión)

ATM Modo Asincrónico de Transmisión

- Tecnología de Transmisión de datos de Alta velocidad desarrollada por AT&T y US Print.
- Los primeros productos que la soportan empezaron a aparecer partir del año 1994.
- Se pueden utilizar para Redes Privadas, Interconexiones de LANS o WANS.
- Su ancho de Banda permite la Transmisión de voz, vídeo y Datos.
- Conmutación de Circuitos ⇨ Telefonía
- Conmutación de Paquetes ⇨ Telegrafía
- Asincrónico se refiere a la discontinuidad entre celdas del mismo usuario.
- Routers que conectan a Redes ATM.
- Swiches ATM o con módulos opcionales.
- Swiches de Grupo de Trabajo para Introducir ATM a altas velocidades en computadoras de escritorio.
- Adaptadores ATM.
- Tecnología de Banda Ancha, de alta velocidad (1 Gbps).
- La conexión entre los Conmutadores se realiza con Medios de de Alta Velocidad.
- Todos los paquetes (Celdas) Transmitidos tienen el mismo tamaño (Longitud Fija) evitando retardos en la Comunicación. Examina cabecera de paquete e inmediatamente retransmite.
- Las redes de este Tipo contienen conmutadores ATM, Dispositivos multipuertos que realizan conmutación de Celdas.
- La conmutación se hace a Nivel de Hardware.
- Colocan Información a nivel de Celda y la envían (Paquete Rápido).
- **En Nodo ATM se realiza verificaciones de errores, sin corrección para evitar evitan los atascos**. Perdida / Errores originan retransmisión de la Celda.
- Opera dentro del Nivel de Enlace del Modelo OSI.
- Las Velocidades de Transferencia son escalables de acuerdo al medio físico utilizado.
- **Los canales establecidos o conmutados se los denominan canales virtuales y el trayecto circuitos virtuales**.
- Caminos Virtuales ▸ Ventajas :
    - Arquitectura Simplificada
        - Canal Virtual ⇨ Lógica Individual
        - Camino Virtual ⇨ Grupo de Conexiones

- Incremento de Eficiencia y Fiabilidad
- Procesamiento/tiempo de conexión ⇨ Pequeño
- Servicios de red Mejorados
    - Grupos de usuarios fijos (Redes fijas de haces de canales virtuales)

- NAP : Network Access Point (Primeros Naps)
  (Switch ATM /FDDI)
  - ✓ NAP de Sprint ➔ Pennauken –NJ
  - ✓ NAP de Pac BELL ➔San Francisco – California
  - ✓ NAP AADS ➔ Chicago
  - ✓ NAP de MFS Datanet ➔ Washington D.C.
- NAP : Network Access Point (Estructura Internet Inicial en Argentina)
  - ✓ NAP de Telefónica ➔ Buenos Aires
  - ✓ NAP de Telecom ➔ Buenos Aires
  - ✓ NAP de Cabase ➔ Buenos Aires (Cámara Argentina de Base de Datos/ ahora llamada Cámara Argentina de Internet)

Tecnologías WAN

WAN Red de Área Amplia ISDN (Telecom)

- **Red Digital de Servicios Integrados.** Conmutación de Paquetes/Conmutación de Circuitos.
- Integra bajo conmutadores Servicio de red de datos con Servicio Telefónico de Voz.
- Divide el ancho de banda en canales con los servicios de :
    - (D) Digital de Marcaje Telefónico - Establecer conexiones
    - (B) Datos de Computadora/Voz Digitalizada (Modulación por Codificación de Pulso =Amplitud)
- Acceso Básico Canales 2B+D: Este tipo de servicio encaja en las necesidades de usuarios individuales.
    - **1 Canal D full duplex - Establecer conexiones – 64 Kbps**
    - **2 Canales B full duplex - Datos - 64 kbps**
    - Señalización y Delimitación de Tramas**.**

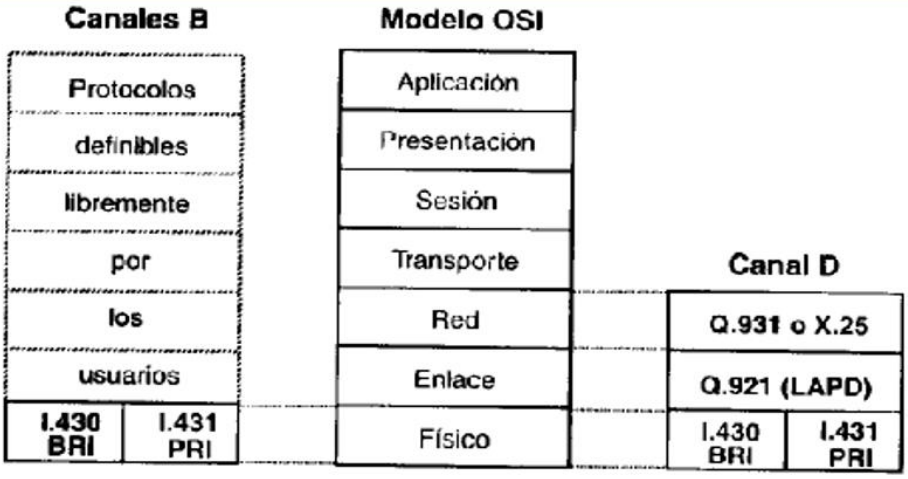
      » 192 Kbps
- Acceso Primario Canales H+D: Este tipo de servicio lo contratan entidades con gran demanda.

30 canales B(64)+ 1 canal D(64)+señalización+framing(64) – Europa - 2 048 kbps.
23 canales B(64)+ 1 canal D(64)+señalización+framing(8) - EEUU, Japón y Canadá - 1 544 kbps.

- Uso de Hardware o módulos especiales/conversores que responden a la a dos normas – EEUU Y EUROPEA.
- Los módulos van conectados a los conmutadores de la señal en ambos extremos del Canal Establecido para las transmisión de paquetes.
- Trabaja en las Capas física, Enlace y Red del Modelo OSI.
- Dentro del transporte contiene un valor de CRC para detección de errores en el receptor.
- Trabaja con TDM (Multiplexión por división de tiempo).
- Muchos fabricantes de hardware para ISDN permiten la agregación de canales utilizando protocolos propios.

Canal B Los canales tipo B transmiten información a 64Kbps, y se emplean para transportar cualquier tipo de información de los usuarios, bien sean datos de voz o datos informáticos.
Estos canales no transportan información de control de la RDSI.
Este tipo de canales sirve además como base para cualquier otro tipo de canales de datos de mayor capacidad, que se obtienen por combinación de canales tipo B.
Canal D Los canales tipo D se utilizan principalmente para enviar información de control de la RDSI, como es el caso de los datos necesarios para establecer una llamada o para colgar. Por ello también se conoce un canal D como "canal de señalización". Los canales D también pueden transportar datos cuando no se utilizan para control. Estos canales trabajan a 16Kbps o 64kbps según el tipo de servicio contratado.
Canales H Combinando varios canales B se obtienen canales tipo H, que también son canales para transportar solo datos de usuario, pero a velocidades mucho mayores. Por ello se emplean para información como audio de alta calidad o vídeo.
Hay varios tipos de canales H:
Canales H0, que trabajan a 384Kbps (6 canales B).
Canales H10, que trabajan a 1472Kbps (23 canales B).

Canales H11, que trabajan a 1536Kbps (24 canales B).
Canales H12, que trabajan a 1920Kbps (30 canales B).



WAN Red de Área Amplia Frame Relay (Telefonica)

- Protocolo de Transmisión de Ráfagas de Datos de Alta Velocidad (1.5 Mpbs) a través de Canales Digitales.
- **Se basa en Conmutación de Circuitos.**
- Se utiliza para líneas alquiladas de ancho de banda fijo.
- **Transfiere utilizando Tecnología ATM los paquetes denominados FRAMES.**
- No tiene control de flujo en la Transmisión
- Tecnología Estructurada de acuerdo al Modelo OSI.
- Los paquetes son de tamaño variable.
- Aplica teoría de Circuitos Virtuales (ATM) y puede superar la velocidad de 1500 MBPS.
- Es una extensión de Estándar ISDN.
- Solo hay chequeo (Paquete) y Retransmisión.
- Las conexiones pueden ser del tipo:
    - Permanente, (PVC, Permanent Virtual Circuit).
    - Conmutadas (SVC, Switched Virtual Circuit).
- Aplicaciones de CAD/CAM.
- Intercambio de información en tiempo real. dentro del ámbito empresarial.
- Construcción de bases de datos distribuidas.
- Correo electrónico.
- Aplicaciones host-terminal.
- Aplicaciones cliente-servidor.
- Acceso remoto a bases de datos.
- Transferencia de ficheros e imágenes.
- Impresión remota.

WAN Red de Área Amplia xDSL

- **xDSL** DIGITAL SUBSCRIBER LINE
    - **Tecnología Estandarizada para Comunicaciones Digitales de Alta Velocidad.**
    - FDM – Multiplexación por División de Frecuencias.
        - Canal Ascendente – Descendente –Distintas Frequencias
    - Principal Tecnología de última milla en Cablemodem.
    - Utiliza equipos como "modems" (DTU/DTE) digitales para líneas físicas, siendo utilizados en pares Telefónicos y coaxiles.
    - Distancia máxima de transmisión: 5,5 Km.
- ADSL = Asymmetrical Digital Subscriber Line
    - Velocidades distintas en los sentidos ISP-Abonado
    - 32 kbit/s a 8,192 mbit/s Entrada.
    - 32 kbit/s a 1,088 mbit/s Salida.
- RADSL = Rate-adaptive ADSL
    - Permite ajustar la velocidad a la aplicación, automáticamente o por definición previa.

- **HDSL** = High-bit-rate Digital Subscriber Line
  - **Para el transporte bi-direccional simétrico. (Asincronico)**
- SDSL = Symmetric Digital Subscriber Line
  - DSLs simétricas con velocidades variables entre 160 kbit/s y 2048 kbit/s.
  - Cada velocidad acomoda una cierta distancia.
- VDSL = Very-high-bit-rate Digital Subscriber Line
  - hoy, hasta 51 Mbit/s
  - 13 Mbit/s, hasta 1300 m
  - 26 Mbit/s, hasta 900 m
  - 51 Mbit/s, hasta 300 m
  - Está diseñado para soportar los servicios conocidos como "Triple Play", tales como voz, video, datos, televisión de alta definición (HDTV) y juegos interactivos
- Características ADSL:
  - **En una línea ADSL se establecen tres canales de comunicación, que son el de envío de datos, el de recepción de datos y el de servicio telefónico normal.**
  - Esta tecnología se denomina asimétrica debido a que la velocidad de descarga y de subida de datos no es igual.

PDH- T-CARRIER PLESIOCHRONOUS DIGITAL HIERARCHY Modo Plesincrónico de Transmisión de Datos

- **Protocolo de Transporte para Redes de Comunicación Digital** introducido por AT&T en 1983 que comenzó a funcionar a mediados de 1990.
- Basado una Comunicación Casi Sincrónica donde los equipos involucrados en el circuito no transmiten todos a la misma velocidad.
- Utilizada sobre canales de comunicación Punto a Punto.
- **Existen 3 Estándares correspondientes a EEUU (T), Europa (E1) y Japón (J).**
- Trabaja sobre Canales con Multiplexación por División de Tiempo.
- Aplica Modulación PCM (Amplitud) en sus Canales Digitales.

SDH-SONET - SYNCHRONOUS DIGITAL HIERARCHY - SYNCHRONOUS OPTICAL NETWORK

- **Protocolo de Transporte para Redes de Anillos de Fibra Óptica.**
- Basado en una Estructura de Comunicación Sincrónica.
- Se Utiliza en las Redes Troncales de Fibra y anillos WAN.
- Es utilizado en la mayoría de las Topologías Híbridas de Cablemodem.
- Se ubica en la Capa Enlace del modelo OSI.
- **El modelo de referencia de las redes SDH/ Arquitectura SDH se separa en cuatro capas:**
  - **Física:** Características físicas de la red: señales eléctricas de entrada, tipo de fibra, ventana de trabajo del Láser, etc.
  - **Sección:** Parte de red comprendida entre dos regeneradores de señal ópticos o eléctricos.
  - **Línea:** Parte de red comprendida entre dos equipos multiplexores.
  - **Trayecto:** Parte de red comprendida entre los dos extremos de la transmisión.
- **Cuando transportamos datos en un canal STM-4 para una portadora de WAN de acceso a Internet, que nos permite tener un ancho de banda de 622 MBPS, el tipo de tecnología utilizada corresponde a SONET.**

LRE – Long Reach Ethernet

- ***Extensión aplicada de las redes Ethernet sobre un par de cable trenzado a distancias de más de 1,800 metros (LANs / MANs).***
- *Encapsula los paquetes Ethernet para una transmisión robusta y de alta frecuencia a través de líneas telefónicas.*
- *Alta velocidad: Es muy flexible y sus variables incluyen velocidades de 5 Mbps, 10 Mbps y 15 Mbps (dependiendo de la distancia de acceso).*
- *Transmisión simultánea en tiempo real de datos, voz y video para aplicaciones integradas como voz, datos, video y multicasting.*

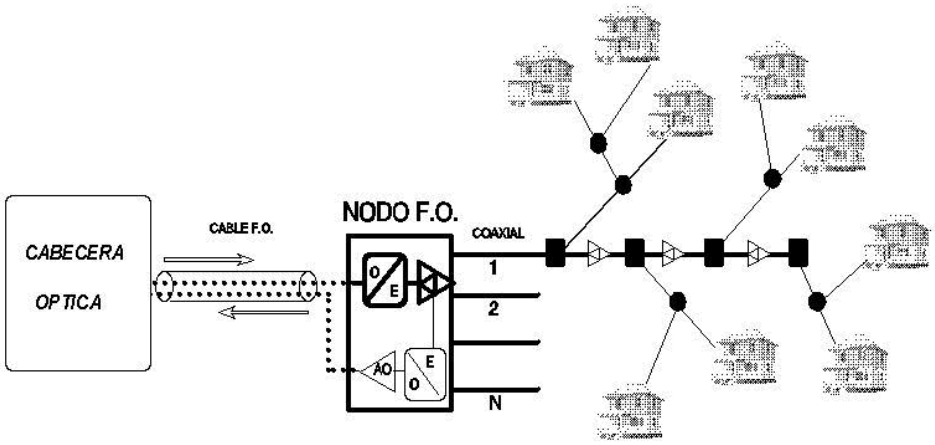
Cablemodem – HFC

- HFC ➔ Red de Telecomunicaciones por Cable de Banda Ancha (Video, Audio y Datos).
- Topología Híbrida.
- Soporte de Transmisión de Señales
  - Fibra Óptica
  - Cable Coaxial
- **El soporte tiene 4 partes claramente diferenciadas.**
  - **Cabecera**
  - **Red Troncal**
  - **Red de Distribución**
  - **Red de Abonado**
- Plataforma Digital ➔ Modulación 64-QAM

(Modulación de Amplitud en Cuadratura).

Cabecera:

- Centro de Control del Sistema.
- Monitoriza la Red y supervisa su funcionamiento.
- Dispone de equipos de recepción de televisión terrenal, satelital y microondas.
- Posee enlaces con otras cabeceras y estudios.
- Su complejidad depende de los servicios que presta.
- Las señales de video, audio y datos que forman los canales de televisión digital se multiplexan para formar el flujo de transporte.



Red Troncal:

- Estructura de anillos de Fibra Óptica redundantes.
- Une un conjunto de Nodos Primarios.
- Emplea tecnología SDH y PDH que permite constituir redes alta velocidad.
- Los nodos primarios alimentan a los nodos secundarios con otros anillos o enlaces punto a punto.

Red de Distribución:

- Los Nodos Secundarios convierten las señales ópticas en eléctricas.
- Distribuyen la señal a través de una estructura bus coaxial que constituyen la distribución.
- Cada nodo da servicios a 500 hogares.
- Permite distribuir señal a 2 o 3 amplificadores en cascada para controlar el ruido y la distorsión del canal descendente.

Red de Abonado:

- Ultima derivación de cable coaxial hasta la base de conexión de abonado.
- Cada derivación conecta la señal a la computadora a través de una DTU.
- La distribución es asimétrica tanto del canal descendente como el ascendente.
- El DTU de cable demodula la señal recibida y encapsula el flujo de bits en paquetes Ethernet. El PC del abonado ve la red HFC como una enorme red local Ethernet.
- LA DTU se conecta a la PC a través de una interfaz de RED.

- El Canal Descendente puede entregar más de 512 Kbps de señal de banda ancha.

MPLS (Multiprotocol Label Switching)

- Definido en el RFC 3031
- **Opera en la capa de enlace de datos y de red.**
- Proporciona circuitos virtuales en las redes IP.
- Es independiente del protocolo que se use en los extremos.
- El camino esta prefijado desde el origen (como en ATM – frame Relay)
- Solución al problema de procesamiento que presentan los routers externos IP (grandes tablas de enrutamiento: IP + interfaz).
- Introduce mejoras a IP:
  - **Redes privadas virtuales**
  - **Ingeniería de tráfico**
  - **Mecanismos de protección frente a fallas**

Caracteristicas

- Agrega etiquetas al paquete para enrutarlo.
- No utiliza la IP de origen y destino para enrutarlo.
- Sus Paquetes son de Log. Variable.
- Tabla de enrutamiento:
  - **Interfaz de entrada**
  - **Etiqueta de entrada**
  - **Intefaz de salida**
  - **Etiqueta de salida**
- LSP - Label Switch Pad: Camino designado entre routers MPLS.
- Si hay 2 rutas con igual cantidad de saltos, entonces se hace balanceo entre las 2 rutas.

- Label (20 bits): Es la identificación de la etiqueta.
- Exp (3 bits): uso en diffserv (servicios diferenciados).
- S (1 bit): stack, sirve para el apilado jerárquico de etiquetas. Cuando S=0 indica que hay más etiquetas añadidas al paquete. Cuando S=1 estamos en el fondo de la jerarquía.
- TTL (8 bits): Time-to-Live, misma funcionalidad que en IP, se decrementa en cada enrutador y al llegar al valor de 0, el paquete es descartado.
- Label 1: Etiqueta obligatoria MPLS
- Label 2: Etiqueta utilizada para establecer VPNs en MPLS. Solo es leida por los routers de los extremos.
- Label 3: Utilizado para el protocolo RSVP. Permite seleccionar un camino que no es el de menor saltos, sino que es más eficiente.
- El uso de MPLS con ATM presenta un problema. Ya que no se pueden agregar las etiquetas al mensaje, dado que ATM usa celdas de longitud fija.

SLA (Service Level Agreement)

Acuerdo de Nivel de Servicio (ANS)

- **Protocolo plasmado en un documento de carácter legal por el que una compañía que presta un servicio a otra se compromete a prestar el mismo bajo unas determinadas condiciones y con unas prestaciones mínimas.**
- Secciones:
  - Categorias:
    - Disponibilidad
    - Calidad de Servicio
    - Administración del servicio
    - Seguridad del servicio
  - Indicadores: BER – **Jitter** – delay – tiempo de respuesta.
  - Nivel de acuerdo: valor del indicador.
  - Métrica: definición de cada indicador.
  - Penalidades.
  - Medio de comprobación.
- Jitter – Variación en el tiempo en la llegada de los paquetes, causada por congestión de red, perdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino. Entre el punto inicial y final de la comunicación debiera ser inferior a 100 ms.
- Tiempo Minimo Medio entre Fallas por mes. (Ej : 30 Horas).
- Tiempo Minimo entre Fallas por Mes. (Ej : 5 Horas).
- Tiempo máximo en restauracíon del Servicio (Ej 3 horas).

Centro de Comunicaciones y Redes - Tendencias de Red

- Conexiones de comunicaciones de datos redundantes.
- **Servidores virtuales de alta velocidad granjas de servidores o clústeres de servidores**.
- Sistemas de almacenamiento redundante – SAN.
- Fuentes de alimentación redundantes o de respaldo (UPSs /Generadores).
- Controles ambientales Integrales
  - Accesos Restringido
  - Aire Acondicionado
  - Extinción de Incendios
- Dispositivos de Seguridad.

Servicios de Internet

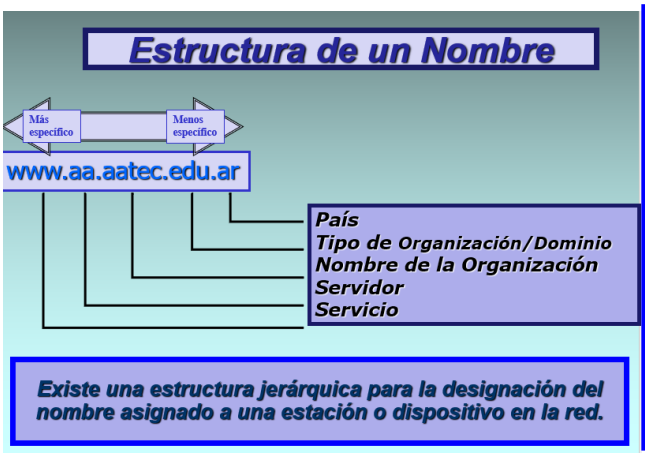
- *Se identifican con:*
  - *Dirección IP.*
  - *Nombre de Dominio Único.*
  - *Puerto Asociado a cada Servicio Solicitado.*
  - *Cada Servicio (Server).*

  - *Escucha permanentemente cada Puerto.*
- *Puerto: identificador único del servicio Deseado.*
- *Lo utiliza TCP para identificar los Servicios.*
- *El protocolo usa el identificador para dirigir las solicitudes de entrada al servidor adecuado.*
- *Numero Entero de 32 Bits (IPv4).*
- *Numero Hexadecimal de 128 Bits (IPv6).*
- *WWW Web Internet*
- *WWW2 Web Internet 2*

ftp://	FTP server (file transfer)
news://	Usenet newsgroups
mailto://	e-mail
wais://	Wide Area Information Server
gopher://	Gopher server
file://	file on local system
telnet://	applications on network server
rlogin://	applications on network server
tn3270://	applications on mainframe

DNS - Sistema de Nombres de Dominio

- ***Conjunto de protocolos y servicios sobre una red TCP/IP, permite a los usuarios de red utilizar nombres jerárquicos sencillos para comunicarse con otros equipos, en vez de memorizar y usar sus direcciones IP****.*
- *Usado en Internet y en Redes Privadas Actuales.*
- *Servicios como: browsers, servidores de Web, FTP y Telnet; utilizan DNS.*
- ***Un modelo de base de datos para almacenar información sobre direcciones.***
- *Un mecanismo para preguntar y actualizar información sobre direcciones en la base de datos.*
- ***Un mecanismo para replicar información entre servidores.***
- *El Nombre consta de una Secuencia de segmentos alfanuméricos separados por puntos.*
- ***Sistema de Nombres Jerárquicos siendo la parte mas significativa a la Derecha.***
- *La parte de la izquierda corresponde al nombre de una computadora.*
- ***Los otros segmentos del nombre corresponden al Grupo al cual pertenecen.***

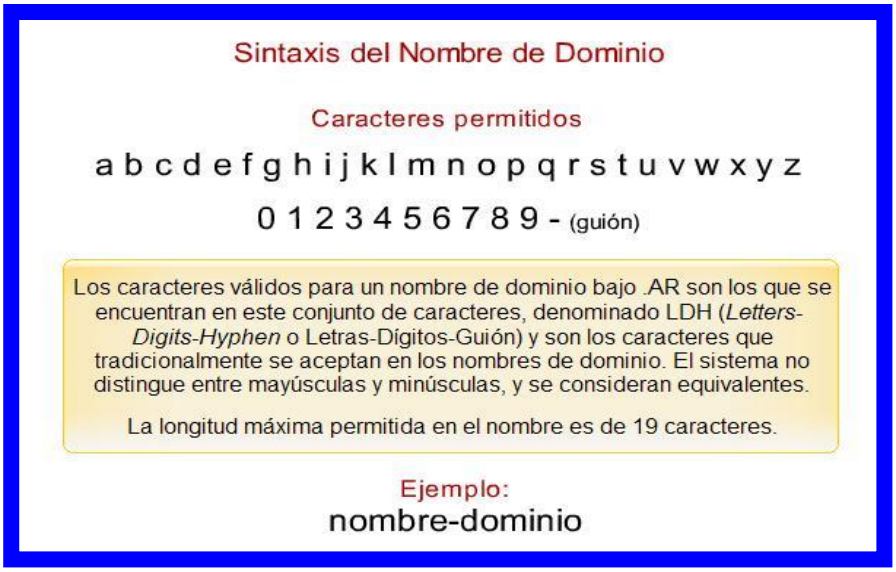


- *Estructura Geográfica de Registro identificando al País.*
- *Las Organizaciones Propietarias del Domino Registrado con Direcciones IP ante NIC local/InterNIC pueden decidir si agregan alguna estructura jerárquica adicional.*
- *No existen Normas ni patrones informes para las Estructuras Jerárquicas Adicionales.*
- *Cada Servidor sabe como llegar a la raíz y los mismos son autoridades de los nombres de inferior Jerarquía.*

Resolución del nombre ⇨ ***RESOLUTOR.***

- *Componente del Sistema Operativo del cliente y servidor que realiza solicitudes de DNS.*

- *El Software toma el argumento o cadena de caracteres y devuelve el listado de direcciones que corresponden al nombre Especificado.*
- *Cada Resolutor se configura con la lista del Servidor local de nombres de dominio (NIC).*



Servicios de Internet - Wais - Servidores de Información de Largo Alcance

- ***Son Bases de datos de documentos indexados.***
- ***Basado en el Protocolo ANSI Z39.50.***
- ***Pueden accederse a través de Telnet.***
- *Pueden accederse a través de WWW.*
- *Busca un tópico en todas las bases de datos disponibles en la red.*
- *El Servidor mantiene un índice global de todo el mundo lo que permite una búsqueda de alto detalle.*

Servicios de Internet – Gopher - Servicio de Distribución de Información

- ***Gopher permite visualizar Directorios y bajar información.***
- *Posee una interfaz basada en menú y trabaja con los siguientes componentes.*
  - ***Items → Directorios, Archivos de Texto, Una Imagen o Búsqueda.***
  - ***Documento → Información incluida en un Item.***
  - ***Bookmark → Señalador o entrada de menú asociada.***
  - ***Server → Servidor de Documentos.***

Servicios de Internet – Archie - Servicio de Distribución de Información

- *Permite la localización de información y transferirlos utilizando FTP.*
- *También las búsquedas pueden encararse a través de Telnet o Correo Electrónico.*
- ***Trabaja con Arquitectura Cliente-Servidor, necesita de la interfaz de cliente para el usuario.-***
- *Descendiente del servicio Gopher.*
- *Protocolo que interpreta ficheros de una maquina remota.*
- *Puede interpretar Texto, , imágenes, sonidos y Secuencias de video.*
- *Para ello utiliza el HTML (Hypertext Markup Language) Mucha información en archivos pequeños.*

Servicios de Internet - WWW - WORLD WIDE WEB

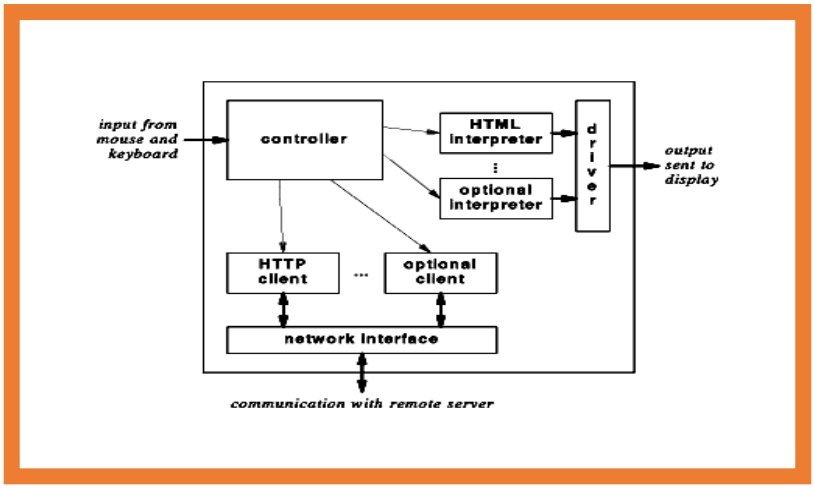
- *Colección de Ficheros o Páginas WEB que incluyen información en forma de textos, gráficos, sonidos y video además de Links o Vínculos con otros ficheros.*
- *Los ficheros son identificados por un Localizador Universal de Ficheros (URL) que especifica el Protocolo de Transferencia, la dirección de Internet de la máquina y el Nombre del fichero .*

https://www.argentina.gob.ar/salud/sarampion

- *El visualizador (Navegador) es un programa interactivo que permite al usuario ver la información de la WWW. La información tiene objetos seleccionables para que el usuario vea otra información.*

La mayoría tiene una interfaz para apuntar y seleccionar elementos de Hipertexto/Hipermedia.

Servicios de Internet – WWW - Visualizador - Componentes



Servicios de Internet - FTP :Protocolo de Transferencia de Archivos

- *Aplicación que opera sobre TCP. (RFC 959).*
- *Se utiliza para Operaciones Básicas sobre Archivos y Transferencias en Redes de Área Extensa.*
- *Normalmente, para acceso a un Host solicita Nombre de Usuario y Contraseña.*
- *Las contraseñas las envía encriptadas ⇨ garantiza su privacidad (No Hay Encriptación de Datos) .*
- *Establece un canal Lógico entre ambos Host.*
- *Conexión de control ⇨ Puerto 21*
- *Transferencia de los datos ⇨ Puerto 20 o superior a 1023*

Servicios de Internet - TFTP :Protocolo de Trivial de Transferencia de Archivos

- *Diseñado para realizar transporte de archivos en forma sencilla ⇨ Variante del protocolo FTP.*
- *Prescinde de la conexión de control.*
- *Sin autenticaciones de seguridad.*
- *Se utiliza para anular la carga de trabajo de FTP. Es muy eficiente.*
- *Es usado normalmente dentro de una LAN.*
- *Es arriesgado su Uso en WAN.*

Servicios de Internet - SFTP :Protocolo de Transferencia de Archivos Seguro

FTPS : Protocolo Seguro de Transferencia de Archivos

- *Protocolo de Transferencia de Archivos Seguro para conexiones remotas.*
- *Puede utilizar para la encripción de datos en el transporte:*
  - *SSH en el Puerto 22 ⇨ SFTP*
  - *SSL /TLS Puerto 990 ⇨ FTPS*
- *Servicios que sincronizan Usuarios habilitados en AD/LDAP.*
- *Puede Trabajar con:*
  - ***Certificados SSL /X509***
  - *Claves Publicas/Privadas SSH*

Servicios de Internet - SMTP :Protocolo Simple de Transferencia de Correo

- Protocolo Simple de Transferencia de Correo.
- Protocolo orientado a la conexión.
- Basado en RFC 2821 y 822 (Formato de Mensajes).
- **Utiliza los Puertos 25 y 587 para conectividad entre cliente y el servicio de transporte**.
- Los Puertos 25, 465 y 475 son utilizados para el transporte al buzón de correos.
- Una transacción SMTP tiene 3 secuencias:
  - MAIL: Dirección Remitente/retorno.
  - RCPT: Destinatario del mensaje.
  - DATA: Envió de mensaje de texto.
- *MTA : Agente de Transferencia de Correo.*
- *El más conocido es SENDMAIL (Unix).*
  - ***Envía y recibe paquetes desde/hasta otros servidores de correo.***
  - ***Proporciona una interfaz para las aplicaciones accedan al sistema de correo.***
  - ***Proporciona a los usuarios buzones de correo dotados de una dirección.***

Servicios de Internet - POP 3 :Protocolo de Oficina de Correo Versión 3

- *UA : Agente de Usuario (Usuario final)*
- *El UA utiliza POP 3 para comunicarse con el MTA.*
- *El UA Envía y recibe paquetes desde/hasta otros Servidores.*
- *No trabaja en tiempo Real (Carga de la Red).*

Servicios de Internet - Servidor (Relevador) de Correo Electrónico

- Configuración del Buzón de Correos
  - Nombre de la Cuenta pepe@gmail.com
  - Alias.
  - Fecha de Expiración.
  - Nombre del archivo buzón de correos.
  - Dirección de Forwardeo.

Servicios de Internet - Webmail

- *Correo electrónico en sitio WEB*
- *Acceso a cuenta a través de Navegador WEB*
- *Administración de Correo electrónico a través de Internet.*
- *Espacio de Almacenamiento Limitado.*
- *Puede replicar con Servidor SMTP.*
- *Privacidad*
  - *Nombres de Usuario*
  - *Contraseña*

Servicio DHCP - Protocolo de Configuración Dinámica de Hosts

- *DHCP (Dynamic Host Configuration Protocol).*
- *Servicio de asignación automática de direcciones IP.*
- ***Protocolo Cliente -Servidor - Asigna parámetros (Mascara de Subred, Puerta de enlace y Otros).***
- *Servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres.*
- *Mantiene estado de la posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.*

Servicios de Internet - Telnet

- *Acceso en modo terminal remoto.*
- *Emulación de terminal en modo Texto.*
- ***Característica Crítica de Un Sistema de Computación.***
- *Puede realizarse mediante conexión Telefónica.*
- *La sensación que percibe el usuario es que la sesión de terminal tiene lugar en la computadora local mientras que el Host Remoto procesa interactuando con la terminal local .*

Servicios de Internet - Secure Shell o SSH

- ***Protocolo de red que permite el intercambio de datos utilizando un canal seguro entre dos dispositivos conectados en red.***
- *Acceso en modo terminal remoto.*
- *Emulación de terminal en modo Túnel.*
- *Puede realizarse mediante conexión Telefónica.*
- *La sensación que percibe el usuario es que la sesión de terminal tiene lugar en la computadora local mientras que el Host Remoto procesa interactuando con la terminal local .*
- ***SSH utiliza la criptografía de clave pública para autenticar el ordenador remoto y permitir autenticar al usuario.***
- *SSH es utilizado habitualmente para entrar en una máquina remota y ejecutar comandos, sino que también soporta túneles, transmisión arbitraria en puertos.*
- *Un servidor SSH, por defecto, escucha en el puerto 22. Es utilizado para el establecimiento de conexiones a un demonio / conexiones remotas.*
- *Ambos están presentes comúnmente en la mayoría de sistemas operativos modernos.*
- *Autentifica los dos extremos de la conexión.*
- *– El servidor se autentica ante el cliente con un certificado*
- *– El cliente se autentica ante el servidor*

- *Usuario y Password*
- *Certificados*
- *Encripta los datos intercambiados.*
- ***No se transmiten usuarios ni Passwords en claro. La información transmitida viaja también encriptada***

Servicios de Internet - Chat

- *Protocolo Mundial que se utiliza para comunicar intercambiando mensajes de texto en Internet (Ciberespacio).*
- *Por medio del Chat se realiza una comunicación en tiempo real para Intercambiar Mensajes que pueden Ser :*
    - ***Temáticos***
    - ***Segmentos de Población***
    - ***Libre acceso***
    - ***Restringidos***

REDES SDN

Las **redes convergentes** o **redes** de multiservicio hacen referencia a la integración de los servicios de voz, datos y video sobre una sola **red** basada en IP como protocolo de nivel de **red**. Este sistema ha fomentado la creación de soluciones en comunicaciones unificadas.

- Las redes convergentes pueden transmitir voz, streams de video, texto y gráficos entre diferentes tipos de dispositivos.
- Utilizan el mismo canal de comunicación y la misma estructura de red.
- Infraestructura de Red⇨ Plataforma Común.
- Mismo Conjunto de reglas, acuerdos y estándares de implementación ⇨Protocolo
- Red de datos con múltiples protocolos.
- Complejas Interacciones entre ellos.
- Inteligencia Distribuida en elementos activos/dispositivos intermedios.
- El Plano de control de Rutas se realiza a Través de Capa 2 o Capa 3 – OSI.
- Rutas Definidas – Tráfico de Red con trayectorias programadas.

Elementos Activos-Dispositivos intermedios: Routers/Switches

- Sistemas Abiertos y Estándares.
- Componentes Monolíticos.
- Soluciones Propietarias.

Redes definidas por software

Definición:

- Conjunto de técnicas relacionadas con el área de redes computacionales.
- Su objetivo es facilitar la implementación de servicios de red de una manera determinista, dinámica y escalable.
- Libera al administrador de red gestionar dichos servicios a bajo nivel.
- Paradigma que ***posibilita servicios de computación a través de red, usualmente es internet.***
- Una nueva forma de organizar y programar las redes de computadoras; configurar y administrar el comportamiento de la red de forma dinámica y escalable.
- Permite, centralizar y automatizar la administración de la red.
- Aplica virtualización en la red, optimizando un gran control de la ingeniería de tráfico.
- Se iniciaron a partir de 1990.
- Cambio de paradigma
    - ⇨ Redes Tradicionales.
- Funciones programables en la red.
- Separación del plano de control y de datos.
- Protocolo Openflow.
- Programable ⇨ Control de la Red.
- Ágil ⇨ Flujo de Tráfico.
- Gestión Centralizada. ⇨ Conmutador Lógico.

- Configuración Pragmática. ⇨ Dinámica y Automatizada.
- Arquitectura Abierta. ⇨ Independientes del Hardware.

Componentes – Interfaz Norte

La interfaz norte carece actualmente de estándar y podría complicar la interoperabilidad entre aplicaciones y controladores.

La interfaz norte, permite que aplicaciones SDN puedan modificar comportamientos del controlador, a través de APIs.

- • Configurar flujos para alterar rutas entre dos equipos de red.
- • Balancear el trafico a través de múltiples caminos de red.
- • Reaccionar en forma tempranas a cambio en la topologías de la red, mediante la detección de fallas de enlaces, inserción de nuevos dispositivos y enlaces de red.
- • Redirigir trafico con la finalidad de inspeccionar, autenticar, segregar.
- • Realizar algunas otras tareas relacionadas con la seguridad

Protocolo Openflow – Interfaz Sur

- Surgido en la Universidad de Standford.
- Protocolo emergente y abierto de comunicaciones.
- Permite a un servidor de software determinar el camino de reenvío de paquetes que debería seguir en una red con dispositivos intermedios (Switches, Routers, Firewalls).
- Transmite Políticas de acuerdo al flujo/tipo de paquetes (Datos, Audio y Video).
- Respecto a las tablas de Flujo y sus acciones trabaja en modo proactivo y reactivo.

Componentes – Controlador

- Panel de control de la red.
- Traducir las necesidades o requisitos de la capa aplicación a los elementos de red.
- Comunicación entre los distintos tipos de enlaces. (Mpls-Lte, Vsat. ETC.).
- Segmenta la red global y unifica en redes regionales (mallas regionales).
- Provee información a las aplicaciones SDN, incluyendo estadísticas y eventos.

Componentes – Orquestador

- Cerebro de la Red.
- Topología de la red - Plantillas de configuración.
- Director o Administrador
  - Enrutamiento, seguridad, Optimización y Balanceo de carga.
  - Cantidad muy granular de configuraciones.
  - Calidad de servicio para C/Tipo de enlace (QoS).
  - Configuraciones de los dispositivos finales.
  - Configuraciones hacia la LAN y los circuitos WAN.
  - Configuraciones de BGP.
  - Servicios Virtuales.
- Aprovisionamiento de los equipos, el despliegue o instalación de los mismos en la red y su posterior Administración.

Componentes – Interfaz Norte

- Vmware NSX Data Center.
- Cisco Open Network Environment (ONE).
- Microsoft Azure.

Componentes de un Host de Internet - Encaminador Dinámico (Router) :

- Permite el enrutamiento punto a punto de los paquetes entre la red y el nodo.
- Trabaja en la Capa Red (3).
- Se lo denomina fronterizo y utiliza el encaminamiento bajo búsqueda en tabla.
- Las tablas suelen ser dinámicas.
- Selecciona las rutas de los paquetes basados en estas rutas.
- El Proveedor del Servicio le asigna una Dirección IP.

- Examina los paquetes de datos entrantes y selecciona las ruta basada en la información en las tablas de enrutamiento.
- Utiliza Protocolos de Enrutamiento como por Ejemplo :
    - RIP – IGRP = Interiores
    - EGP – BGP = Exteriores
- Para el cálculo de la mejor ruta utilizan distintas métricas como numero de saltos, retardos etc.

Componentes de un HOST - Servidor de Acceso (ACCESS SERVER)

- Se Encarga de filtrar los Accesos Remotos Vía Módem a través de un Software de Seguridad que almacena a los accesos con su clave de autenticación.
- Normalmente lo componen una cantidad de módems en Línea conectados a accesos telefónicos unitarios o rotativos.
- Se le asigna un Rango de Direcciones IP Fijas que le permita asignar a cada usuario una Dirección Dinámica en el momento de la conexión.

Radius - Remote Authentication Dial-In User Service

- **Software de Administración y control para Servidores de Acceso Remoto (RAS).**
- **Autentica las acciones de acceso remoto sobre los RAS mediante las llamadas, protocolos y filtros.**
- **Soporta la Seguridad Adicional de Los Servidores Proxy**
- **Radius - Software nativo dentro de cualquiera de los Servidores que constituyen una Instalación Internet.**
- Actúa complementándose con todos los protocolos que constituyen la Pila TCP/IP.
- Tiempo de respuesta de Autenticación Inmediato.
- Asigna Direcciones IP Dinámicas en el momento de la conexión.
- Mantiene una Base de Datos con el Nombre de Usuario (LOGIN) y su Password.
- Simplifica y Consolida la Administración de Usuarios de Acceso Remoto al Nodo
- Facilita el Seguimiento y Documentación de Accesos Remotos.
- Administración y Configuración bajo Entorno Windows.
- Permiten configuración, comunicación y Autenticación en VPNs usando L2TP.
    - LDAP LAYER 2 TUNNELING PROTOCOL
        - Protocolo de Tunneling para Usuarios Remotos.
        - De Acuerdo al Usuario y configuración dentro de la VPN los paquetes son dirigidos aplicando Tunnelling en forma Dinámica en el momento de la Conexión Dial-UP

Componentes de un HOST - FIREWALL

- **Servidor con Interfaz de Red Multipuerto que limita los Servicios/Procesos con respecto a nuestra red con respeto al resto de los componentes de Internet.**
- **Habilita/Deshabita servicios en forma parcial/global de acuerdo con las políticas establecidas en la Administración del Nodo: EJ. FTP, Telnet, Chat, Etc.**
- Servidor especifico compuesto por Hardware y Software que actúa como barrera de seguridad de los recursos Informáticos de nuestra organización.
- Barrera de Seguridad entre la Intranet y la Extranet.
- Se encuentra ubicado inmediatamente después del Router Fronterizo.
- Puede albergar el DNS Externo.
- La regla básica es asegurar que todas las comunicaciones entre la Extranet y la Intranet se realicen conformes a las políticas de seguridad de la organización o corporación.
- Técnicas Utilizadas
    - Filtros a nivel paquete
    - Filtros a nivel circuito
    - Filtros a nivel aplicación
    - Filtros dinámicos a nivel paquete
- **Un Firewall suele tener un mínimo de tres** Zonas, aunque las primeras implementaciones sólo incluían dos.
    - **Interior**

    - **Exterior**
    - **DMZ (zona desmilitarizada)**
- Dispositivos de defensa perimetral: Separa redes.
- **Filtra tráfico dependiendo de reglas predefinidas**. (Editor de Reglas)
- No protege de ataques internos.
- No protege de accesos no autorizados.
- No protege de todos los ataques dañinos.

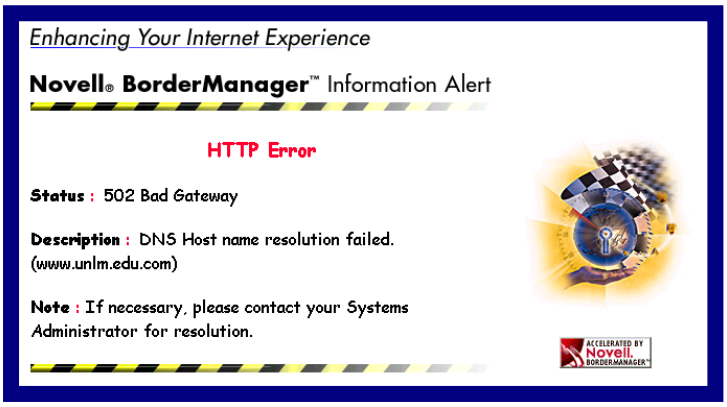
Servicios

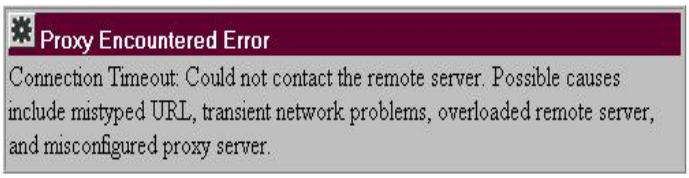
- Conexiones de Intranet a Extranet
- Correo Electrónico
- FTP
- SSH
- Telnet
- Conexiones de Prueba desde el monitor de Red.
- Pruebas de Conectividad (Ping)
- Pruebas de Conectividad con Proxy y Otros
- Exploración de Redes de Terceras Partes (Extranet)
- **IRC/ICQ (Chat).**
- Real Audio (Entrantes y Salientes).

Componentes de un HOST - Proxy Server

- Gestionador de comunicaciones entre Internet e Intranet de una LAN.
- Proporciona Protección a nuestra LAN utilizando EL SOFTWARE N.A.T. (Administrador de Traducciones de Red).
- Proporciona Restricciones de Servicios parciales a nivel Individual.
- Aislamiento completo de Nuestra Intranet.
- Gestionador de comunicaciones entre Internet e Intranet de una LAN.
- Proporciona Protección a nuestra LAN utilizando EL SOFTWARE N.A.T. (Administrador de Traducciones de Red).
- Proporciona Restricciones de Servicios parciales a nivel Individual.
- Aislamiento completo de Nuestra Intranet.
- **Puede Mantener un Cache Configurable (Activo/Pasivo) de los datos más solicitados o recientemente recuperados para mejorar la performance de respuesta ante solicitudes**.
- Posee un Direccionador asociado al NAT.
- **Asocia Puertos (8080-80) ▸ ▸ Peticiones del usuario**
- El Servicio se basa en HTTP pero admite
- FTP - Gopher - SSL (Datos Encriptados)

Errores





LDAP SERVER (Active directory)

- Servicio de Internet, que implementa un directorio (metadirectorio) Jerárquico y Distribuido.
- Repositorio centralizado de usuarios, aplicaciones y recursos.
- Define permisos, configurados por el administrador para permitir el acceso a ciertos usuarios a la base de datos, y mantener información en privado.
- Control de Acceso a Recursos a través de reglas de provisionamiento .
- Uso de canales seguros para comunicarse con el cliente.
- Tres tipos de autenticación: No autenticación, Autenticación Simple y Usando SASL o SSL/TLS.

Componentes de un HOST - Web Server

- Colección de Ficheros o Páginas WEB que incluyen información en forma de textos, gráficos, sonidos y video además de Links o Vínculos con otros ficheros.
- Dependiendo de la configuración del Proxy o Firewall puede ser :
  - Interno
  - Externo o Institucional
- Acepta peticiones HTTP desde clientes web, y envía la información solicitada.
- Almacena información detallada acerca de las peticiones de los clientes y las respuestas del servidor.
- Funcionalidades: Autenticación, Manejo de Contenido Estático y Dinámico, **HTTPS**, Compresión, Limitación de Ancho de Banda.

Componentes de un HOST - Mailserver o Servidor de Correo

- SMTP: Protocolo Simple de Transferencia de Correo
- MTA: Agente de Transferencia de Correo.
  - Envía y recibe paquetes desde/hasta otros servidores de correo.
  - Proporciona una interfaz para las aplicaciones accedan al sistema de correo.
  - Proporciona a los usuarios buzones de correo dotados de una dirección.

Servicios de Internet – Webmail

- Correo electrónico en sitio WEB
- Acceso a cuenta a través de Navegador WEB
- Administración de Correo electrónico a través de Internet.
- Espacio de Almacenamiento Limitado.
- Puede replicar con Servidor SMTP.
- Privacidad
  - Nombres de Usuario
  - Contraseña

Componentes de un HOST – Antivirus

- Programa de chequeo de archivos de tráfico Entrante/Saliente trabajando sobre los Servicios :
  - FTP
  - HTTP
  - MAIL

Componentes de un HOST - Monitor de Pagina WEB o W-Manager

- **Bloquea el acceso a usuarios o grupos a sitios WEB No productivos o no aceptados por las políticas de la Empresa.**
- Interactúa con Base de datos de Categorías de Sitios para limitar Accesos(Cyberpatrol).
- Registra Tráfico de WEB de la Empresa.
- Configura límites de Tiempo y volúmenes de Información para cada Usuario/grupos.

Componentes de un HOST - Monitor de WEB (Web Manager)

- **Bloquea el acceso a sitios Web maliciosos según la reputación**.

- Bloquea las amenazas de malware, incluidos los ataques de día cero.
- Detecta y bloquea las descargas de spyware.
- Activa la limpieza automática de archivos de spyware y malware.
- **Bloquea la navegación por sitios relacionados con políticas ajenas a la empresa**.
- Protege frente a las instalaciones automáticas mediante el análisis de código móvil.

Componentes de un HOST - Monitor de Correo Electrónico - (E-Manager)

- Filtro de Contenidos: Para material confidencial o inapropiado.
- **Filtro de Atacheados**
- **Filtro SPAM: Bloqueador de E-Mails no solicitados**.
- Administración de EMAILS: Monitor de Patrones de Trafico.

Bandwindth Manager (B-Manager) - Monitor de Ancho de Banda

- Sistema de Máquina Virtual utilizado para Administrar Ancho de Banda.
- Trabaja Sobre el canal adjudicando ancho de banda de acuerdo a las Políticas de Uso.
- Editor Integrado de Políticas de Uso del Canal.
- Adjudica en Forma General o Particular a usuarios conectados.
- Trabaja sobre Algún Servidor del Nodo Internet o del ISP.
- Monitoreo Gráfico en Tiempo Real.
- Sus Políticas son complementarias a las de un Firewall.
- El uso apropiado evita la congestión del canal cortando procesos que ocupan mucho Ancho de Banda.
- Puede operar en combinación con VPNs, y NAT en caso de Tener Intranets.

Diodo de Datos

- **Dispositivo que separa/protege dos redes asegurando la unidireccionalidad en el flujo de información permitiendo que la información de una red llegue a otra red (pero no viceversa).**
- Hardware que asegura la unidireccionalidad en el tránsito de información de dos redes o dos servidores.
- Dispositivos de protección de perímetro utilizados habitualmente en interconexiones entre sistemas con diferentes categorías o políticas de seguridad.
- Separar redes, permitiendo el flujo de información en un único sentido y haciendo inviable la transmisión de información en el sentido opuesto.
- Casos de Uso:
    - ENTRADA DE INFORMACIÓN A RED INTERNA.
    - SALIDA DE INFORMACIÓN DESDE RED INTERNA.

Procesador Front-End (FEP) Comunicaciones Unificadas

- Plataforma de comunicaciones de presencia, mensajería instantánea, conferencia y voz para organizaciones distribuidas en WAN.
- Sobre una base de usuarios (Directorio) integra mensajes existentes en la organización y la infraestructura de telefonía.
- Permite a los usuarios realizar, recibir, reenviar o redireccionar las llamadas directamente desde su PC, teléfono fijo o teléfono móvil.
- Utilizan para validar usuarios certificado digital.
- Mensajería Instantánea y presencia ⇨ Comunicación en tiempo real de persona a persona mediante texto, voz y video, a través de una organización.
- Conferencias Web
- E-mail y calendarios compartidos y contactos
- E-Manager (Protección/preservación e-mail).
    - Filtrado (Spam)
    - Archivo (backup)
    - Continuidad (Replicando)
    - Cifrado (TLS)

WORLD WIDE WEB - WWW - Balanceo de Carga

- **Es una técnica de balanceo de solicitud de pedidos para optimizar el flujo de Información y la carga de procesamiento.**
- **Los Pedidos dejan de ser asignados a un único servidor para ser distribuidos en varios servidores ante las peticiones y/o sesiones Web.**
- **Permite preconfigurar redistribución de solicitudes ante tareas de mantenimiento o contingencia por caídas (redundancia).**
- Asegurar una distribución de carga pareja para brindar un servicio mas rápido.
- **Existen varios tipos de balanceo:**
    - **RR – DNS (Round Robin DNS)**
    - **Reverse Proxy Server**
    - **Servicios Avanzados de Redes y Clustering.**
    - **Routers de Capa 4**
    - RR-DNS (Round Robin DNS): Se aplica una técnica de Round Robin sobre un servidor DNS particular que determina a que servidor asignara la petición, en función de su disponibilidad.
    - Estas asignaciones pueden realizarse a partir de dos características a analizar:

WORLD WIDE WEB - WWW - RR-DNS

- **Por sesión:** El servidor asigna la conexión de un usuario en un momento determinado a una dirección IP (la que toque en el RR) y mantiene la asignación hasta que el usuario finalice la sesión de http hacia el mismo.
- **Por IP:** El servidor DNS puede tener asignado el método de RR para direccionar la solicitud en función de la ubicación geográfica de la dirección IP origen, para así mejorar los tiempos de transmisión y evitar "hops" innecesarios.

WORLD WIDE WEB - WWW - Reverse Proxy Servers

- Basan su performance en un método llamado: "Cache de asignación", donde se mantiene un Log de "a quien le dieron" la conexión anterior. -
- Pueden ser configurados para que mantengan un monitoreo de la cantidad de sesiones que están atendiendo cada uno de sus servidores para ver a cuál asignar la próxima petición.
- **Ventajas:**
    - Fácil Implementación.
    - Configuración Adecuada del DNS.
    - Persistencia y redundancia en la disponibilidad de los servicios.
    - Evita ataques directos de tipo DDoS sobre los servidores web.
- **Desventajas:**
    - Se requiere equipamiento extra, o al menos un procesador e interfaz de red asignados de forma exclusiva.
    - Puede sufrir ataque DDoS al servicio DNS.
- **Balanceo en Peticiones:**
    - Sistema con grado de análisis que resuelve la petición de usuario y asigna el servidor que lo atenderá.
    - El Usuario no posee información acerca de cuál será el servidor que finalmente resolverá su petición.
    - Aumenta la Disponibilidad.
    - Costo Computacional: Paquetes de datos, Administración de Tablas, ETC.
    - Soluciones a nivel de Hardware / Software

WORLD WIDE WEB - WWW - *Balanceo en Peticiones – Hardware*

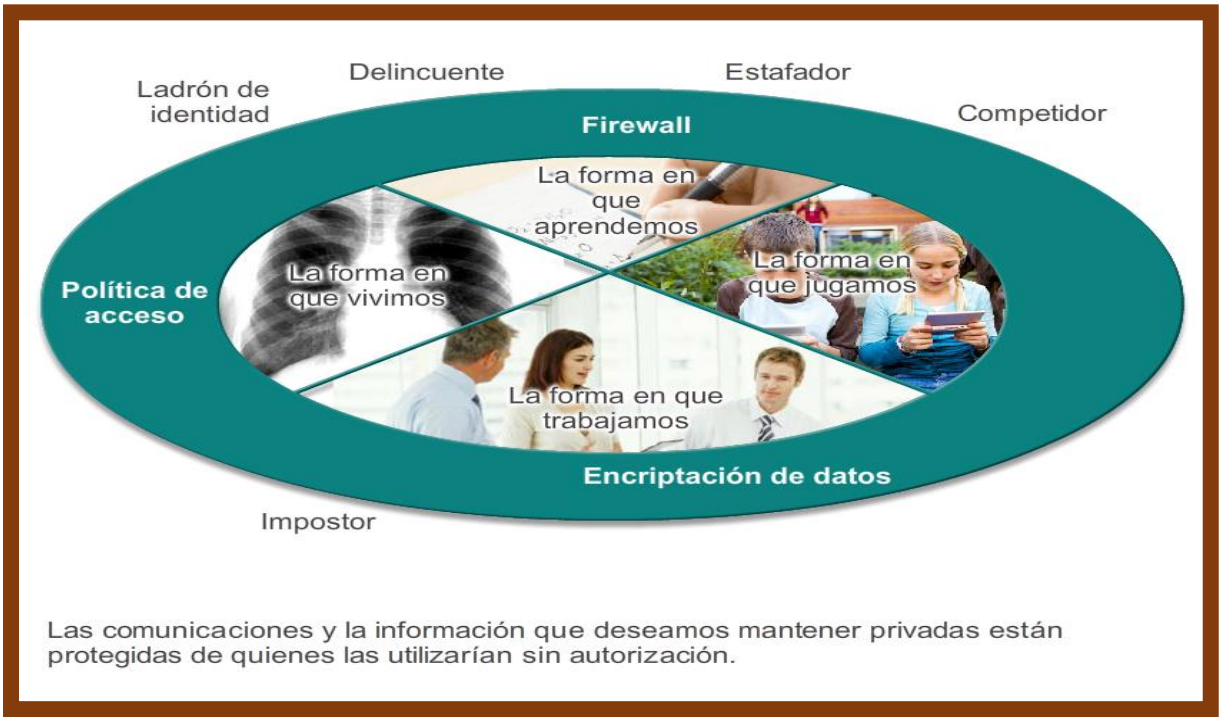
- **Switch por contenido:**
    - Análisis de contenido de paquetes
    - Redireccionan pedidos dentro del ambiente LAN
    - Utilizan Capas Altas del Protocolo TCP/IP **(4 a 7)**
    - "Conmutación Basada en Contenidos" – Poseen "Reglas de Filtrado básicas" pudiéndose definir otras manualmente.

- Asumen la función de Directores Locales y se configuran en par (Primario –Secundario) para prever caídas o contingencias.
- Se puede controlar ancho de banda usado por cliente (estadísticas de tiempos).
- **Redefinir Sub-Granjas de acuerdo a la aplicación.**
- Analisis sobre puertos TCP, URLs, HTTP Cabecera y Cookies, SSL Sessión ID, etc.

WORLD WIDE WEB - WWW - *Balanceo en Peticiones – Software*

- **Aplicación Bajo S.O. :**
  - Software embebido.
  - Nodos en Clustering (una subred).
  - Filtro Instalado en el servidor de WEB.
  - Cuando el cluster es muy numeroso (Subgranja) se lo combina con un DNS Local aplicando RR-DNS.
  - Se instalan en par - Contingencia ante caídas.
  - Algunos trabajan con “Inundación de Red”.

Seguridad informática



Las amenazas externas más comunes a las redes incluyen las siguientes:

- Virus, gusanos y caballos de Troya.
- Spyware y adware.
- Ataques de día cero, también llamados “ataques de hora cero”.
- Ataques de piratas informáticos.
- Ataques por denegación de servicio.
- Interceptación y robo de datos.
- Robo de identidad.

Por lo general, los componentes de seguridad de red incluyen lo siguiente:

- Sistemas de firewall dedicados.
- Filtrado de firewall.
- Software antivirus y antispyware.
- Sistemas de prevención de intrusión (IPS).
- Redes privadas virtuales (VPN)
- Listas de control de acceso (ACL).

Conficker (2008)

- ***Aparición en Ucrania-Configure-Ficker.***
- ***Ataca W2000, XP, Vista, Server 2003 y 2008.***
- ***Desactiva Servicios de Update, Windows Security Center, Defender,Etc.***
- *Bloquea Cuentas de Usuario, Inunda ARP (Scaneo), vuelve los controladores de dominio lentos.*
- *Hace inaccesibles actualizaciones de Antivirus y Parches de Windows.*

Stuxnet (2010-2011)

- *Gusano informático descubierto en Bielorrusia.*
- *Dedicado a espiar y programar sistemas industriales (SCADA).*
- *Ataca los sistemas de control y monitoreo de infraestructura crítica (Centrales Nucleares).*
- *Capaz de Reprogramar PLCs (Circuitos Lógicos Programables)*
- *ROOTKIT – Programa de acceso de privilegios Root y comanda accesos para extraer datos.*
- *Kapersky: Prototipo de Arma Cibernetica – producido para la Central Nuclear Natantz (Bushehr)*
- *En 2012 infecto a la Petrolera Chevron.*

Ciberguerra -Malwares - Ciberarma

- *Stars – Abril – 2011.*
- *Duqu – Sep – 2011.*
- *Frame – May – 2012.*
- *Tritón – Dic – 2017.*

Seguridad Informática

- **Integridad de la Información.**
- **Operatividad de la Información.**
- **Confidencialidad de la Información.**

$$Seguridad = \frac{1}{Operatividad}$$

Introducción Seguridad en Internet

- Internet representa riesgos de seguridad importantes que las organizaciones ignoran o subestiman por su propia cuenta y riesgo.
- Estar conectado a la red pública implica estar expuesto a permanentes ataques de diferente índole: virus, spoofing, sync flooding, denial of services, entre otros.
- *Los ataques pueden producir perdidas:*
  - *Imagen corporativa (Ej: Deface de páginas web).*
  - *Económicas (Robo de información, transferencias de dinero).*
  - *Infecciones de Malware.*

Tendencias actuales de riesgos en Internet

- *Año tras año son encontradas vulnerabilidades en cantidades exponenciales respecto de años anteriores.*
- *La cantidad de vulnerabilidades en los softwares existentes resulta enorme.*
- *A raíz de la cantidad de vulnerabilidades surgen figuras como "Patch Manager" en las estructuras de TI.*
- *Escaso tiempo desde que se descubre y anuncia una vulnerabilidad hasta el momento en que los hackers saben cómo aprovecharla.*
- *Los ataques son cada vez más eficaces llegando a poder infectar 300.000 equipos en 14 minutos (virus MyDoom Enero de 2004)*
- *La rápida propagación de estas amenazas hace muy difícil responder con la suficiente rapidez para evitar los daños*

Principios Fundamentales ISO 17799

- *Principio del eslabón más débil*
- *Defensa en profundidad*
- *Punto de control centralizado*
- *Seguridad en caso de fallo*
- *Participación universal*

- *Simplicidad*
- *Principio de menor privilegio*
- *La seguridad no se obtiene a través de la oscuridad*

Blancos de Infraestructura

• ***Web Servers / Web Services*** • ***DataBase Servers*** • ***E-mail servers*** • ***Routers*** • ***LDAP / Identity services*** • ***DNS*** • ***FTP Services*** • ***Clients*** • ***Wireless***	***Secuencia de ATAQUE*** • *Reconocimiento* – *Ingeniería Social* – *DNS Bases* • *Intento de transferencia de zona* • *Enumeración de zona* • *Investigar lacnic.net eq* • *Huellas de S.O. y Aplicaciones* – *Actividad inusual en servds* – *Escaneo (Ports, Robo, 802 y Bluetooth)* • ***Investigación – Construir la Herramienta*** • *Explotar la vulnerabilidad*

¿Por que triunfan los ataques?

- ***La operación normal de la seguridad puede encargarse aproximadamente del 95% de la infraestructura de IT.***
- *Existen 3 brechas importantes:*
  - *La **ventana de vulnerabilidad** entre el surgimiento de un incidente y la aplicación de la solución (Ej.: Parche).*
  - ***Sistemas no controlados**. Son aquellos que son ajenos pero inevitablemente interactúan con los propios. Pueden no poseer todas las actualizaciones y software de seguridad adecuados para la prevención de incidentes.*
  - ***Ataques rápidos :** se esparcen más rápido de lo que pueden reaccionar o responderlos Procesos, Tecnologías o Personas.*

Políticas de Seguridad

- Conjunto de Decisiones que, tomadas en conjunto, definen una Postura respecto a la Seguridad .
- Define los alcances y limites de uso de los Servicios de la Red para un comportamiento aceptable y cual debería ser la respuesta en cada caso
- Debe ser Aprobada al mas alto nivel ejecutivo.
- Un plan de gerenciamiento de seguridad debe contar con :
  - Definición funcional.
  - Resumen de Intención/Alcance
  - Diseño de la documentación.
  - Precondiciones de trabajo (Relevamiento)
  - Resultados de análisis del relevamiento, conclusiones.
- Un plan de gerenciamiento de seguridad debe contar con :
- Definición de políticas de seguridad, estándares y procedimientos.
  - Manejo de usuarios, contraseñas y accesos.
  - Rutinas de recupero de desastre.
- Recomendaciones y plan de seguridad física.
- Recomendaciones de segurización extendida.
- Apéndices:
  - Cumplir con las mejores practicas de la industria
  - Cumplir con los estándares de los S.O. que se utilizan

    - Evaluación de riesgos perimetrales o circundantes (de las 3ras partes que interactúan con nuestra red o computador)

Proactividad vs Reactividad

- La utilizacion de software reactivo (Antivirus, Anti-Spam, Parches de seguridad, Herramientas de remoción, etc) no es suficiente.
- Es Necesario utilizar softwares proactivos para detectar vulnerabilidades y posibles fallas en los sistemas de computadoras.
- Pero fundamentalmente, es necesario TENER UNA ACTITUD PROACTIVA, es decir, no esperar la falla, sino tratar de evitarla lo antes posible.

Modelo de N-Tiers - (N-Capas)

- **Concepto utilizado en Arquitectura-Cliente Servidor en Redes de Procesamiento de datos distribuidas**.
- Nace con la necesidad de compartir aplicaciones distribuidas en distintas computadoras y que las mismas otorguen servicios a través de Internet.
- Normaliza las Aplicaciones distribuyéndolas en capas para que el Procesamiento sea seguro y confiable.

Ejemplo

- Aplicaciones corriendo en un único servidor
    - Tier One / Una Capa.
- Aplicaciones corriendo en dos computadoras, Un servidor y un Cliente
    - Tier two / Dos Capas.
- Aplicaciones corriendo en dos computadoras y una base de datos, Un servidor , un Cliente y una base de datos que entrega datos a dicha aplicación
    - Tier Three / Tres Capas.

Seguridad en el Transporte - Protocolos de Transporte Seguros

- Para mantener la integridad de la información/ mensajes se hace necesario aplicar medidas especiales durante el transporte entre el remitente y en destinatario.
- Los Protocolos de Red tradicionales no ofrecen garantías suficientes de seguridad para Internet.

Seguridad Conceptos

- Criptografía: es el arte de transformar mensajes de modo tal que sean ilegibles para todos aquellos a los que no se les confiere el modo de acceder a los mismos.
- Criptoanálisis: es el estudio de las técnicas para quebrar mensajes criptografiados.
- Criptología: es el estudio de la Criptografía y el Criptoanálisis
- Texto plano: es un mensaje original.
- Texto cifrado: es el resultado de criptografiar un texto plano.
- Encripción: es cualquier procedimiento para transformar un texto plano en un texto cifrado.
- Desencripción: es el procedimiento de transformar un texto cifrado en el correspondiente texto plano.

X.509 - Estándar para Certificación Digital

- Pieza electrónica que prueba la identidad de su propietario , así como el derecho a acceder a la información
- **Los certificados digitales autentican usuarios y servidores. Guardan el formato de la Norma X.509.**
- Prueba la Identidad del destinatario Previsto

Protocolos de Seguridad

- *SSL - Secure Sockets Layer.*
- ***TLS - Transport Layer Security.***
- *HTTPS-Extensión de HTTP (S-HTTP)*
- ***S/MIME - Secure Multipurpose Internet Mail Extension.***
- *IPSec - IP Secury.*
- ***SET.***

SSL - SECURE SOCKETS LAYER

- *Protocolo de Transporte desarrollado por NETSCAPE para Transmisión de información Privada Vía Internet.*
- *Utiliza Métodos de Encriptación basado en la RSA (Tecnología de Clave publica encriptada).*
- *Se Ubica entre TCP/IP y HTTP y realiza la autenticación con el servidor y el cliente (X.509).*
- *Capa de Sockets Seguros*
    - *Identifica Mutuamente Cliente y Servidor.*
    - *Encripta todos los Datos para asegurar la Privacidad.*
- *Atiende exclusivamente a la confidencialidad de la información en el momento de la Transacción entre el cliente y el servidor*
- *No opera sobre la información que se guarda en el servidor.*
- *Es un Estándar aprobado por IETF - RFC 2246.*
- *Trabaja a nivel de Sockets (Puertos).*
- *Se ejecuta en una capa entre los protocolos de aplicación (HTTP, SMTP) y sobre el protocolo de transporte TCP.*

TLS (TRANSPORT LAYER SECURITY)

- Evolución del Protocolo SSL (RFC 2246).
- El protocolo se debe emplear para establecer una conexión segura entre dos partes. Tiene 2 Niveles :
    - Protocolo de registro TLS (TLS Record Protocol).
    - Protocolo de mutuo acuerdo TLS (TLS Handshake Protocol)
- Certificado X.509 v3 del interlocutor
- Utiliza Cifrado Simétrico
- Circuíto privado virtual entre dos puertos IP. Opcionalmente, asegura la autenticidad de una o ambas partes y la confidencialidad de los datos transmitidos.
- Establece una session.
    - Acuerdo de algoritmos
    - Realiza autenticación
    - Compartir de secretos
- Transferencia de datos de aplicación.
    - Asegura privacidad e integridad.

S-HTTP Secure HTTP

- Es una Extensión del Protocolo HTTP.
- Protocolo de Comunicaciones diseñado para el envío de Mensajes individuales Seguros solo con conexiones HTTP.
- Trabaja a Nivel de Aplicación, utiliza el método de encriptación PEM (Correo de privacidad mejorada).
- Trabaja Junto con SSL.
- No maneja ni voz , ni datos corrientes.
- Es un Estándar aprobado por IETF (Internet Engineering Task Force).
- Canal de cifrado apropiado que el protocolo http para poder traficar información sensible.
- El nivel de cifrado depende del navegador y del servidor remoto.
- Es utilizado principalmente en entidades bancarias y otras operaciones que requieran contraseñas y/o envío de datos personales
- Los navegadores que soportan https son: Safari, Internet Explorer, Mozilla Firefox, Opera, entre otros.

S/MIME - Secure Multipurpose Internet Mail Extension

- Protocolo de Mensajería Segura
- Trabaja a Nivel de Aplicación con certificados digitales de modo que el remitente queda autenticado.
- Utiliza tecnologías de Encriptado
- Es un Estándar aprobado por IETF (Internet Engineering Task Force). Utilizado por Explorer y Firefox
- Usa Formatos X.509 parta los certificados Digitales de Autenticación.

SET - Transacciones Electrónicas Seguras

- Norma técnica anunciada por VISA y MASTERCARD (1998) que incluye el uso de Certificados Digitales.
- Asegura y autentica la integridad de los participantes en una operación económica
- Su código aplica técnicas de criptografía manteniendo el carácter confidencial de la información**.**

IPSEC - IP SECURITY

- **Conjunto de Protocolos para soportar seguridad de intercambio de paquetes en VPNs.**
- Desarrollado por el IETF con dos modos de encriptación.
- Modo Transporte: Encripta solo Datos.
- Modo Túnel: Encripta Cabecera y Datos.
- Puede Utilizar Certificación Digital.

Tunneling - PPTP (Point to Point Tunneling Protocol)

- Protocolo de Encapsulamiento utilizado en Comunicaciones Remotas.
- Se utiliza en Redes LAN o Redes con Servidores de Acceso Remoto (RAS).
- Utiliza un ¨Túnel¨ para que Paquetes de un Protocolo se transporten a través de una Red que utilice otro Protocolo.
- El Paquete de Protocolo Origen puede ser encapsulado dentro de paquetes IP.
- El Encapsulamiento incluye un método de Encriptación.
- El Túnel establecido por medio de PPTP constituye un canal de VPN sobre Infraestructura Pública.

SLIP Serial Line Internet Protocol - PPP Point to Point Protocol

- Son Estándares de Internet para la Transmisión de Paquetes de Protocolo IP a través de línea Serie en modo Full-Duplex (Línea Telefónica).
- Recibe/Transmite los Paquetes IP (Unidad de Pequeño tamaño Transmisible).
- El más reciente y utilizado es PPP
- Para establecer la conexión Punto a Punto cada terminal dialoga con los paquetes del Protocolo LCP (Link Control Protocol), para luego ser Autenticado.
- Para realizar el intercambio de la conexión utiliza el Protocolo NCP (Network Control Protocol).
- El mas reciente y utilizado es PPP.

PAP/CHAP - PPP Autentication Protocol - CHAP Challenge Handshake Autentication Protocol

- Protocolos encargados de Autenticar al usuario en lo que respecta a Login y Password para que se realice la conexión PPP.
- Ambos almacenan Login y Password Encriptados.
- PAP Transmite en Texto Claro (No Encripta).

Seguridad Wireless

- Esquemas de encripción de datos para comunicaciones inalámbricas son:
  - WEP (56bit y 128bit)
  - WPA
  - WPA2
- Existen varios métodos que van desde el uso casero al corporativo.
  - PSK (Pre Shared Key)
  - Radius.
  - Etc.

WEP - Wired Equivalency Privacy

- “Privacidad equivalente a cableado”.
- Primer estándar de encriptación inalámbrico con el objetivo de proveer confidencialidad, control de acceso e integridad.
- Está basado en :
  - Claves de 64, 128 o 256 bits.
  - RC4, algoritmo de cifrado de datos
  - Vector de inicialización de 24bits
  - CRC, algoritmo de chequeo de integridad

- "WEP encripta los datos con el cifrado RC4 que es un cifrado simétrico que utiliza un conjunto de bits (keystream) que se combinan con el mensaje con un XOR para producir un mensaje cifrado.
- Para reproducir el mensaje, el destinatario procesa el mensaje cifrado utilizando la misma clave (keystream).
- VENTAJAS:
    - Soportado por todos los equipos, fácil de implementar.
- DEFECTOS:
    - Vectores de inicialización pequeños, pueden encontrarse dos mensajes con el mismo vector de inicialización.
    - Aumentar los tamaños de las claves de cifrado sólo aumenta el tiempo necesario para romperlo.
    - Clave de Encriptación Estática

WPA (Wi-Fi Protected Access)

- WPA fue desarrollado con el objetivo de fortalecer el protocolo WEP, (Reemplazo temporario) solucionando todas las debilidades de su antecesor.
- Basado en
    - WEP mejorado, vector de inicialización de 48 bits.
    - Temporal Key Integrity Protocol (TKIP)

  "Protocolo de Integridad de Clave Temporal", cambia claves de 128 bits dinámicamente.
    - Integridad por un código de integridad del mensaje "Message Integrity Code" (MIC)
- Dos modos de operación
    - Servidor de autenticación (RADIUS).

Distribuye claves diferentes a cada usuario.

    - "Clave pre-compartida". Pre-Shared Key (PSK) Menos seguro - uso hogareño.
- Protección contra ataques de "repetición" (replay attacks)

WPA - C/Servidor de autenticación (RADIUS)

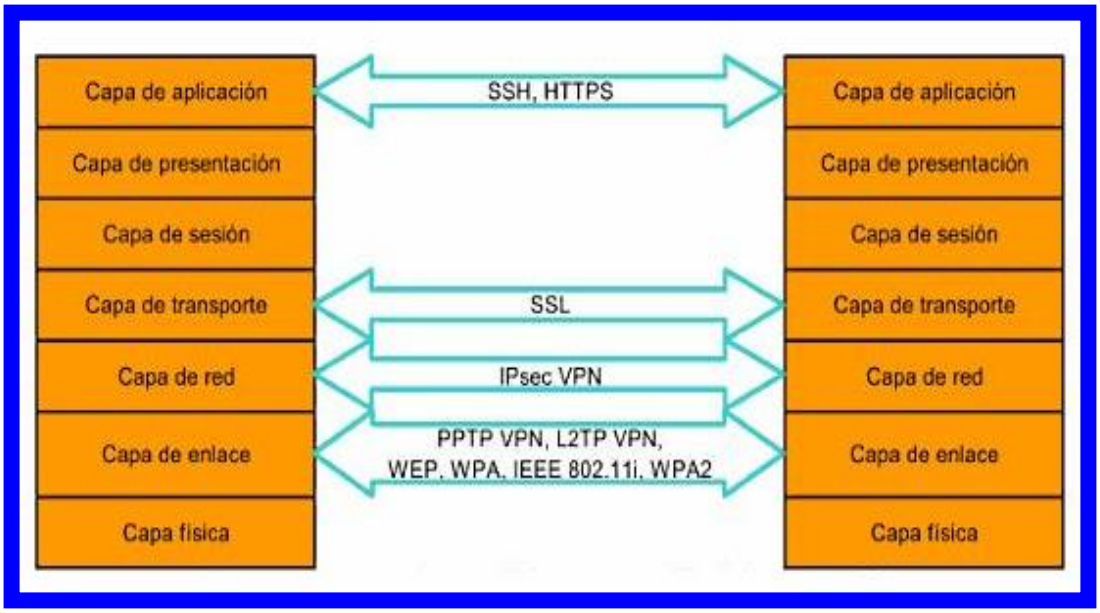
- El Servidor de autenticación luego de aceptar las credenciales del usuario, utiliza 802.1X para producir una clave única maestra para esa sesión.
- TKIP distribuye esta clave al Access Point y al cliente, creando un sistema jerárquico de administración de claves, y utiliza este par de claves únicas para generar dinámicamente claves de inscripción de datos únicas, las cuales encriptan todos los paquetes que son transmitidos en forma wireless durante la sesión del usuario.
- Cuando un usuario solicita el acceso a la red, el cliente envía las credenciales del usuario al Servidor de autenticación a través del AP.
- Si el servidor acepta las credenciales del usuario, la clave TKIP maestra es enviada tanto al cliente como al AP.
- Se completa el proceso instalando las claves entre el AP y el cliente.
- Usuarios hogareños y las pequeñas empresas que no tienen Servidor RADIUS.
- Para estos casos, WPA provee la opción de utilizar Pre shared key (PSK).
- La diferencia básicamente radica en que la contraseña es manualmente ingresada en los clientes y en los AP's y es utilizada para la autenticación.

WPA 2 (Wi-Fi Protected Access)

- Este protocolo de encriptación forma parte del estándar IEEE 802.11i
- Reemplaza formalmente a WEP y otras funcionalidades originalmente creadas en el estándar original 802.11i.
- Nuevo algoritmo basado en AES (Advanced Encryption Standard, sucesor de DES - DataEncryption Standard).
- AES es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de EEUU el Instituto Nacional de Estándares y Tecnología (NIST).
- Requerimientos de inscripción más fuertes.
- Agrega dos mejoras para soportar el roaming de los clientes que se mueven entre los diferentes Access Points:

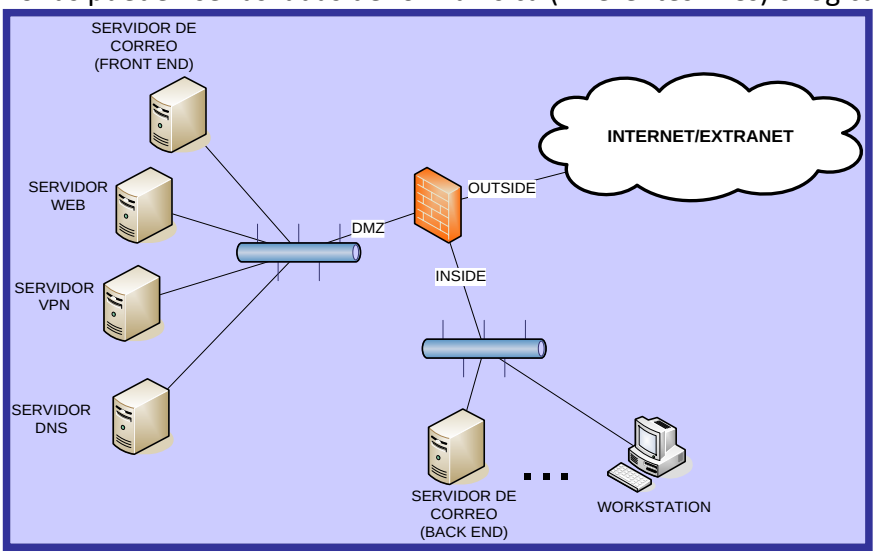
- El soporte caching de la clave PMK (Pair-wise Master key) utilizada en cada sesión entre el AP y el cliente permiten reconectar al cliente a un Access Point que ya haya utilizado si la necesidad de re-autenticar.
- El soporte de pre-autenticación en WPA2 permite a un cliente pre-autenticar con el Access Point al que se dirige mientras mantiene la conexión con el Access Point que abandona.

Seguridad Modelo OSI



Configuración de Nodo de Internet - Topología y Zonas

- Son secciones aisladas a través de un dispositivo Firewall. Habitualmente existen 3 zonas básicas: Inside, DMZ, Outside.
- Cada una de estas zonas posee un nivel de seguridad distinto, yendo de mayor a menor nivel respectivamente.
- Estas zonas deben ser definidas en función de los servicios que debe prestar cada equipo conectado a las mismas, considerando los accesos seguros y no seguros que deben soportar.
- Estas zonas pueden ser asiladas de forma física (Diferentes NICs) o lógica (VLANS)



Configuración de Nodo de Internet - Topología y Zonas – Outside

- Es el área no segura.
- Los dispositivos que se encuentran conectados a esta sección o zona se encuentran fuera del control de los administradores de seguridad o de la compañía.
- Puede ser origen de conexiones con malas intenciones, por lo que deben proveerse los mecanismos de defensa y restricciones adecuados para evitar intrusiones o accesos indebidos.

Configuración de Nodo de Internet – Inside

- Es la zona más segura de la red.

- Se distingue por la configuración restrictiva respecto de las otras zonas de seguridad.
- NUNCA debe poder ser accedida desde el exterior en forma directa.
- En esta zona pueden residir los Servidores de Correo Electrónico Interno (SMTP), el Servidor Proxy , el Servidor de Web Interno , el Servidor de Nombre de Dominio Interno (DNS Interno) Etc.

Configuración de Nodo de Internet – DMZ

- Es donde se alojan los equipos que podrán ser accedidos desde el exterior y el interior de la red.
- Se caracteriza por poseer cierta flexibilidad en las políticas de servicios en comparación a la zona INSIDE (Inflexible).
- En esta zona pueden residir los Servidores de Correo Electrónico Externo (SMTP), El Servidor de Web Externo ,Webmail Etc.

Configuración de Nodo de Internet - Otras Zonas

- Son aquellas que contienen equipos que, aun cuando pertenecen a la Institución , no se consideran suficientemente seguros como para ser integrados dentro de la Red institucional.
- En esta zona pueden residir los Servidores de Acceso Remoto para usuarios externos conectados por módem, Maquinas para Capacitación, Etc.

Configuración de Nodo conectado a Internet – Zona de Sistemas Legacy

- Corresponde a la parte de la topología del nodo que contiene a la Red Con Servidores de Sistemas que perduran en el tiempo y son los Sistemas Administrativos y De gestión más sensibles de la Organización.
- Es la zona de mayor Seguridad dentro de la Topología de la Red.
- Puede Estar Protegido Por un Firewall, Proxy o Servidor de Transacciones Seguras.

Servidor de Web de Transacciones Seguras

- Posee Un sistema operativo asegurado que permite resguardar dentro de esta Zona Servidores Legacy con sistemas críticos (Financieros, Administrativos, Logísticos) .
- Prohíbe todos los servicios de Internet que accedan a esta zona y pongan en peligro la Operatividad de los Mismos.
- Ej FTP, TELNET , ETC
- Es Un Servidor de Seguridad para Nodos de Internet diseñado para proteger los Sistemas Legacy y las bases de datos puestas a disposición para consultas de usuarios de Internet.
- Consiste en un computador con una Interfaz de Red de doble boca , que hace de Pasarela (Gateway) entre la Zona de Intranet / Internet y la Zona de Seguridad en la Red definida a tal efecto.

Servidor de Web de Transacciones Intermedias

- En caso que el Usuario de Internet necesite acceder a servicios de esta zona se debe establecer un servidor intermedio de Web que atienda las consultas de usuarios y solicite los datos a los Sistemas Legacy cumpliendo así con la teoría del modelo de N-capas.
- Ningún usuario habilitado a realizar consultas podrá acceder directamente a los Servidores Legacy, teniendo que comunicarse mandatoriamente a través de este servidor de Web Intermedio.
- Este servidor intercambia los Set de Datos necesarios para cumplir con las consultas solicitadas y las entrega a los usuarios como una página Web.
- Por lo tanto es mandatorio definir con autorización de los Usuarios que sistemas se podrán acceder y que usuarios están autorizados a realizar dichas consultas.

Políticas de Restricción de Servicios protegidos por el firewall

- FTP Seguridad
- TELNET Prohibido
- SSH Restringido
- IRC – ICQ Ancho de Banda
- REAL AUDIO Ancho de Banda
- File Mgmt. Restricción de Lugares y Cuotas
- Mail Mgmt. Restricción de Atacheados
- Mail Mgmt. Filtro Spam Activado
- Bw Mgmt. Restricción de Ancho de Banda

- Antivirus HTTP, MAIL , FTP y Aplicaciones

Sistemas de detección de intrusos

- **Los sistemas de detección de intrusos (IDS/IPS –Intrusion Detection/Prevention Systems-) permiten detectar ataques registrar y dar aviso en la medida que se produzcan.**
- Identifican el tráfico que viola las políticas de seguridad a través de análisis de protocolo y búsquedas de contenido pudiendo finalizar de manera automática cualquier sesión transgresora.
- Programa encargado de Vigilar y Auditar los Puertos Disponibles en un nodo de Internet.
- Sobre los Accesos Indebidos o Servicios prohibidos de Intentos de Usuarios no autorizados

⬇

Genera las Alertas necesarias registrando la información respectiva de la solicitud o incursión.

- A través de una consola de gestión centralizada permiten monitorear y controlar toda la red así como definir reglas y políticas.
- Manejan en forma automática la gestión e instalación de parches.
- Registra en un Archivo el Origen de donde proviene la incursión (Dirección IP), El Servicio , el Puerto , la Fecha y Hora de cuando fue realizado el Intento ☛ Archivo de Alertas.
- Estos datos permiten rastrear de donde se realizó la incursión (InterNIC/NIC).
- Permite configurar los envíos a cuentas de Mail, Radio llamado o Te celulares

Políticas de Restricción de Servicios

- Protocolo sencillo de Administración de Redes (SNMP) : puede utilizarse para examinar la tabla de ruteo en un dispositivo, esto sirve para aprender los detalles más íntimos acerca del objetivo de la topología de red perteneciente a una organización.
- Es un servicio prohibido para usuarios externos con respecto a los servidores de los nodos y topologías de Intranet.
- **TraceRoute: puede utilizarse para relevar el número de redes intermedias y los ruteadores en torno al servidor especifico.**
- Por medio de dicho programa se puede verificar la ruta que realiza un conjunto de Paquetes o bloques de información a través de una Red de Internet.
- Los nodos de Internet prohíben el uso de dicho programa a través de sus servidores o su Intranet.

Whois :

- Es un servicio de información que provee datos acerca de todos los dominios DNS y el Administrador del sistema responsable para cada dominio.
- No obstante que esta información normalmente es anticuada.

DNS

- Es el Servicio que permite la concesión de los usuarios colocando un nombre y que el mismo le devuelve la dirección de Internet de la Red.
- Si el servicio no es protegido un usuario experto puede acceder para obtener una lista de las direcciones IP y sus correspondientes nombres utilizando el Programa Nslookup.

Finger :

- Es un protocolo que permite revelar información detallada acerca de los usuarios respecto a nombres de Login, números telefónicos, tiempo y última sesión, etc. de un servidor en específico.

Ping:

- Es un Software que puede ser empleado para localizar un servidor particular y determinar si se puede alcanzar.
- Esta simple herramienta puede ser usada como un programa de escaneo que por medio de solitudes a la dirección de un servidor haga posible construir una lista de los servidores que actualmente son residentes en la red.

Rutinas Anti-Spoofing :

- Los Firewall están dotados de una regla que evita el procedimiento que cambia la fuente de origen de un conjunto de datos en una red, por ejemplo, adoptando otra identidad de remitente para engañar al mismo.
- Esta regla se la denomina Zero Spoofing y es activada para identificar correctamente a corresponsales y remitentes para que no oculten su identidad o procedencia dentro de la Red.

Principales ataques: Denegación de Servicio (DoS)

- Busca la imposibilidad de la víctima de acceder y/o permitir el acceso a un recurso determinado.
- Intenta corromper/saturar los recursos de un sistema por medio de peticiones para lograr la desactivación o impedir el acceso a otros usuarios.
- Provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema.
- Consumo de recursos computacionales, tales como ancho de banda, espacio de disco, o tiempo de procesador.
- Alteración de información de configuración, tales como información de rutas de encaminamiento.
- Alteración de información de estado, tales como interrupción de sesiones TCP (TCP reset).
- Interrupción de componentes físicos de red.
- Obstrucción de medios de comunicación entre usuarios de un servicio y la victima, de manera que no puedan comunicarse adecuadamente.
- **Inundación SYN (SYN Flood)**
- Inundación ICMP (ICMP Flood)
- SMURF (ICMP Flood)
- Inundación UDP (UDP Flood)
- Peer-to-peer
- Utilización de recursos
- A nivel de aplicación
- Degradación de servicio
- Slowloris (HTTP requests parciales. low-rate)
- BotNet.

Principales ataques: Jamming o Flooding (DoS)

- **Busca generar solicitudes maliciosas a un servicio con la finalidad de hacer que el mismo se sature o entre en un modo de espera, de esta forma anula o limita su funcionamiento.**
- Ataques que saturan los recursos del sistema: memoria, disco o red.
- Se producen mediante peticiones de conexión utilizando una IP falsa.
- Los mas conocidos de este tipo son el “ping de la muerte” (bloqueando el equipo) o el envío de cientos de mails al mismo tiempo.

Principales ataques: Syn Flood (DoS)

- El ataque se basa con el comienzo de cientos de conexiones a un servidor, e interrumpiéndola inmediatamente.

Principales ataques: BotNet(DoS)

- Conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática.
- Conjunto de terminales que ejecutan software que permite su control total o parcial desde ubicaciones remotas.
- Las terminales se denominan bots o zombies.
- El artífice de la botnet puede controlar todos los terminales/servidores infectados de forma remota.

Principales ataques: Denegación de Servicio (DoS)

- **Connection Flood:** Se basa en la característica de los ISP de tener un tope máximo de conexiones por falta de balanceo de carga.
- **Mail Bombing:** Envío masivo de mails a un mismo destinatario saturando la casilla de mail.
- **Mail Spamming:** Es enviar publicidad sin la previa autorización del usuario.
- El concepto de spamming se aplica a Blogs, Redes Sociales y Telefonía Móvil.

Principales ataques - Port Scanning (Escaneo de Puertos)

- Se Busca encontrar puertos abiertos mediante un escaneo de IP, el escaneo se realiza por rangos o a una IP en particular.
- Los Firewalls actuales identifican el escaneo de puertos consecutivos y detienen el ataque.
- Aunque hay escaneos no consecutivos y alternativos entre IP para despistar a los dispositivos de seguridad.

Tipos de Escaneo

- **Conexión TCPconnect():** búsqueda un puerto abierto.
- **FTP Bounce Attack**: Conexión mediante FTP desde un servidor Proxy para dificultar conocer origen del ataque.
- **TCP SYN**: Envío de un paquete de comienzo de comunicación determinando puertos abiertos.
- **TCP FIN Stealth Port Scanning**: Envío de un paquete de fin de comunicación para conocer puertos abiertos o cerrados.
- **Escaneo de Fragmentación:** Transmisión de pequeños paquetes para monitorear la red.
- **Eavesdropping-Packet Sniffing:** se "olfatea" los paquetes para detectar IP's.
- **Snooping-Downloading:** ídem al anterior y además se hacen copias locales de los paquetes.

Principales ataques: Autenticación

- Estos ataques se caracterizan por la disponibilidad de credenciales reales por parte de un atacante malintencionado.
- Se toman sesiones ya establecidas por la victima o se obtiene su nombre de usuario y password.

Ataques de autenticación – Phishing

- **Tienen por objeto, el robo de datos personales de identidad e información de credenciales financieras**.
- **Se simula un sitio web para capturar datos de login con una pantalla de ingreso al sistema.**
- Utilizan en combinación Ingeniería Social y tecnología para alcanzar sus objetivos.
- Algunos ejemplos utilizados son:
  - Emails falsificados y forjados.
  - Llamadas telefónicas para "Corroborar" información.
  - Robo de identidad autoritativa para la obtención de información por niveles menores.

Ataques de autenticación - Pharming

- **Consiste en el robo de identidad, pero no de un usuario, sino de un Sitio Web.**
- **Utilizan técnicas de "DNS Hijacking" y "DNS Poisoning" que consisten en la publicación ilegitima de resolución de un dominio mediante la modificación de los registros de un servidor DNS.**
- Otra técnica es registrar un dominio parecido y "Pescar" a los desprevenidos.

Ataques de autenticación – Spoofing

- Consiste en sustituir la fuente origen por datos adulterados, adoptando una identidad falsa.
- El objetivo es engañar a la seguridad para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado (Firewall/Filtro de Red).
  - IP spoofing
  - ARP spoofing
  - DNS spoofing
  - Web spoofing
  - E-mail spoofing
- Fake-mail: es otra forma de Spoofing, consta con el envío de mail con un remitente falso.

Ataques de autenticación

- **Hoping:** el atacante ingresa en un sistema ajeno, luego a otro, a otro, para hacer imposible la verdadera localización.
- **IP Session Hijacking:** una vez que el usuario verdadero ingresa al sistema, se toma esa conexión sin restricciones de seguridad.
- **Obtención de passwords:** se obtiene la password mediante técnicas de espionaje y aprovechando la poca frecuencia de cambios de password.
- **BackDoors:** se utiliza un código puesto en sistemas finales para ingresar sin restricciones de seguridad.
  - Permite saltearse métodos de autenticación para realizar determinadas tareas.
- **Exploits :** Son programas que aprovechan la debilidad , fallo o error de un sistema para ingresar al mismo.

Ramsomware

- **“Secuestro de Datos”.**
- **Programa que restringen el acceso a determinadas partes o archivo del sistema operativo infectado.**
- Retienen el control del equipo.
- Encriptan la información almacenada en el mismo para que no pueda ser accedida.
- Solicitan un rescate financiero en criptomonedas para que sean desactivados.
- Algunos ejemplos son “Peyta, Reveton, Cryptolocker, TorrentLocker, Cryptowall, TeslaCrypt. Mamba, WannaCry. ETC.

Ataques Wireless

- **Man in the Middle:** Consiste en una técnica de sniffing de paquetes circulante e inyección de datos malignos para producir determinados resultados.
- **ARP Poisoning:** Envenenamiento de las tablas de ARP existentes mediante el reclamo de direcciones IP asignadas a otras direcciones físicas.

- **WEP/WPA header sniffing:**

Un atacante puede generar a propósito la reconexión de los clientes ya conectados mediante diferentes técnicas, logrando así que se re-genere el “Handshake” de conexión inicial (El cual no es encriptado).
DDoS: Son utilizados para inhabilitar dispositivos momentáneamente y obligar a los clientes auténticos a solicitar una reconexión a la red.
Robo de identidad (MAC Spoofing): “Escuchar” el tráfico de red e identificar la dirección MAC de una computadora para clonarla.
Inyección de red: Inyectar comandos de reconfiguración que afecten a routers, swithes.

Virus

- ***Programa de Terminal que puede infectar otros programas modificándolos para incluir una copia de sí mismo.***
- *Tienen la función de propagarse, replicándose, y algunos contienen además una carga dañina (payload).*
- ***Puede provocar desde una simple broma hasta daños importantes en los sistemas o bloquear las redes informáticas generando tráfico inútil.***
- *Los virus inician su dispersión debido a una ejecución intencional (inocente) que provoca la infección y propagación de este software malintencionado.*
- *Se pueden prevenir.*
- Se adjuntan a programas o archivos e insertan su propio código “genético” dentro de ellos para propagarse.
- GUSANO
- TROYANO
- VIRUS DE MACRO
- VIRUS DE SCRIPT
- NUEVO DISEÑO
- CÓDIGO JAVA MALICIOSO
- CÓDIGO ActiveX MALICIOSO
- VIRUS DE SECTOR DE ARRANQUE
- VIRUS DE FICHERO DE ACCIÓN DIRECTA

Prevencion de Virus

- El 50% de los casos de infecciones de virus se debe a una ejecución autorizada por el usuario.
- Las aplicaciones de seguridad, no presentan ninguna ventaja si el usuario no es educado respecto de los virus informáticos.
- Las políticas de seguridad resultan fundamentales.

Gusano (Worms)

- *Tienen la propiedad de residir en memoria y duplicarse a si mismo (Consumo de Recursos).*
- *No requieren intervención del usuario.*

- *Se transmiten generalmente por fallas o "agujeros" de seguridad existentes, los cuales aprovechan para vulnerar los sistemas.*
- *La infección de una sola estación puede significar el contagio de toda una red.*
- *La velocidad de propagación y transmisión de estos puede provocar saturaciones de sistema y de la red.*

Caballos de Troya (Trojans)

- *Un troyano es un "Malware" escondido dentro de una aplicación que aparenta ser legitima o fidedigna.*
- *El nivel de daños que pueden provocar varia ampliamente.*
- *En la mayoría de los casos los usuarios no se percatan que tienen uno instalado en su maquina.*
- *Abren puertas traseras, o "Backdoors" que son utilizadas para acceder a las computadoras "Victima" de forma remota y usarlas como "Zombies".*
- *Recientemente, virus troyanos se expanden masivamente por ordenadores no protegidos (sin Firewall).*
- *Las terminales/Computadras infectadas son utilizados por el spammer como "zombis", que envían spam a sus órdenes, pudiendo incluso rastrear los discos duros o correos nuevos (sobre todo cadenas) en busca de más direcciones.*
- *El usuario ignora haber sido infectado (que no tiene por qué notar nada extraño) y al ser identificado como spammer por los servidores a los que envía spam sin saberlo, lo que puede conducir a que no se le deje acceder a determinadas páginas o servicios.*
- *Actualmente, el 40% de los mensajes de spam se envían de esta forma.*

Antivirus

- *Son una necesidad básica de cualquier computadora, desde hogareñas hasta servidores corporativos.*
- *La defensa de estos ante un virus informático dependen de la brecha de tiempo entre el reporte del incidente de seguridad y la respuesta y solución por parte del fabricante.*
- *Las diferentes empresas de seguridad se atribuyen la mejor detección, pero la realidad es que el disponer de un Antivirus instalado no asegura la protección total de una computadora o servidor.*
- *Su función primordial es la prevención de ejecución de código malicioso y su replicación en memoria.*
- *Analizan desde archivos hasta comunicaciones (E-mail, trafico Web, etc.)*
- *NO protegen la computadora de vulnerabilidades particulares de algunas aplicaciones de servicio, sin embargo generalmente si lo hacen con los servicios estándar del S.O.*

Appliances Antivirus

- *Dispositivos de hardware avocados al análisis de protocolos y aplicaciones en particular.*
- *Colocados de forma perimetral pues estos no pueden actuar directamente sobre las estaciones de trabajo sino sobre las comunicaciones que se llevan a cabo en la red.*
- *Proveen una independencia en cuanto a capacidad de procesamiento de las computadoras que protegen.*
- *Son independientes del sistema operativo usado en la estación de trabajo.*

Política Antivirus

- Ejecutar siempre el antivirus corporativo y mantener actualizados tanto el engine como los patrones de virus.
- Nunca abrir archivos o macros de remitente desconocido, no confiable sospechoso. Borrarlos y vaciarlos de la papelera.
- Eliminar el spam, cadenas de correo y correo basura similar, sin reenviar; de acuerdo con la Política Corporativa de Uso Aceptable de e-mail
- Nunca descargar archivos de fuentes sospechosas. En la media de lo posible, ejecutar solamente los programas descargados de la URL original o de la intranet corporativa.
- Evitar las carpetas compartidas salvo que sea requisito indispensable.
- *Pasar SIEMPRE el antivirus a los Dispositivos USB.*
- *Hacer copia de seguridad regular de los datos críticos y de las configuraciones, y almacenarlos en lugar seguro.*

- *En caso de conflicto de pruebas de aplicaciones con el antivirus, pasarlo primero antes de deshabilitarlo. Pasar posteriormente la prueba e inmediatamente volver a activar el antivirus.*
- *Comprobar esta política frecuentemente, debido a que prácticamente a diario se descubren nuevas formas de infección que podrían requerir un cambio en el procedimiento.*

Spyware

- ***Se llama "pest" (peste o alimaña) a toda aplicación instalada en el PC de un usuario, sin su consentimiento o como parte de un consentimiento genérico, habitualmente se ejecuta en background y es resistente a su desinstalación. (quedan incluidos por definición los virus)***
- ***El objetivo suele ser ilícito o por lo menos no acordado con el usuario***
- *Son aplicaciones cuyo objetivo es enviar información del sistema donde reside mediante la utilización de la conexión de red en forma oculta a empresas de publicidad en Internet.*
- *Teniendo una gran similitud con los Troyanos, estos programas no presentan un peligro (manipulación o daño) para el sistema afectado, pero si violan la privacidad de la información*

SPAM

- *SPAM son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico…"*
- *Generalmente el origen de estos correos son servidores fantasma y las direcciones de remitente son falsas.*
- *Este tipo de envió de correo masivo son utilizados para el fraude electrónico tipo PHISHING.*

Software & Appliances AntiSpam

- *Su función es la del análisis de del contenido de los correos electrónicos para clasificarlos y determinar si estos cumplen con los requisitos para ser clasificados como SPAM y separarlos de los mails legítimos.*
- *Este tipo de aplicaciones trabajan sobre los protocolos de correo electrónico (Pop3, ESMTP, SMTP, IMAP, etc.)*
- *Existen listas de bloqueo llamadas "Blacklists" donde figuran listados de direcciones de mail, dominios, y proveedores de Internet que realizan SPAM.*
- *También pueden ser identificados por bloque de dirección IP (Generalmente asociado a un ISP)*

Centro de Operaciones de Seguridad (SOC)

- ***Unidad centralizada compuesta por personas capacitadas, procesos y tecnologías que trabajan en conjunto para brindar capacidades de seguridad integrales.***
- *Incluyen la prevención, detección e investigación, y respuesta a amenazas e incidentes de ciberseguridad.*
- *Visibilidad centralizada de toda la actividad que ocurre en su entorno.*
- *Detección y respuesta de amenazas en tiempo real.*
- *Supervisión 24x7 de los datos del registro del sistema y del tráfico de la red.*
- *Una visión integral y centralizada de la postura de seguridad de una empresa.*
- *Caza e investigación de amenazas*.
- *Administración de Usuarios, Aplicaciones y Procesos.*

Monitores de Seguridad - (Ends Points) – DLP

- Impide la introducción de software malicioso o no autorizado.
- Proporciona mayor control - puede bloquear dispositivos por clase, extensiones de archivo, puerto físico o identificador de dispositivo, desde un único lugar.
- Permite conceder acceso temporal al dispositivo o puerto durante un período de tiempo estipulado.
- Monitoriza centralizadamente la red, detecta dispositivos conectados y realiza varias tareas
- Protege automáticamente equipos detectados desplegando un agente y una directiva de bloqueo predefinida.
- Data Lost Prevention.
- Evita la fuga y el robo de información mediante el control integral del acceso a dispositivos portátiles de almacenamiento con mínimo esfuerzo administrativo.

- Protección de Red de Dispositivos Portátiles como :
  - Unidades USB
  - iPods, iPhones, Smartphones
  - PDAs.

Conclusión

- Prevención, detección y reacción constituyen tres conceptos clave en todo sistema de protección.
- Internet es una herramienta poderosa para las organizaciones actuales y es importante entender los riesgos inherentes a la seguridad cuando se implementa esta tecnología**.**

Firewall Personal

- Proporciona un balance óptimo entre seguridad y accesibilidad.
- Barrera de seguridad para el acceso a las comunicaciones de la terminal.
- Habilita / Desabilita el acceso a servicios.

Firewall Personal - Control de Puertos

- Consiste en controlar puertos abiertos mediante una aplicación de seguridad en Memoria.
- Los Firewalls actuales controlan los Puertos actuando sobre los paquetes y aplicaciones.
- Pueden configurarse en forma manual o automática.

Recomendaciones – Generales

- *Si recibe un correo o por teléfono solicitud de información personal de un banco , entidad financiera o tarjeta de crédito ▶ NO RESPONDA.*
- *No envié información reservada por mail sin no está cifrada o encriptada.*
- *No acceda a entidades publicas o financieras de locutorios o lugares dudosos.*

Keylogger

- ***Key-tecla / logger- registrador: es un software o hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet.***

Recomendaciones – Generales

- Mantenga actualizado el Antivirus.
- Revise en los resúmenes bancarios cargos u operaciones no autorizadas.
- No descargue ni abra archivos de fuentes no confiables.

Firma Digital

- **Es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje**

Beneficios

- Garantía de Procedencia
- Seguridad de no Intervención
- Identificación del firmante

Funcionamiento

- No es una firma escrita
- Es un software
- Se basa en algoritmos (números primos de hasta 2048 bits)

Algoritmos

- W. Diffie y Martin Hellman (1976)
- RSA (Rivest/Shamir/Adleman) (1977)
  - Internet Explorer
  - Netscape Navigator
- DSA (Digital Signature Algorithm)
  - Departamento de Estado
- PGP (Pretty Good Privacy) – (1991)
  - Philip Zimmermann

- e-mail

Método

- Todos los algoritmos se basan en un mismo método:
- Se utilizan dos claves
  - Privada
  - Pública.
- Encriptado/Desencriptado de claves.
- Operaciones matemáticas con números primos (512 a 1048 bits).

Remitente

- Escritura del mensaje.
- Hashing del texto (algoritmo).
- Encriptación con clave privada.
  - Firma Digital
- Envío del texto con la Firma Digital.

Destinatario

- Recepción Texto del mensaje y Firma.
- Hashing del texto (c/clave pública).
- Desencriptado de la Firma.
- Comparación de los mensajes.
- Igualdad de mensajes
- Remitente Válido
- Mensaje sin alteraciones.

Métodos Criptograficos

- Método simétrico: es un algoritmo de encripción tal que la clave para encriptar es la misma que para desencriptar.
- Algunos de estos algoritmos son:
  - DES (block, clave de 56 bits)
  - 3DES (block, clave de 112/168 bits)
  - RC2 (Block,reemplazo DES, tamaño clave variable)
  - RC4 (stream, clave variable)
  - IDEA (block, clave de 128 bits)
- Método asimétrico: es un algoritmo que utiliza claves distintas para encriptar y para desencriptar. Son los únicos métodos que permiten identificar al emisor de un mensaje, y por lo tanto los únicos que permiten implementar la firma digital. Algunos de estos algoritmos son:
  - RSA (Rivest, Shamir, Adelman)
  - DSA (Digital Signature Algorithm)

Ventajas y desventajas de los algoritmos simétricos y asimétricos.

- Los algoritmos simétricos son mucho más rápidos que los asimétricos, pero tienen el problema de que es necesario distribuir las claves, dado que el emisor y el receptor deben usar las mismas en cada comunicación.
- Los algoritmos asimétricos usan claves distintas con lo que evita el problema de la distribución – pero son lentos.
- La solución usada universalmente es llegar a claves comunes con un método asimétrico y luego cambiar a uno simétrico para la transmisión masiva.

Valor

Firma Digital = Firma Holográfica

Fima Electronica

- *La firma electrónica es una manera de representación y confirmación de la identidad de un sujeto en el medio electrónico.*

- *Técnicamente, es un conjunto de datos únicos encriptados.*

FIRMA ELECTRÓNICA	FIRMA DIGITAL
No hay transformación.	*Es la transformación de la firma de un mensaje.*
No se usan claves.	*Se utiliza una clave pública y otra privada.*
Se utiliza para identificar a su emisor (signatario).	*Asegura la autoría.*
No asegura su integridad.	*Asegura la integridad del mensaje.*
Puede ser la representación electrónica de una firma hológrafa.	*No es una representación electrónica de una firma hológrafa.*
Puede ser estampada por medio de elementos de Digitalización	*Es una subcategoría dentro de la firma electrónica.*
Lo electrónico se vincula con otras tecnologías como la mecánica, magnética, eléctrica, óptica.	*No se vincula con otra tecnología especifica*
En caso de ser desconocida corresponde a quien la invoca acreditar su validez.	*Se presume valido, salvo prueba en contrario.*

Aplicaciones de Firma Digital

- Mensajes con autenticidad asegurada
- Contratos comerciales electrónicos
- Factura Electrónica
- Transacciones comerciales electrónicas
- Dinero electrónico
- Notificaciones judiciales electrónicas
- Voto electrónico
- Decretos ejecutivos (gobierno)
- Contratación pública
- Declaraciones Juradas
- Etc.

Seguridad de la Firma Digital

- Autenticación
- Imposibilidad de Suplantación
- Integridad
- No repudio
- Auditabilidad
- Acuerdo de Claves secretas

Certificado de Seguridad

- Imagine que envía cartas por correo en un sobre transparente, Cualquiera que tenga acceso a él podrá ver los datos. Si parece valiosa, pueden hacerse con esa información o modificarla.
- Autoridad de certificación, es la encargada de emitir los certificados, verifican el nombre de dominio y la existencia de su empresa, la propiedad del nombre de dominio y su potestad para solicitar el certificado.
- Un certificado SSL establece un canal de comunicaciones privado que permite cifrar los datos durante su transmisión.
- El cifrado codifica los datos, fundamentalmente creando un sobre que preserva la confidencialidad del mensaje
- Una Entidad Autorizada, denominada autoridad de certificación, es la encargada de emitir los certificados SSL

Marco Legal

- Ley Nº 25.506 de Firma Digital
- (B.O.del 14/12/2001)
- Decreto Reglamentario Nº 2628/02
- (B.O. del 20/12/2002) establecen una Infraestructura de Firma Digital de alcance federal y la creación del Ente Regulador de la Firma Digital
    - Firmadigital.gov.ar
    - pki.gov.ar

Marco regulatorio

- Neutralidad tecnológica: se distingue entre la firma digital (una tecnología específica) y la firma electrónica, esta última incluye a la anterior pero está abierta a otro tipo de firmas como la biométrica (ADN, retina, etc.)

Clave Publica

- PKI – Public Key Infrastructure
- Estructura
    - Organismo Licenciante.
    - Organismo Auditante.
    - Autoridades Certificantes.
    - Suscriptores.

Organismo Auditante

- En nuestra legislación el Organismo Auditante es el Ente Regulador y sus funciones como tal son:
- Auditar periódicamente al Organismo Licenciante y a las Autoridades Certificadoras Licenciadas.
- Realizar los informes correspondiente

Actividades del Organismo Licitante

- Otorgar las licencias que acreditan a las AC
- Denegar solicitudes, Revocar licencias
- Verificar que las Autoridades Certificadas Licenciantes utilicen sistemas técnicamente confiables.
- Aprobar el manual de procedimientos
- Preparar el Plan de Auditoría junto con el Organismo Auditante.

Actividades de la AC

- Emitir certificados
- Ofrecer o facilitar servicios de registro y estampado cronológico en la transmisión y recepción de datos.
- Ofrecer servicios de archivo y conservación de mensajes.
- Revocar/Suspender certificados
- Renovar certificados

Actividades del Suscriptor

- Proveer todos los datos a la Autoridad Certificante Licenciada
- Mantener el control de su clave privada
- Informar cambios de datos