¿Usted dejaría que
en una oportunidad
cualquiera,
un millón de pesos
entre a su casa?

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Juan Fdo. Hurtado R.

juan.hurtado@comfenalcoantioquia.com
fhenet@yahoo.es

Comfenalco ANTIOQUIA

OBJETIVOS

- Definir conceptos básicos de comunicación en redes.
- Socializar el concepto que se tiene de Internet y los servicios que ofrece.
- Conocer algunos servicios utilizados para la conexión a Internet.
- Acceder a Internet desde un navegador seguro.
- Dar a conocer elementos fundamentales que permitan tener un acercamiento inicial a los diferentes aspectos relacionados con la seguridad informática.

AGENDA

1. Conceptos de redes
2. Internet
3. ¿Qué es seguridad informática?
4. Principios de seguridad informática
5. Seguridad física y seguridad lógica
6. Vulnerabilidades y amenazas
7. Análisis de riesgos
8. Normas internacionales
9. Los diez mitos de la Seguridad Informática
10. Conclusiones

¿QUÉ ES UNA RED?

Una red informática son varios computadores conectados entre sí con el fin de compartir recursos

Uso de las redes

Compartir recursos:

- Lógicos (archivos, comunicados, programas, etc.)
- Físicos (impresoras, módem, etc.)

CLASIFICACIÓN

Las redes se pueden clasificar según su extensión en:

- **LAN** (Local Area Network)

  Red de Área Local. Edificio
- **MAN** (Metropolitan Area Network)

  Red de Área Metropolitana. Ciudad
- **WAN** (Wide Area Network)

  Red de Área Extensa. Nacional e Internacional

TOPOLOGÍAS

La topología es la forma como se distribuye el cableado para conectar los diferentes equipos:

- Bus
- Anillo
- Estrella
- Híbrida
- Malla
- Jerárquica

Bus

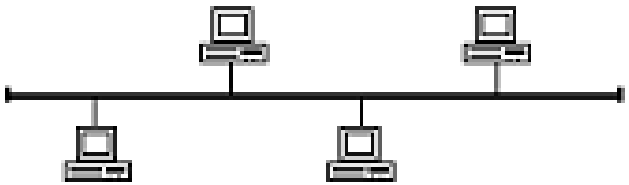
Todas las estaciones van conectadas a un único cable.

Características

- Frecuente en LAN.
- Fácil control flujo de la red.
- Una estación difunde información a todas las demás.

Desventajas

- Como hay un solo canal, si este falla, falla toda la red.
- Dificultad para aislar averías.



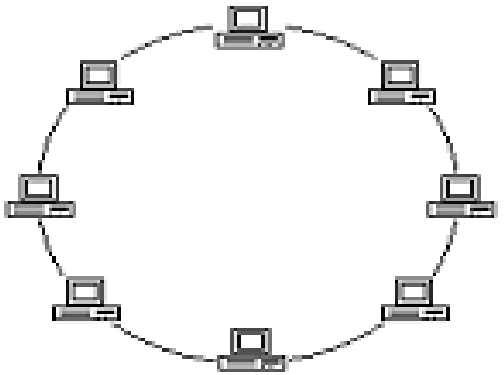
Topología Bus

Anillo

En la estación donde comienza el cable, allí mismo termina

Características:

- Los datos fluyen en una sola dirección.
- Cada estación recibe/envía los datos al siguiente equipo.



Topología Anillo

Desventajas:

- Como están unidos, si falla un canal entre dos nodos, falla toda la red.
- (Se soluciona con canales de seguridad o conmutadores que redirigen los datos)

Estrella

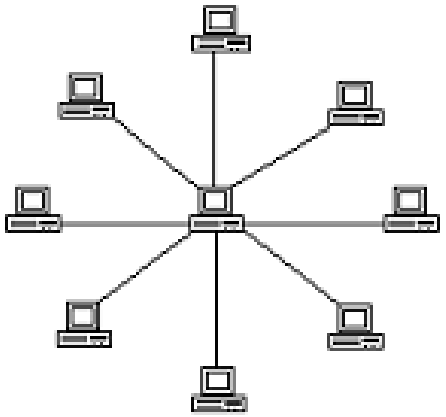
Las estaciones están conectadas a un concentrador.

Características:

- Fácil de controlar, software no complicado y flujo de trafico sencillo.
- Todo el flujo esta en el nodo central que controla a todos.
- El nodo central encamina el trafico, localiza averías y las aísla fácilmente.

Desventajas

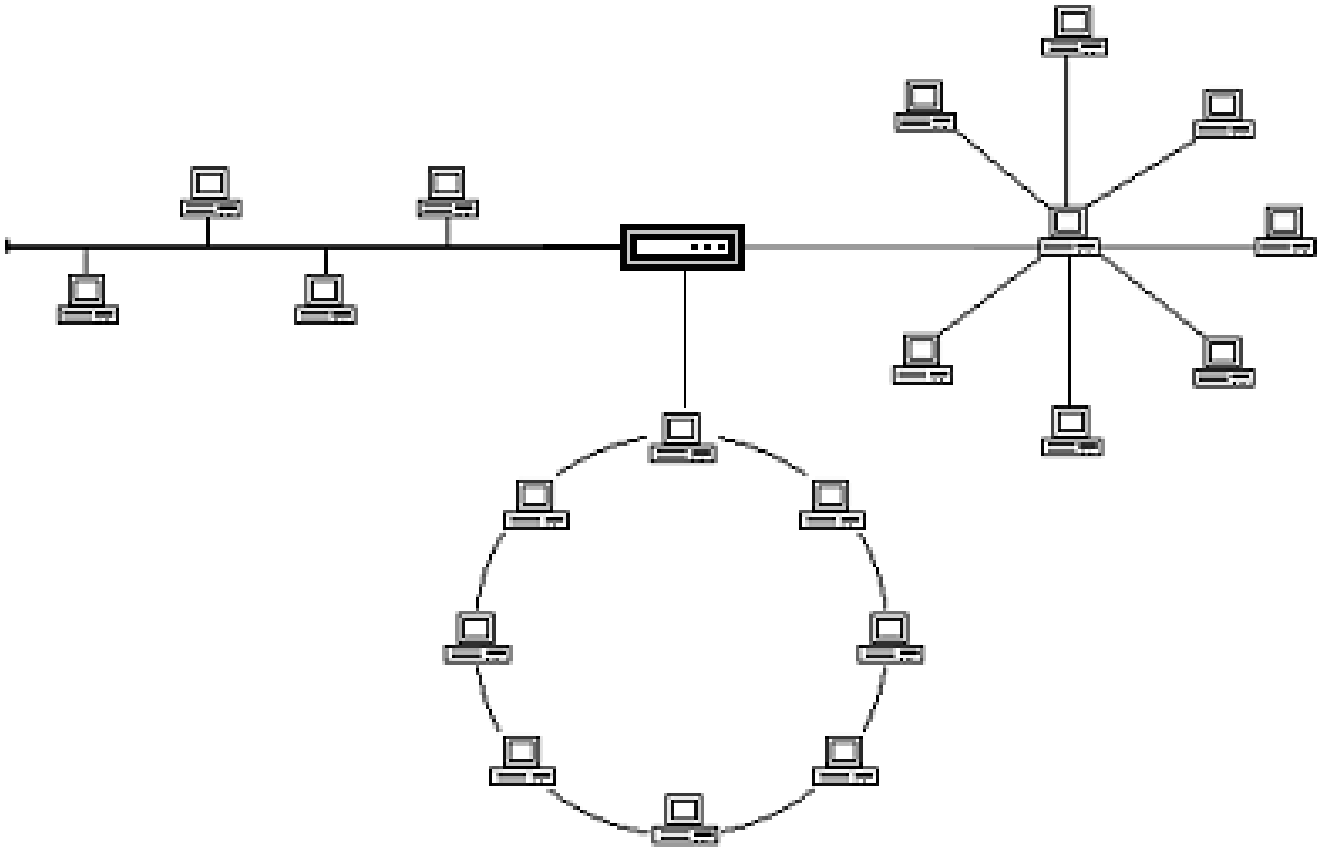
- Hay saturaciones y problemas si se avería el nodo central



Topología Estrella

Híbrida

Unión de diferentes topologías

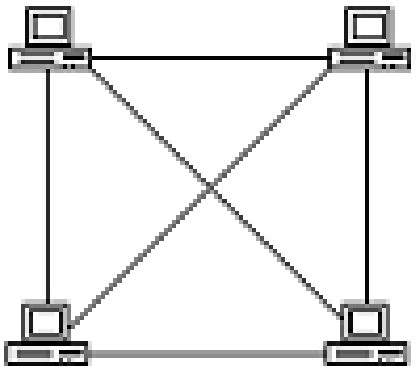


Malla

Uso de trayectorias alternativas

Características:

- Inmunidad a embotellamientos y averías.
- Uso de trayectorias alternativas.



Topología Malla

Desventajas

Control y realización demasiado complejo pero maneja un grado de confiabilidad demasiado aceptable.

Jerárquica

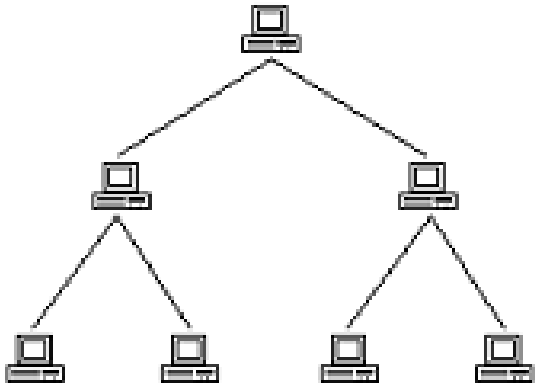
El equipo de la parte superior controla los demás

Características

El software que la opera es simple y fácil.

Desventajas

- Fácil que se presenten cuellos de botella.
- Saturaciones, problemas con la fiabilidad.
- Si el equipo principal falla deja de funcionar toda la red.



Topología Jerárquica

HARDWARE

Son los componentes físicos mínimos necesarios para conectar los equipos en red:

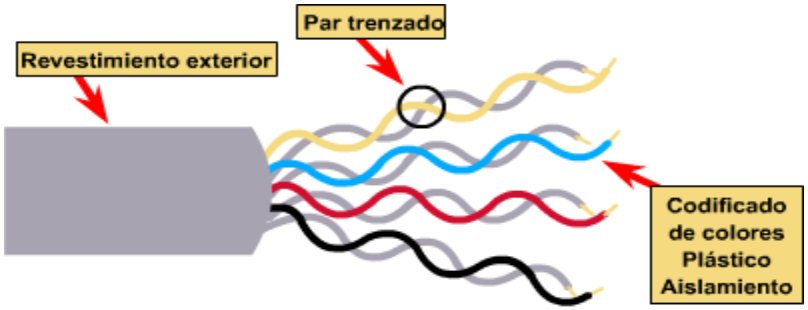
- Cableado
- Conectores
- Tarjetas
- Otros dispositivos

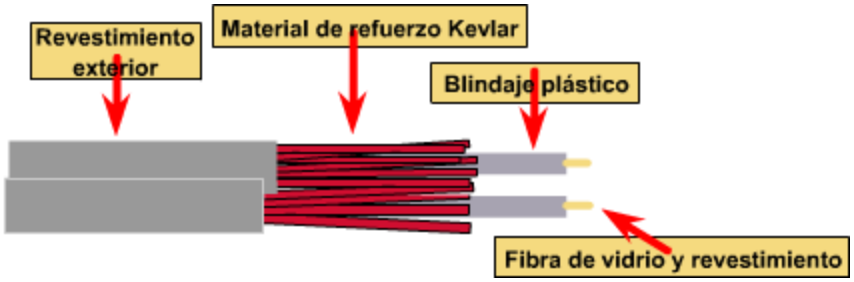
ANCHO DE BANDA

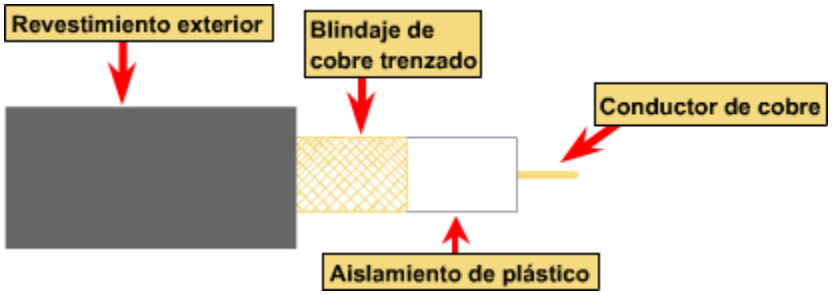
Cableado

Medio de enlace. Depende de la topología, distancia y velocidad:

- **Cable de par trenzado**
- **Cable coaxial**
- **Cable de fibra óptica**







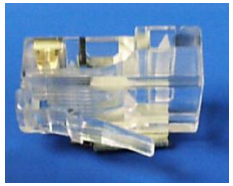
Relación según el medio

Typical Media	Maximum Theoretical Bandwidth	Maximum Theoretical Distance
50-Ohm Coaxial Cable (10BASE2 Ethernet; Thinnet)	10 Mbps	185 m
50-Ohm Coaxial Cable (10BASE5 Ethernet; Thicknet)	10 Mbps	500 m
Category 5 Unshielded Twisted Pair (UTP) (10BASE-T Ethernet)	10 Mbps	100 m
Category 5 Unshielded Twisted Pair (UTP) (100BASE-TX Ethernet)	100 Mbps	100 m
Category 5 Unshielded Twisted Pair (UTP) (1000BASE-TX Ethernet)	1000 Mbps	100 m
Multimode Optical Fiber (62.5/125mm) (100BASE-FX Ethernet)	100 Mbps	2000 m
Multimode Optical Fiber (62.5/125mm) (1000BASE-SX Ethernet)	1000 Mbps	220 m
Multimode Optical Fiber (50/125mm) (1000BASE-SX Ethernet)	1000 Mbps	550 m
Singlemode Optical Fiber (9/125mm) (1000BASE-LX Ethernet)	1000 Mbps	5000 m

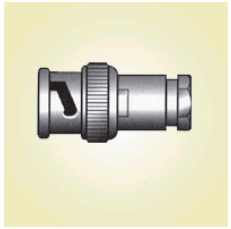
Conectores

Se encargan de unir los cables entre sí o con la tarjeta de red:

- RJ45



- BNC



- Resistencias

- Conector en T

- Conectores de punta recta

Tarjetas de red

También conocidas como NICs (Netware Interface Card). Es el circuito que interpreta las instrucciones de comunicación para integrar el sistema de cables y conectores al computador. Varían de acuerdo al cable y a la tecnología.

Otros dispositivos

- **Concentrador (Hub)**

- **Switche**

- **Enrutador (Router)**

- **Módem**

TIPOS DE REDES

Se pueden diferenciar según el papel que desempeñan las diferentes máquinas en la red:

- Red cliente/servidor
- Red de trabajo en grupo

Red Cliente/Servidor

En este tipo de red existe una máquina (Servidor) que se encarga de realizar una administración de los diferentes recursos disponibles (Ej. Acceso a la red, conexión a Internet o uso de las impresoras). Las estaciones (Clientes) son aquellas que acceden a la red y disponen de los servicios ofrecidos por el Servidor.

Red de trabajo en grupo

En este tipo de red todas las estaciones son autónomas e independientes y a la vez pueden utilizar la red para acceder a los recursos disponibles en otras máquinas. Así, cada estación se encarga de hacer un control sobre los recursos que posee y que desea compartir con otras estaciones.

Software

- Servidor. Ej: Windows Server 2003
- Cliente. Ej: Windows XP Profesional

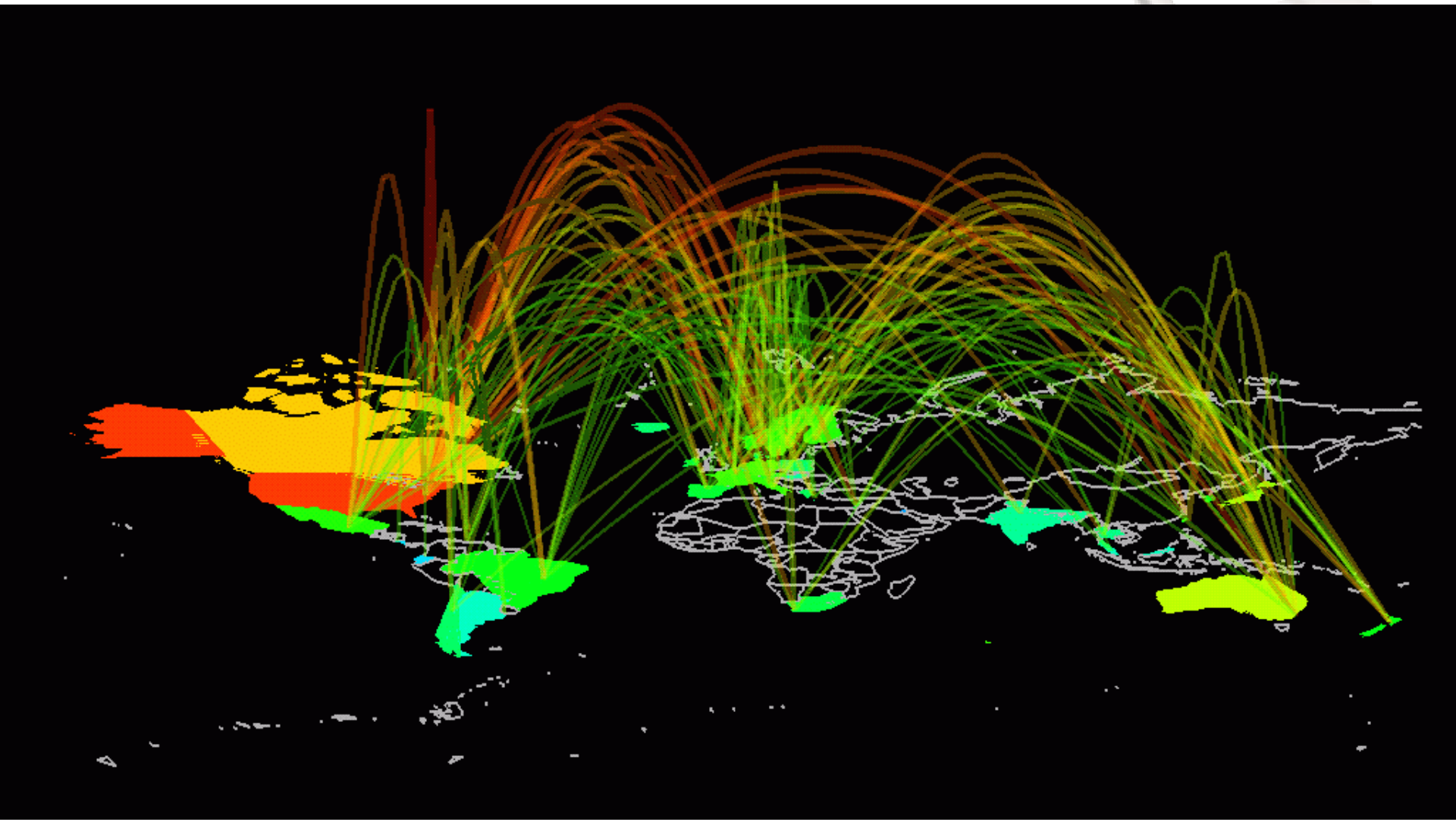
Nota: Se debe configurar un protocolo.
Ej: NETBEUI, TCP/IP, etc.

INTRODUCCIÓN

¿QUÉ ES INTERNET?

Interconection **Net**Work

Internet es el mayor conjunto que existe de computadores conectadas entre sí, se conoce como la red de redes, donde se maneja todo tipo de información, personas, máquinas y software funcionando de forma cooperativa, publicando y organizando información, e interactuando a nivel global.

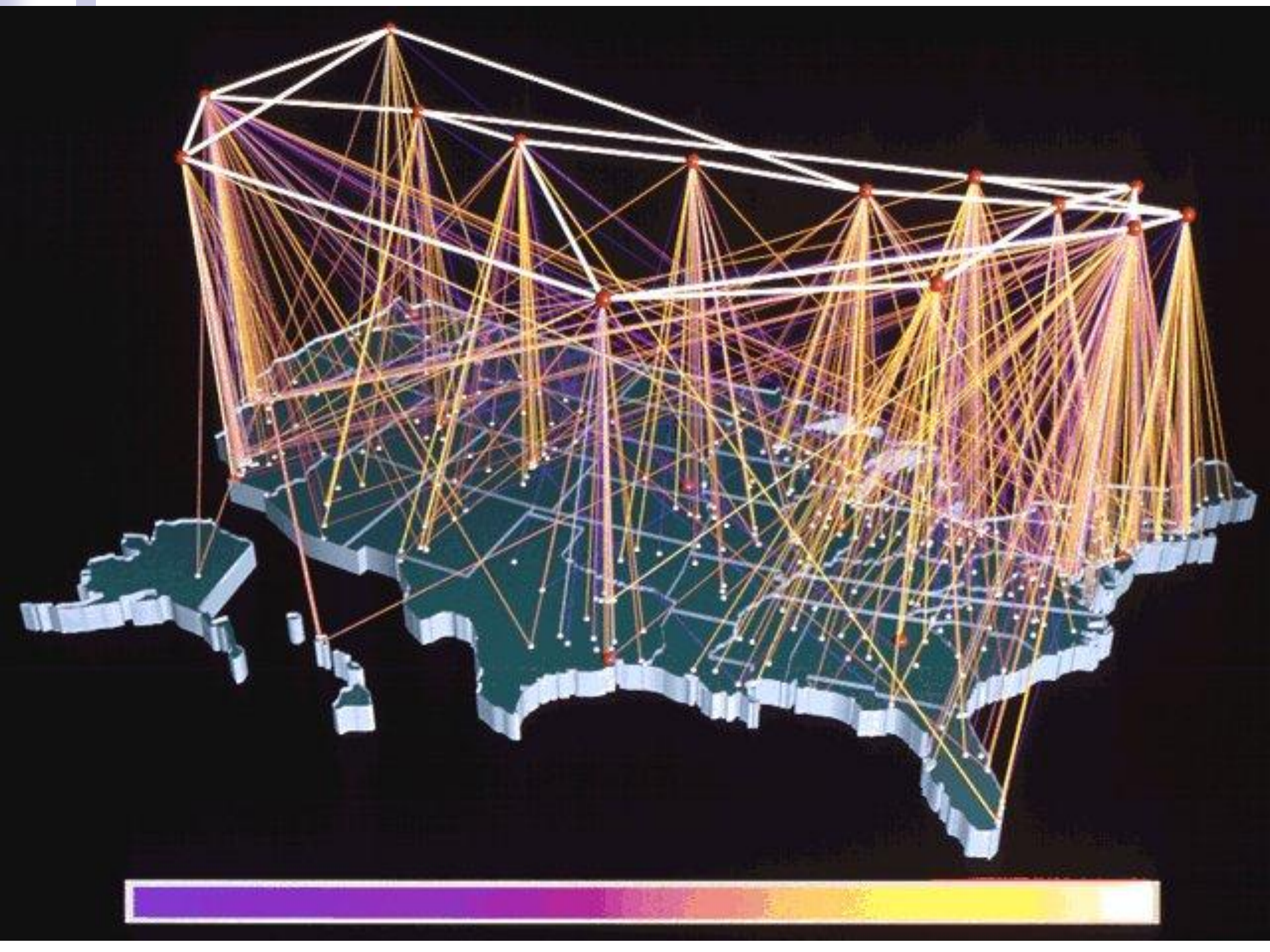


¿CÓMO SURGIÓ?

Internet se inició como un proyecto de defensa de los Estados Unidos. A finales de los años 60, la ARPA (Agencia de Proyectos de Investigación Avanzados) del Departamento de Defensa definió el protocolo TCP/IP. Aunque parezca extraño, la idea era garantizar mediante este sistema la comunicación entre lugares alejados en caso de ataque nuclear. Ahora el TCP/IP sirve para garantizar la transmisión de los paquetes de información entre lugares remotos, siguiendo cualquier ruta disponible.

En 1975, ARPANET comenzó a funcionar como red, sirviendo como base para unir centros de investigación militares y universidades, y se trabajó en desarrollar protocolos más avanzados para diferentes tipos de computadores y cuestiones específicas. En 1983 se adoptó el TCP/IP como estándar principal para todas las comunicaciones, y en 1990 desapareció ARPANET para dar paso, a otras redes TCP/IP a Internet. Por aquel entonces también comenzaron a operar organizaciones privadas en la Red.

Poco a poco, todos los fabricantes de computadores personales y redes han incorporado el TCP/IP a sus sistemas operativos, de modo que en la actualidad cualquier equipo está listo para conectarse a Internet.



¿QUIÉN LA ADMINISTRA?

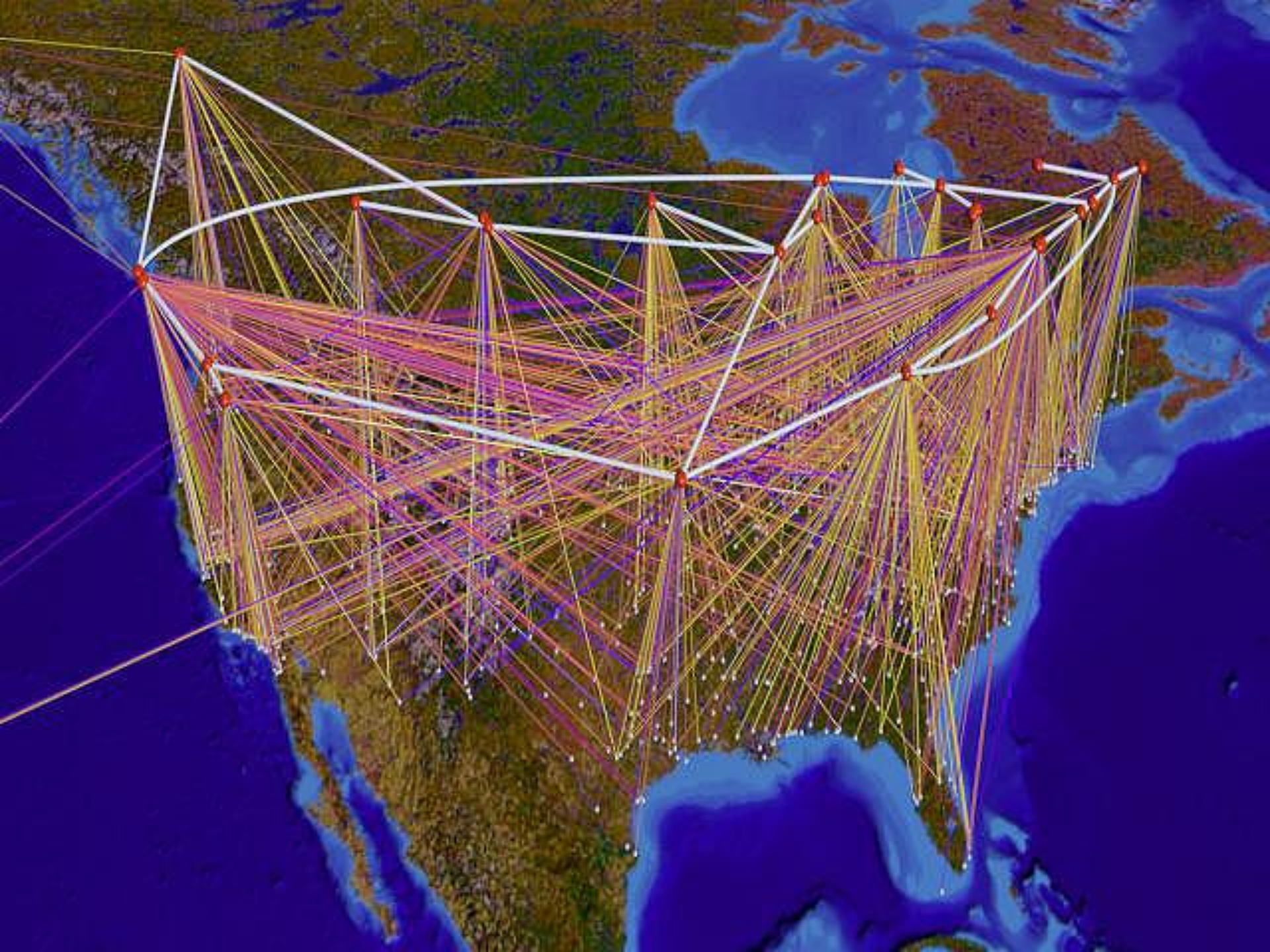
Varias entidades coordinan aspectos técnicos esenciales de la red, siendo los principales:

El IAB (Internet Architecture Board) trata la arquitectura de la red.

El IETF (Internet Engineering Task Force) trabaja en la ingeniería.

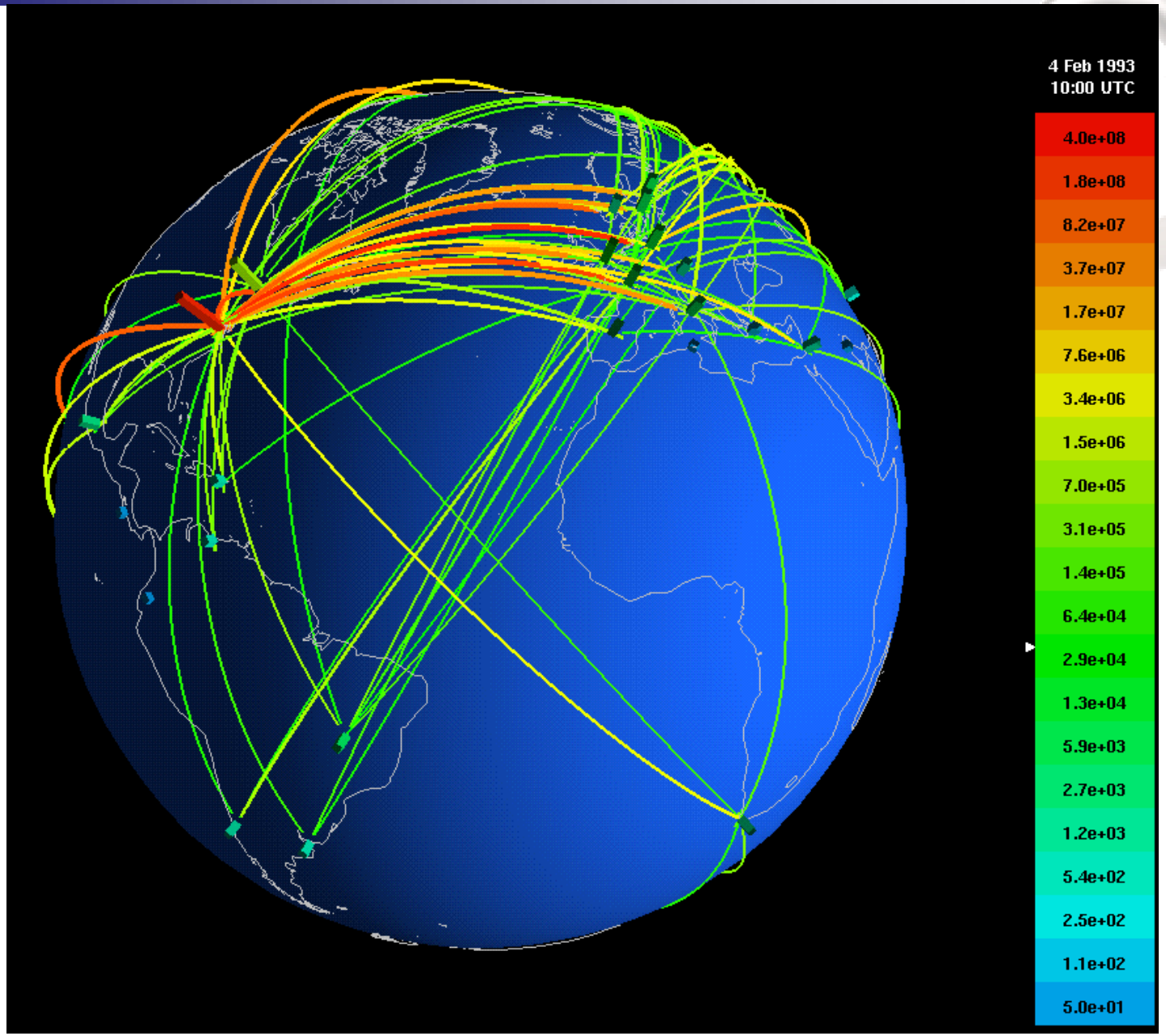
El IANA (Internet Assigned Numbers Authority) registra oficialmente los nombres de las redes, como epm.net.co, nasa.gov, etc. llamados dominios

Una nueva entidad, denominada ICANN ("Internet Corporation for Assigned Names and Numbers") está en proceso de reorganizar todo este sistema de asignaciones para darle al asunto un manejo más internacional, más competitivo, y para corregir algunos problemas que hay actualmente, por ejemplo en cuanto a marcas registradas.



¿CÓMO FUNCIONA?

La comunicación en Internet, o en cualquier red, se realiza siempre entre dos programas, uno que se ejecuta en el computador del usuario (local) y otro que se ejecuta en el computador remoto, es decir, en el computador al cual deseamos acceder. El primero se denomina programa cliente y el segundo programa servidor. el programa servidor es el que proporciona un determinado recurso o información y el programa cliente utiliza dicho recurso. Ambos programas deben tener la familia TCP/IP. Este es el mismo esquema que se usa en cualquier red, sin importar si es o no de gran extensión.


4 Feb 1993
10:00 UTC
4.0e+08
1.8e+08
8.2e+07
3.7e+07
1.7e+07
7.6e+06
3.4e+06
1.5e+06
7.0e+05
3.1e+05
1.4e+05
6.4e+04
2.9e+04
1.3e+04
5.9e+03
2.7e+03
1.2e+03
5.4e+02
2.5e+02
1.1e+02
5.0e+01

¿De quien es Internet?

La red no tiene un único dueño; es una interconexión de redes y canales pertenecientes a diferentes entidades, cada una administrada autónomamente, de manera federal. A pesar de ser autónomas, cooperan y negocian entre sí, y utilizan unos mismos protocolos y estándares para poder interconectarse.

¿Cómo se identifican los computadores entre sí?

A todo computador en Internet se le asigna un número único que lo identifique ante los demás. Este número es llamada dirección Internet o dirección IP. Un ejemplo sería el número 200.24.18.13 ó 255.255.255.0, entre otros. En general son cuatro números, ninguno de las cuales puede ser mayor que 255 ni menor que cero (0).

Una dirección equivalente a la IP es el llamado nombre de dominio, por ejemplo www.caribe.physics.com.co. Normalmente, uno no necesita saber la dirección IP (o sea la numérica) de una máquina, tan solo el nombre. La traducción entre este nombre y la dirección numérica la realiza un sistema llamado DNS

DNS - (Domain Name Server, Servidor de Nombres de Dominio). Cualquiera de los servidores automáticos de Internet que convierten nombres fáciles de entender (como www.miempresa.com) a números IP (como 192.555.26.11).

URL (Uniform Resource Locator, Localizador Universal de Recurso) - Es el nombre que reciben las diversas cosas e información que se pueden encontrar en la Red: páginas Web (http), archivos (ftp) o grupos de noticias (news). Al escribir el nombre completo de un recurso en este formato, se accede a él, normalmente desde un programa navegador o software específico.

¿Como se conecta a Internet?

- En general, hay dos tipos de conexión a Internet, denominadas: **conmutada** y **dedicada**.
- La conexión conmutada es la que se realiza cuando el sistema del usuario hace una llamada a un número telefónico del Proveedor de Acceso y se conecta por la línea telefónica normal a través de un MODEM.
- La conexión dedicada es una conexión permanente a Internet utilizando, por ejemplo, cable MODEM o banda ancha. Es utilizada por empresas o usuarios que hacen mucho uso de la red.

¿De qué depende la velocidad con que llega la información?

- La velocidad del MODEM que usted esté utilizando.
- La velocidad del MODEM de su proveedor de Internet.
- De la calidad de su línea telefónica.
- De la capacidad de tráfico.
- De la cantidad de tráfico de datos que esté manejando en ese momento su Proveedor de Acceso.
- De la congestión de tráfico de datos que haya en las rutas de la red mundial por donde viajen sus datos.
- De la capacidad que tenga el sitio del cual usted está recibiendo los datos.
- Del diseño de la página WEB.

Los servicios de Internet

- El correo electrónico.
- La World Wide Web.
- Usenet: los grupos de noticias.
- FTP: transmisión de ficheros.
- IRC: canales de charla.
- Telnet: conexión remota a otro computador, como si se hiciera desde un terminal local.
- Gopher, Archie, Verónica, WAIS: búsqueda de información a base de menús.
- Buscadores: sitios para buscar información por temas o palabras claves.

http://es.selfhtml.org/introduccion/internet/servicios.htm

World Wide Web

- Tim Berners-Lee de origen británico, informático en la Organización Europea de Investigaciones Nucleares CERN, entre 1988 y 1990 se decidió a desarrollar un sistema para extenderlo a todas las computadoras. Desarrollo tres conceptos:
  - La especificación para la comunicación entre los clientes web y los servidores web - el llamado protócolo HTTP (HTTP = Hypertext Transfer Protocol)
  - La especificación para el encaminamiento de cualquier tipo de archivos y fuentes de datos en la web y el internet restante - el esquema de los llamados URIs (URI = Universal Resource Identifier, identificador de recurso universal).
  - La especificación para un lenguaje de marcación para documentos web, al cual Berners-Lee le dió el nombre de HTML (HTML = Hypertext Markup Language, lenguaje de marcación de hipertexto)
- También escribió el primer software para un servidor web. En una conferencia internacional sobre hipertexto en 1991 junto con sus colaboradores dieron a conocer el proyecto. Se establecieron contactos con otros programadores para diferentes sistemas y entonces así fue como apareció el primer navegador web.

http://es.selfhtml.org/introduccion/internet/www.htm

Navegadores Web

- Un navegador web, hojeador o web browser es una aplicación software que permite al usuario recuperar y visualizar documentos de hipertexto, comúnmente descritos en HTML, desde servidores web de todo el mundo a través de Internet. Esta red de documentos es denominada World Wide Web (WWW) o Telaraña Mundial. Los navegadores actuales permiten mostrar o ejecutar: gráficos, secuencias de vídeo, sonido, animaciones y programas diversos además del texto y los hipervínculos o enlaces.
- Entre los navegadores Web mas conocidos se encuentran Google Chrome, Mozilla, Opera e Internet Explorer.

http://es.wikipedia.org/wiki/Navegador

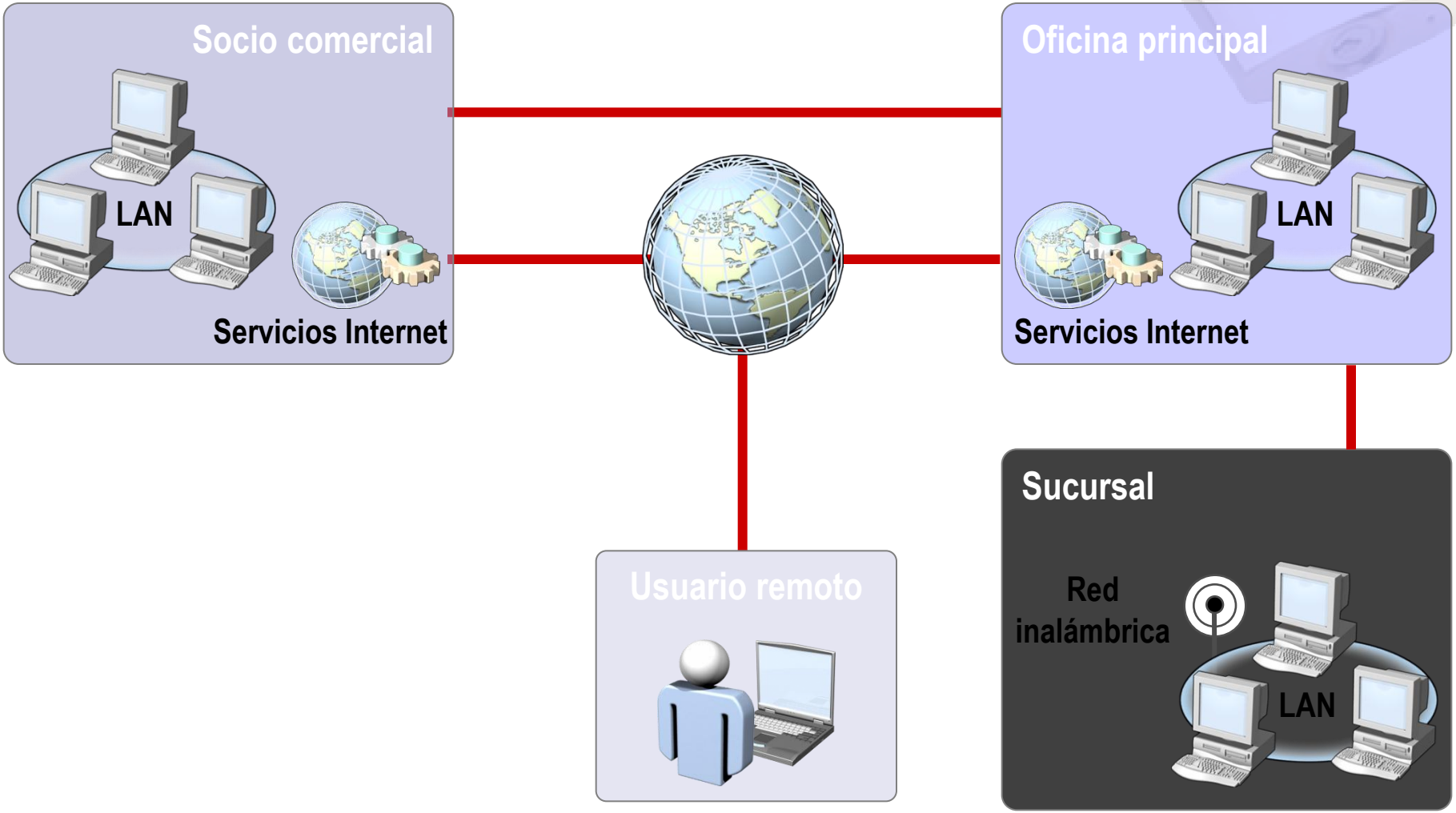
Navegador Web

- Descargar del sitio
- Características del navegador
- Instalación
- Navegación

¿Qué es seguridad informática?

Sistemas de información

Un sistema de información se puede definir como un conjunto de funciones o componentes interrelacionados que forman un todo, es decir, obtiene, procesa, almacena y distribuye información (datos manipulados) para apoyar la toma de decisiones y el control en una organización.


Socio comercial
LAN
Servicios Internet
Oficina principal
LAN
Servicios Internet
Usuario remoto
Sucursal
Red inalámbrica
LAN

¿Qué es seguridad informática?

Evolución

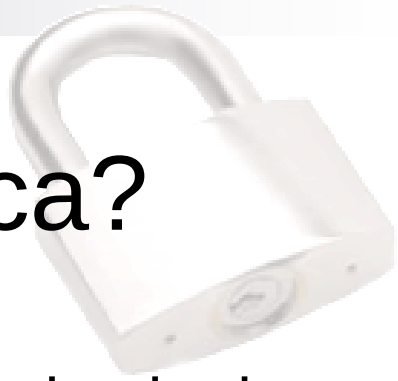
- A partir de los años 80 el uso del computador personal comienza a ser común. Asoma por tanto la preocupación por la integridad de los datos.
- En la década de los años 90 aparecen los virus y gusanos y se toma conciencia del peligro que nos acecha como usuarios de PCs y equipos conectados a Internet.
- Además, comienzan a proliferar ataques a sistemas informáticos. La palabra hacker aparece incluso en prensa.
- Las amenazas se generalizan a finales de los 90; aparecen nuevos gusanos y malware generalizado.
- En los años 00s los acontecimientos fuerzan a que se tome muy en serio la seguridad informática.

¿Qué es seguridad informática?

Evolución

- Principalmente por el uso masivo de Internet, el tema de la protección de la información se ha transformado en una necesidad y con ello se populariza la terminología técnica asociada a la criptología:
  - Cifrado, descifrado, criptoanálisis, firma digital, ...
  - Autoridades de Certificación, comercio electrónico, ...
- Ya no sólo se comentan estos temas en las universidades. Cualquier usuario desea saber, por ejemplo, qué significa firmar un e-mail o qué significa que en una comunicación con su banco aparezca un candado en la barra de tareas de su navegador y le diga que el enlace es SSL con 128 bits.
- El software actual viene con seguridad añadida o embebida.

¿Qué es seguridad informática?



- Si nos atenemos a la definición de la Real Academia de la Lengua RAE, seguridad es la “cualidad de seguro”. Buscamos ahora seguro y obtenemos “libre y exento de todo peligro, daño o riesgo”.
- A partir de estas definiciones no podríamos aceptar que seguridad informática es “la cualidad de un sistema informático exento de peligro” (para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro), por lo que habrá que buscar una definición más apropiada.

La seguridad no es un producto, sino un proceso.

¿Qué es seguridad informática?

Por lo tanto, podríamos aceptar que una primera definición más o menos aceptable de seguridad informática sería:

- Un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas. Concienciarlas de su importancia en el proceso será algo crítico.
- Recuerde: la seguridad informática no es un bien medible, en cambio sí podríamos desarrollar diversas herramientas para cuantificar de alguna forma nuestra inseguridad informática.

Principios de seguridad informática

Para lograr sus objetivos, la seguridad informática se fundamenta en tres principios, que debe cumplir todo sistema informático:

- Confidencialidad
- Integridad
- Disponibilidad

Principios de seguridad informática

Confidencialidad

- Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático.
- Basándose en este principio, las herramientas de seguridad informática deben proteger al sistema de invasiones, intrusiones y accesos, por parte de personas o programas no autorizados.

Los componentes del sistema serán accesibles sólo por aquellos usuarios autorizados

Principios de seguridad informática

Integridad

- Se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático.
- Basándose en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos.

Los componentes del sistema sólo pueden ser creados y modificados por los usuarios autorizados

Principios de seguridad informática

Disponibilidad

- Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático.
- Basándose en este principio, las herramientas de Seguridad Informática deben reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran.

Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen

Principios de seguridad informática

No repudio

- Este término se ha introducido en los últimos años como una característica más de los elementos que conforman la seguridad en un sistema informático.
- Está asociado a la aceptación de un protocolo de comunicación entre emisor y receptor (cliente y servidor) normalmente a través del intercambio de sus respectivos certificados digitales de autenticación.
- Se habla entonces de No Repudio de Origen y No Repudio de Destino, forzando a que se cumplan todas las operaciones por ambas partes en una comunicación.

Si se cumplen los principios vistos anteriormente, diremos en general que los datos están protegidos y seguros.

Esto se entiende en el siguiente sentido: los datos sólo pueden ser conocidos por aquellos usuarios que tienen privilegios sobre ellos, sólo usuarios autorizados los podrán crear o bien modificar, y tales datos deberán estar siempre disponibles.

Seguridad física y seguridad lógica

Es muy importante ser conciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos (hackers, virus, ataques de DoS, etc.); la seguridad de la misma será nula si no se ha previsto como combatir un incendio o cualquier otro tipo de desastre natural y no tener presente políticas claras de recuperación.

Seguridad física y seguridad lógica

- **La Seguridad Física**

  Es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos de seguridad física básicos se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de cómputo de la misma, no. Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de backup de la sala de cómputo, que intentar acceder vía lógica a la misma.

Seguridad física y seguridad lógica

- **La Seguridad Física**

  Consiste en la "**aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial**". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

Seguridad física y seguridad lógica

Las principales amenazas que se prevén en Seguridad Física son:

- Desastres naturales, incendios accidentales, tormentas e inundaciones
- Amenazas ocasionadas por el hombre
- Disturbios, sabotajes internos y externos deliberados.

Evaluar y controlar permanentemente la seguridad física de las instalaciones de cómputo y del edificio es la base para comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.

Seguridad física y seguridad lógica

Tener controlado el ambiente y acceso físico permite:

- Disminuir siniestros
- Trabajar mejor manteniendo la sensación de seguridad
- Descartar falsas hipótesis si se produjeran incidentes
- Tener los medios para luchar contra accidentes

Seguridad física y seguridad lógica

Luego de ver como nuestro sistema puede verse afectado por la falta de seguridad física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputo no será sobre los medios físicos sino contra información por él almacenada y procesada.

Así, la seguridad física sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física que la aseguren. Estas técnicas las brinda la Seguridad Lógica.

Seguridad física y seguridad lógica

- **La Seguridad Lógica**

  Consiste en la "**aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo**".

  Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

Seguridad física y seguridad lógica

Los objetivos que se plantean serán:

- Restringir el acceso a los programas y archivos
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Se recomienda que este tipo de seguimientos sean realizados a la par con procedimientos de Escaneo de vulnerabilidades internas y externas para conocer los puntos débiles de la organización en cuanto a software y poder ofrecer soluciones integradas de seguridad.

Vulnerabilidades y Amenazas

"El único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de concreto, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aún así, yo no apostaría mi vida por él".

Gene Spafford

Vulnerabilidades y Amenazas

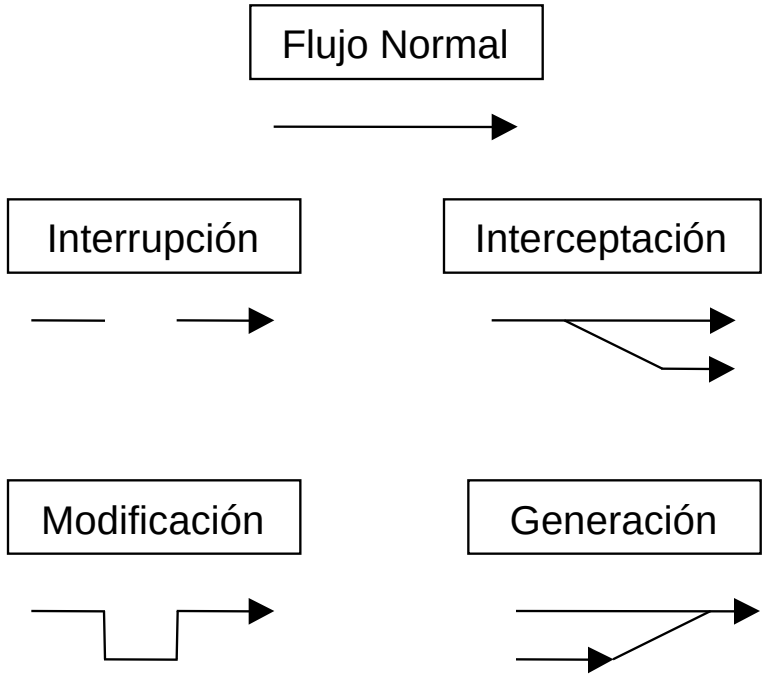
Términos relacionados con la seguridad informática

- **Activo**: recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.
- **Amenaza**: evento que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- **Vulnerabilidad**: posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.
- **Impacto**: consecuencia de la materialización de una amenaza.
- **Riesgo**: posibilidad de que se produzca un Impacto determinado en un Activo, en un Dominio o en toda la Organización.
- **Ataque**: evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Amenazas

Las amenazas afectan principalmente al hardware, al software y a los datos. Éstas se deben a fenómenos de:

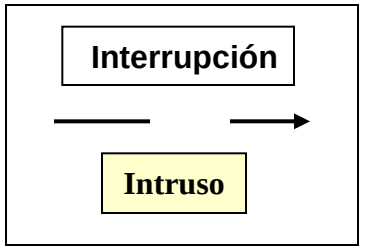
- Interrupción
- Interceptación
- Modificación
- Generación



Amenazas

Interrupción

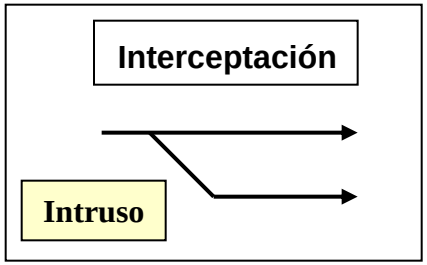
- Se daña, pierde o deja de funcionar un punto del sistema.
- Su detección es inmediata.
- Ejemplos:
  - Destrucción del hardware.
  - Borrado de programas, datos.
  - Fallos en el sistema operativo.



Amenazas

Interceptación

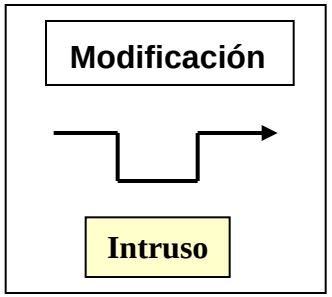
- Acceso a la información por parte de personas no autorizadas. Uso de privilegios no adquiridos.
- Su detección es difícil, a veces no deja huellas.
- Ejemplos:
  - Copias ilícitas de programas.
  - Escucha en línea de datos



Amenazas

Modificación

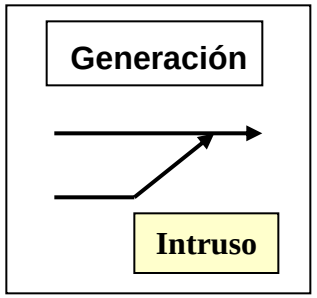
- Acceso no autorizado que cambia el entorno para su beneficio.
- Su detección es difícil según las circunstancias.
- Ejemplos:
  - Modificación de bases de datos.
  - Modificación de elementos del HW.



Amenazas

Generación

- Creación de nuevos objetos dentro del sistema.
- Su detección es difícil: delitos de falsificación.
- Ejemplos:
  - Añadir transacciones en red.
  - Añadir registros en base de datos.



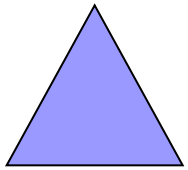
Amenazas

Escenarios de las amenazas del sistema

Interrupción	**Interceptación**	**Modificación**	**Generación**
(pérdida)	(acceso)	(cambio)	(creación)

Los datos serán la parte más vulnerable del sistema

Datos



Hardware

Software

Interrupción (denegar servicio)

Interceptación (robo)

Modificación (falsificación)

Interrupción (borrado)

Interceptación (copia)

Amenazas

Algunas amenazas características

- **Hardware**:

  Agua, fuego, electricidad, polvo, cigarrillos, comida.
- **Software**:

  Además de algunos típicos del hardware, borrados accidentales o intencionados, estática, fallos de líneas de programa, bombas lógicas, robo, copias ilegales.
- **Datos**:

  Tiene los mismos puntos débiles que el software. Pero hay dos problemas añadidos: no tienen valor intrínseco pero sí su interpretación y, por otra parte, habrá datos de carácter personal y privado que podrían convertirse en datos de carácter público: hay leyes que lo protegen.

Análisis de riesgos

Riesgo:

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema

Análisis de riesgos

- Es el proceso de identificación y evaluación del riesgo a sufrir un ataque y perder datos, tiempo y horas de trabajo, comparándolo con el costo que significaría la prevención de este suceso.
- Su análisis no sólo nos lleva a establecer un nivel adecuado de seguridad, sino que permite conocer mejor el sistema que vamos a proteger.

Análisis de riesgos

Información que se obtiene en un análisis de riesgo:

- Determinación precisa de los recursos sensibles de la organización.
- Identificación de las **amenazas** del sistema.
- Identificación de las vulnerabilidades específicas del sistema.
- Identificación de posibles pérdidas.
- Identificación de la probabilidad de ocurrencia de una pérdida.
- Derivación de contramedidas efectivas.
- Identificación de herramientas de seguridad.
- Implementación de un sistema de seguridad eficiente en costes y tiempo.

Muchos estudios indican que, en el caso de la mayoría de las organizaciones, las verdaderas perdidas causadas por los usuarios internos son mucho mayores

Análisis de riesgos

En resumen, el análisis de riesgo implica determinar lo siguiente:

- ¿Que necesita proteger?
- ¿De que necesita protegerlo?
- ¿Cómo protegerlo?

Norma internacional

La norma ISO 17799 (27001)

- Presenta normas, criterios y recomendaciones básicas para establecer políticas de seguridad.
- Éstas van desde los conceptos de seguridad física hasta los de seguridad lógica.
- Parte de la norma elaborada por la BSI (British Standards Institution), adoptada por International Standards Organization ISO y la International Electronic Commission IEC.
- Documento de 70 páginas que no es de libre distribución.

Desde finales de 2005 estas normas se están revisando y cambiando de numeración a partir del número 27001.

Norma internacional

Entornos de la norma ISO 17799

Se trata de un código de buenas prácticas para la Gestión de la Seguridad de la Información.

- Antecedentes
- Introducción
- Objeto y campo de la aplicación
- Términos y definiciones
- Política de seguridad
- Aspectos organizativos para la seguridad
- Clasificación y control de los archivos
- Seguridad ligada al personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Desarrollo y mantenimiento de sistemas
- Gestión de continuidad del negocio
- Conformidad

Los diez mitos de la Seguridad Informática

1. "Mi antivirus está al día, así que no puede entrar ningún virus." Actualizar el antivirus es una de las condiciones para mantener la PC saludable, pero está lejos de ser suficiente. Aun al día, el antivirus puede no detectar ciertos invasores que todavía están en "estado salvaje". Es decir, su código no ha llegado todavía a los laboratorios de las compañías antivirus. Por añadidura, los antivirus ni son infalibles ni sirven para detectar otras amenazas, como el phishing (estafas por email) y el spyware (software espía).

2. "Tengo un firewall, así que no corro peligro." Falso. Aunque los cortafuegos son esenciales, no son perfectos. ¿Qué hace un firewall? Fiscaliza lo que entra y sale de la PC desde y hacia Internet. Así que es tan sólo un programa de computadora que, como tal, puede (y suele) contener errores. Estos errores pueden ser explotados por los piratas para burlar esta defensa. Ataques de esta clase son raros contra una PC individual, pero consignan que el cortafuegos puede ser desactivado por un virus. Para nuestra modesta computadora personal, el firewall es sólo un buen arquero, pero hay penales que nunca podrá atajar.

Los diez mitos de la Seguridad Informática

3. "Uso dos antivirus a la vez, ¿qué puede salir mal?" Si un solo antivirus no es una receta mágica, tampoco lo serán dos. Y, además, pueden interferirse mutuamente.

4. "Mi PC no le interesa a nadie, no hay peligro." Esto era relativamente cierto hasta hace cinco o diez años. Pero ahora nuestra humilde PC hogareña vale oro. ¿Por qué? Porque hay muchas. Si el pirata consigue, por medio de un virus, arrear unos cuantos miles de PC para que intenten conectarse simultáneamente con un sitio Web, éste caerá bajo el peso de la demanda. Además, nuestra PC puede usarse para enviar spam, phishing y otros virus.

Los diez mitos de la Seguridad Informática

5. "Mi backup está al día, así que si pasa algo, puedo restaurar el sistema." Uno de los mitos más difundidos; no contempla que también los virus pueden guardarse en un backup. Como otras medidas que se tienen por mágicas, el backup sin una política racional detrás no nos sacará de una emergencia.

6. "Nunca dejo mi mail en ningún sitio ni estoy registrado en páginas Web, así que es imposible que me roben la dirección." Falso. Este dato está inscripto en varias partes de la computadora, y en las computadoras de las personas con las que intercambia mensajes. Los virus y sitios maliciosos están diseñados para extraer nuestra dirección de allí.

Los diez mitos de la Seguridad Informática

7. "Después de que entró un virus, reinstalé Windows y listo." Si se reinstala Windows sin dar formato al disco, el virus seguirá ahí. El problema de dar formato es que luego habrá que volver a instalar todas las aplicaciones y, previamente, hacer un backup de nuestros documentos, y esta medida no debe darle al virus la oportunidad de escapar al formato.

8. "Tengo todos los parches de Windows instalados, no puede pasar nada." Sin duda, mantener el sistema actualizado es una gran medida de seguridad, como el firewall y el antivirus, pero no alcanza. No todos los ataques se producen por medio de errores del sistema.

Los diez mitos de la Seguridad Informática

9. "No uso Outlook Express ni Internet Explorer, así que estoy a salvo." Es cierto que estos programas son atacados con mayor frecuencia que otros y que han exhibido docenas de vulnerabilidades. Pero la inmensa mayoría de los virus infectará la PC independientemente del software que usemos para recibir mail o bajar archivos de la Web.

10. "No abro ningún adjunto, los virus no pueden entrar." Falso. Hay virus, como el Blaster, que ingresan a la PC sólo por estar conectadas con Internet, si Windows no está debidamente actualizado

CONCLUSIONES

- Para realizar buenas practicas de seguridad se deben conocer los diferentes componentes del sistema de información.
- Existen varias formas de implementar seguridad a la hora de navegar en Internet, pasando desde el propio navegador Web hasta los sitios que visitamos.

CONCLUSIONES

- Ningún sistema de información es 100% seguro y siempre estará expuesto ante alguna amenaza.
- Implementar procesos de seguridad informática en la organización reduce el riesgo de ser atacado tanto de elementos externos como internos.
- La seguridad informática requiere de la participación de todos los niveles de la organización y es una responsabilidad compartida.

BIBLIOGRAFÍA

- Libro Electrónico De Seguridad Informática Y Criptografía. Jorge Ramió Aguirre. Universidad Politécnica De Madrid - España
- http://es.wikipedia.org/wiki/Portada
- http://www.monografias.com
- http://www.internet-solutions.com.co/
- http://seguinfo.blogspot.com/2006/05/los-diez-mitos-de-la-seguridad.html
- http://es.tldp.org/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node77.html
- http://www.anamariajaramillo.com/images/silencio.jpg
- www.fotos.org

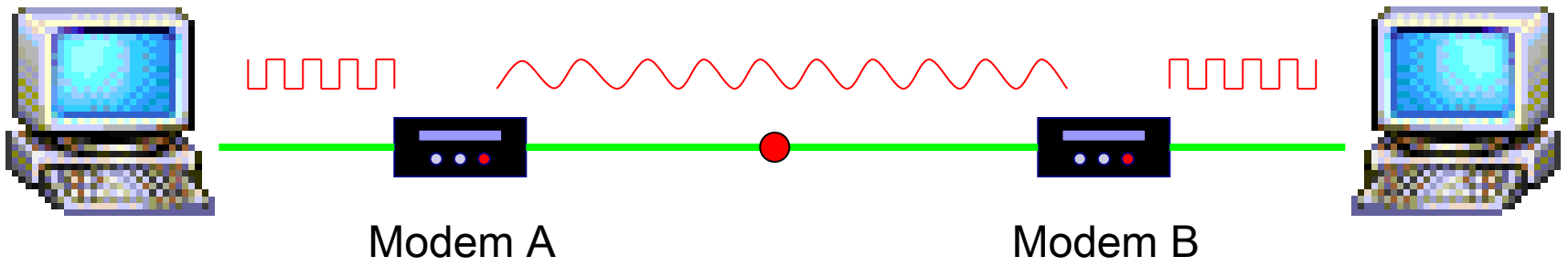
BIBLIOGRAFÍA

- http://www.grupoice.com/esp/serv/hogar/tele/internet/cab_modem.htm
- http://es.wikipedia.org/wiki/Cablem%C3%B3dem
- http://www.dit.upm.es/doc/acceso/introduccion.html
- http://www.maestrosdelweb.com/editorial/segecom/

Dudas o comentarios

Muchas gracias por su atención

Conexión a través de MODEM



Datos

Señal Digital

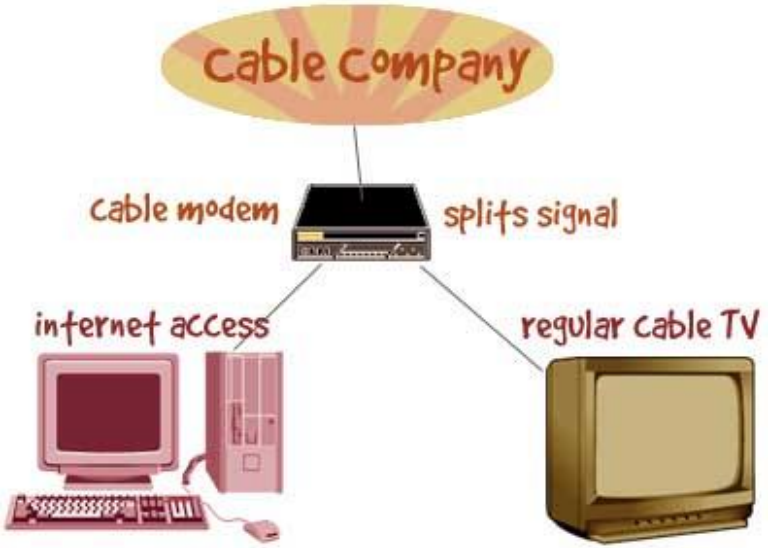
Señal Análoga

Línea Telefónica

VOLVER

Cable MODEM

El acceso a Internet aprovechando la red de cable coaxial de la televisión (cable módem), es un sistema que permite la transferencia de información desde y hacia la red mediante la misma plataforma de recepción de la señal de televisión por cable. La conexión se hace dividiendo la señal que llega al cliente a través del cable, conectando la computadora a Internet y entregando la señal de televisión al televisor del usuario.



VOLVER

Banda ancha

El concepto inicial de Redes de Banda Ancha se introduce formalmente en Agosto de 1989 en la Asamblea Plenaria del CCITT (actualmente denominado Unión Internacional de Telecomunicaciones o UIT) celebrada en Brasilia, donde se definieron las nuevas redes públicas de servicios integrados. Define que un servicio es de banda ancha cuando requiere canales de transmisión con capacidad mayor que un acceso primario (2,048 Mbit/s). Ej: xDSL

VOLVER

xDSL

- DSL sigla de Digital Subscriber Line (Línea de abonado digital) es un término utilizado para referirse de forma global a todas las tecnologías que proveen una conexión digital sobre línea de abonado de la red telefónica local: ADSL, ADSL2, ADSL2+ SDSL, IDSL, HDSL, SHDSL, VDSL y VDSL2.
- Tienen en común que utilizan el par trenzado de hilos de cobre convencionales de las líneas telefónicas para la transmisión de datos a gran velocidad.

- La diferencia entre ADSL y otras DSL es que la velocidad de bajada y la de subida no son simétricas, es decir que normalmente permiten una mayor velocidad de bajada que de subida.

VOLVER

Hacker

- Hacker (del inglés hack, recortar) es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con las Tecnologías de la Información y las Telecomunicaciones: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc.
- Un cracker es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño a su objetivo. El término deriva de la expresión "criminal hacker", y fue creado alrededor de 1985 por contraposición al término hacker, en defensa de estos últimos por el uso incorrecto del término. Se considera que la actividad de esta clase de cracker es dañina e ilegal.

volver

Malware

La palabra malware proviene de una agrupación de las palabras (**mal**icious soft**ware**). Este programa o archivo, que es dañino para el computador, está diseñado para insertar virus, gusanos, troyanos, spyware o incluso los bots (Eliza, correo), intentando conseguir algún objetivo, como podría ser el de recoger información sobre el usuario o sobre el computador en sí.

volver

Criptología

Ciencia que estudia e investiga todo aquello relacionado con la criptografía: incluye cifra y criptoanálisis

volver

Criptografía

La criptografía es aquella rama inicial de las Matemáticas y en la actualidad también de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar, y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando una o más claves.

volver

Person

No existe pa

volver

Bombas lógicas

Las bombas lógicas son en cierta forma similares a los troyanos, se trata de código insertado en programas que parecen realizar cierta acción útil. Pero mientras que un troyano se ejecuta cada vez que se ejecuta el programa que lo contiene, una bomba lógica sólo se activa bajo ciertas condiciones, como una determinada fecha, la existencia de un fichero con un nombre dado, o el alcance de cierto número de ejecuciones del programa que contiene la bomba; así, una bomba lógica puede permanecer inactiva en el sistema durante mucho tiempo sin activarse y por tanto sin que nadie note un funcionamiento anómalo hasta que el daño producido por la bomba ya está hecho.

volver