3. INTRANET

"Intranet.- aplicación corporativa interna similar a Internet" (New York Times, 1994)

3.1. LA INTRANET ENTRA EN ESCENA

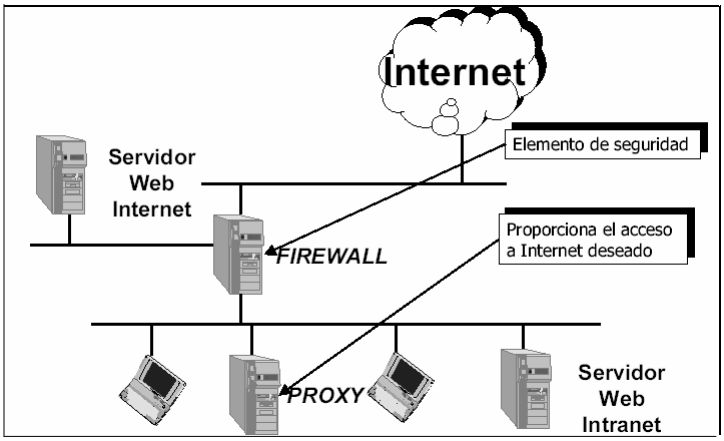
Auge Internet ⟶ **intranets**

Intranet.- Red privada que incorpora los protocolos, procesos y estándares encontrados en Internet. (1995)

- ✓ LAN basada en TCP/IP
- ✓ Conectada o no con Internet a través de un FIREWALL

3.1. LA INTRANET ENTRA EN ESCENA

ESQUEMA TÍPICO DE UNA INTRANET:



3.1. LA INTRANET ENTRA EN ESCENA

CARACTERÍSTICAS:

- Rápida implantación (horas/días).
- Escalable (se puede diseñar en función de las necesidades).
- Fácil navegación.
- Accesible a través de la mayoría de las plataformas informáticas del mercado.
- Puede integrar entornos distribuidos.
- Se puede añadir a fuentes de información propietarias (bases de datos, documentos, realizados con procesador de texto, bases de datos groupware).
- Es extensible a todo tipo de aplicaciones con sonido, vídeo, interactivas, etc.

BENEFICIOS:

- No es cara de instalar y requiere una pequeña inversión de dinero e infraestructuras.
- El usuario requiere poca formación para familiarizarse con el nuevo entorno.
- Libertad de elección. Tecnologías abiertas, no limitan elección hw y/o sw.

3.1. LA INTRANET ENTRA EN ESCENA

¿PORQUÉ INSTALAR UNA INTRANET?

❖ La empresa ha crecido gracias al uso de la tecnología:

⇨ 70's: los grandes ordenadores centrados soportaron el crecimiento comercial de las empresas.
⇨ 80's: los ordenadores personales automatizaron muchas funciones de oficina.
⇨ 90's: la red de comunicaciones se convirtió en el activo tecnológico más importante de una compañía.

❖ Establecer una intranet puede suponer hablar de:

- ✓ Potente sistema de comunicaciones.
- ✓ Reducción de costes.
- ✓ Mayor productividad y calidad.
- ✓ Mejora la relación con proveedores y clientes.

3.1. LA INTRANET ENTRA EN ESCENA

¿PORQUÉ INSTALAR UNA INTRANET? (cont.)

❖ La instalación de una red interna dentro de la empresa supone una reconciliación con cuatro mundos dispersos:

- ✓ Sistema de información y bases de datos (sistemas de compra y finanzas,...).
- ✓ Documentación técnica (planes, sw, ...)
- ✓ Comunicación (correo electrónico, revistas, ...)
- ✓ El mundo exterior.

3.1. LA INTRANET ENTRA EN ESCENA

NIVELES DE UTILIZACIÓN

1. Repositorio Documental

- Formularios, manuales, procedimientos de seguridad, información de productos.
  - Ahorro de tiempo y dinero.
  - Distribución de información al tiempo que evita redundancia.

2. Compartición de datos de negocio

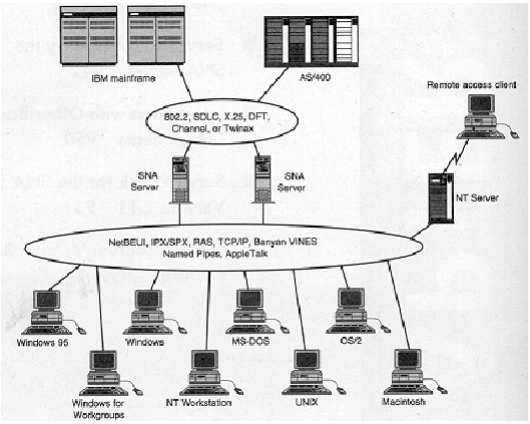
- Mantenimiento de información dinámica.
  - Inventarios comunes, ventas semanales, etc.
- Bases de Datos (Acceso via SQL)
- Acceso a Aplicaciones comerciales IBM AS400
  - Sistema MMS (Merchandise Management System)
  - Protocolo SNA (Integración PC & Host)

- Concepto Seguridad de Acceso
  - Flexibilidad vs. Velocidad

3.1. LA INTRANET ENTRA EN ESCENA

NIVELES DE UTILIZACIÓN (cont.)

2. Compartición de datos de negocio: Ejemplo

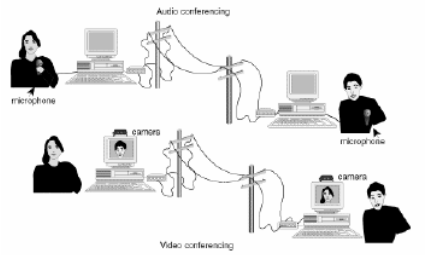


3.1. LA INTRANET ENTRA EN ESCENA

NIVELES DE UTILIZACIÓN (cont.)

3. Comunicación interactiva

- Nivel de colaboración entre miembros en tiempo real.
- Colaboración entre equipos de trabajo.
  - I+D, Desarrollo de producto, Marketing, Fabricación, Departamento publicitario y ventas.
  - Reduce *deadlines* debido al solapamiento de fases



3.1. LA INTRANET ENTRA EN ESCENA

INTRANETS vs. SISTEMAS TRABAJO EN GRUPO

Intranets

- Sistema cliente/servidor basado en TCP/IP.
- Arquitectura abierta (PC, Power Mac, o OS/2).
- Documentación: HTML estándar -> Conectividad Internet

Sistemas Groupware *(Lotus Notes)*

- Software propietario basado en IPX y basado en PC's.
- Difícil conectividad integrada con Internet.
- Desarrollo de herramientas de conectividad: Groupware + Internet
    - Lotus mail + POP3+SMTP
    - Servidores groupware + FTP
    - Bases de Datos con interfaces Web

3. INTRANET

3.2. COMPONENTES DE UNA INTRANET.

① INFRESTRUCTURA DE RED LOCAL

✓ Proporciona la conectividad necesaria que permite acceder a la información desde cualquier punto de la organización.
✓ Protocolo de red: TCP/IP
    • Activo y en funcionamiento para cada cliente y cada servidor de la red.
✓ Protocolo HTTP, sobre TCP/IP, para transmitir la información Web.

BENEFICIOS (uso TCP/IP en intranet):

✓ **Intercambio de paquetes**: un método de direccionamiento y envío rápido.
✓ **Transporte de contenido irrelevante**: puede transmitir datos y salidas de otros protocolos sin importar su contenido.
✓ **Envío de datos fiable**: enrutamiento automático de paquetes cuando existen enlaces defectuosos.

3.2. COMPONENTES DE UNA INTRANET

BENEFICIOS (uso TCP/IP en intranet):

- ✓ **Soporte de compresión y encriptación** para transmitir datos, reduciendo el tiempo de transferencia, aumentando la privacidad y garantizando aún más la entrega al receptor correcto.
- ✓ **Totalmente escalable**: de 2 a 200.000.000 de máquinas.
- ✓ **Usuarios simultáneos ilimitados.**
- ✓ **Compatibilidad** con casi todas las plataformas informáticas y modernos SO's y NOS.
- ✓ **Solución a largo plazo.**
- ✓ **Estándar abierto**: TCP/IP es propiedad de la comunidad de usuarios.

"INCONVENIENTES":

- ✓ Aumento necesidades potencia del sistema y de la RAM necesaria en todos los dispositivos de la intranet.

3.2. COMPONENTES DE UNA INTRANET

② **SERVIDOR WEB**

- ➢ Almacenan documentos y atienden las peticiones de los usuarios para visualizarlos.
- ➢ Puede estar integrado con un servidor de bases de datos, correo electrónico, ftp...

Tecnología WEB:

- ✓ Bajo coste.
- ✓ Facilidad de uso.
- ✓ Basada en estándares abiertos.
- ✓ Conjunto de herramientas integradas que permite al usuario acceder a varias aplicaciones mediante una interfaz única.

3.2. COMPONENTES DE UNA INTRANET

Áreas de Servicios:

- ✓ Correo electrónico.
- ✓ Entornos Web.
- ✓ Chat, conferencia por voz, videoconferencia.
- ✓ Grupos de noticias, USENET.
- ✓ Acceso remoto (TELNET) y mecanismos de manipulación y control.
- ✓ Protocolo de transferencia de archivos (FTP).
- ✓ Almacenamiento de información y motores de búsqueda en BD, interfaces para sistemas documentales.
- ✓ Utilidades de colaboración interactiva (pizarras).
- ✓ Aplicaciones de agenda.
- ✓ Comercio electrónico, cobros y sistemas de inventario.
- ✓ Administración de sistemas de intranet, seguridad, puertas de enlace y cortafuegos.

3.2. COMPONENTES DE UNA INTRANET

③ **DOCUMENTOS**

- Formato HTML

¿Por qué el HTML?

- ✓ Fácil de transmitir por la red.
- ✓ Independiente de la plataforma.
- ✓ Estándar público.

3.2. COMPONENTES DE UNA INTRANET

④ **NAVEGADOR**

- Aplicación para explorar la Intranet y acceder a los documentos (texto, multimedia, ...)
- Interfaz de información universal
- Los más conocidos:
  - Netscape
  - Internet Explorer

Otros clientes:
- De correo electrónico
- De ftp
- De news
- ...

⑤ **APLICACIONES**

- Desarrolladas para resolver problemas específicos.

3. INTRANET

3.3. ASPECTOS DE UNA INTRANET

3.3.1. VENTAJAS

- **Ahorros significativos en los costes de transmisión de datos.**
  Con las intranet, las "redes privadas virtuales" son una alternativa válida a las redes públicas.
- **Ahorro coste de formación de personal.**
  La interfaz universal de la informática Internet/intranet, "*apuntar y hacer click*", no requiere prácticamente ningún tipo de formación.
  Los estándares de Internet HTML y CGI son relativamente sencillos.
- **La forma más efectiva de organizar y distribuir información corporativa.**
- **Tecnología viable y de coste eficiente.**
- **Coste de distribución reducidos.**
  Sustitución del papel por la publicación electrónica.
- **Capacidad para distribuir software.**
  No duplicación y actualización simultánea de software.

3.3. ASPECTOS DE UNA INTRANET

3.3.2. INCONVENIENTES

- **Inercia**
  Adaptación de los usuarios acostumbrados a otra forma de hacer las cosas.
  Integración de aplicaciones y documentos existentes.
- **Tecnofobia**
  Puede evitar que los empleados aprovechen todos los recursos de las intranet.
- **Falta de privacidad**
  Poder capturar información valiosa de sus usuarios para utilizarla cuando sea necesario, se puede convertir en un inconveniente.
- **Integración de la interfaz**
  Problemas de accesibilidad en la integración de las BD existentes y otros recursos de información.
- **Curva de aprendizaje**
  La de una intranet suele ser menor que la de la mayoría de las aplicaciones sw.
- **Seguridad**
  Las intranet son mucho más fáciles de controlar cuando permanecen en un entorno cerrado.

3.3. ASPECTOS DE UNA INTRANET

3.3.2. INCONVENIENTES

- **Rendimiento**
  Igual que en la implementación de cualquier nueva tecnología, a corto plazo habrá unas cuantas áreas en las que se reducirá el rendimiento:

  - ✓ **Ancho de banda**
    - Las soluciones intranet óptimas suelen necesitar redes con un gran ancho de banda.
    - Si la intranet no está preparada para el aumento de tráfico, suele ralentizarse y volverse inestable.
    - Las redes poco fiables tienen un indudable efecto en la productividad.
    - El ancho de banda de una intranet está relacionado con el CÓMO y PORQUÉ se utiliza la red.
    - Importante: planificación previa (mejor pasarse que quedarse corto).

3.3. ASPECTOS DE UNA INTRANET

3.3.2. INCONVENIENTES

- **Rendimiento (cont.)**

  - ✓ **Productividad**
    - Efecto del uso (mal uso) de la Web y del correo electrónico por los empleados.
    - Solución: Monitorizar las actividades del empleado.

  - ✓ **Coste**
    - Creación de la red.
    - Justificar el coste.
    - Beneficios financieros a largo plazo.
    - Ahorro a corto plazo.

3. INTRANET

3.4. DISEÑO DE UNA INTRANET

- **Selección de los servicios.**

- **Selección del software del servidor.**

- **Selección del software del cliente.**

- **Selección otras aplicaciones para el sistema.**
  - Procesadores de texto, aplicaciones gráficas, utilidades de administración archivos, etc.

- **Selección plataformas hardware y S.Os.**
  - Compatibilidad y rendimiento.

- **Complementar cada estación de trabajo.**
  - Accesorios, periféricos (se pueden compartir): tarjetas de sonido, altavoces, impresoras, escáner, unidad ZIP, cdrom, micrófonos, videocámara, módem, etc.

3.4. DISEÑO DE UNA INTRANET

- **Determinar los periféricos de cada servidor.**
- **Selección de hardware y medio de red.**
- **Selección de un ISP (Proveedor de Servicios de Internet).**
- **Diseñar los nombre y direcciones de los clientes y servidores.**
- **Planear los perfiles de acceso de los usuarios.**
- **Prepararse para lo peor.**
  - Sistema de copia de seguridad fiable y redundante.
  - Reguladores eléctricos (SAI).

3.4. DISEÑO DE UNA INTRANET

3.4.1. SELECCIONAR SOFTWARE DEL SERVIDOR

- ❖ Sistema operativo: multitarea.
- ❖ Sistema de ficheros: Estructura de directorios jerárquica.
- ❖ Sistema de red.

① **Servidor Web**

- ✓ HTTP para Unix/Linux
  - •Descripción de la NCSA (National Computer Security Association): *"un protocolo con la sencillez y velocidad necesaria para un sistema de información hipermedia de colaboración distribuido"*.
  - • Las solicitudes HTTP pueden crear múltiples procesos HTTPD (demonio HTTP) para satisfacer múltiples solicitudes.
- ✓ Apache
- ✓ Internet Information Server
- ✓ Netscape Enterprise Server para Unix y Windows

3.4. DISEÑO DE UNA INTRANET

3.4.1. SELECCIONAR SOFTWARE DEL SERVIDOR

② **Servidor de correo**

- ✓ SENDMAIL, la base del correo basado en Unix
- ✓ Exchange de Microsoft
- ✓ Netscape MailServer

- ✓ Protocolos
  - SMTP.- Simple Mail Transfer Protocol.
  - POP3.- Post Office Protocol v3.

③**Servidor de FTP**

- ✓ Servidor de transferencia de ficheros.
- ✓ Unix/Linux: demonio FTPD
  lo lanza el INETD cuando recibe una solicitud de FTP.
- ✓ Windows: Serv-u

3.4. DISEÑO DE UNA INTRANET

3.4.1. SELECCIONAR SOFTWARE DEL SERVIDOR

④ **Servidor de Nombres de Dominio (DNS)**

- ✓ Permite obtener números IP en las traducciones de nombres de hosts o nombres de dominio.
- ✓ Demonio IN.NAMED (Unix)
- ✓ Windows 2000 – Configuración de red
- ✓ Ficheros de configuración

⑤ **Servidor de Noticias**

- ✓ NNTP (Unix): Network News Transfer Protocol.
  - Protocolo base de los grupos de noticias en Internet.
  - Soporta clientes NNTP y otros servidores NNTP.
  - Demonio NNTPD
- ✓ Netscape News Server

3.4. DISEÑO DE UNA INTRANET

3.4.2. SELECCIONAR UNA PLATAFORMA Y UN NOS

✓ Es extremadamente importante comprender claramente las necesidades de información y de la red, actuales y futuras, de su organización antes de intentar seleccionar una plataforma y/o un NOS.
✓ Seleccionar en un primer momento las aplicaciones, clientes, servidores y utilidades que quiere utilizar.

3.4.2.1. PLATAFORMAS.

- X86 (Intel, Pentium, Pentium Pro)
- RISC - Power PC (Apple, IBM, Motorola)
- RISC - SPARC (Sun)
- RISC - Alpha (Digital)

3.4. DISEÑO DE UNA INTRANET

3.4.2. SELECCIONAR UNA PLATAFORMA Y UN NOS

3.4.2.2. INTRANET MULTIPLATAFORMA.

Una red TCP/IP con servidores y clientes que no tienen el mismo tipo de plataforma.

VENTAJAS:
- ✓ Reutilizar hardware existente.
- ✓ Posibilidad uso de mayor número de aplicaciones.
- ✓ La mayoría de los servicios de información no necesitan una plataforma cliente específica, sólo requieren el mismo protocolo.

INCONVENIENTES:
- ✓ Necesidad de adquirir múltiples aplicaciones, servidores, clientes y utilidades para cada plataforma.
- ✓ Dificultad para el control de las versiones.
- ✓ Mayores conocimientos y experiencia de los administradores del sistema.
- ✓ Dificultad en la resolución de problemas debido a las diferentes conexiones de red y al sw de cada plataforma.

3.4. DISEÑO DE UNA INTRANET

3.4.2. SELECCIONAR UNA PLATAFORMA Y UN NOS

3.4.2.3. COMPONENTES.

✓ Pueden mejorar o reducir el rendimiento de la computadora.
✓ La clave para obtener un ordenador rápido y eficiente es eliminar los *cuellos de botella* en la comunicación interna.

Cualquier componente de un ordenador que no es capaz de transmitir datos de forma rápida y eficiente.

① CPU

⇨ En ella se realizan la mayoría de los cálculos.
⇨ Buscar siempre la CPU más rápida.
⇨ Sobre el "último" procesador, tener en cuenta :
- Ampliamente soportado.
- Verificado.
- Más caro.

3.4. DISEÑO DE UNA INTRANET

3.4.2. SELECCIONAR UNA PLATAFORMA Y UN NOS

3.4.2.3. COMPONENTES.

② PLACA BASE

⇨ Conecta todos los componentes para que se puedan comunicar.
⇨ Todas las placas base están diseñadas en base a una plataforma CPU, una configuración RAM y un tipo de bus (ISA, PCI, USB).

③ RAM

⇨ Factor extremadamente importante en la velocidad y fiabilidad de un ordenador.
⇨ Poca memoria producirá bajo rendimiento, fallos en el sistema, bloqueos en las aplicaciones e imposibilidad de multitarea.

3.4. DISEÑO DE UNA INTRANET

3.4.2. SELECCIONAR UNA PLATAFORMA Y UN NOS

3.4.2.3. COMPONENTES.

④ DISCO DURO

⇨ Tener en cuenta:

- ➢ Capacidad de almacenamiento (Al menos un 40% (entre 60% y 80% para servidores) después de instalar y configurar todas las aplicaciones.
- ➢ Velocidad de rotación / Tasa de transferencia
- ➢ Tiempo de acceso
- ➢ Tamaño del buffer
- ➢ Interfaz IDE / SCSI

USUARIO NORMAL	USUARIO ALTAS PRESTACIONES	SERVIDOR O ESTACIÓN GRÁFICA
4,5 Gb	6,5 Gb	6,5 Gb
5400 RPM (10 Mb)	7200 RPM	7200 – 10000 RPM
10 ms	8 ms	8 ms
128 kb	512 kb	1Mb
UltraDMA 33	UltraDMA 33 / SCSI	Ultra SCSI / Ultra Wide SCSI

3.4. DISEÑO DE UNA INTRANET

3.4.2. SELECCIONAR UNA PLATAFORMA Y UN NOS

3.4.2.3. COMPONENTES.

⑤ VIDEO/MONITOR

⇨ Monitor: como mínimo compatible SVGA.
⇨ Tarjeta de vídeo:

- 16 Mb VRAM (SDRAM, SGRAM, WRAM, EDO RAM)
- Tecnología de 64 o 128 bits.
- Soporte resoluciones 640x480, 800x600, 1024x768

⑥ PUERTOS E/S

⇨ Incluye puertos serie y paralelo, conexiones de red y otras conexiones de comunicaciones (por ej. dispositivos SCSI externos, teclado, impresora, ...).
⇨ UART (Universal Asynchronous Receiver / Transmitter): estándar puertos serie.

3.4. DISEÑO DE UNA INTRANET

3.4.2. SELECCIONAR UNA PLATAFORMA Y UN NOS

3.4.2.3. COMPONENTES.

© PUERTOS E/S (cont.)

⇨ USB (Universal Serial Bus): estándar de entrada/salida de velocidad media-alta que va a permitir conectar dispositivos que hasta ahora requerían de una tarjeta especial para sacarles todo el rendimiento.
⇨ Todos los caminos de comunicaciones de, o bien hasta, un ordenador necesitan optimizarse para obtener mayor *velocidad, fiabilidad y eficiencia*.

3.4. DISEÑO DE UNA INTRANET

3.4.2. SELECCIONAR UNA PLATAFORMA Y UN NOS

3.4.2.4. SISTEMA OPERATIVO DE RED.

- ✓ Administra los recursos de la red y controla las operaciones en ella.
- ✓ Pueden convivir varios sistemas operativos de red en una LAN.
- ✓ Algunos NOS:
  - Microsoft Windows 2000 Server.
  - Novell Netware.
  - Apple Open Transport.
  - IBM OS/2 Warp Advanced Server.
  - Solaris Internet Server.
  - Linux

3.4. DISEÑO DE UNA INTRANET

3.4.2. SELECCIONAR UNA PLATAFORMA Y UN NOS

3.4.2.5. SISTEMA OPERATIVO DE CLIENTE.

✓ Cualquier ordenador de sobre mesa o portátil que soporte TCP/IP y que pueda conectarse a la intranet puede utilizarse como estación de trabajo.
✓ En la mayoría de las organizaciones:
- Windows
- Mac OS
- Solaris desktop (Unix)
- Linux

3.4. DISEÑO DE UNA INTRANET

3.4.3. SELECCIÓN DE UN ISP.

➢ Internet Service Provider (Proveedor de Servicios de Internet)
➢ Una organización que "vende" acceso a Internet.
- Derecho uso equipos acceso.
- Ancho de banda.
- Tiempo de conexión.

➢ Se obtiene aquello por lo que se paga (calidad del servicio).

➢ Características "deseables" en un ISP:
- Atención al cliente las 24 horas.
- Base de operaciones local.
- Clientes satisfechos.
- Paquetes de acceso flexibles (adaptables a las necesidades del usuario).
- Al menos tres años de antigüedad.
- Velocidad de conexión.

3.4. DISEÑO DE UNA INTRANET

3.4.3. SELECCIÓN DE UN ISP.

➢ Aspectos a considerar al seleccionar un ISP:

① Soporte Técnico
- ✓ Fiable e inteligente.
- ✓ Mantenimiento continuo (24x7)
- ✓ Solución de problemas.

② Servicios de Internet
- ✓ Acceso *sin restricciones* a todos los servicios de información públicos de Internet.

③ Tarifas
- ✓ Costes asociados a:
  - Servicio.
  - Velocidad de conexión.
  - Tiempo de conexión.
  - Direcciones de correo electrónico adicionales.

3.4. DISEÑO DE UNA INTRANET

3.4.3. SELECCIÓN DE UN ISP.

  - Registro del nombre de dominio.
  - Uso direcciones IP.
  - Espacio en disco.
  - Alojamiento páginas web.
  - Transmisión de datos.

④ Fiabilidad
- ✓ Información sobre los tiempos de desconexión y de descenso de rendimiento.

⑤ Proveedores de acceso al nodo
- ✓ Cuanto más cerca está el ISP de uno o más nodos de alta velocidad, más probabilidad ancho de banda constante.

3.4. DISEÑO DE UNA INTRANET

3.4.3. SELECCIÓN DE UN ISP.

- Velocidad de conexión
  - ✓ En función de la necesidad de acceso a la información y los servicios de Internet.
  - ✓ Servicios disponibles mayoría ISP:
    - Dedicado: uso exclusivo de un dispositivo de comunicaciones localizado en el ISP.
    - No dedicado: no garantiza el acceso a un velocidad de conexión constante.

*Depende del método de conexión***:**

MODEM

- Modo de acceso más extendido.
- Líneas telefónicas estándar.
- 56 K.
- No suficiente intranet más de dos usuarios.

3.4. DISEÑO DE UNA INTRANET

3.4.3. SELECCIÓN DE UN ISP.

RDSI

- Entre 56 y 128 K.
- Coste bajo o moderado.
- Ancho de banda de 2 a 12 veces mayor que una conexión vía modem.
- Recomendable intranets pequeñas y medianas con bajos niveles de uso.

ADSL (Asymetric Digital Subscriber Line)

- Acceso asimétrico y de alta velocidad a través de la conexión a la red telefónica.
- Velocidades *descendentes* (central-usuario) entre 1.5 Mbps. (entre 5 ´ó 6 kms.) y 9 Mbps. (9 kms.)
- Velocidades *ascendentes* (usuario-central) de 16 a 640 kbps. Sobre los mismos distancias. (Garantiza velocidad mínima).
- Tarifa plana.
- Gran fiabilidad.
- Cubre 95% usuarios.

3.4. DISEÑO DE UNA INTRANET

3.4.3. SELECCIÓN DE UN ISP.

T1 - Línea Dedicada (punto a punto)

- Organizaciones alto presupuesto para comunicación.
- Velocidad de transferencia desde 1.54 Mbps (T1) hasta 154 Mbps (T3).
- Para conectar WAN's, grandes organizaciones e ISP comerciales.
- Las líneas T1 son agrupaciones de 24 líneas que se fraccionan a 64 kbps.
- El coste depende del ancho de banda contratado.

3. INTRANET

3.5. SEGURIDAD DE UNA INTRANET

✓ En el mismo momento en que alguien encendió el primer ordenador personal, alguien más empezó a pensar cómo podría acceder a él.

✓ Ninguna red es totalmente segura frente a los intrusos.

✓ La seguridad es un proceso continuo, en evolución constante, que requiere paciencia y diligencia para manejarlo correctamente.

✓ Para evitar que un intruso pueda conseguir acceder sin autorización a su red, debe comenzar pensando como un intruso:

- *¿Cómo podría entrar en la oficina?*
- *¿Cómo podría conectarme a la red para empezar a buscar una forma de entrar?*
- *¿A quién podría llamar de la compañía para que me proporcionara las pistas necesarias para entrar?*
- *¿Qué estoy intentando proteger y de quién lo quiero proteger?*

3.5. SEGURIDAD DE UNA INTRANET

✓ Internet y las intranets, desafortunadamente cada vez con mayor frecuencia, son redes expuestas a riesgos de seguridad.

✓ Dentro de los sistemas de información, la seguridad es el asunto más popular y peliagudo.

✓ El desafío está en garantizar que las personas puedan acceder fácilmente a la información que necesitan, pero no acceder a información para la que no están autorizados.

✓ Los **requerimientos de seguridad** para poder establecer una red segura son:

- **Confidencialidad:** Garantizar que los datos no sean comunicados incorrectamente.
- **Integridad:** Proteger los datos para evitar posibles corrupciones o cambios no autorizados.
- **Autenticación:** Tener confianza en la identidad de usuarios, servidores y clientes.
- **Verificación:** Comprobar que los mecanismos de seguridad son sólidos, potentes y que están correctamente implementados.
- **Disponibilidad**: Garantizar que los recursos estén disponibles cuando se necesiten.

3.5. SEGURIDAD DE UNA INTRANET

3.5.1. SISTEMAS DE SEGURIDAD

✓ Pueden construirse con hardware o con software (excepto los sistemas de protección contra virus que son en forma de software).

✓ Algunas categorías:

① **Sistema de protección antivirus**.

➢ Esenciales en una buena implementación de seguridad, especialmente cuando existe una conexión a Internet.
➢ Los virus pueden infiltrarse en la red de numerosas formas.

② **FIREWALLS**

➢ Tipos:
- Gateways de aplicaciones.
- Sistemas de filtrado de paquetes.
- Gateways a nivel de circuitos.

3.5. SEGURIDAD DE UNA INTRANET

3.5.1. SISTEMAS DE SEGURIDAD

② **FIREWALLS(cont.)**

- Impedir o limitar que ciertos tipos de tráfico de red entre o salga de la red.
- A menudo incluido en el hardware de comunicaciones (router Cisco, equipos RDSI Ascend).
- Disponibilidad de servicios como autentificación, redes privadas y traducción de direcciones de red.
- La mejor protección contra los fallos de seguridad es una fuerte combinación de firewall, contraseñas y sistemas de autentificación de red.

Lo que no está permitido expresamente, es negado. (De dentro a fuera y viceversa).

3.5. SEGURIDAD DE UNA INTRANET

3.5.1. SISTEMAS DE SEGURIDAD

③ **Proxy**

- Basados en sw que actúan en beneficio de los clientes de la red.
- Generalmente se sitúa un servidor proxy entre una red de confianza y una que no lo es (por ej. Internet).
- Los servidores proxy trabajan ocultando la dirección real del cliente.

3.5. SEGURIDAD DE UNA INTRANET

3.5.2. SEGURIDAD EN EL DISEÑO DE UNA INTRANET

"La seguridad de una intranet es una tecnología que permite a la empresa hacer uso de la tecnología internet sin que Internet haga uso de ella"

(Alex Sharpe, experto en seguridad de Rapid System Solutions, Inc.)

✓ Estudiarla en las fases iniciales del diseño de la intranet.
✓ De vital importancia a lo largo de todo el proyecto de intranet.

(1) PRINCIPALES AMENAZAS

① **Acceso no autorizado a la LAN corporativa**.
- Si el servidor Web externo está conectado a la LAN, millones de personas tienen, en teoría, la posibilidad de acceder a ella.
- Solución 1: FIREWALL
  - Una necesidad, no una alternativa.
  - Dos tipos:
    - Basados en router (filtran las IP)
    - Servidores de aplicaciones/proxy (IP para Internet/IP interna)

3.5. SEGURIDAD DE UNA INTRANET

3.5.2. SEGURIDAD EN EL DISEÑO DE UNA INTRANET

① **Acceso no autorizado a la LAN corporativa (cont)**
- Solución 2: AUTENTICACIÓN DEL SERVIDOR
  - Asegura al cliente que el servidor con el que se está comunicando es realmente el servidor con el que debería comunicarse.
  - Autoridad de certificado (Certificate Authotity).
  - Los CA:
    - Actúan como fuente de certificados.
    - Mantiene el espacio del nombre.
    - Guardan listas actualizadas de los controles de acceso.
    - Llevan un control de las revocaciones de los usuarios.

② **Husmeo de paquetes.**
- Los intrusos retiran paquetes IP de Internet y extraen información útil de ellos.
- Objetivos típicos: paquetes no encriptados que contienen información sobre tarjetas de crédito o claves de acceso.
- Solución: ALGORÍTMOS CRIPTOGRÁFICOS
  - Clave privada, clave pública, DES

3.5. SEGURIDAD DE UNA INTRANET

3.5.2. SEGURIDAD EN EL DISEÑO DE UNA INTRANET

③ **Abuso de Acceso**

- Los empleados sobrepasan sus niveles de seguridad del sistema asignados, para acceder a información o a áreas para las que no están autorizados.
- Cómo:
  - Vigilar cómo se conectan al sistema otros empleados y memorizar sus claves de acceso.
  - Acceder a los ficheros del administrador del sistema.
  - Registrar las claves de acceso mientras se transmiten por el sistema y reproduciéndolas.
  - Ejecutar programas de descifrado de claves de acceso.
- Solución:
  - Productos que integran el proceso de identificar al usuario con la seguridad de acceso incorporada en la mayor parte de las aplicaciones principales.
  - Transparente al usuario.

3.5. SEGURIDAD DE UNA INTRANET

3.5.2. SEGURIDAD EN EL DISEÑO DE UNA INTRANET

④ **Bloqueo de Servicio**

- Los ordenadores se programan para hacer muchas llamadas de acceso a un servidor. (Propósito: evitar que otros accedan).
- Difícil de evitar.
- Solución:
  - Localizar la fuente del ataque y desactivarla en un nodo superior de la ruta.
  - Programar el cortafuegos para que excluya la dirección IP de dónde proceden los ataques.

⑤ **Otras amenazas potenciales**

- Infraestructura de comunicaciones:
  - Módem de la red.
  - Servidores de terminales.
  - Aplicaciones de conectividad de scripts CGI.
  - BD del servidor.

3.5. SEGURIDAD DE UNA INTRANET

3.5.2. SEGURIDAD EN EL DISEÑO DE UNA INTRANET

(2) PROTOCOLOS DE SEGURIDAD

✓ SSL (Secure Sockets Layer)
- Original estándar de Netscape.
- Proporciona encriptado de enlaces a nivel de transporte.

✓ S-HTTP (Secure Hypertext Transfer Protocol)
- Protege toda la información mediante sesiones de transporte seguras.
- Actualmente no existen muchas implementaciones de S-HTTP.

✓ RSA (Rivest-Shamir-Adleman)
- Método de encriptado por clave privada .
- Utiliza pares de claves por cada usuario.
- Exige gran potencia de cálculo.
- Se usa también para autentificación.

3.5. SEGURIDAD DE UNA INTRANET

3.5.2. SEGURIDAD EN EL DISEÑO DE UNA INTRANET

(2) PROTOCOLOS DE SEGURIDAD (cont.)

✓SET (Secure Electronic Transaction)
- Estándar adaptado por VISA y MasterCard para resolver sus dos estándares diferentes.
- Basado en tecnología RSA.

✓ PGP (Pretty Good Privacy)
- Actualmente un buen sistema de encriptado para la mayoría de las aplicaciones.
- Basado en una combinación de métodos de encriptado por clave pública y privada que combinan las ventajas de la primera con la velocidad de la última.
- Se usa principalmente para encriptado de mensajes de correo electrónico.

3.5. SEGURIDAD DE UNA INTRANET

3.5.2. SEGURIDAD EN EL DISEÑO DE UNA INTRANET

(3) CONSEJOS PARA MINIMIZAR RIESGOS DE SEGURIDAD

- ✓Definir una política de uso aceptable de la Web y del correo electrónico. Plantear limitaciones de acceso y temas de seguridad.
- ✓ Política de confidencialidad de la compañía extrapolada al acceso externo a la intranet.
- ✓ Las áreas en la que se recibe y envía información deberían ser examinadas cuidadosa y frecuentemente en busca de formatos de archivos extraños (VIRUS).
- ✓ El contenido del material publicado debería evaluarse periódicamente.
- ✓ Asegurarse de que las personas que dejan la compañía de malas formas ya no tengan acceso a la intranet.

3.5. SEGURIDAD DE UNA INTRANET

3.5.2. SEGURIDAD EN EL DISEÑO DE UNA INTRANET

(4) SEGURIDAD POR NIVELES

- ✓ Seguridad física.
- ✓ Seguridad de passwd (usuarios).
- ✓ Secure Socket Layer (SSL)
- ✓ Seguridad de aplicaciones y CGI.

“El mejor ataque es una buena defensa”