

# Intranets

Antonia González Mangas

El concepto Intranet está de moda. A ello están contribuyendo de manera decisiva las continuas referencias que sobre el término se realizan tanto en artículos como en los mensajes publicitarios de los productos de los fabricantes de software (sistemas operativos de red, aplicaciones para Intranets...) y hardware (encaminadores, cortafuegos, conmutadores...).

Tras el auge de Internet como tecnología de compartición, publicación y captación de recursos en una sociedad global y sin fronteras, surge el concepto de Intranet como la reorientación de esta misma tecnología hacia el uso privado y restringido. Es evidente que ello implica la modificación del modelo actual de empresa al proponer un nuevo concepto organizativo y de estructuración del flujo de la información dentro de las compañías.

En la primera parte del artículo intentaré dar respuesta a preguntas sobre su origen y composición (¿Qué es y de dónde viene? ¿De qué se compone una Intranet?), en la segunda sobre su uso y finalidad (¿Para quién y cuándo? ¿Para qué? ¿Qué ventajas e inconvenientes tiene?) para al final ofrecer unas breves conclusiones y un anexo de productos de software Intranet. Léalo en el orden que más le interese.

## ¿QUÉ ES UNA INTRANET Y DE DÓNDE VIENE?

Aunque mi objetivo no es realizar un análisis exhaustivo de lo que es una Intranet, sí me parece interesante hacer algunas precisiones sobre el concepto de las Intranet y los requisitos que han de cumplir para poder recibir esta denominación.

El término Intranet define una **red** privada que aplica la tecnología Internet dentro de una organización, por lo que sus usuarios acceden a la información con las mismas herramientas (navegadores) y de manera tan sencilla, transparente e intuitiva. Por ello, para poder hablar de Intranet en sentido estricto, es necesario que se cumplan estos requisitos:

1. Que el diseño de su arquitectura sea similar al de Internet; es decir, que se empleen los protocolos TCP/IP de comunicaciones estandarizados para Internet, ofreciendo a través de ellos los servicios propios de Internet.

2. Que se trate de una red privada, es decir, que sea de acceso restringido (de ahí el prefijo "Intra"). Una estación de trabajo conectada a una Intranet no es accesible desde el exterior, sin embargo ella sí puede tener acceso al conjunto de los servidores públicos de Internet.
3. Que la interfaz de usuario sea un navegador Web y la mayor parte de la información se la facilite a través de servidores Web HTTP:
  - Un navegador es una aplicación software que permite realizar consultas de documentos en servidores Web, soporta el lenguaje de descripción de páginas HTML y es aceptable sobre múltiples plataformas. Los más conocidos, son: Internet Explorer, de Microsoft, y Navigator, de Netscape.
  - El protocolo HTTP controla la transferencia de documentos entre servidores y clientes. Es también totalmente independiente de la plataforma.

Algunos definen *Intranet* como una evolución de la arquitectura cliente/servidor, una evolución que conlleva la coexistencia de un cliente con requerimientos mínimos, servidores de aplicaciones Web y servidores de bases de datos:

- Es evidente que los fundamentos de una Intranet son muy similares a la arquitectura cliente/servidor, únicamente que se reduce el papel del puesto del usuario.
- Los datos se almacenan de forma centralizada en el servidor Web. Algunos procesos pasan de la estación del usuario a los servidores.
- El control de las aplicaciones y del entorno operativo reside en los servidores en lugar de en los puestos de trabajo, comunicándose ambos mediante protocolos estándar.
- Las aplicaciones, interfaces del usuario y datos se encuentran bajo el control del departamento de tecnología de la información, si bien los usuarios tienen la flexibilidad y el acceso a los datos característico de las redes cliente/servidor.

Pero la mayoría de la tecnología que facilita a las organizaciones la creación de redes Intranet tiene su origen en Internet y la World Wide Web.

## ¿DE QUÉ SE COMPONE UNA INTRANET?

Los diferentes componentes de una Intranet son una serie de redes de área local (LAN) conmutadas y unas redes de área extendida (WAN) encaminadas todas ellas usando el protocolo TCP/IP. Estas redes LAN y WAN permiten el acceso a diferentes servidores Web corporativos, que podrán ser o no accedidos desde Internet.

## PROTOSCOLOS DE RED

Durante las primeras tendencias de la informática, sólo se empleaba un protocolo, y este era el protocolo propietario utilizado por los fabricantes de minis y mainframes.

A principios de los 90 una red media tenía en ejecución tres protocolos, con múltiples soluciones de gestión, una para cada familia de protocolos. TCP/IP es un conjunto de protocolos (más de 100) desarrollados y contrastados en Internet que da soporte a ocho millones de ordenadores. Sus puntos fuertes se encuentran en el encaminamiento y la fiabilidad de las comunicaciones globales entre dispositivos.

El sistema operativo de la organización deberá utilizar TCP/IP como protocolo de red. Windows 95, OS/2 y Macintosh llevan incorporado TCP/IP; LAN Windows NT, Novell NetWare y Banyan Vines se pueden comunicar con TCP/IP; en la parte del servidor de bases de datos y aplicaciones del espectro TCP/IP reside el protocolo natural para todos los sistemas basados en Unix. La arquitectura que no soporta TCP/IP se puede incorporar a una Intranet mediante servidores HTTP que hagan la función de puertas de acceso.

## SEGURIDAD

El primer punto a tener en cuenta es si una Intranet tiene conexión física o lógica con Inter-

net. Una Intranet se limita a emplear gran parte de la tecnología utilizada en Internet.

Todos los servidores HTTP permiten el acceso a los documentos y bases de datos mediante nombre de usuario y contraseña. Si se desea ir más allá en cuanto a medidas de seguridad, se pueden añadir tecnología de encriptación a todos los servidores y navegadores de la organización. Con ello se podrán codificar todos los paquetes TCP/IP a medida que avanzan por la red corporativa.

Esta utilidad se puede utilizar no sólo en solicitudes HTTP, sino también en cualquier paquete TCP/IP, tales como videoconferencia, correo y grupos de trabajo.

El protocolo HTTP no es un protocolo seguro, ya que no garantiza:

- Integridad, es decir, que los datos lleguen íntegros a destino. Podrían ser interceptados y modificados en su recorrido.
- Confidencialidad. Al poder ser interceptados los datos en su recorrido hasta su destino, éstos pueden ser leídos por una persona ajena a la compañía.

El protocolo SSL (Secure Sockets Layer) se sitúa entre HTTP u otro protocolo y la pila TCP/IP. Permite conexiones seguras utilizando certificados digitales y ofreciendo los servicios de **autenticación** (garantiza a los clientes y servidores la seguridad de que la persona con la que se están comunicando es quien dice ser); **confidencialidad** (asegura que nadie no autorizado pueda leer la información que se transmite); e **integridad** de la información (garantiza que la información no ha sido modificada durante la transmisión).

SSL está disponible en Netscape Enterprise Server, Microsoft IIS y ApacheSSL. SSL sólo puede trabajar con navegadores que entiendan SSL. Si el navegador utilizado no entiende dicho protocolo no se podrá comunicar con el servidor.

El protocolo SSL requiere un certificado digital. El certificado digital contiene, entre otras informaciones: el nombre del servidor, la clave pública, la fecha de caducidad y el nombre de la autoridad de certificación (AC). Mediante la

autoridad de certificación se garantiza que la clave pública pertenece a su dueño real.

S-HTTP (Secure Hypertext Transfer Protocol) es una versión del protocolo HTTP que permite transacciones seguras. Garantiza la integridad de los datos, encriptación y autenticación. El cliente genera una clave simétrica mucho más rápida y segura. El cliente encripta el mensaje con la clave simétrica y, encripta la clave simétrica con la clave pública del servidor. De esta forma, la clave simétrica sólo puede ser obtenida por el servidor. El proceso de encriptación/desencriptación se acelera.

Aunque una Intranet no necesita conectividad con Internet, para una organización geográficamente dispersa o que necesite comunicarse con un grupo de usuarios externos, resulta más fácil ampliar la Intranet corporativa sobre Internet que invertir en líneas alquiladas o módem.

Sin embargo una conexión entre sistemas corporativos e Internet conlleva un importante riesgo de seguridad que no debe tomarse a la ligera. Tan pronto como se establece una conexión cualquiera de los más de ocho millones de ordenadores que conforman Internet pueden, en teoría, hablar con cualquier otro ordenador de su organización que utilice TCP/IP.

Deberá implementar un sistema de seguridad entre la Intranet e Internet, como por ejemplo un **cortafuegos**.

Un cortafuegos es una máquina de seguridad dedicada, sin funcionalidades de propósito general, que se coloca entre una red interna (red corporativa o Intranet) y la red global externa (Internet), y su misión es filtrar paquetes de acuerdo con diferentes criterios que se pueden configurar.

El cortafuegos debe considerar cuestiones como quién está autorizado a acceder a Internet, qué actividades están autorizadas en el acceso a Internet, etc.

Los sistemas cortafuegos pueden clasificarse según su grado de seguridad en cortafuegos de filtrado de paquetes y cortafuegos de doble interfaz de red.

El **cortafuegos de filtrado de paquetes** (Fig. 1.1) descarta selectivamente los paquetes

en base a lo que se configure, por ejemplo, direcciones de red (no permitir paquetes entrantes con dirección fuente que pertenezca del lado de la red interna) y permite a algunos sistemas de la red interna comunicarse con el exterior, o a algunas direcciones de fuera que se comuniquen con la red interna. Para cada dirección, el cortafuegos se debería configurar con un conjunto de direcciones fuente y destino legales y rechazar los paquetes que no lo verifiquen. Este procedimiento se denomina filtrado de direcciones.

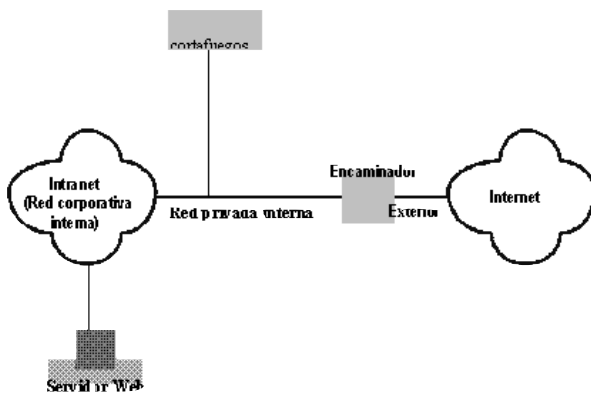


Figura 1.1

La principal ventaja es el menor coste que implica, ya que normalmente se integran en el software del encaminador. Los principales inconvenientes son el coste necesario para su administración, la complejidad para el mantenimiento de las tablas de filtrado de encaminamiento y que el filtrado de direcciones IP es fácil de falsificar. Los cortafuegos de filtrado de paquetes convencionales no es aconsejable utilizarlos con los servicios de FTP, ni para proteger servicios DNS y aplicaciones de servidor dedicadas, ni para proteger servicios con un gran número de llamadas entrantes.

Los **cortafuegos de doble interfaz de red** (Fig. 1.2) o **de nivel de aplicación** son máquinas computadoras (normalmente estaciones de trabajo) con dos tarjetas de interfaz de red separadas, una conectada a la red interna (Intranet) y la otra a la red global externa (Internet). Estos cortafuegos impiden el tráfico directo entre las dos redes, de modo que para obtener acceso a Internet desde la red interna actúan pequeños programas llamados “agentes apoderados” en la

máquina que hace de cortafuegos. El agente apoderado deberá aceptar peticiones de una máquina de la red interna y cuestionar el acceso de acuerdo con la política de seguridad establecida por la organización y entonces reenviarlas al mundo exterior (Internet). Para que los navegadores Web puedan llamar hacia fuera deben existir agentes apoderados que puedan reenviar cada uno de los protocolos que los navegadores Web soportan incluyendo Telnet, Ftp, Wais, Gopher, así como el propio Http.

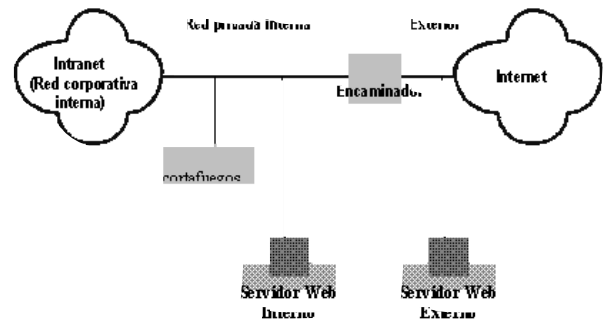


Figura 1.2

## SERVIDOR WEB

Al estar basada una Intranet en estándares y protocolos abiertos no se encontrará ligado a un único proveedor, sin embargo, antes de elegir deberá asegurarse de cubrir sus requisitos básicos.

### Requisitos del servidor

- Escalabilidad. Deberá tener en cuenta que la solución crecerá al mismo ritmo que las necesidades de la organización y del proceso de datos.
- Solidez y madurez. Un argumento en contra de las Intranets es, que si la red falla, todos los usuarios deben dejar de trabajar.

Esto se soluciona eligiendo un sistema tolerante a fallos:

- Redundancia de componentes.
- Estabilidad del sistema operativo (qué versión tiene).

- Soporte de fabricantes de software independientes. Elegir un entorno operativo que soporten los más importantes suministradores de bases de datos.
- Interoperatividad. El sistema operativo y la solución de hardware elegida deberán ser capaces de interoperar con los protocolos existentes e integrados con las LAN ya instaladas basadas en IPX y NetBUI. Aunque las Intranets se ejecutan en TCP/IP, muchas organizaciones no podrán hacer el cambio de hoy a mañana.
- Servicio y soporte. Por el fabricante, por los desarrolladores, y también mediante una red de distribuidores autorizados (hard, sistema operativo, aplicaciones y de integración).

## ¿PARA QUIÉN Y PARA CUÁNDO?

A pesar del explosivo crecimiento de las Intranet —cerca de un 75% de las compañías de Fortune están involucradas en proyectos Intranet, y en los próximos tres años las inversiones en Intranets en Estados Unidos superarán en 3 o 4 veces las de Internet— deben tenerse en cuenta múltiples factores a la hora de decidir su implantación, y un estudio pormenorizado de las propias características de cada empresa debe preceder a su instalación.

No son sólo soluciones idóneas para grandes empresas con implantación nacional o internacional donde ya se utilizan de forma destacada estas tecnologías (conexión permanente de Departamentos y Sedes...), sino también para las pequeñas y medianas empresas al permitirnos extenderla hasta donde queramos (clientes, proveedores, teletrabajadores...).

Asimismo, será una herramienta imprescindible en lo que se conoce como “empresas virtuales” fruto de la colaboración entre diferentes organizaciones de áreas de actividad concreta de ámbito local o nacional, las cuales necesitarán estar en contacto permanente para coordinar con efectividad su actividad.

Para el año 2.000 se considera que el desarrollo de Intranet habrá alcanzado su madurez y

será el principal sistema de acceso a las aplicaciones y a la información corporativa. Hoy su uso se centra en la difusión de la información interna: publicación de documentos, transferencia de datos, correo electrónico, multimedia, videoconferencia...

Este año de 1997 será el año de las aplicaciones de mensajería y groupware basadas en la tecnología Web.

Según un estudio de Business Research Group, de Massachusetts, en el año 2.000 el mercado comercial de Intranet moverá cerca de 25.000 millones de dólares.

## ¿PARA QUÉ?

Los campos de acción en los que el uso de una Intranet pueden ser óptimos, serían:

- Marketing y ventas.
- Recursos humanos.
- Comunicación interna.
- Atención al cliente.
- Aplicaciones financieras.
- Formación.
- Soluciones de acceso remoto.

Los servicios que se pueden ofrecer a través de estas redes son tantos como el lector pueda imaginar, y dependerá mucho del tipo de actividad en que se vea envuelta la empresa, pero por citar dos ejemplos situados en ambos extremos de la complejidad, se podrían usar para hacer público un memorándum interno, o para consultar una gran base de datos corporativa residente en un superordenador remoto.

Las Intranets pueden convertirse en escaparates para ser consultadas por miles de usuarios —dejando al margen la política de seguridad y cortafuegos de las compañías—. De este modo, y mediante la tan comentada convergencia de tecnologías, es previsible que en un futuro no muy lejano paradigmas como el de cliente/servidor, comercio electrónico, y tecnología Web, se den la mano en un mundo mucho más global.

## ¿QUÉ VENTAJAS OFRECE?

Entre las múltiples ventajas que aporta el uso de Intranet en redes corporativas, se pueden destacar:

- **Ventajas económicas** al reducirse los costes, en comparación con otros sistemas informáticos basados en tecnologías más convencionales:
  - El ahorro de papel al disminuir el fotocopiado de los datos para ser distribuidos a todos los empleados de la empresa y en el envío y recepción de datos por fax.
  - Al utilizar en Intranets los mismos servicios que en Internet la formación del personal con experiencia en Internet es innecesaria.
  - Bajos costes referidos a la integración de herramientas y al propio mantenimiento de la Intranet.
- **Uso de la arquitectura cliente/servidor en una conversación HTTP:**

Al enviar un cliente (navegador) una solicitud a un servidor Web, envía también información propia al mismo; al registrar esta información el servidor origina **información de auditoría y análisis de uso por parte del responsable del sistema.**

Antes de devolver una solicitud del cliente, el servidor comprueba si el documento tiene asignado algún control de acceso. Si es así solicitará al cliente un nombre de usuario y una clave de acceso antes de enviarle el documento. Este proceso **permite a los administradores del sistema varios niveles de acceso a la información.**

Como parte de la respuesta el servidor envía un identificador MIME estándar que indica qué tipo de documento envía. El cliente lee este identificador para saber interpretar el documento enviado.

Los servidores HTTP ya se encuentran disponibles en todo tipo de plataformas hardware y sistemas operativos.

Las organizaciones con LAN basadas en Windows NT o Novell Netware pueden implementar un servidor HTTP que se ejecute dentro del servidor existente de ficheros y de impresión; los usuarios Unix tendrán que añadir otro software HTTP al sistema.

- **Mejora del flujo de información** (Fig. 1.3) especialmente en comunicaciones entre empleados o departamentos y mejora de la estructuración interna de la información. Se evita el desorden. No se pierden los informes y están organizados en el servidor Web.

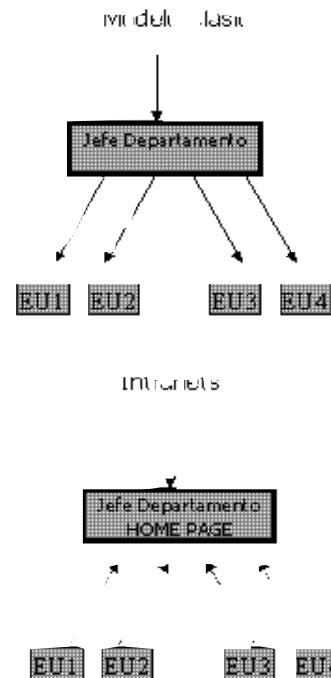


Figura 1.3

- **Mejora de la interacción con el cliente.** Al usar TCP/IP utilizamos el correo electrónico con el consiguiente ahorro de tiempo y dinero. Con su velocidad podrá mantener contactos continuos mejorando el rendimiento. Se supera el inconveniente de la llamada telefónica cuando el interlocutor se encuentra ausente o con la línea ocupada.
- **Utilización de diferentes plataformas hardware y software.** Uno de los funda-

mentos de una Intranet es la independencia de la plataforma; es la clave del éxito y la cada vez mayor adopción de esta tecnología. Se puede utilizar prácticamente cualquier tipo de ordenador y comunicarse con otro de forma totalmente transparente. Esto se logra mediante la utilización de protocolos estándares.

La tecnología abierta de la Intranet elimina las barreras de las comunicaciones. Usuarios de diferentes plataformas hardware pueden utilizar el mismo tipo de aplicaciones, permitiendo la creación de grupos, tanto de los propios empleados como con interlocutores externos y así comunicarse y compartir información.

La Intranet corporativa ofrece el medio ideal para aplicar el groupware. La comunicación y la colaboración se hacen bajo el mismo lenguaje universal basado en Web.

Siempre que disponga de un navegador podrá acceder a la información almacenada en un servidor de una Intranet o Internet. El lenguaje HTML le permitirá crear documentos que contengan gran cantidad de medios (sonido, vídeo, gráficos, texto...) que se puedan ver desde cualquier plataforma los sencillos sistemas para las respuestas de los usuarios mediante formularios; HTML no va más allá de la visualización de la información. Mediante la Common Gateway Interface (CGI) todos los servidores Web pueden interactuar con cualquier otra aplicación externa como bases de datos, y posteriormente darles formato HTML a la respuesta para enviarla al navegador.

El uso del lenguaje de programación Java permite navegar por la red mediante una máquina virtual Java y ejecutar los applets Java (pequeñas aplicaciones Java) de los servidores.

**Java** se diseñó para eliminar los vínculos fijos entre aplicaciones y sistemas operativos, de forma que los desarrolladores puedan crear aplicaciones que se ejecuten por igual en cualquier ordenador, por ejemplo, un documento Web que pueda visualizarlo cualquier navegador.

Los programas escritos en Java se distribuyen con un formato especial llamado bytecode. Para convertir el código en aplicación de trabajo, el ordenador tiene que ejecutar un proceso independiente, que se conoce como "máquina virtual Java". Máquina virtual Java es un software que interpreta los ficheros Java en bytecode, y los convierte en instrucciones que el ordenador y el sistema operativo puedan entender. La cantidad de código de todas las máquinas virtuales es de unos 200 K, y ya se han incorporado en los principales navegadores Web. Esto implica que todos los ordenadores de una Intranet llevarán incorporado Java, sólo con tener el navegador Web actualizado. De esta forma, sólo se desarrolla un tipo de aplicación, independientemente de la plataforma. Cuando se actualiza la aplicación en el servidor todos los usuarios descargan la aplicación totalmente actualizada. Esto ahorra tiempo al evitar que se tenga que actualizar la aplicación en cada puesto.

## ¿TIENE INCONVENIENTES?

El mantenimiento de una Intranet como se ha mencionado anteriormente supone grandes ventajas, pero su uso tiene algunos inconvenientes:

- El administrador de la misma debe poseer formación especializada y dominar las tecnologías necesarias, que pueden pasar por el conocimiento de lenguajes HTML, Java, etc.
- La utilización de una Intranet como medio de comunicación empresarial conlleva un aumento de tráfico que circula por la red. Los encaminadores (routers) utilizados deberán ser más potentes. Aunque HTML es un lenguaje hipertexto, cada vez es más frecuente la utilización de gráficos, sonido, imagen, etc., esto hace que el ancho de banda necesario sea mayor para obtener tiempos de respuesta razonables.
- Seguridad. La seguridad en la Intranet debe preocupar a la empresa dependiendo del tipo de información que ésta difunda.

Si la Intranet corporativa no tiene conexión a Internet, se deberán vigilar los posibles ataques que se producen desde dentro de la empresa. Se estima que el 80% de los ataques informáticos se producen desde dentro de la empresa.

Si la intranet tiene conexión a Internet, los ataques pueden venir de cualquiera de los aproximadamente 50 millones de usuarios conectados a Internet. Existen soluciones al problema de la seguridad que ya hemos desarrollado anteriormente..

## CONCLUSIONES

Como en casi cualquier tema relacionado con las tecnologías de la información, es difícil dar hoy una conclusión definitiva, pues ni las mismas empresas implicadas saben qué va a pasar mañana o cuál será el siguiente paso.

Pero haya algunas cosas en las que sí existe acuerdo:

1. Lo importante en una Intranet no es tanto la tecnología que la soporta como la información que se distribuye. El uso de estas tecnologías no arreglará por sí solo los problemas de comunicación interna en su empresa.
2. El tema de la seguridad, sin acabar de estar resuelto, cada vez presenta menos problemas.
3. Según un reciente estudio, casi las dos terceras partes de las compañías que operan en Estados Unidos se están planteando introducir una Intranet en el año 97. Debemos tener en cuenta que las tendencias en tecnología no las marca el mercado español, sino el americano.
4. En algún momento próximo, tanto su vida como su negocio quedarán atrapados en la red, así que cuanto antes lo piense, algo llevará por adelantado.

## ANEXO: FABRICANTES DE SOFTWARE INTRANET MÁS SIGNIFICATIVOS DEL MERCADO.

- **Lotus/IBM:** la tecnología Lotus Domino ha convertido al producto estrella Notes en un servidor interactivo para Intranets. Notes, que ya se venía utilizando en ámbitos empresariales desde hace ocho años, tiene la ventaja de resolver aspectos que la red aún no ha resuelto, como la seguridad y discreción de la información y la posibilidad de estructurar grandes cantidades de documentos. Como contras se podría citar la generación anárquica de aplicaciones y que es un sistema propietario y costoso. Aunque la estrategia Internet de Lotus y la integración de Notes-Web le permitirá seguir compitiendo en este ámbito.

Lotus Domino utiliza el servidor Web de Lotus para publicaciones de información y aplicaciones interactivas. Lo más destacado de Domino, es:

- Tecnologías de servidores integradas. Mantenimiento automático de vínculos, correo electrónico, servidor Web para publicaciones empresariales, directorio para nombres y contraseñas de los usuarios, grupos, número de teléfono, etc., certificados de seguridad RSA, prestaciones de bases de datos totalmente multimedia, catálogo, colaboración con funciones ya incluidas (foros de debate entrelazados), Entorno gráfico de desarrollo de aplicaciones con bases de datos corporativas existentes.
- Soporte completo para: sedes Web ya existentes, HTML, Java, JavaScript, CGI, SSL, GIF con animación, imágenes de fondo, marcos y formularios.
- Gestión flexible de la seguridad: servicio de directorios, autenticación de usuario y la contraseña, acceso e iteración mediante navegadores de forma individual y personalizada, SSL para autenticación de servidores y codificación de



datos, codificación de datos durante la replicación entre servidores.

- Potentes herramientas de desarrollo que permiten crear aplicaciones dinámicas e interactivas para Internet/Intranet.
- **Microsoft:** Actualmente el 85% de los proyectos de desarrollo de software que realiza la compañía de Bill Gates están relacionados de alguna manera con la red.

Los productos que aporta Microsoft para responder a las necesidades de las compañías que están implementando una Intranet, son:

**Windows NT Server 4.0:** sistema operativo de servidor escalable tan fácil de utilizar como Windows 95 y que combina la compartición integrada de recursos, el servidor de comunicaciones y un rico entorno de aplicaciones.

**Dynamic Host Control Protocol (DHCP):** como servicio de red distribuido que permite las comunicaciones dentro y fuera de la empresa, incluye gestión automática de direcciones TCP/IP y búsqueda y resolución de nombres con WINS y DNS.

**Microsoft Exchange Server:** servicio de directorios nativo. En la actualidad, las empresas ven sus redes, además de como una base para compartir recursos, como un sistema de información distribuida que soporta aplicaciones críticas de negocio. En este sentido, Microsoft pretende que la nueva generación del servidor de directorios vaya dirigido a obtener beneficios en áreas clave de la empresa, proporcionando un servicio de directorios de propósito general asociado con múltiples espacios de nombres para todos los usuarios, servicios y recursos de red.

**Internet Information Server:** proporciona la base para la publicación de Web y para compartir información dentro de la empresa a través de Internet. Forma parte de Windows NT Server y soporta la misma plataforma hardware que éste.

Proporciona una importante innovación con una implementación CGI de alto rendimiento, llamada **Internet Server API**.

**Front Page:** es una herramienta de publicación visual cliente/servidor de páginas Web para usuarios que no sean programadores.

Microsoft añadirá a la familia BackOffice productos servidores, incluyendo:

**Microsoft Proxy Server:** permite a los usuarios obtener acceso de alto rendimiento hacia la Intranet de una forma controlada y segura.

**Microsoft Merchant Server:** combina los componentes necesarios para una operación de venta virtual al detalle (comercio electrónico) incluyendo procesamiento de pedidos y pagos, seguridad, autorización de tarjetas de crédito, informes y herramientas de gestión del sistema, además de interfaces para sistemas existentes en la actualidad.

**Microsoft Media Server:** ofrece servicios multimedia de forma que los clientes puedan aprovechar los enlaces de gran ancho de banda en la Internet y, proporcionar un acceso al contenido multimedia en tiempo real o a un contenido almacenado.

- **Sun:** gracias a Java, la compañía tiene un conjunto de herramientas hardware, software, soporte y servicio, como Java WorkShop 1.0, diseñadas para ayudar a la empresa a desarrollar, desplegar y gestionar redes internas corporativas.
- **Novel:** ocupa una posición de liderazgo en redes de área local con su programa NetWare, al que han sacado un sucesor, el IntranetWare, al que han añadido aplicaciones de mensajería y acceso a redes en remoto.

IntranetWare proporciona acceso tanto desde IPX como desde TCP/IP a recursos Intranet, servidores Web, servidores FTP y conexiones remotas a Internet o a Infovia. Le permitirá utilizar su actual infraestructura de red para que sus redes hagan aún más por usted y su negocio.

- **Oracle:** la estrategia global para entornos Intranet de Oracle engloba a todos sus productos, como la base de datos, herramientas de desarrollo y aplicaciones de gestión, que son capaces de gestionar grandes cantidades de datos.
- **Informix:** como uno de los líderes del mercado de bases de datos, el objetivo de Informix es simplificar y agilizar el acceso a cualquier fuente de información. El lanzamiento de Universal Server viene a marcar un punto de inflexión en la evolución de los sistemas de gestión de bases de datos, el origen de una nueva generación de gestores que cambiará la forma en que las organizaciones manejan sus fuentes de información.
- **Netscape:** su concepto de "Intranet de servicio completo" estaría compuesto por dos tipos básicos de servicios:

1. **Servicios de usuario.** Suministran recursos y aplicaciones al usuario final, como:

Compartición y administración de la información.

Conmutación y colaboración.

Navegación.

Acceso a aplicaciones.

Para acceder a estos servicios, Netscape apuesta por un cliente universal, **Navigator**. Al ser un cliente universal implica su

disponibilidad para prácticamente todas las plataformas y sistemas operativos.

Para la creación de páginas Web propone **Administration Kit**, que permite, además, personalizar el navegador según las necesidades de cada empresa.

2. **Servicios de red.** Para interconectar y ejecutar el entorno de red global. Podemos citar como fundamentales:

**Directory Server.** Un servicio de directorios que permite organizar y guardar información relativa a los usuarios de la Intranet de forma que se pueda acceder a ella fácilmente.

**Proxy Server.** Se puede almacenar una copia de la información más solicitada en un servidor local para minimizar las transacciones de información a través de la red.

**Certificate Server.** Para asegurar la confidencialidad de la información que viaja por la red. Además, se puede impedir la manipulación de la misma mediante el uso de certificados.

**Enterprise Server.** Permite un fácil acceso a todas las herramientas de administración de la red. Desde un solo puesto es posible administrar todos los servidores de la red, sea cual sea su situación geográfica.