

# 23

## LEXNET: UNA SOLUCIÓN PRAGMÁTICA

José Vences  
Responsable del Área de Sistemas  
SATEC S.A.



Una definición sencilla y concisa de los objetivos cubiertos en el servicio LexNET puede ser: “Permitir a los distintos actores judiciales el intercambio electrónico seguro de toda la documentación necesaria para el ejercicio de su trabajo. Concediendo a los documentos intercambiados plena validez jurídica, y respetando las competencias y flujos de información existentes en la actualidad”.

Esta idea tan ambiciosa tiene su fundamento en la gran cantidad de documentación que la Administración de Justicia recibe, gestiona y comunica en su relación con los abogados, procuradores, entidades oficiales que aportan información aneja, y hasta finalmente el propio ciudadano. Los escenarios a considerar tienen una naturaleza muy diversa, por ejemplo, el procurador que presenta una demanda dirigida a un juzgado, o el juez que notifica una resolución a un abogado acompañada de un análisis financiero emitido por un banco.

Es precisamente por esta complejidad del objetivo, por lo que el diseño del sistema se ha orientado precisamente al polo opuesto; la simplicidad y el pragmatismo en la búsqueda de una solución estándar, abierta, modular y escalable.

**Estandar:** El diseño de la solución tecnológica debe ser estándar puesto que los distintos intermediarios tendrían entornos de muy diversa índole y se facilitará cualquier integración.

**Abierta y modular:** Para poder moldearse fácilmente a los escenarios que se planteaban y también a los que el propio devenir tecnológico precipitará. Por ejemplo, que la sentencia dictada por un juez, suponga de forma automática y telemática, la inscripción de un ciudadano en el Registro de Protección a las víctimas de violencia doméstica.

**Escalable:** Los incrementos de carga en el sistema por la incorporación de nuevos usuarios y colectivos, debe ser asimilada con la simple adición de nuevo hardware.

**Simplicidad y pragmatismo:** En la idea de identificar los requisitos estrictamente necesarios, así como la tecnología más probada y abierta, por encima de soluciones posiblemente más potentes, o tecnológicamente más sofisticadas; pero que exceden de los requerimientos y necesidades reales.

## UN MODELO CONTRASTADO

Un sistema de estas características, suscita la primera y más básica cuestión de diseño: ¿qué tecnología utilizar para el intercambio seguro y telemático de mensajes con firma digital?

Existen en el mercado varios patrones y productos orientados al intercambio telemático; pero la mayoría de las soluciones, o son excesivamente caras, o no permiten una fácil integración con los clientes, o bien utilizan tecnologías propietarias para la firma electrónica.

En cambio, el patrón de diseño de los sistemas estándar de correo electrónico encajaba perfectamente con los requisitos descritos. Se trata de una tecnología madura para la que existen estándares, y que se encuentra plenamente contrastada. Diariamente, se envían millones de correos electrónicos en todo el mundo.

Existen multitud de productos comerciales y de software libre que permiten el enrutamiento y almacenamiento de los mensajes. Puesto que los mensajes de correo electrónico tienen un formato definido por estándares, existen herramientas genéricas para que los usuarios gestionen sus mensajes (OutLook, Netscape, etc.), o sistemas WebMail (Hotmail, GMail, etc.).

LexNET se ha desarrollado como un WebMail para adaptar y ocultar al usuario final los detalles de correo electrónico e incorporar la firma digital y un workflow específico en el envío de mensajes judiciales.

El correo electrónico dispone de extensiones (S/MIME) para incorporar la firma digital, y dispone de patrones de plataformas hardware contrastadas para soportar enormes cargas de trabajo, alta disponibilidad y balanceo de carga.

## ESTÁNDARES Y SOFTWARE LIBRE

En el ámbito tecnológico de las telecomunicaciones y la informática, existe una fuerte corriente de estandarización y de normalización que es sumamente beneficiosa para el sector y para la sociedad en general. Huir de los sistemas propietarios y de las tecnologías cautivas, ha sido una máxima en el diseño de LexNET.

LexNET se ha construido en gran medida haciendo uso de paquetes y soluciones de software libre. Su uso se deriva de cuatro hechos fundamentales, como son;

- Estar basados en estándares
- Rendimiento adecuado a las necesidades del servicio
- Ofrecer en la actualidad un nivel confortable de soporte
- Existir un equivalente en productos comerciales.

Estos cuatro puntos permiten justificar su elección desde un plano meramente técnico, no siendo en ningún caso el coste económico el motor de la decisión.

	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003
<b>Microsoft</b>	7,0%	18,1%	25,6%	35,3%	38,3%	38,1%	38,5%	39,0%	40,5%	41,0%
<b>Novell</b>	39,6%	34,7%	32,1%	26,7%	22,8%	19,1%	15,0%	13,0	12,0%	10,0%
<b>Linux</b>	0,0%	0,0%	6,5%	6,8%	15,8%	24,8%	30,0%	34,0%	36,0%	38,0%
<b>Unix</b>	28,6%	25,4%	20,1%	20,9%	18,8%	15,5%	15,0%	13,0%	11,0%	10,0%
<b>Otros</b>	24,8%	21,8%	15,7%	10,3%	4,3%	2,5%	1,5%	1,0%	0,5%	1,0%

Evolución del mercado de sistemas operativos

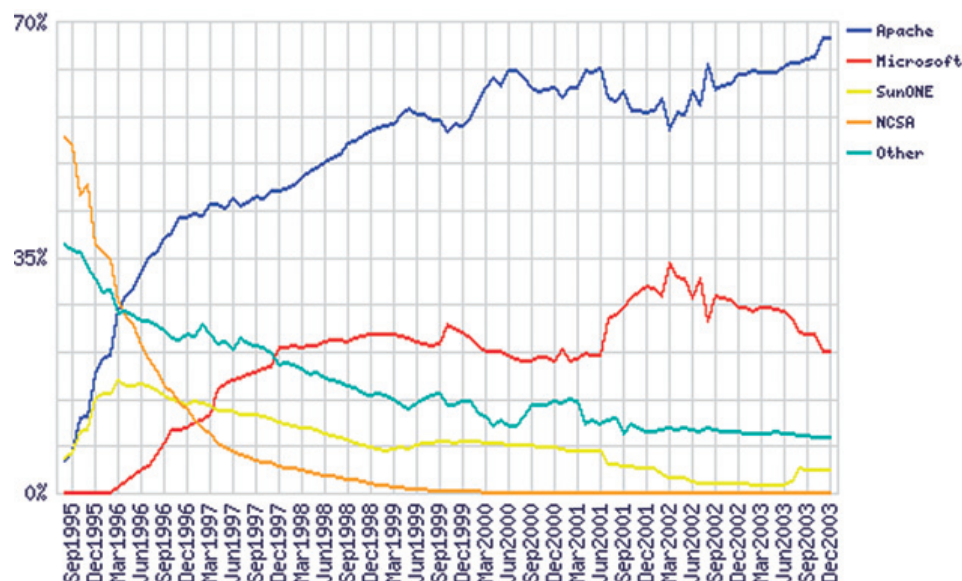
Los paquetes empleados en la creación del servicio son:

- Sistema Operativo: Red Hat Linux ES/AS
- Servidor de directorio: OpenLDAP
- Servidor POP/IMAP: CurierIMAP
- Servidor SMTP: Postfix
- Servidor WEB: Apache/Tomcat
- Servidor de base de datos. ORACLE 9i

La elección de estos elementos software esta basado en el cumplimiento de las cuatro reglas antes expuestas, no todos los paquetes citados son los que ofrecen el mejor rendimiento del mer-

cado de manera global, pero si que sus prestaciones son adecuadas a los requerimientos actuales así como a la arquitectura planteada.

En esta arquitectura únicamente se expone al exterior en una DMZ, los servicios WEB, en este caso la utilización del servidor Apache esta contrastado con la tendencia de uso, como se refleja en el gráfico siguiente<sup>1</sup>:



La utilización de OpenLDAP viene justificada en este caso por la propia arquitectura del LexNET, En esta los servidores LDAP que soportan todo el tráfico de usuarios son únicamente servidores de consulta, estando minimizado al máximo las actualizaciones. De hecho los servidores accesibles a los usuarios externos son réplicas de un directorio maestro residente en la VLAN de administración.

En esta configuración la utilización de OpenLDAP es sostenible, dado que su rendimiento en lectura es razonablemente bueno como queda demostrada en la siguiente comparativa:

<http://www.carnet.hr/CUC/tnc-cuc2003/program/papers/p1d1.pdf>

	10K	100K	1 M	10 Ms
<b>Critical Path inJoin Directory Server 4.0</b>	1.515,2	1.515,2	1.515,2	
<b>IBM Secure WAY Directory 3.2.2</b>	1.724	1.612,9	1.724,1	
<b>IPlanet/SunOne Directory Server 5.1</b>	2.272,7	2.173,9	2.272,7	2.272,7
<b>Microsoft Active Directory</b>	2.272,7	2.272,7	1.562,5	
<b>OpenLDAP 2.0.23</b>	2381,0	1923,1	2381,0	
<b>Syntegra Aphelion 2002</b>	2381,0	2173,9	2272,7	23981,0

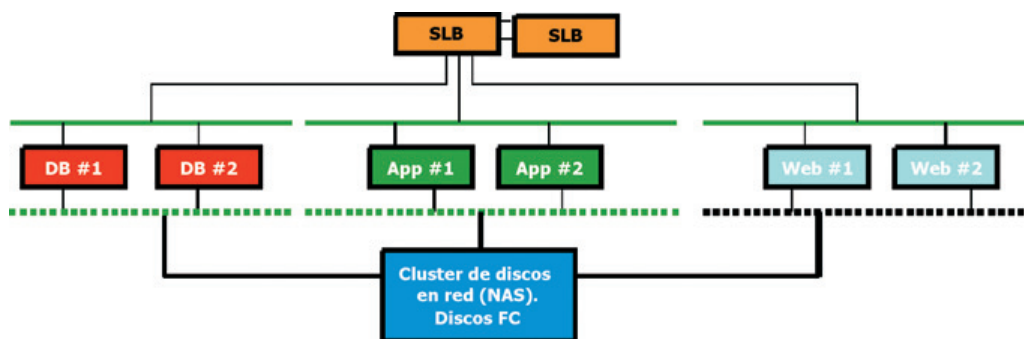
Búsqueda exacta de un atributo (operaciones por segundo)

## PLATAFORMA HARDWARE Y ESCALABILIDAD

Dos requisitos fundamentales del sistema son los de garantizar la más alta disponibilidad del mismo, así como su crecimiento y escalabilidad.

Para conseguir estos dos requisitos se ha planteado una arquitectura basada en dos elementos hardware especializados:

- Balanceadores de carga: Switch de nivel 4-7, con capacidad de balanceo de carga de cualquier servicio TCP/IP.
- Servidor de ficheros especializado Network Appliance: Servidor NFS de alto rendimiento con capacidades certificada para el soporte de base de datos (ORACLE) bajo protocolo NFS.



En esta arquitectura se presupone que todos los elementos se encuentran redundados, y que todos los servicios fundamentales del sistema, se ejecutan en al menos dos equipos. En este escenario, la caída de un equipo es detectada por el balanceador, el cual redirige todo el tráfico TCP, al nodo activo.

El único elemento del sistema cuya disponibilidad y balanceo de carga no está ligado al uso de balanceadores externos es el gestor de base de datos ORACLE, no obstante la opción RAC (Real Application Cluster) de dicho gestor ofrece la misma capacidad de crecimiento horizontal buscada, con lo que todos los elementos de la solución pueden crecer en sentido horizontal<sup>2</sup>.

## SEGURIDAD

En un sistema, como LexNET que otorga plena validez jurídica a los documentos intercambiados a través de él, la seguridad es el criterio fundamental en la validación de cualquier solución técnica. En el caso de LexNET, esta seguridad se ha fundamentado en las siguientes líneas

- Arquitectura de seguridad: La arquitectura de seguridad definida se ha basado en la creación de VLANs estancos para la ejecución de trabajos especializados. La accesibilidad a estas VLANs está controlada por una doble capa de firewalls de diferentes fabricantes.
- Elementos de custodia de claves: Todas las claves privadas necesarias en el funcionamiento del sistema se hayan custodiadas en dispositivos especializados e inviolables que cumplen la norma FIPS-140

- Virus Informáticos: Todos los mensajes transmitidos y recibidos a través del sistemas son analizados, de forma que se minimice la posibilidad de que LexNET se convierta en un difusor de Virus Informáticos.
- Aplicación: En el diseño de la aplicación no solo se ha contado con la existencia de una DMZ donde se ejecutan los servicios WEB, sino que en realidad estos están absolutamente aislados del resto de la infraestructura de forma que son los servidores de aplicaciones internos los que acceden a la información recibida en el entorno WEB, en otras palabras no existe nunca un flujo de escritura proveniente de la DMZ.

### CERTIFICADOS DIGITALES

Si bien podríamos incluir los certificados digitales en el apartado de seguridad, explicitando que el acceso al sistema esta restringido a usuarios en posesión de un certificado X509 v3; es importante resalta el hecho de que LexNET es un sistema abierto en relación tanto a las autoridades de certificación como al carácter de los certificados X509 V3 empleados.

Este último punto es muy importante en el sistema, dado que en el mismo conviven tanto los certificados de carácter personal emitidos por autoridades de certificación generalistas (FNMT, Generalita Valenciana, CATCERT, como certificados profesionales emitidos por autoridades de certificación privadas de colectivos profesionales como la Autoridad de certificación de la Abogacía

En este escenario cuando el certificado no posee información del ROL que el usuario ejerce en el sistema (Procurador, Secretario Judicial, Oficial administrativo) es el servicio de directorio privado de LexNET el que cualifica en el sistema a dicho usuario. Esta aproximación permite se extremadamente flexibles tanto en las funciones de los distintos agentes, como en el reconocimiento de entidades de certificación válidas.

### UN SERVICIO, MÚLTIPLES INTERFACES

Desde el primer momento se planteo la arquitectura de LexNET desde dos aproximaciones:

- LexNET debia ser un sistema completo que permitiese a usuarios con una informática básica acceder a los servicios ofrecidos a través de un interfaz WEB.
- LexNET no debería ser un sistema complejo que resuelva todos los problemas y necesidades de los distintos colectivos soportados (Abogados, Procuradores, Secretarios Judiciales, etc)

Este segundo requisito, ha querido facilitar la integración a aplicaciones con LexNET a través de WebServices (SOAP) y ficheros de intercambio (XML). Esta aproximación permite que el sistema pueda ser visto y explotado (en potencia) desde las aplicaciones particulares de los distintos colectivos, facilitando a las distintas organizaciones el ofrecer servicios de valor añadido a sus afiliados.

El siguiente esquema, muestra una interacción entre un agente externo de la Justicia, con el sistema LexNET para incorporar de forma automática un documento a un procedimiento en un juzgado. Para ello se utilizan los WebServices creados a tal efecto.



## BIBLIOGRAFÍA

- 1- Servidores WEB: Fuente Netcraft
- 2- La opción de montaje de ORACLE RAC sobre servidores NetApp se encuentra certificada por ORACLE.