EUSKO JAURLARITZA
GOBIERNO VASCO

— Ejemplar en Castellano (*) —

Aurrera!

Nº 29

Marzo de 2008

Boletín Divulgativo de Nuevas Tecnologías en Informática y Telecomunicaciones

Publicado por el Gabinete Tecnológico de la DIT

ÍNDICE

Una vez tratado el tema del **Software Libre** en ejemplares anteriores, explicando desde cuál fue su origen, hasta la exposición de distintas experiencias desarrolladas en otras Comunidades Autónomas, en esta ocasión nos hemos querido centrar en nuestro entorno. Es por ello que, a lo largo del primer tema, recogemos las distintas iniciativas y/o soluciones software que desde hace tiempo se vienen utilizando en los Sistemas de Información del Gobierno vasco y, de este modo, dar a conocer cuál es la postura y uso real que la administración pública vasca hace de este tipo de soluciones.

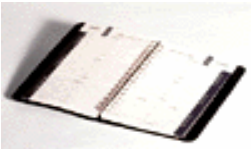
El segundo de los temas de hoy centra su foco sobre la **seguridad de las redes**. En este sentido, hay que señalar que el problema que desde siempre han tenido los Administradores de red, ha sido el ofrecer a sus "clientes" (los usuarios) un entorno de trabajo lo más seguro posible y, siempre, a un precio razonable. Son muchas las soluciones y productos que se han venido utilizando para conseguir ese objetivo, sin embargo, parece que la tendencia actualmente es centrarse en potenciar las comunicaciones seguras, es decir, controlar y asegurar de la misma forma los accesos de todos los usuarios (tanto si son externos como internos).

Por su parte, la sección Alboan nos presenta una de las funcionalidades que más se va a utilizar en las aplicaciones del Gobierno de aquí en adelante, esto es, el Sistema de Localización bautizado como **NORA**. Dicha solución, que ha sido promovida por la Dirección de Informática y Telecomunicaciones, ha contado con la participación de distintos Departamentos, entre los que cabe destacar, Eustat, Medio Ambiente y Ordenación del Territorio y la Dirección de Administración Electrónica y Atención a la Ciudadanía, así como EJIE.

Finalmente, dentro del apartado Breves, por un lado, os trasladamos una reflexión sobre las típicas notas que se incluyen al final de muchos **correos electrónicos**, donde, por ejemplo, se amenaza al destinatario que podría estar cometiendo delito si divulga el contenido ¿son legales?, ¿son efectivas?, ...; y por otro lado, os adelantamos la propuesta que una empresa de telefonía móvil acaba de mostrar (llamada **Morph**) y, que a medio plazo, puede revolucionar el aspecto y funcionalidades de estos aparatos.

El Software Libre en el Gobierno vasco

El presente artículo pretende resumir las iniciativas mas significativas de promoción y uso del software libre dentro del Gobierno Vasco; que tal y como se podrá comprobar a lo largo del mismo, son más numerosas de lo que nos podríamos imaginar.



DICCIONARIO

(1) **Coste Total de Propiedad** (o Total Cost of Ownership): es un método de cálculo diseñado para ayudar a los responsables de áreas a determinar los costes directos e indirectos, así como los beneficios, relacionados con la compra de equipos o programas informáticos. El análisis del TCO fue creado en 1987 por el **Grupo Gartner**.

El TCO ofrece un resumen final que refleja no sólo el coste de la compra sino aspectos del uso y mantenimiento (formación del personal de soporte y de usuarios, el coste de operación, y de los equipos o trabajos de consultoría necesarios, etc.)

Habitualmente, el coste de licencia de un programa informático tiene una relación de 1 a 10 frente a su coste total de propiedad.

Por ejemplo, la compra de un PC incluiría la compra en sí misma, reparaciones, mantenimiento, actualizaciones, servicios y soporte, redes, seguridad, formación y costes de licencias.

Son muchas las iniciativas llevadas a cabo en los últimos tiempos por parte de distintos Organismos y Administraciones Públicas para apoyar e impulsar el uso del Software Libre (SL). La Administración Pública vasca, no está al margen de este tipo de acciones, y es por esa razón que, en esta ocasión, expondremos, por una parte, el uso que el Gobierno vasco hace de las soluciones de SL y/o las distintas iniciativas llevadas a cabo dentro de su ámbito y, por otra parte, los criterios que en todo momento se evalúan para su adopción; como pueden ser, por ejemplo, el cumplimiento de las funcionalidades requeridas por el usuario y/o el coste total de propiedad(1).

USO DEL SOFTWARE LIBRE EN EL GOBIERNO

Desde hace varios años, el Gobierno vasco viene utilizando diversas soluciones basadas en Software Libre. A continuación detallamos los productos que actualmente ya se están empleando dentro de su Red Corporativa:

- **Productos**

Relación de productos que forman actualmente parte de los estándares informáticos:

- Servidor de FrontEnd y BackEnd: Linux RedHat AS
- Servidor Web: Apache
- Servidor de Aplicaciones: TomCat
- Servidor de Base de Datos: MySQL
- Navegador Web de Desarrollo de Aplicaciones: Firefox
- Control de Versiones: CVS
- Pruebas de Software: JUnit
- Entorno de Desarrollo Integrado: Eclipse
- Herramientas de Listados e Informes: FOP

- **Servidores**

La mayoría de los servidores que dan servicio web (Apache) y servidores de aplicaciones, son equipos con sistema operativo Linux, como por ejemplo, los servidores web y de Aplicaciones de euskadi.net. Actualmente existen más de 160 servidores con Linux en las instalaciones de EJIE.

- **Educación-Formación**

El portal de aprendizaje permanente www.hiru.com del Dpto. de Educación, Universidades e Investigación ofrece mediante la provisión de contenidos gratuitos, servicios públicos de educación a través de Internet y está basado en varios productos de Software Libre como pueden ser Linux, TomCat, Zope o MySQL.

Existen otros portales, como www.ikasbil.net de HABE, basado en las tecnologías de gestión de portales JetSpeed y MMBase y con un albergue de datos en MySQL o http://www1.eeuskadi.net donde se gestionan las pruebas de certificación para la IT-Txartela.

"El Gobierno Vasco también está promoviendo una distribución en euskera de Debian".

Existen otras iniciativas que tienen definido el uso de Moodle como sistema de gestión de cursos. Basado en el uso de Linux, PHP y MySQL.

- **Colaboración ciudadana**

El portal www.konpondu.net es un sitio de participación donde se ofrece la posibilidad de recoger opiniones, propuestas e ideas para la construcción de la paz. Es el máximo exponente de lo que se conoce por Web 2.0, donde se ofrecen servicios de blogs, foros y vídeos con herramientas como WordPress o phpBB,

desarrollos realizados en PHP, bases de datos MySQL y todo funcionando sobre sistema operativo Linux.

El blog de la Dirección de Juventud (Gazteaukera http://blog.gazteaukera.euskadi.net) creado para recabar información sobre las inquietudes de la juventud vasca, ha sido desarrollado sobre WordPress y está albergado sobre sistemas de Software Libre.

- **Ámbito interno**

A nivel más interno, se utilizan diferentes aplicaciones y sistemas operativos que podemos englobar dentro de Software Libre y que su uso también está muy extendido.

Para el soporte al desarrollo, por ejemplo, se usa CVS (Concurrency Version System), como herramienta de control de versiones y Mantis, como gestor de dependencias de aplicaciones. Existen otras herramientas estandarizadas asociadas al ciclo de vida de aplicaciones englobadas en el concepto de software libre como pueden ser extensiones de accesibilidad para navegadores, aplicaciones para pruebas de código, funcionales y de carga, descompiladores, herramientas de Bases de Datos como Tora, cliente de CVS como Tortoise CVS o aplicaciones cliente como Firefox y GIMP.

En el ámbito de la explotación de las infraestructuras, es frecuente el uso de herramientas como las que se emplean para la monitorización: Nagius, Cricket o NfSen.

OTRAS INICIATIVAS DEL GOBIERNO

A continuación, y de forma resumida, detallamos algunas de las iniciativas llevadas a cabo por el Gobierno (a través de distintos Departamentos) y que van dirigidas hacia el mundo empresarial.

- **Subvención KZ Lankidetza**

Se subvencionan desarrollos de aplicaciones informáticas que pueden ser utilizadas por las empresas. Dichas aplicaciones o herramientas de gestión deberán ser desarrolladas con herramientas de Software Libre, y deberán ser registradas como aplicaciones GPL (General Public License) al objeto de que cualquier empresa pueda utilizarlas sin limitaciones. www.spri.es/kzlankidetza

- **Enpresa Digitala**

Actuaciones relacionadas con el Software Libre:

- Jornadas y/o eventos de divulgación sobre el Software Libre. (www.enpresadigitala.net)
- Encuentros sobre Software Libre para fomentar el intercambio de experiencias entorno a la adopción de este tipo de Software, los cuales se organizan de forma periódica.
- Weblog sobre Software Libre (http://weblog.bizkaiadigitala.net) con el fin de servir de herramienta de comunicación entre sus miembros.

- **Traducción de Software Libre**

La Viceconsejería de Política Lingüística del Departamento de Cultura, ha puesto a disposición de los usuarios (http://www.euskara.euskadi.net) las traducciones del paquete de ofimática OpenOffice.org (año 2002 y 2003), así como los manuales de referencia tanto de OpenOffice 1.0.2 y de StarOffice 6.0.

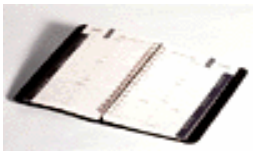
En relación a los correctores ortográficos, en 2006, se publico el motor Hunspell de OpenOffice.org 2.2.

- **Distribuciones desarrolladas en Euskadi**.

El Gobierno vasco también está promoviendo una distribución en euskera de Debian, siguiendo el camino emprendido por las comunidades extremeña y andaluza con Linex y Guadalinex, respectivamente. El problema es que dichas acciones no tienen la misma repercusión mediática que las realizadas por otras Comunidades Autónomas, porque las referidas distribuciones tienen un público objetivo más reducido, al ser traducciones en Euskera. En concreto, hasta la fecha, se han elaborado las siguientes:

- EusLinux 2002, basada en Mandrake 8.2
- EusLinux 2004, basada en Mandrake 10.0
- EusLinux 2005, basada en Debian

- En todos los **KZGunea** se dispone de parte de los puestos con Software Libre.
- Euskadi-n Floss: dentro de este proyecto se ha realizado un estudio cuyo objetivo es definir la



Consultas del Parlamento vasco relativas al Software Libre

Relación de iniciativas o consultas realizadas por el Parlamento Vasco sobre el Software Libre y la Administración Pública vasca:

Números de Expediente:
07\10\05\03\1409
07\10\05\03\1596
07\11\02\01\0200
08\10\04\01\0068
08\10\07\02\0322
08\10\07\02\0323
08\10\05\03\1568
08\11\03\00\0028

http://parlamento.euskadi.net/

estrategia para el Software abierto-libre en Euskadi y elaborar propuestas de proyectos piloto. A fecha de hoy se han identificado, por una parte, 4 posibles proyectos pilotos, y por otro lado, 6 actividades de impulso al Software Libre.

ESTUDIO DE SITUACIÓN

A petición del Parlamento vasco el Gobierno, de forma paralela a la elaboración del Plan de Informática y Telecomunicaciones (PIT) 2006-2009, llevó a cabo en su momento un completo y detallado estudio para valorar la posibilidad de sustituir el software ofimático en el cliente por soluciones de "software libre". Finalmente, dicho estudio fue ampliado más allá de la simple ofimática del puesto de trabajo, con la idea de contemplar el posible uso de otros componentes de software libre en el conjunto de las aplicaciones corporativas del Gobierno.

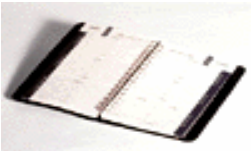
El estudio mencionado analizó con detalle las configuraciones de productos que proporcionan los servicios demandados, agrupados según las características de dichos servicios, en cinco plataformas tecnológicas diferenciadas:

1. Puesto de trabajo (puesto ofimático básico)
2. Servicios de colaboración y correo electrónico
3. Servicios de administración técnica de los puestos de trabajo
4. Gestión documental y producción administrativa
5. Plataforma de administración electrónica e interoperabilidad

LOS RESULTADOS

Las conclusiones obtenidas del análisis de situación realizado fueron las siguientes:

- A día de hoy, ninguna opción "pura" de software libre cumple con el total de las necesidades requeridas por el Gobierno vasco, ni siquiera en la configuración del puesto de trabajo.
- En la mayoría de las soluciones alternativas que podrían ser consideradas, es necesario realizar un **proceso de adaptación** que proporcione al software libre las funcionalidades requeridas que le faltan, lo que generaría unos costes de desarrollo y soporte técnico, en todo caso superiores a los costes de licencias y soporte de la opción equivalente actualmente empleada.
- A pesar de lo anterior, se considera que pueden introducirse aplicaciones, productos o soluciones de software libre de forma puntual, en los casos que alcancen un grado de madurez suficiente (según los criterios de selección[2] habitualmente usados), dando origen a configuraciones mixtas de código licenciado y libre, integradas en torno a estándares abiertos. Esta estrategia de componentes, que el mercado viene denominando arquitectura SOA (ver Boletín Nº 24, pág. 21), permitirá incrementar paulatinamente el número de componentes basados en software libre, mucho más allá del simple puesto de trabajo.



DICCIONARIO

[2] Los **criterios de selección** básicos que sigue el Gobierno para incorporar cualquier producto software por otro equivalente en prestaciones, son:

- cumplimiento de **estándares abiertos**
- cobertura de las **funcionalidades** requeridas
- disponibilidad de **soporte técnico** adecuado
- **grado de implantación** suficiente
- **coste de propiedad** del producto a evaluar

Actualmente, todos los componentes software que constituyen la infraestructura informática del Gobierno cumplen los estándares abiertos, tanto "de iure" como "de facto". Esto permite en todo momento evaluar la posibilidad de incorporar o sustituir aplicaciones, con licencia o libres, basándose en criterios de "mérito" de dichas piezas tecnológicas; pero siempre respetando su perfecto encaje (**interrelación**) con las piezas ya existentes, evitando las posibles incidencias inducidas (efectos colaterales).

EUSKO LEGEBILTZARRA
PARLAMENTO VASCO

LIBERTAD DE OPCIÓN

Según acuerdo del 27 de junio de 2007, el Parlamento vasco insta al Gobierno vasco a establecer como principio general que la ciudadanía disponga de **libertad de opción y elección**, garantizando la adopción de estándares públicos y posibilitando así la comunicación entre la ciudadanía y la Administración General del País Vasco.

En este sentido, la presencia en Internet (a través del portal euskadi.net) garantiza lo solicitado, puesto que todos los desarrollos se prueban en los navegadores más habituales (IExplorer, Firefox, etc.); es más, en los Pliegos de Bases Técnicas (PBTs) se requiere que las pruebas se hayan realizado en los navegadores más habituales (contemplando los de Software Libre). Actualmente, se encuentra en ejecución el plan de revisión de los elementos que ya se encuentran en producción.

Asimismo, a la hora de la presentación de documentos por parte de la ciudadanía y/o empresas se admiten los formatos de Microsoft Office, OpenDocument, PDF, HTML, RTF,...

En lo referente a la sustitución del software de ámbito ofimático por software libre, en este momento, no se considera oportuno realizar un cambio del software actual del puesto cliente para migrar a un entorno de software libre, por los siguientes motivos:

- ✓ De acuerdo con los análisis realizados, el **coste total de propiedad (TCO)** de una configuración de puesto de trabajo basada en software libre es, hoy en día, mayor que el de la configuración actual equivalente basada en software con licencia, básicamente por las necesidades de soporte técnico.

"El Gobierno mantiene el compromiso de seguir atentamente la evolución de las aplicaciones, productos y soluciones basadas en software libre."

- ✓ Los componentes libres disponen de menor capacidad de uso que los que se encuentran operativos en la plataforma actual, no cubriéndose todas las **funcionalidades** necesarias. Asimismo, la mayor dificultad en la interconexión de los dispositivos móviles con las herramientas ofimáticas, la no disponibilidad de funciones avanzadas del cliente de correo electrónico en combinación con la plataforma propietaria de servidor de correo corporativo, las menores capacidades avanzadas de las hojas de cálculo, o la menor capacidad gráfica de las herramientas de presentación aconsejan no realizar todavía la migración planteada.

  En la actualidad, el desarrollo de estas funcionalidades requeridas(3) se encuentran retrasadas en las posibles plataformas libres.

- ✓ Una plataforma basada en software libre dificultaría la **administración centralizada** de los puestos cliente. El Gobierno vasco gestiona hoy en día más de 6.000 puestos operativos dentro de la Red Corporativa Administrativa, que requieren una administración remota de los mismos. En este momento, no existe un producto o solución basado en software libre que cubra esta función con las garantías suficientes de soporte que exige el servicio público.

- ✓ Existe una gran dificultad en la interconexión e integración de la ofimática con los **sistemas corporativos**. Actualmente, esta integración en las plataformas libres se realiza mediante "conectores" desarrollados por terceras partes, que no ofrecen la garantía de funcionamiento adecuada para una Administración de nuestro tamaño.

- ✓ Existen, asimismo, problemas de **compatibilidad** de diferentes tipos de dispositivos hardware con los entornos de software libre. Ello provoca dificultades en el soporte, por parte de los fabricantes de hardware, cuando la configuración del puesto de trabajo es compleja, sin limitarse simplemente a un sistema operativo con software ofimático básico.

- ✓ El grado de **implantación** del software libre en instituciones de tamaño similar al Gobierno vasco es bastante bajo. En otras Administraciones europeas existen experiencias incipientes en la implantación de software libre en el puesto de trabajo, pero los resultados son desiguales. Desde el Gobierno, se considera que no deben introducirse factores de riesgo adicionales en un momento que es crítico para el correcto desarrollo de la Administración Electrónica.

El Gobierno vasco considera que todos los aspectos negativos anteriores, sin duda se solventarán con el tiempo, en la medida en que las plataformas libres maduren y, con ello, se implanten en grandes organizaciones.

El Gobierno, por tanto, mantiene el compromiso de seguir atentamente la **evolución** de las aplicaciones, productos y soluciones basadas en

software libre, del mismo modo que se hace con el software propietario, manteniendo buena predisposición para su implantación y uso, pero cumpliendo una estrategia inflexible de estándares que permitan sustituir los componentes de las plataformas tecnológicas establecidas, implantando los mejores componentes del mercado en cada momento, facilitando la utilización y mejora de la administración electrónica en nuestro país.

DICCIONARIO

(3) **Funcionalidades requeridas**: Es cierto que, para algunos usuarios, estas funcionalidades no son estrictamente necesarias, pero, dado que no existe gran diferencia en el coste total de propiedad (tal y como se concluye del estudio realizado), y la plataforma licenciada actual cumple los estándares, no se justificaría el mantenimiento de dos entornos de trabajo diferentes (uno más avanzado y otro más sencillo) con las consecuencias que ello conlleva: incremento de costes de soporte, mantenimiento, atención de usuarios y resolución de incidencias, es decir, el denominado Coste Total de Propiedad o TCO.

Redes seguras vs. Comunicaciones seguras

Hoy día se buscan redes corporativas que sean inteligentes y seguras; para ello, es necesario incorporar seguridad en todos los puntos de la red, actualizar cortafuegos, routers, conmutadores y el resto de equipamiento de la red. Todo ello implica un coste demasiado elevado. Vamos a intentar explicar cuál puede ser la tendencia en este ámbito en un futuro no muy lejano.

DICCIONARIO

(4) **Modelo OSI**: (Open Systems Interconnection) Formato creado por la ISO (Internacional Standard Organization), estructurado en capas, y que puede integrar todas las tecnologías de comunicación existentes. Las siete capas que lo componen son las siguientes: física, enlace, red, transporte, sesión, presentación y aplicación.

(5) **Sinergia**: podemos decir que la palabra sinergia proviene del griego y su traducción literal sería la de cooperación; no obstante se refiere a la acción de dos (o más) causas cuyo efecto es superior a la suma de los efectos individuales. Es la integración de elementos que da como resultado algo más grande que la simple suma de éstos, es decir, cuando dos o más elementos se unen sinérgicamente crean un resultado que aprovecha y maximiza las cualidades de cada uno de los elementos.

Es conocido que las conexiones a las redes corporativas utilizan cada vez con mayor frecuencia las redes públicas existentes, es decir, estas conexiones no se establecen desde nuestra propia red privada, sino que se realizan desde redes que no están bajo nuestro control, ya que hoy en día el número de usuarios que necesitan estar permanentemente conectados a nuestra red interna, independientemente de la ubicación física en la que se encuentren, es mayor.

Además, a parte de usuarios internos de nuestra red corporativa, la situación previsible es que proveedores y contrataciones externas, y en nuestro caso, como administración pública que somos, también la ciudadanía, interactúen con nuestros sistemas.

ASEGURAR LA RED

El proceso de securizar la red puede resultar cada vez más complejo y sobre todo, en función del tamaño de la misma, bastante caro. Al mismo tiempo puede resultar difícil de conseguir y, a su vez, requiere una atención diaria y una actualización constante.

> **"La idea clave de esta nueva tendencia no es centrarse en redes seguras, sino en comunicaciones seguras."**

La **tendencia** en un futuro podría ser, según los expertos, la de **mantener unas redes simples y rápidas a la vez que fiables**. Para ello los puntos a reforzar deberán ser los ***switches*** (nivel 2 del modelo OSI(4)) y ***routers*** (nivel 3 del modelo OSI), mantenerlos a salvo de ataques y evitar que se puedan "caer" fácilmente.

Además, se están implementando mecanismos en los **clientes finales** (PC's, PDAs y servidores) para que dichos dispositivos solo puedan acceder a la red después de que han sido verificados para cumplir completamente con las políticas de seguridad establecidas.

CAMBIAR LAS PRIORIDADES

La idea principal de esta tendencia no sería dejar de garantizar la seguridad de las redes, sino en **cambiar las prioridades de la inversión**, es decir, invertir en las comunicaciones entre el usuario y los recursos y aplicaciones de la red a las cuales necesite acceder, con ello se conseguiría una sinergia(5) entre las dos redes, evitando construir una estructura privada que, seguramente, sería muy costosa.

Las redes, *per se,* son inseguras, ya que en nuestras redes internas hay equipos que trabajan desde dentro de la red, pero también hay un número creciente de equipos que trabajan desde fuera de ella.

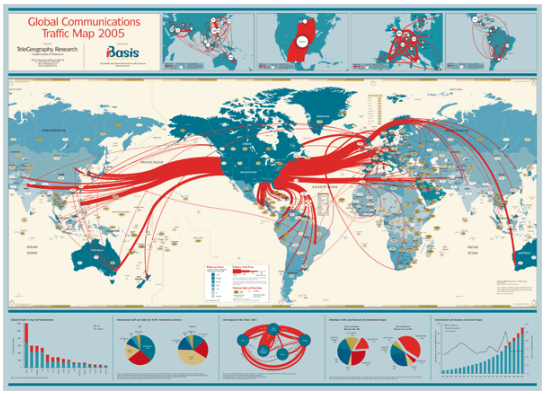
La inversión que se realiza en securizar la red no suele estar en consonancia con los resultados que se deben obtener, es decir, aun aportando mucho dinero en securizar las redes, no dejan de recibir ataques de todo tipo, cada vez más perjudiciales y potentes. Cabe destacar que los ataques más dañinos que recibe una red privada suelen venir desde dentro de la propia organización.

La idea clave de esta nueva tendencia no es **centrarse en redes seguras, sino en comunicaciones seguras**, o lo que es lo mismo, unos canales de comunicación seguros entre dos interlocutores que, por otro lado, no poseen el control sobre dichos canales, y para los que existen dos claros peligros:

- El acceso a estos canales por parte de personas no autorizadas (confidencialidad).
- La alteración de los datos que circulan por los canales (integridad).

Para que un sistema sea atacado necesariamente debe de existir un acceso físico al mismo; algunos servicios de nuestra red, como los servicios Web y DNS, requieren estar abiertos, por lo que están expuestos a los ataques externos.

Hoy día, los equipos de cualquier red procesan informaciones provenientes de otras redes externas, con lo que habrá que autenticar el origen, mediante aplicaciones que protegen el acceso a los recursos de la propia red corporativa. Todo esto exige **sistemas de cortafuegos** (firewall) más eficaces y más **filtros de tráfico TCP/IP**. Los primeros, los **sistemas de cortafuegos**, deben separar nuestra red corporativa (de confianza) del resto de equipos del exterior, no es sino un control de acceso a nivel de red. Dado que el sistema cortafuegos es un punto de entrada a la red, puede llevar a cabo una autentificación adicional a la que efectúan los servicios ofrecidos por la misma. En el



segundo caso, los **filtros de tráfico**, permiten reducir el tamaño de las tablas de rutas en los elementos de nuestra red, y evitan que los usuarios puedan alcanzar zonas de red no permitidas (esta solución puede presentar problemas en usuarios móviles cuyas IPs no son fijas).

Por otro lado, la autentificación de usuarios en un **sistema de cortafuegos** tendrá la finalidad de permitir o rechazar la conexión al usuario que solicita una conexión con un servicio interno (normalmente, mediante un mecanismo más fuerte que el implantado por el servicio al que se conecta). Pero esto tiene una parte negativa, la construcción de servicios adicionales en un **sistema de firewalls** incrementa el número de vulnerabilidades sobre éste y, por lo tanto, el riesgo.

"Ventajas de las VPNs: la seguridad que proporcionan a las comunicaciones y los costos frente a los enlaces dedicados; desventajas: se aumenta el procesamiento y el tamaño de los paquetes."

En un modelo teórico de comunicación segura, **el trato que se dispensaría a todos los usuarios de la red debería ser el mismo**. Es decir, sería independiente del lugar desde el cual se establezca la comunicación, si fuese desde el interior de la propia red o si se realizase desde fuera de la misma.

Cada conexión se analizaría de igual modo, esto es, cada conexión sería catalogada como "**a analizar**" y cada red, por defecto, se asumiría

Cómo instalar servidores seguros

*El primer paso es disponer de un servidor que soporte SSL, cosa bastante común hoy día, después se debe elegir una empresa certificadora (p.ej **IZENPE**) que respalde la identificación del servidor, para, posteriormente, rellenar los formularios establecidos por la empresa certificadora, y al cabo de unos días, esta enviará el Certificado de Servidor Seguro, junto con las instrucciones para su instalación.*

RED "LISTA" vs. RED "TONTA"

- ✓ La red "lista" se puede hacer cada vez más inteligente y segura, a cambio, el coste y el mantenimiento de la misma se disparan de una forma exponencial; la red "tonta" asume por defecto que todas las redes son inseguras, y con esa premisa actúa, es decir, procura que todas las comunicaciones sean seguras, o lo que es lo mismo, considera a cualquier otra red hostil, incluida, por supuesto, Internet.
- ✓ La red "lista" utiliza cada vez más *routers*, más cortafuegos y mas redes privadas; la red "tonta" utiliza más infraestructura pública, es decir, más infraestructura compartida.
- ✓ La red "lista" debe estar perfectamente actualizada para garantizar la seguridad; la red "tonta" centra su inversión en un único apartado: la fiabilidad.
- ✓ En la red "lista" el acceso remoto es un caso especial, y como tal lo trata; en la red "tonta" todo es remoto, por lo tanto, la excepcionalidad de este caso deja de ser especial, pasando a denominarse a todo "**accesos**".

como insegura. El hecho de conectarse a tres metros del centro de datos o a cientos de kilómetros no sería un hecho diferenciador, a ambos usuarios se les trataría teóricamente del mismo modo.

La situación actual, debido al aumento de las comunicaciones móviles e inalámbricas, ha sido la de procurar que el acceso de los usuarios móviles esté protegido y securizado. Estos conceptos de protección y securización, dentro de la filosofía que estamos explicando, también se aplicaría a los usuarios cuyos equipos de conexión estuviesen ubicados físicamente dentro de nuestra red, a los usuarios no móviles, lo cual supone un cambio de mentalidad en cuanto al tratamiento de las conexiones se refiere que se lleva a cabo hoy en día.

CONTROL EN EL ACCESO

Como sabemos, un ***gateway*** (pasarela) es un elemento de la red que actúa como punto de entrada a otra red.

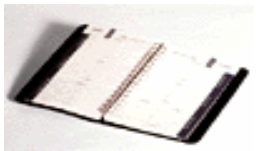
Para realizar un control de acceso efectivo se utiliza un gateway de acceso a aplicaciones seguro (SAAG), como un SSL VPN (el cual establece túneles en la capa de aplicación, mientras que, como hemos señalado antes, los cortafuegos trabajan en la capa de red), también permite acceso controlado a recursos específicos (seguridad granular en la capa de aplicación). En el mercado, este tipo de "**cajas negras**" que permiten realizar este tipo de trabajo (además de permitir el establecimiento de redes privadas virtuales -VPN-, son capaces de hacerlo de forma segura, encriptando los datos que viajan punto a punto entre los interlocutores, de tal forma que, si existe algún tipo de riesgo de ser monitorizados por usuarios no autorizados, estos nunca puedan interpretar la información que obtienen, salvaguardando la integridad de la información que transmitimos o recibimos) se denominan "**appliances**". Gracias a estas "cajas negras", en cualquier momento y desde cualquier sitio se pueden proporcionar accesos seguros a los recursos críticos de una organización, en tiempo real, con la ventaja de poder auditar el acceso a estos recursos y securizar los mismos a distintos niveles.

Si bien, actualmente las SSL VPNs se utilizan para el acceso remoto seguro, en un futuro, tal y como hemos comentado en el apartado sobre las redes "listas" y las redes "tontas" [ver cuadro "la Red Lista y la Red Tonta"], el término remoto tendería a desaparecer, y **solo existirían conexiones**.

Podemos subrayar que el comercio electrónico utiliza el protocolo SSL para establecer transacciones seguras, sin embargo, el uso de este protocolo no supone ninguna dificultad para el usuario, de hecho resulta transparente para el.

El modelo de acceso a redes corporativas, y siguiendo con la nueva filosofía recogida en este artículo, debería seguir el ejemplo del comercio virtual, es decir, **plataformas sencillas de utilizar**, con un acceso transparente y fácil, en cuyo entorno todo el mundo es tratado por igual, como si fuese un usuario externo, y estableciendo políticas comunes para realizar la gestión de la red corporativa, lo que facilita enormemente el trabajo de gestión.

Lo que debe quedar claro es que nuestro trabajo va a utilizar cada vez con mayor frecuencia



DICCIONARIO

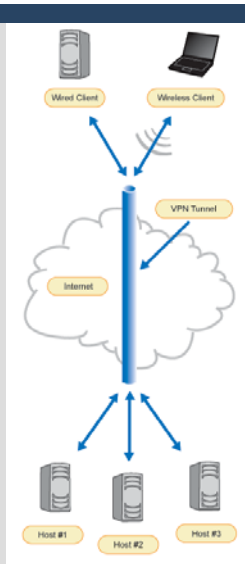
(6) **Herramientas de movilidad**: ver Boletín AURRERA nº 18 (en el apartado Alboan, el artículo sobre "soluciones de movilidad") de junio de 2005, en el cual se enumeran las diferentes formas de conexión a la Red Corporativa Administrativa del Gobierno Vasco (RCAGV).

RED PRIVADA VIRTUAL

Una **red privada virtual** (VPN) es una configuración que combina el uso de dos tipos de tecnologías:

• Las tecnologías de seguridad que permiten la definición de una **red privada**, es decir, un medio de comunicación confidencial que no puede ser interceptado por usuarios ajenos a la red.

• Las tecnologías de encapsulamiento de protocolos



que permiten que, en lugar de una conexión física dedicada para la red privada, se pueda utilizar una infraestructura de red pública, como Internet, para definir por encima de ella una **red virtual**.

Por tanto, una VPN es una red lógica o virtual creada sobre una infraestructura compartida, pero que proporciona los servicios de protección necesarios para una comunicación segura.

herramientas de movilidad[6], empujado por la tendencia de las conexiones inalámbricas y los requisitos de nuestros usuarios, tanto internos como externos.

Así mismo, la infraestructura de Internet va a permitirnos el disponer de las infraestructuras públicas para cualquier tipo de conexión y en cualquier lugar, con lo que habrá que sacar el máximo partido de esta ventaja.

"El objetivo de esta tendencia es tener una red simple, "tonta", rápida y fiable."

Por nuestra parte, y para sacar el máximo rendimiento a las herramientas que disponemos, incluida Internet, deberemos aportar la seguridad a nivel de aplicación, dejando para las redes el trabajo de enrutamiento de paquetes de una forma rápida y fiable, ya que, como hemos comentado, resolver el problema de seguridad en la capa de red es demasiado costoso y, a la larga, se torna un trabajo difícil de realizar.

Partiendo de estas premisas y para proteger los activos de red, cualquier organización debe implementar políticas para confirmar el buen funcionamiento de los clientes antes de permitir el acceso o la comunicación a la red.

Por parte de las grandes firmas de informática y comunicaciones se están desarrollando herramientas que permiten validar la "salud informática" antes de permitir dicho acceso o la comunicación, garantizar el cumplimiento continuo de las políticas, actualización automática de los clientes y, de forma excepcional, aislar los ordenadores que no cumplen con los requisitos en una red restringida, hasta que logren el cumplimiento.

Estas herramientas permiten a la red **identificar**, **prevenir** y **adaptarse** a las amenazas al reforzar automáticamente políticas de seguridad corporativas en todos los dispositivos, tanto locales como remotos, habilitados con dichos mecanismos.

Estas herramientas, denominadas **NAC**[7], son un método cliente/servidor para asegurar el estado de "salud" de los puntos finales antes de que puedan conectarse a una red informática. Podemos destacar las siguientes arquitecturas NAC: NAP de Microsoft, Trusted Network Connect (TNC) del Trusted Computing Group, Network Admission Control de Cisco, Symantec Network Access Control y McAfee Network Access Control.

En definitiva, el objetivo de esta tendencia es tener una red simple, "tonta", rápida y fiable.

COMO FUNCIONA SSL

El protocolo SSL[8] establece de forma sencilla conexiones seguras vía Internet.

Se sitúa en la capa de aplicación, directamente sobre el protocolo TCP, y aunque puede proporcionar seguridad a cualquier aplicación que corra sobre TCP, se usa principalmente para dar seguridad a los protocolos HTTP, SMTP y NNTP.

Su función consiste en interponer una fase de codificación de los mensajes antes de enviarlos a través de la red, de tal manera que, la capa SSL del emisor coge la información, la codifica y la transmite para que el receptor la decodifique y la pase como *texto en claro* a la aplicación destinataria.

SSL también incluye un mecanismo de autenticación que permite garantizar la identidad de los interlocutores.

La comunicación SSL tiene tres fases:

- ✓**Establecimiento** de la conexión, donde se negocia los algoritmos criptográficos que van a usarse en la comunicación.
- ✓**Intercambio** de claves, empleando algún mecanismo de clave pública y autenticación de los interlocutores a partir de sus certificados digitales
- ✓**Cifrado** simétrico del tráfico.

Una de las ventajas de usar un protocolo de comunicaciones, en lugar de un algoritmo, es que ninguna de las fases del **protocolo** queda atada a un algoritmo, por lo que si en el futuro aparecen otros algoritmos, el cambio se puede realizar sin modificar el mismo.

Existen implementaciones de SSL que permiten construir los llamados *túneles SSL* que dirigen cualquier conexión a un puerto TCP a través de una conexión SSL previa, de forma transparente para las aplicaciones.

DICCIONARIO

(7) **NAC:** son las siglas en ingles de Network Access Control. Links de interés para conocer más en detalles sobre estas soluciones:

http://en.wikipedia.org/wiki/Network_Access_Control

http://www.networkcomputing.com/showArticle.jhtml?articleID=201001835

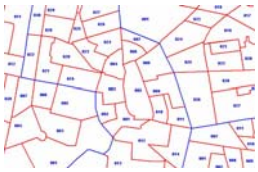
(8) **SSL:** (Secure Socket Layer) Es una propuesta de estándar para cifrado y autenticación en la Web. Fue diseñado en 1993 por Netscape para proteger la información que un usuario envía a un servidor web.

SSL permite que un servidor se autentifique frente su cliente y, opcionalmente, también a la inversa. Se basa en un esquema de llave pública para el intercambio de claves de sesión. Estas llaves son usadas para cifrar las transacciones sobre HTTP. Cada transacción usa una de estas claves. Esto dificulta a un atacante el comprometer toda una sesión.

ALBOAN:

El sistema de localización NORA

"Muchos de los programas desarrollados por el Gobierno utilizan Datos de Localización (provincia, municipio, calle, portal...) dentro de sus aplicaciones."



La puesta en marcha del proyecto Zuzenean ha acentuado la necesidad que tienen todos los Departamentos y Organismos Autónomos del Gobierno vasco de utilizar **denominaciones oficiales**. Esto, unido a las grandes posibilidades que ofrece el nuevo GIS Corporativo, ha propiciado la aparición de este proyecto común, promovido por la Dirección de Informática y Telecomunicaciones, en el que han tomado parte el Eustat, como propietario y responsable de la actualización de los datos oficiales, Medio Ambiente y Ordenación del Territorio, como coordinador del GIS, la Dirección de Administración Electrónica y Atención a la Ciudadanía, como representante de las necesidades de los Departamentos, y EJIE, que hasta ahora sólo disponía de los **FCA**'s (Ficheros Comunes de la Administración) para proporcionar este tipo de información oficial a las aplicaciones. El Sistema de Información de Localización resultante del proyecto recibe el nombre de "**NORA**".

Muchos de los programas desarrollados por los Departamentos y Organismos Autónomos del Gobierno utilizan Datos de Localización (provincia, municipio, calle, portal...) dentro de sus aplicaciones. Un ejemplo de este uso podrían ser los datos relativos a la sede social de una empresa que participa en la **tramitación de un expediente** de ayudas con un Departamento.

El objetivo principal del proyecto ha sido establecer un marco de trabajo con el Eustat en lo que se refiere a datos (direcciones oficiales de edificios, portales, etc.) con el fin de:

- Garantizar que los datos disponibles en el Eustat, y los ofrecidos a los Departamentos para sus aplicaciones, estén en **concordancia** (usando para ello el concepto de "dato único")
- Notificar de forma automática los **cambios** en las Descripciones Oficiales de las provincias, municipios y/o calles que se puedan dar a lo largo del tiempo.
- Establecer un mecanismo técnico que posibilite el solicitar Calles/Portales no existentes dentro de la base de datos ("Altas Provisionales"), notificar el resultado de esas altas a las aplicaciones y/o notificar los cambios de las descripciones oficiales en provincias, municipios, calles...

El Eustat mantiene **dos tipos de datos**:

- Información **Alfanumérica**: conjunto de tablas con información de países, comunidades autónomas, provincias, comarcas, municipios, localidades, calles y portales.
- Información **Geográfica**: capas gráficas de edificios y portales.

Toda esta información se ha puesto a disposición de todas las aplicaciones mediante NORA.

- Información Alfanumérica: los datos están disponibles en todas las instancias Oracle. Esta información estará en sincronía con la disponible en el Eustat mediante herramientas de replicación.
- Información Geográfica: las capas gráficas se han cargado en una zona específica del GIS Corporativo. Esta información se actualizará trimestralmente.

CICLO DE VIDA DE LA INFORMACIÓN

Si bien el mantenimiento de los datos depende del Eustat, los Departamentos son los "consumidores" de dicha información, por lo que

se ha establecido un **protocolo** para alimentar la base de datos de territorio con nuevas Calles/ Portales; permitiendo a las aplicaciones departamentales el continuar su tramitación (sin detener su actividad) mientras se decide si es válida o no. Es decir, el funcionario del Departamento, que se dedica a registrar la documentación en una ventanilla, intentaría localizar la dirección dentro de NORA y, en caso de no encontrarla, podría solicitar un "Alta Provisional" (Calle/Portal nuevo). Mientras el Eustat resuelve dicha petición la Calle/Portal solicitada estaría a disposición de todos los usuarios pero con claves provisionales.

Tras analizar la petición del Departamento, los técnicos del Eustat podrán resolver la petición con los siguientes resultados:

- **ok**: la calle/portal se da de alta y se le suministra una clave definitiva

- **existente**: la calle/portal ya existe pero con otro nombre, por lo que se indica la clave de calle y portal correspondiente

- **error**: no ha sido posible determinar la existencia de la ubicación requerida (se descarta)

Tras la resolución del Alta Provisional faltaría *notificar* el resultado a las aplicaciones que estén usando dicho dato para que actualicen su modelo con las claves definitivas.

NOTIFICACIÓN

La notificación podrá ser tratada de dos formas:

- Manualmente: los usuarios que lo hayan indicado recibirán un email para que accedan a su aplicación y actualicen los datos
- Automática: se generarán eventos en PLATEA Integración a los que podrán estar suscritas las aplicaciones obrando en consecuencia en su modelo de datos

A continuación, se describe el proceso que siguen las aplicaciones para que puedan ser informadas ante cualquier cambio en NORA:

- Manualmente: técnicamente, NORA enviará un email a los usuarios que estén usando Altas Provisionales pendientes cuando se haya resuelto la solicitud. Esto implica que la aplicación departamental deberá indicarle a NORA, cada vez que use un dato pendiente, que debe enviarle un email al usuario. Esta funcionalidad está disponible como un Servicio dentro del API de NORA, pudiendo ser consumida vía Web Service o vía AJAX (*Asynchronous JavaScript+XML*).
- Automática: técnicamente, NORA generará un evento en la plataforma eAdministración PLATEA Integración. Las aplicaciones departamentales podrán crear suscripciones ante los eventos en los que estén interesados indicando la acción a realizar en cada caso. En el caso de Nora, la propuesta es que los aplicativos aporten procedimientos almacenados que serán invocados por PLATEA Integración cuando el evento sea del interés de la aplicación. Cada aplicación en el procedimiento almacenado incluiría los cambios a realizar en su modelo de datos ante un evento concreto de NORA.

SERVICIOS

NORA pone a disposición de las aplicaciones el acceso vía SQL a los datos de localizaciones. No obstante, ofrece también servicios de valor añadido, como son:

- **Formulario Genérico**: provee un "interfaz web" de captura/edición de datos. Este formulario permite realizar búsquedas sobre cualquier campo y facilitar la captura de múltiples tipos de direcciones (de la CAE, del resto del Estado e incluso del extranjero). [los datos que no existan en la base de datos deberán ser introducidos en modo texto libre]

La principal característica del formulario es que tiene una **interfaz no intrusiva**; ya que ésta se abre en un "iframe" sobre la ventana invocante. Además, esta interfaz que posibilita obtener datos mediante peticiones AJAX, realiza invocaciones de forma **asíncrona** con el fin de no bloquear el navegador del usuario.

- **API**: se proveen un conjunto de "funciones" que posibilitan trabajar con datos de localizaciones sin tener que utilizar SQL. Estas funciones están accesibles vía Web Service o vía AJAX.

En definitiva, NORA trata de ofrecer un servicio de valor añadido que pueda ser usado de forma **horizontal** por parte de todas las aplicaciones departamentales que así lo requieran.

"La interfaz del usuario posibilita obtener datos mediante peticiones AJAX."

Páginas webs:
www.eustat.es

Aplicación ejemplo:
www1.geo.jakina.ejgvdns/t89iUsoSIDLWar/index.jsp

Nº 29

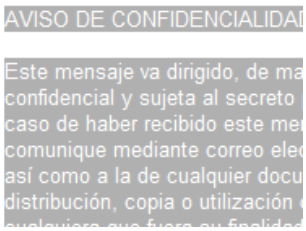
Marzo de 2008

¡¡BREVES!!

Los “disclaimers” de los correos

En los correos electrónicos que solemos recibir podemos encontrar, generalmente al final de los mismos, unos avisos de tipo legal, avisos de confidencialidad o advertencias, los cuales se denominan **disclaimers.**

La utilización de estos no es sino una “copia” del modo de hacer de los norteamericanos, que los incluyen en sus contratos legales, de tal modo que, como una moda, se han ido extendido por nuestras corporaciones y empresas, en el ámbito de los mensajes electrónicos.



Se puede decir que carecen de cualquier base jurídica (ya que las condiciones se establecen de forma unilateral, y el destinatario no puede expresar la aceptación o no de las mismas), asimismo, suelen contener verdades “absolutas” como *“este mensaje va dirigido única y exclusivamente a su destinatario…”*, por lo que la utilidad de los mismos está bastante cuestionada.

A todos nos ha ocurrido alguna vez el enviar un correo a un destinatario equivocado, por un fallo nuestro, pero ello no implica que la culpa sea de ese destinatario, ni que tengamos que **advertirle** ni **amenazarle** con una serie de líneas, como si el culpable hubiese sido él.

La palabra inglesa **disclaimer** tiene diversas acepciones, como pueden ser, *renuncia, descargo de responsabilidad, nota, aclaración, advertencia, cláusula de protección*, etc.

Estas advertencias suelen estar escritas en diversos productos y pueden considerarse como un descargo de responsabilidades (por ejemplo en los medicamentos). En los correos electrónicos se suelen utilizar como una advertencia dirigida a la persona receptora de ese correo.

Por último, indicar que existe otro tipo de pies de correo, por ejemplo los que nos invitan a no imprimir el correo recibido, cuyo carácter es más agradable y su finalidad es la protección de nuestro medio ambiente.

Nokia presenta Morph

Morph es un nuevo concepto de nanotecnología presentado por Nokia y la Universidad de Cambridge, que en un futuro permitirá al usuario dar diversas formas a su teléfono.

Nokia, a través de su Centro de Investigación (NRC) y la Universidad de Cambridge, han presentado Morph, un nuevo concepto basado en la nanotecnología, que demuestra cómo los dispositivos móviles pueden llegar a ser **extensibles y flexibles** en el futuro, permitiendo al usuario transformar su terminal con formas radicalmente distintas. Este sistema está basado en materiales elásticos, electrónica transparente y superficies autolimpiables.

Tanto Nokia como la Universidad de Cambridge, aseguran que algunos elementos de esta nueva tecnología podrían estar disponibles en aproximadamente siete años para su integración en dispositivos móviles, aunque inicialmente sólo sería posible en los de gama alta. Sin embargo, se espera que la nanotecnología pueda dar lugar algún día a soluciones de fabricación de bajo coste, además de ofrecer la posibilidad de albergar funciones complejas a un precio reducido.

Nokia ha expresado su deseo de que este tipo de tecnología muestre el potencial de la nanociencia a un público más amplio, ya que suponen mayores posibilidades en términos de diseño y funcionamiento para los dispositivos móviles.

Web de Nokia: www.nokia.com