MYGNET-MAGAZINE 9

La revista de la comunidad de programación en español

Formulario simple en Win32 con Visual Studio 6 y Visual C++

Resolución del problema de los frascos de prolog

Creación de gráficos en IReports

Excepciones en VB.NET y C#

Mysql más rápido

Grag Drop con Javascript

Programación scripts bash

Aplicaciones Web en Eclipse

Pasar Drupal 4.6.X a iso-8859-1

Captura de actividad en pantalla para demostración de software (Salida AVI y SWF)

Seguridad Informática - Capitulo III. Aplicaciones Criptograficas

Prohibida su venta
Totalmente libre

AÑO 1 - NÚMERO 9 - JULIO 2006
my Group Net http://www.mygnet.com

EDITORIAL

Octava edición digital de **MYGNET-MAGAZINE Julio 2006**

Presentamos una vez más la publicación digital correspondiente a este mes, esperamos que sea de su agrado, hemos incluido una sección de manuales donde se listan todos los que fueron publicados en el mes y a demás nos complace presentar el capitulo III de seguridad informática, “Aplicaciones criptográficas”.

Mandamos nuestros cordiales saludos y agradecimientos a todos los colaboradores que han participado con nosotros, de igual manera para todas las personas que nos han echo llegar sus comentarios que nos han sido de mucha utilidad, a nombre del equipo de mygnet les damos las gracias...

Reiteramos nuevamente la invitación para que participen con nosotros.

Editores
Martín Roberto Mondragón Sotelo.
martin@mygnet.com

Gustavo Santiago Lázaro.
gustavo@mygnet.com

Escríbenos a info@mygnet.com

Visítanos a http://www.mygnet.com o http://www.mygnet.org

CONTENIDO

Aplicaciones

Programación

Seguridad

Aplicaciones web en Eclipse

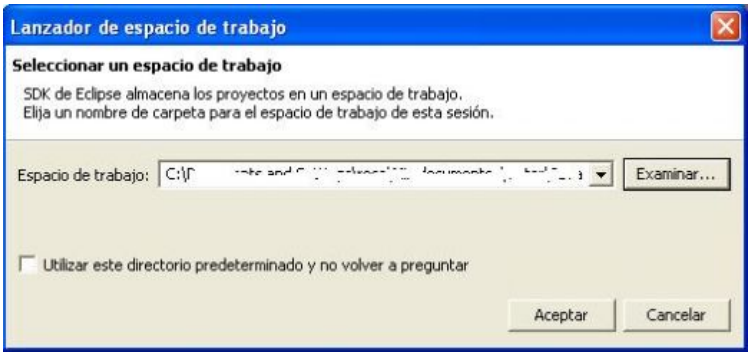
Autor Ehooo
ESPAÑA

Área de estudio: Telecomunicaciones
Conocimientos: C/C++ , PHP, SQL y Java (aún estamos mejorándolos)

JSP y Servlet en Eclipse

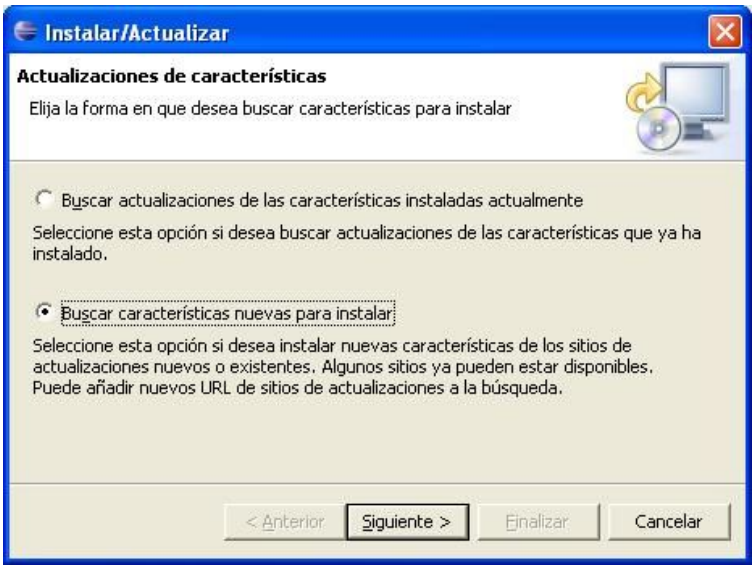
Eclipse es un IDE de java basado en plugins, explicare a continuación como hacer para instalar el plugin que nos permite crear páginas en jsp y servlet.

Primero necesitamos bajarnos el programa desde la pagina web *www.eclipse.org*, este programa no necesita instalación, solo hay que descomprimirlo donde queramos y abrirlo.
Podemos traducirlo bajando desde:
http://download.eclipse.org/eclipse/downloads/drops/L-3.1.1_Language_Packs-200510051300/index.php el lenguaje que queramos.
Al abrirlo nos aparece donde queremos establecer el sitio de trabajo, seleccionamos donde queremos que Eclipse guarde los archivos que creemos.

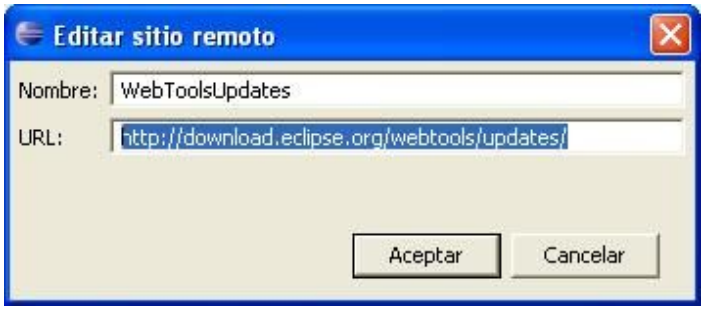


Bueno, después de esta pequeña introducción en Eclipse vamos a explicar como instalamos el plugin que nos permite hacer JSP:

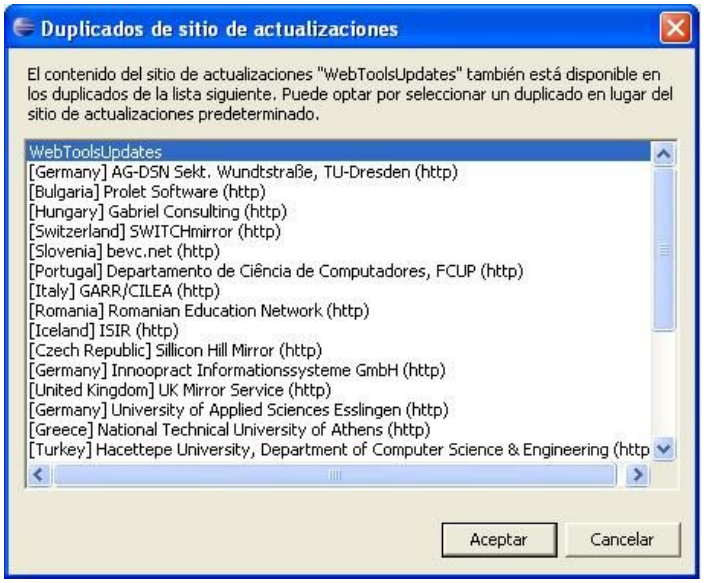
1. Pinchamos en: Ayuda>Actualizaciones de software>Buscar e instalar.
2. Pinchamos en "Buscar características nuevas para instalar" y siguiente.



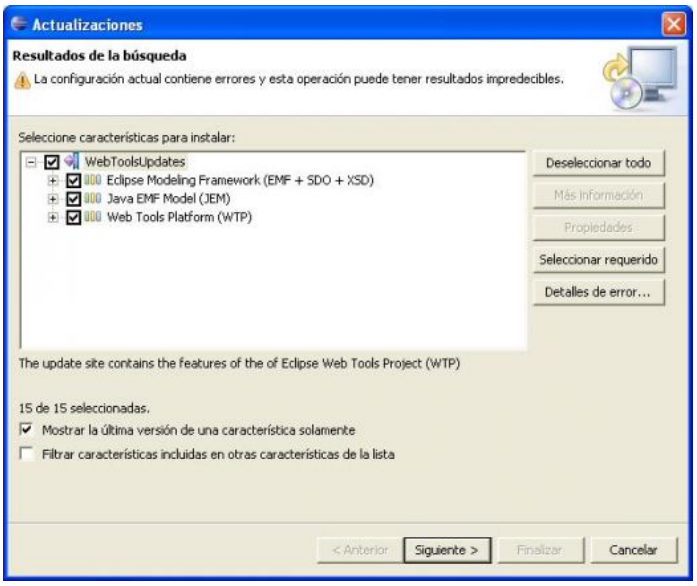
3. Pinchamos en “Sitio remoto nuevo” he insertamos lo siguiente como URL: *http://download.eclipse.org/webtools/updates/* y damos ha aceptar; nos aparecerá el nombre que hallamos puesto en “Nombre” en “Sitios ha incluir la búsqueda”; damos ha finalizar.



4. Nos aparecerá una ventana donde nos sale los distintos sitios de donde podemos descargar las actualizaciones, elegimos el país que más cerca nos pille o la web por defecto que tendrá el mismo nombre que le hallamos puesto; una vez seleccionado damos a aceptar.



5. Tras buscar las actualizaciones marcamos todas las actualizaciones del nuevo sitio y aceptamos la licencia damos a siguiente y a finalizar.

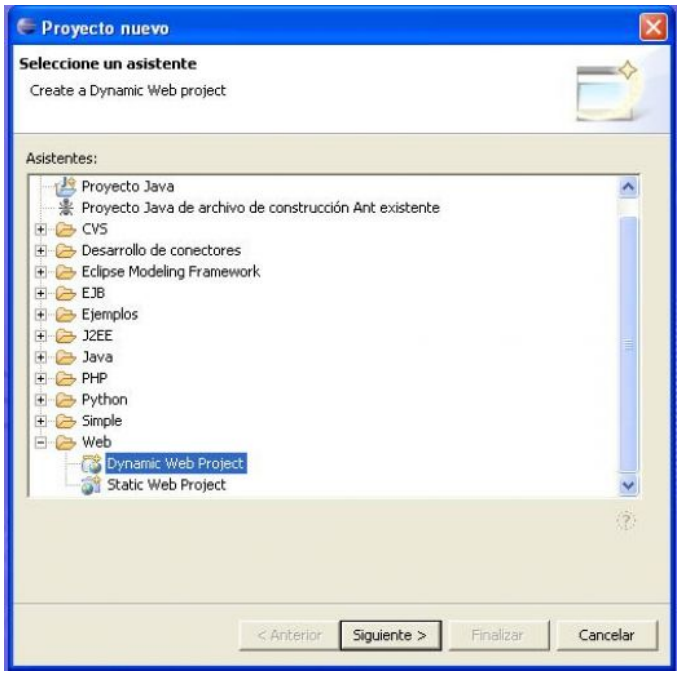


6. Empezara a descargarse los plugins, esto llevará bastante tiempo así que un poco de paciencia no os vendrá nada mal. Tras la espera decimos “instalar todo” y reiniciamos el Eclipse.

Ya tenemos Eclipse listo para hacer paginas en JSP, solo tendremos que instalar Apache Tomcat u otro servidor de aplicaciones java.

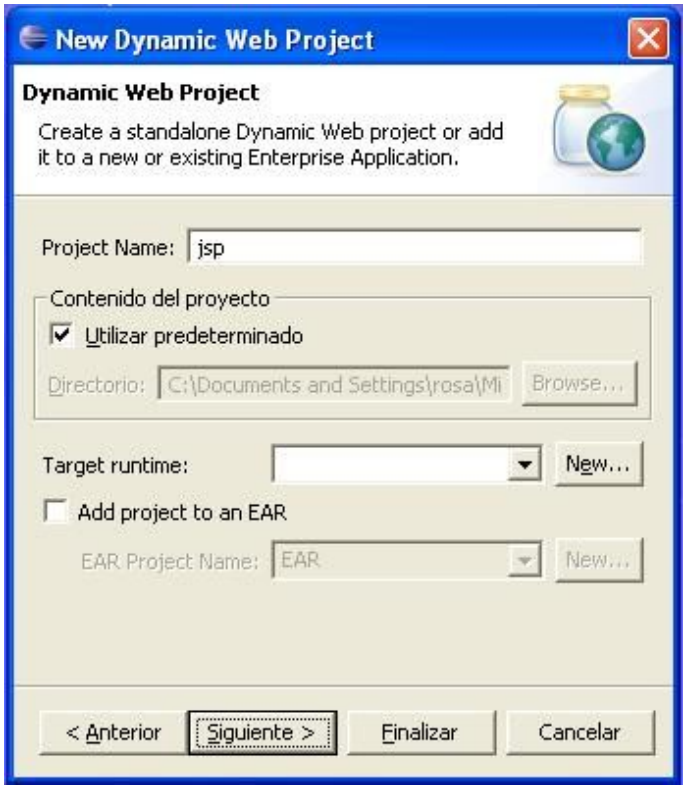
Para confirmar que esta listo y operativo vamos a crear un proyecto nuevo de JSP.

Solo tenemos que crear un proyecto de la carpeta “Web”,y “Dinamic Web Project” veamos como:



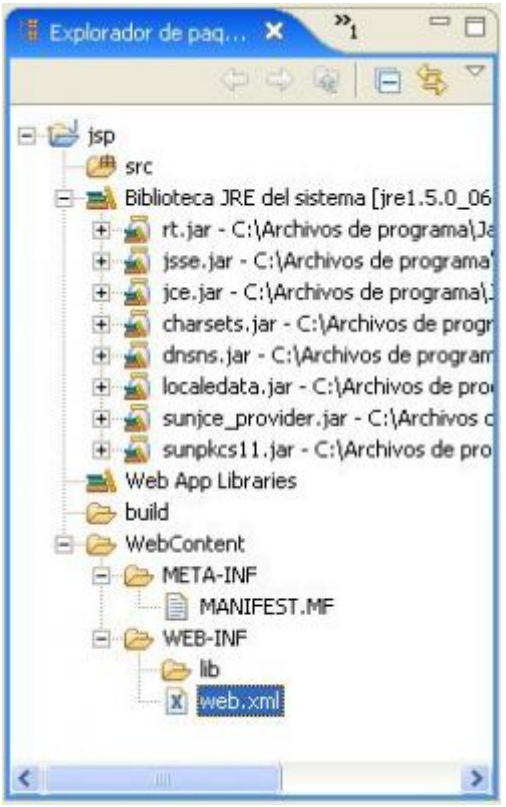
NOTA: Eclipse no viene con PHP, es un plugin instalado

Ahora ponemos nombre al proyecto de damos a Finalizar:



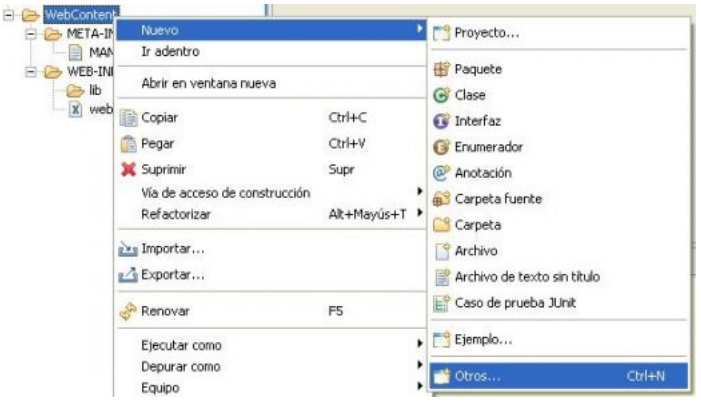
Tras esto tendremos que aceptar la licencia de Java.

Ya tenemos nuestro proyecto hecho, si vamos a la pantalla de java veremos a un lado lo siguiente:

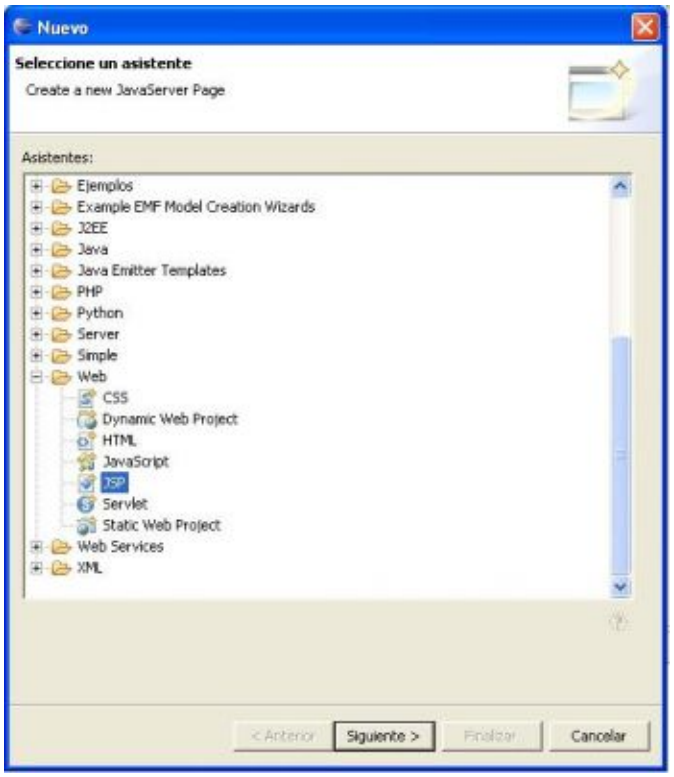


Creación de un JSP

Vamos ha crear un jsp en "WebConten", para ello en la carpeta damos clic derecho y "nuevo>otros...":



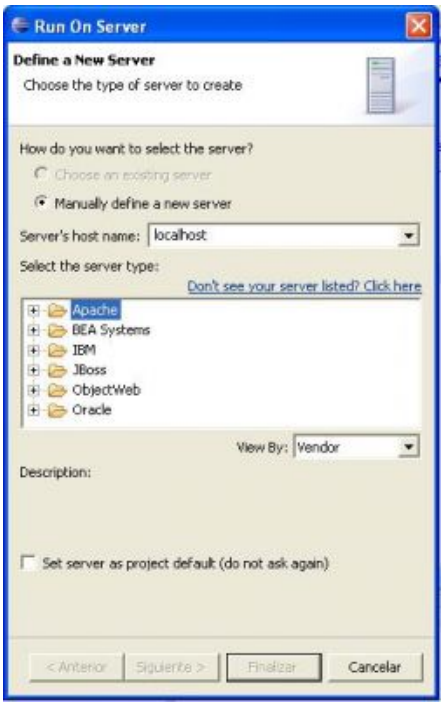
Seleccionamos en la carpeta "Web>jsp" y damos siguiente, luego le ponemos nombre por ejemplo "index.jsp" y Finalizar.



En el ejemplo siguiente he editado un pagina JSP, que aunque es estática nos sirve para configurar el servidor de aplicaciones que necesitamos para que ejecute el jsp.

En la pagina damos clic derecho "Ejecutar como>Run on server":

Nos aparecerá una ventana para configurar el servidor que tenemos instalado en la maquina; (en el ejemplo Apache Tomcat 5.5), seleccionamos la ruta donde esta instalado el servidor y damos a Finalizar.



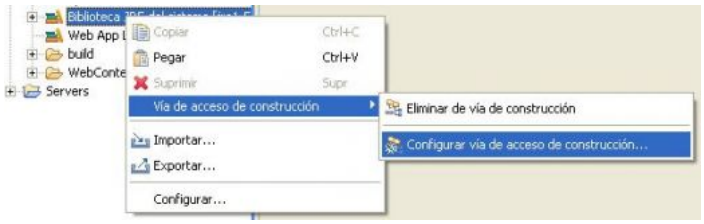
Ahora vemos como aparece en la parte de abajo un pestaña con la palabra "Server" y una maquina con una flecha verde indicando que está funcionando; este símbolo cuando el servidor eres apagado seria azul y un cuadrado.

ATENCIÓN, un error muy común es tener el servidor ya encendido he intentar abrir la pagina con el Eclipse, si hacemos esto nos aparece un mensaje de error, diciendo que el servicio ya esta arrancado y que no se puede hacer otra petición por los mismo puestos, asegurarse que esta apagado.

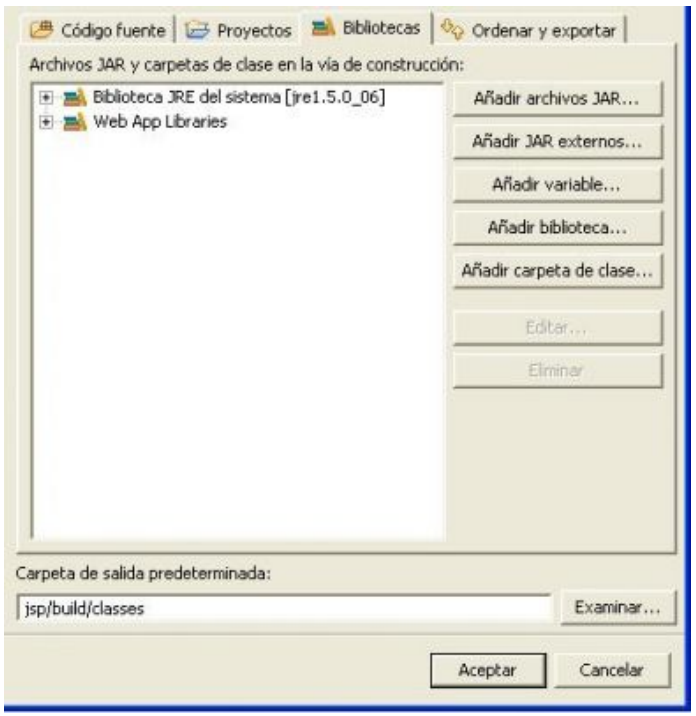
Creación de un Servlet

Para poder utilizar los servlets en Eclipse hay que tener instalado el paquete antes mencionado y además añadir la librería de Apache Tomcat, para ello hay que seguir los siguientes pasos:

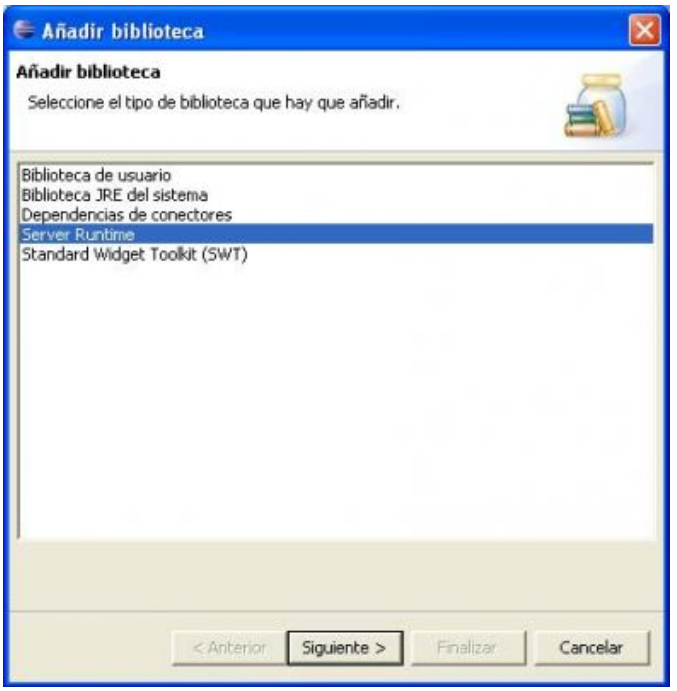
1. Insertamos en el proyecto la librería de Apache Tomcat:
   1.1 Nos ponemos en una de las librerías que ya hay y damos clic derecho "Vía de acceso...>Configurar vía..."



1.2. Seleccionamos la pestaña de librerías o bibliotecas y damos ha "Añadir nueva biblioteca"



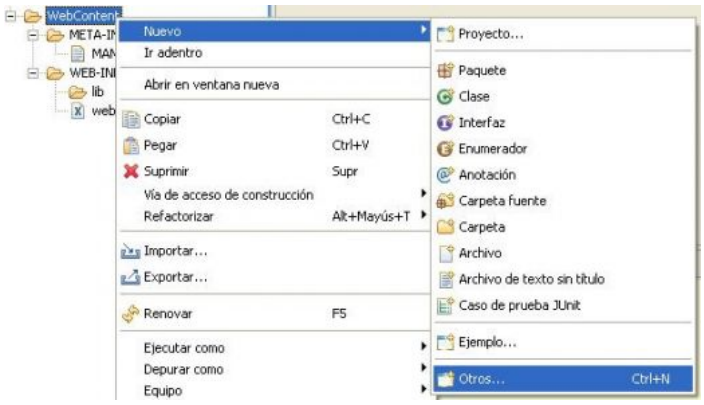
1.3. Seleccionamos "Server Runtime" y damos a siguiente.



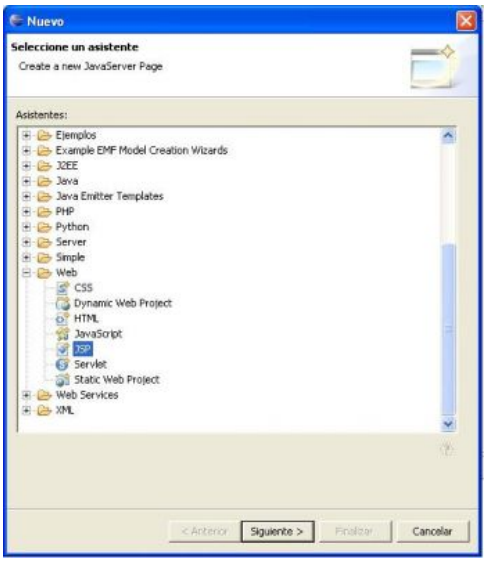
1.4. Seleccionamos "Apache Tomcat v5.5" y finalizar.

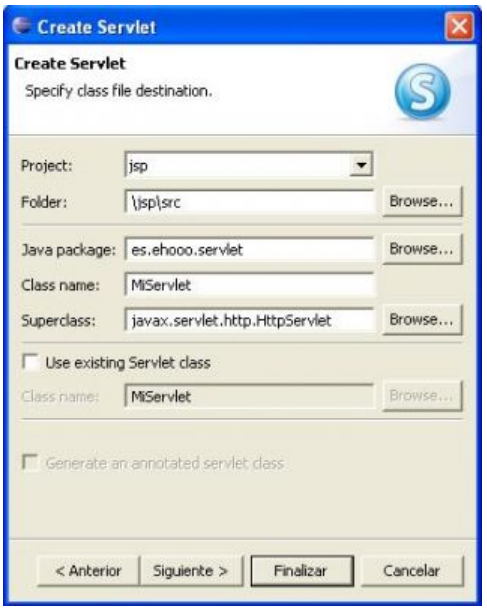
1.5. Observaremos que se ha insertado correctamente y daremos a aceptar.

2. Ahora en el proyecto vamos ha crear un servlet, para ello:
2.1. Damos clic derecho y “nuevo>otros...”:

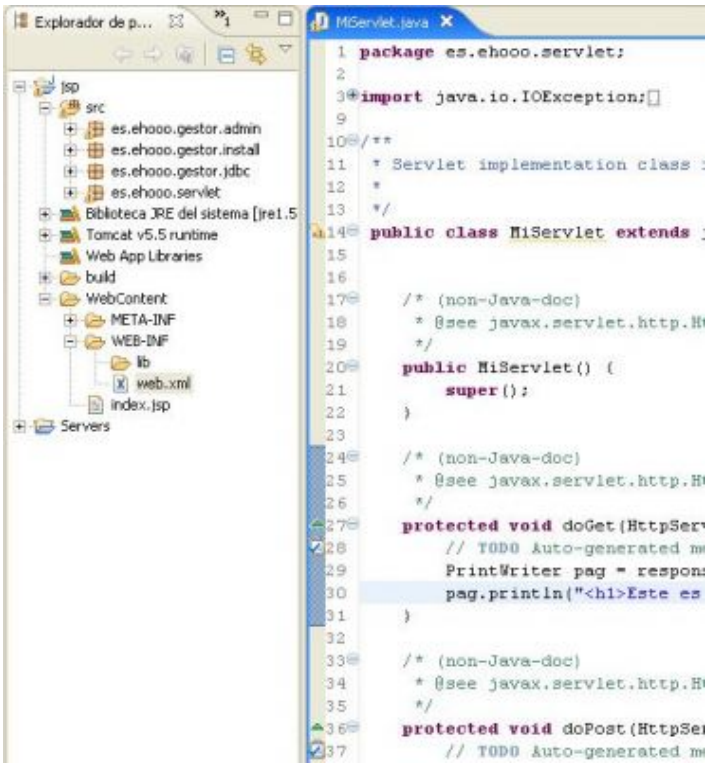


2.2. Seleccionamos en la carpeta “Web>servlet” y damos siguiente, luego le ponemos nombre y le asignamos un paquete y Finalizar.





2.3. Se nos creará el paquete y la clase con los métodos doGet(...) y doPost(...).



2.4. En la pagina damos clic derecho “Ejecutar como>Run on server” (sino hemos elegido el servidor por defecto nos aparecerá una ventana donde nos preguntará que servidor usar) y aparecerá el resultado del servlet en un navegador; Eclipse actualiza en "Web.xml" automáticamente, pero a veces no lo hace y puede que no veamos el servlet por eso.

Captura de actividad en pantalla para demostración de software (Salida AVI y SWF)

Autor:Filiberto Ugarte Castañeda
fugartex@hotmail.com
País: MÉXICO

Nivel de estudios: Licenciatura o profesional | **Área de estudio:** Lic. en Electrónica | **Objectivo(s):** Aprender cada dia mas y obtener los mejores beneficios para quienes estén involucrados(as). | **Experiencia laboral:** Sistemas, bases de datos, páginas web, archivos compilados HTML de ayuda. | **Experto en:** Siempre hay algo que aprender. | **Actividades:** Capacitación continua autodidacta en lenguajes de computación, sistemas y equipos, traducción de aplicaciones. | **Conocimientos:** C, Pascal, Ensamblador para microcontrolador 8051/8052, HTML, CSS, VRML, Just BASIC v1.01, JavaScript, Visual Basic 6.0, Programación en escalera de PLCs, Windows, Ubuntu Linux 5.10, Mandriva Linux 10.1, Puppy Linux 1.0.1 | **Idioma(s):** Inglés 80%`, Esperanto (principiante)

En varias ocasiones al desarrollar aplicaciones, nos encontramos con la necesidad de documentar en tiempo de ejecución las características mas importantes o elaboradas del programa, ya sea para crear tutoriales con lo que el usuario podrá usar la aplicación de forma eficiente. Aún más, los usuarios experimentados podrán registrar errores y reportar asi el procedimiento exacto con el que se produce el error.

Para esta tarea existe una aplicación de código abierto llamada CamStudio 2.0 y que puede ser hallada en http://sourceforge.net/projects/camstudio o en http://www.camstudio.org. La historia del desarrollo de CamStudio es interesante de acuerdo a este ultimo sitio, donde el autor ofrece también la versión 2.0 y el codec de video CamStudio Lossless Codec v1.0 para mantenerlos públicos en caso de falla en Sourceforge.

La aplicación fue publicada originalmente por una empresa llamada Rendersoft la cual fue comprada posteriormente por una compañia llamada eHelp quien usó parte de la tecnología en su programa RoboDemo. Tiempo después, eHelp fue comprada por Macromedia -ahora parte de Adobe- quien estaba interesada en RoboDemo para transformarse en Captivate (http://www.adobe.com/products/captivate).

Sabiendo que CamStudio realizaba en forma gratuita algunas de las características que RoboDemo hacía (principalmente la exportación a Flash), publicaron una versión mas nueva de CamStudio (2.1) que corrigió algunos errores, pero aún más importante, eliminó algunas características, primordialmente la creación de archivos SWF y se requería registrarse para usarla. Al paso del tiempo, los vínculos a varios sitios que tenían CamStudio y su código fuente desaparecieron.

Como es obvio en las aplicaciones de código abierto, se requieren programadores en Visual C++ con experiencia en Flash, producción de video y codecs para crecer y mejorar el proyecto ya que como indica el autor de este sitio, quien dice no ser programador, será muy valiosa la colaboración por la que se planea recompensa para resucitar esta aplicación con algunas fallas.

Una vez descargados e instalados CamStudio 2.0 y el codec, la pantalla inicial es esta:

La aplicación tiene una ayuda muy clara para usarla. He aquí lo básico para comenzar.

Toma en cuenta que si en el programa está indicado "Record to AVI" podrás producir el video AVI y posteriormente podrás convertirlo a SWF. Si esta indicado "Record to SWF" obtendrás directamente el archivo Flash y no el AVI.

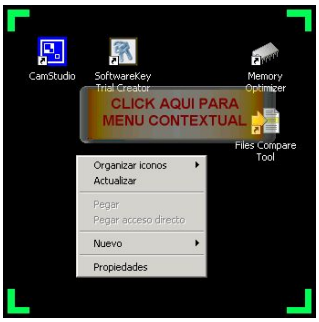
Elige el codec de CamStudio oprimiendo en Options > Video Options.

En el menú "Región", oprime "Región" para grabar el área delimitada por el puntero del ratón.

En el menú "Tools" elige "Screen Annotations" y da doble click en la forma "Orange Gradient". Una vez que se despliegue, cierra la ventana "Screen Annotations" y oprime con el botón secundario del ratón sobre la forma para desplegar el menú contextual y modificar su texto (Edit Text...) a "CLICK AQUÍ PARA MENU CONTEXTUAL" Puedes tambien redimensionar la forma y el letrero y establecer transparencia.

Oprime "Options > Program Options" y elige "Minimize Program on start recording".

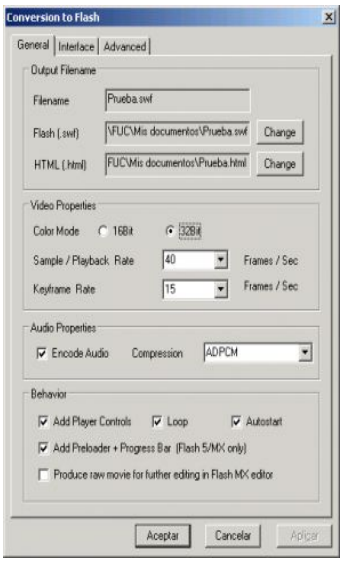
Oprime F8 para comenzar a grabar. Dibuja un área cuadrangular alrededor de la anotación en pantalla. Se delimita el area con indicadores verdes intermitentes. Comienza a mover el puntero del ratón y/o escribir lentamente dentro del area para lograr una captura uniforme. Puedes oprimir nuevamente F8 para pausar la captura o F9 para detener la grabación.



Al terminar la grabación, dependiendo de la configuración del programa en "Options > Program Options" se te pedirá el nombre del archivo AVI y donde guardarlo. Y también, dependiendo de la configuración, podrás ver inmediatamente la grabación con el reproductor propietario de CamStudio.

Para convertir este archivo AVI a SWF, en el menu oprime "Tools > SWF Producer (Convert AVI to Flash)". Abre el video AVI y oprime Convert to SWF.

En la ventana "Conversion to Flash", elige el nombre del archivo SWF, el archivo HTML donde se incrustará la



animación Flash y selecciona los parámetros, la interfaz, el comportamiento, propiedades de audio para la conversión.

Un nota importante mencionada en el sitio http://www.camstudio.org con respecto al código HTML generado es que la animación Flash no se despliega correctamente en navegadores diferentes a Microsoft Internet Explorer. La forma de arreglar esto es abriendo el archivo HTML en modo texto. Se busca la línea de código que contiene la etiqueta <EMBED> y se cambian los valores de ancho (WIDTH) y altura (HEIGHT) de manera que concuerden con los valores de estas propiedades mostrados en la etiqueta <OBJECT>.

Para incrustar estas animaciones Flash en tus aplicaciones Visual Basic, agrega el componente Shockwave Flash a tu proyecto.

Una vez que esté dibujado el control Shockwave en el formulario, ajusta la propiedad ScaleMode del formulario en pixeles.

En la propiedad Movie del control Shockwave escribe la ruta absoluta del archivo SWF. Para que el archivo Flash sea desplegado de manera uniforme en tamaño, escribe en las propiedades Height y Width del control Shockwave las mismas dimensiones de estas propiedades especificadas en el archivo HTML generado por CamStudio para incrustar el archivo SWF.

Ojala este artículo te sea útil. Saludos.

De manera que si realmente deseas ayudar al mundo, lo que vas a tener que enseñar es como vivir en él. Y eso no lo puedes lograr a menos que tu mismo(a) hayas aprendido a vivir en el gozoso dolor y en el doloroso gozo del conocimiento de la vida como tal.

Joseph Campbell

MySQL más rápido

Autor: Alejandro Benavides
País: COSTA RICA
abenavidescr@gmail.com

Área de estudio: Análisis, diseño e implementación de software | **Experiencia laboral**: Software contables, puntos de venta (código de barras y bandas magnécticas), sistemas de géstion de torneos de golf y cálculo de handicaps | **Experto en:** Microsoft Visual Basic | **Conocimientos:** Visual Basic, Visual Foxpro, MySQL, PHP, Java Script, Gambas, Fedora Core, SuSE | **Pasatiempo(s):** Tocar guitarra, jugar futbol salón, ver T.V, Cine, Biblia

Como resultado del creciente papel de MySQL en grandes organizaciones, su uso se está convirtiendo más y más de alto rendimiento. Esto significa, por supuesto, que MySQL necesita proporcionar más capacidad de respuesta, alto rendimiento, y fiabilidad. Ya conocido en la industria por ser un servidor de bases de datos increíblemente rápido, muy a menudo MySQL está ya preparado para la tarea directamente después de instalarlo.

Sin embargo hay un par de cosas que pueden fácilmente hacerlo lento, aunque no es extraño, que esto se deba también a un pobre diseño de la aplicación. Otras veces la configuración por defecto de MySQL no es lo suficientemente buena como para realizar la tarea que tiene entre manos. Y otras veces se necesita tener un poco más de hardware.

Cuando intentamos hacer más rápida una aplicación de bases de datos, hay que empezar con la aplicación en sí y asegurarse de que las tablas están normalizadas de forma adecuada, y las columnas están indexadas, esto es siempre un buen comienzo. Pero si ya se ha hecho todo lo anterior y las cosas siguen siendo lentas, llega el momento de echarle un ojo al servidor MySQL en sí.

No es tecnología aeroespacial

Aunque puede ser que suene intimidante, el ajuste del rendimiento sólo trata de sacar el mayor rendimiento posible de un sistema. Para hacer esto es necesario entender cuales son las variables que están involucradas y como pueden afectar el buen funcionamiento del servidor.

Antes de entrar en los detalles, vale la pena reiterar un hecho importante: las técnicas que se van a mostrar no arreglarán búsquedas mal escritas o sin optimizar, un mal diseño de la base de datos, u otros problemas del diseño de la aplicación. Puede que sirvan para aliviar el esfuerzo de un servidor ocupado, pero simplemente se está posponiendo lo inevitable. La única solución a una aplicación mal escrita o un diseño pobre de la base de datos es irse al código y arreglarlo. Realmente, arreglar las consultas lentasy/o una aplicación pobremente diseñada conseguirá mejores resultados que perder el tiempo con el ajuste del servidor.

Si no se está seguro por donde empezar, se tiene que habilitar el archivo de registro para las búsquedas lentas (slow query log) tal y como se explica en el manual de MySQL, y luego simplemente observar y revisar cualquier búsqueda que no se esperaba que sea lenta. También es posible que se encuentren algunas búsquedas rápidas en el archivo de las búsquedas lentas. Esto se debe a que MySQL considera cualquier búsqueda como lenta si no usa un índice.

Uso de memoria

Del lado del servidor, el único y más importante factor en determinar cómo de bien rendirá MySQL, es la memoria. MySQL es capaz de ejecutar varios subprocesos a la vez.

Esto significa que cada vez que se realiza una conexión, MySQL crea un subproceso. Cada subproceso consume memoria. El almacenamiento en caché de los resultados también consume memoria. Se puede pensar entonces, que entre más memoria tengamos en el servidor, será lo mejor. Sin embargo no es suficiente con tener mucha memoria disponible, es necesario indicarle a MySQL como queremos que use la memoria.

Las configuraciones por defecto de MySQL son bastante conservadoras para el hardware de hoy en día, sin embargo, si se tiene un servidor MySQL dedicado con varios cientos de mega bytes de RAM, se debe ser capaz de darle a MySQL una porción bastante grande de ella para trabajar. Por defecto, sólo usará una pequeña porción de lo que haya disponible; esto se debe a que no hay ninguna forma de saber si está corriendo en un servidor dedicado donde será usado de forma continua o si está corriendo en un esforzado portátil donde sólo se usa para almacenar una pequeña aplicación.

Mucha de la información presentada a continuación se centrará en el uso de la memoria y se asume que se está usando el tipo de tabla por defecto de MySQL, MyISAM. Actualmente existen otros tipos de tablas transaccionales más avanzadas, tales como InnoDB o Gemini.

MySQL usa la memoria para una variedad de búfferes internos y cachés que influyen en el número de veces que se ha de acceder a archivos que residen en el disco. Cuanto más a menudo tenga que esperar a que responda un disco, más lento será. Aún los discos duros más modernos siguen siendo un orden de magnitud más lentos que la memoria RAM, y dado la reciente baja en los precios de la memoria, es muy factible que se pueda añadir más memoria al servidor y así acelerar los procesos. Actualizar a discos duros más rápidos debería ser la última opción.
Los búfferes y cachés de MySQL son de dos tipos: globales, y por hilo.

Globales: tal y como sugiere el nombre, estas áreas de memoria son reservadas una vez y son compartidas a través de todos los hilos de

MySQL. Dos de los más importantes son el búffer de claves y la caché de tablas. Debido a que son búfferes compartidos, el objetivo es que sean lo más grandes posibles.

Por hilo: estos búfferes reservan memoria individualmente a medida que necesitan realizar operaciones particulares, tales como ordenar o agrupar datos. A propósito, la mayoría de los búfferes MySQL se reservan en esta forma.

A continuación se examina primero que función tienen cada uno de los búfferes y como configurar e inspeccionar sus valores, posteriormente se mostrará como examinar contadores de rendimiento de MySQL y juzgar si los cambios que se realizan tienen implicaciones o no.

Búffer de claves

El búffer de claves es donde MySQL cachea los bloques de índices para tablas MyISAM. Cada vez que una búsqueda usa un índice, MySQL mirará antes de nada a ver si el índice relevante está o no en memoria. El parámetro key_buffer en el archivo my.cnf determina que tan grande puede ser este búffer. Una vez que el búffer este lleno, MySQL hará sitio para nuevos datos reemplazando datos antiguos que no hayan sido usados recientemente.

El tamaño del búffer de claves aparece como key_buffer_size en la salida de SHOW VARIABLES. Con un búfferde claves 384 Mega Bytes, se vería algo como:

```
key_buffer_size 402649088
```

como una recomendación general, en un servidor MySQL dedicado se debería reservar entre el 20 y el 50 por ciento de la memoria RAM para el búffer de claves de MySQL. Si se tiene un giga byte de memoria se puede empezar con algo como:

set-variable= key_buffer= 128M
ó incluso:
set-variable= key_buffer= 256M

Si sólo se permitiera modificar un parámetro en el servidor MySQL, el búffer de claves sería lo primero que se tendría que considerar. Los índices son también muy importantes para el rendimiento global de cualquier servidor de bases de datos por lo que es difícil equivocarse al hacer más espacio en su memoria para ellos.

Si no se especifica un tamaño al búffer de claves, MySQL usará su tamaño por defecto que está cerca de los 8MB. Pero claro, tiene muy poco sentido configurar el valor del búffer de claves tan alto, hacerlo podría matar de hambre al sistema operativo respecto a la memoria que necesita para escrituras de disco y otras tareas.

Caché de tablas

Las tablas MyISAM están compuestas de tres archivos en disco:

El archivo de datos nombredetabla.MYD, el archivo índice nombredetabla.MYI, y finalmente, el archivo de definición de la tabla llamado nombredetabla.FRM. Para poder usar una única tabla, MySQL necesita de hecho abrir los tres archivos. El archivo .FRM se cerrará después de que lea el esquema, pero los demás permanecerán abiertos, MySQL no los cerrará hasta que lo necesite. Esto evita una sobrecarga asociada con la apertura y cierre de los archivos si la tabla se usa frecuentemente. Los archivos normalmente no se suelen cerrar hasta que ocurre uno de los siguientes eventos:

La tabla se ha cerrado de forma explícita mediante FLUSH TABLES.

La tabla se ha desechado
El servidor esta siendo reiniciado
El número total de tablas abiertas ha alcanzado el valor del parámetro table_cache

El último evento es particularmente importante si se tienen muchas tablas que se usan a menudo entre todas las bases de datos. El valor por defecto de table_cache es de 64, así que si se tienen unos cientos de tablas que se usen de forma activa, MySQL va a desperdiciar mucho tiempo y esfuerzo abriendo y cerrando innecesariamente estos archivos.

Incrementar el tamaño de la caché de tablas ciertamente ayudará en esta situación, pero se debe tener cuidado de no hacer el valor demasiado grande, ya que todos los sistemas operativos tienen un límite en el número de los archivos abiertos por un mismo proceso. De hecho. algunos también tienen limitado el número total de archivos abiertos que puede tener un único usuario. Si MySQL intenta abrir demasiados archivos, el sistema operativo se negará a permitirlo y MySQL generará un mensaje de error en el archivo de registro de errores. Ante la duda, se tienen que comprobar las limitaciones del sistema operativo.

En casos extremos, se puede incrementar el número de descriptores de archivos disponibles por medio de las opciones de configuración del kernel. Los descriptores de archivos abiertos están reservados por un único proceso y compartidos por todos sus hilos. Al contrario que muchos de los demás parámetros, la caché de tablas se aplica a todos los tipos de tablas basadas en disco de MySQL.

Búferes de registro

Siempre que MySQL ha de escanear una tabla, el hilo que realiza el escaneo reservará un búffer de registro para cada tabla que ha de escanear. Esto sucede típicamente cuando MySQL decide que es más eficiente escanear la tabla que usar un índice para una búsqueda. También ocurre cuando simplemente no hay un índice que se pueda usar.

Al incrementar el valor de record_buffer en el archivo my.cnf, se permite que MySQL lea las tablas en trozos más grandes. Es probable que esto reduzca el número de búsquedas en el disco y haga que el escaneo sea significativamente más rápido en un servidor muy atareado.
Sin embargo, se tiene que ser muy cuidadoso con el búffer de registro si se tienen muchos clientes que realizan búsquedas completas sobre tablas. Debido a que el búffer de registro se reserva por cada hilo, se puede acabar en una situación donde clientes individuales hagan que se reserven búfferes de registro al mismo tiempo. Si el resto de la memoria está limitada es probable que se empiece a hacer uso de la memoria de intercambio y se verá dramáticamente reducido el rendimiento. En la versión 3.23.41 se introdujo un parámetro relacionado denominado record_rnd_buffer.

Al igual que record_buffer, se usa para escanear un gran número de filas. El record_rnd_buffer se usa para búsquedas que

resultan en una ordenación intermedia del archivo además de algunas lecturas de registro no secuenciales. Afortunadamente, si no se fija el valor de record_rnd_buffer se establecerá por defecto el valor de record_buffer.

Búffer de ordenación

Tal y como implica su nombre, el búffer de ordenación se usa para responder a búsquedas que involucren el ordenamiento de los datos -aquellas con una sentencia ORDER BY en ellas. Además, el búffer de ordenación se usa para las búsquedas que involucren agrupar datos -aquellas con una sentencia GROUP BY. Al igual que los demás búfferes que se han visto, el búffer de ordenación es relativamente pequeño por defecto. Al ajustar la entrada de sort_buffer en el archivo my.cnf:

```
set-variable= sort_buffer= 8M
```

Puedes reducir dramáticamente la cantidad de tiempo que se usa para ordenar grandes grupos de resultados.El búffer de ordenación aparece como sort_buffer en la sálida de SHOW VARIABLES, por ejemplo:

```
sort_buffer 8388600
```

El mismo tipo de aviso se aplica al búffer de ordenación que para el búffer de registros. Es un búffer que MySQL reserva frecuentemente y se reserva por hilo. Así que, hay que incrementarlo con cuidado en un servidor que ejecute muchas búsquedas concurrentes.

Guías generales de ajuste

Antes de discutir como medir o juzgar los efectos de cualquier cambio que se realice, se debe considerar brevemente un acercamiento a la afinación del rendimiento. Hay unas cuantas cosas que se deben tener en mente cuando se empiezan hacer y probar cambios:

Sólo cambiar un parámetro cada vez. Puede que los cambios no resulten siempre en el comportamiento esperado. Si se cambian demasiados parámetros a la vez, se corre el riesgo de asignar un cambio en el comportamiento al parámetro equivocado.

No hacer cambios en sistemas en producción. Si es del todo posible, se debe tener un servidor de pruebas disponible que sea parecido en naturaleza al servidor de bases de datos de producción. Hacer cambios en la configuración de MySQL seguramente requerirá que se pare y reinicie el servidor, lo que hará que los usuarios experimenten interrupciones en el servicio.

Usar datos reales. El tipo de datos que se estén usando afecta a como responde MySQL a las búsquedas. Idealmente, se debería usar una copia de las bases de datos de producción. Si no es posible hacer esto; entonces se debería intentar construir un subconjunto representativo de datos.

Realizar pruebas realistas. Es fácil asumir que se sabe que pruebas aplicar simplemente porque se sabecuales son las áreas problemáticas. Sin embargo, algunos cambios de la configuración acelerán partes lentas de una aplicación al mismo tiempo que ralentizan cosas que antes eran bastante rápidas.

Ser sistemático y registrar descubrimientos. Es importante que se mantenga la pista de los cambios que se realizan y como afectan al rendimiento. Después de varias horas (o incluso días) de pruebas, es más que probable que no se recuerde exactamente que es lo que se ha cambiado y si los cambios fueron positivos o negativos.
Observando los números de rendimiento de la base de datos con los pocos puntos de partida en mente y un concepto de cómo hacer pruebas, ahora se debe considerar cómo monitorizar el progreso.

Afortunadamente, MySQL tiene más de 50 contadores internos (o variables de estado), que mantienen la pista de cuántas veces ocurren varios tipos de eventos.

Dado que el espacio en este artículo sirve para comentar solamente algunas de las variables de estado de MySQL, en el manual de MySQL se describen todas y cada una de ellas en mayor detalle. Para ver estos números, se puede usar la sentencia SHOW STATUS. En este caso se mencionan únicamente las variables relacionadas con el búffer de claves:

```
SHOW STATUS LIKE 'Key%'

Key_read_requests 3844786889
key_reads 16525182
Key_write_requests 303516563
Key_writes 152315649
```

Estas cuatro variables dicen mucho sobre el rendimiento del búffer de claves de MySQL. Cada vez que MySQL sea capaz de leer una clave (o índice) del búffer de claves (en vez de ir a disco), incrementará automáticamente el valor de key_read_requests. Si MySQL ha de leer la clave del disco porque no estaba ya en la caché, incrementará key_reads. La misma lógica se aplica para las escrituras de disco. Sabiendo esto, podemos calcular la eficiencia (o hit rate) para el búffer de claves.

Usando una fórmula como:

```
100 - ((Key_reads / Key_read_requests) * 100)
```

Podemos obtener un porcentaje que representa cómo a menudo es capaz MySQL de leer las claves directamente de la caché en vez de irse a disco. Cuanto más cerca esté el valor de 100, mucho mejor. Usando los números de arriba, se tiene un hit rate de cerca del 99.57 por ciento. Generalmente, suele ser una buena idea mantener este porcentaje por encima del 90 por ciento. A fin de cuentas, de lo que se trata, es de tener una mejora medible del rendimiento de MySQL.

Observando los números de rendimiento del sistema

Monitorear los cambios de rendimiento en MySQL es sólo una parte de la labor, también es necesario ver qué es lo que está pasando desde el punto de vista del sistema operativo, ya que como cualquier otra aplicación, está a merced de lo que el sistema operativo quiera permitirle hacer, así que es importante que se mantenga una vista global sobre toda la actividad del sistema operativo.

Se debe tener una idea de la actividad actual del sistema y características del rendimiento de MySQL antes de empezar a hacer pruebas. Sin una base para la comparación, realmente no se sabrá como ha cambiado el impacto de MySQL en el sistema. Finalmente, cabe mencionar que únicamente se ha descrito una mínima parte de lo que representa el rendimiento en el lado del servidor para MySQL. El manual de MySQL contiene muchas otras ideas sobre cómo incrementar el rendimiento de MySQL y monitorizar los progresos.

Pasar Drupal 4.6.X a iso-8859-1

Autor:Jose Angelini
joseangelini@argentina.com
País: ARGENTINA

Una de las características más sobresalientes de Drupal, a mi entender al menos, es su versatilidad.

Sin embargo en lo referente a la selección del sistema de caracteres (charset) ésta se dejo de lado ya que no existe una forma de seleccionar el mismo, pudiendo utilizar tan solo UTF-8.

Cuando me vi obligado a utilizar una tabla conteniendo datos en ISO-8859-1 e imposibilitado de modificar el charset de la misma, lo primero que hice fue aplicar las funciones que PHP tiene para convertir texto a UTF-8 las que por desgracia no me dieron un resultado satisfactorio. Opté entonces por cambiar el charset que Drupal utiliza lo que logré luego de una serie de modificaciones y pruebas.

Detallo la manera de hacerlo en tres pasos:

1. Pasos

1.1. Modificación del archivo common.inc

El archivo common.inc se lo encuentra en el directorio includes, en el mismo existen dos instrucciones en las que se declara el charset y es necesario modificar:

En la línea 59, en la función drupal_get_html_head. En la misma se define el charset mostrado en la página.

```
$output = "<meta http-equiv=\"Content-Type\"
content=\"text/html; charset=utf-8\" />\n";
```

En la línea 1874, cuando llama a la función drupal_set_header. En esta función se setea el charset enviado al navegador cuando éste lo requiere.

```
drupal_set_header('Content-Type: text/html;
charset=utf-8');
```

En estas declaraciones hay que cambiar utf-8 por iso-8859-1

1.2. Convertir el archivo de traducción al español

Si está utilizando el paquete de lenguaje español y ha aplicado los cambios indicados en el apartado anterior seguramente notará caracteres indescifrables en el menú o en las explicaciones que traen los módulos traducidos. Para corregir ese problema es necesario cambiar la codificación del archivo de lenguaje es.po. Para ello desde una consola de comandos, en Linux basta con ejecutar

```
# iconv -f utf8 -t iso-8859-1 es.po -o es-iso.po
```

Este comando generará un nuevo archivo llamado es-iso.po. El archivo es el resultado de la conversión del archivo es.po a ISO-8859-1. Ahora no queda más que agregar el lenguaje español e importar el archivo es-iso.po para el mismo. Es preferible agregar nuevamente el lenguaje en caso de ya tenerlo instalado debido a que, al menos en mi experiencia, importar lo sobre uno ya existente no logra sobrescribir la información almacenada.

1.3. Modificación del archivo user.module

Cuando un usuario se registra o pide una nueva contraseña, en general, se envía un mail para lo cual está definida la función user_mail en la línea 434 del archivo user.module. En la misma se llama a la función mail de PHP del siguiente modo

```
return mail(
$mail,
mime_header_encode($subject),
str_replace("\r", '', $message),
"MIME-Version: 1.0\nContent-Type: text/plain; charset=UTF-8;
format=flowed\nContent-transfer-encoding: 8Bit\n" . $header
);
```

Los valores pasados a la función mail están codificados, después de las modificaciones aplicadas, en ISO-8859-1 es necesario, en consecuencia, convertirlos a UTF-8. Se puede usar la función utf8_encode [1] de la siguiente manera:

```
$mail_m = utf8_encode($mail);
$subject_m = utf8_encode($subject);
$message_m=utf8_encode($message);
$header_m = utf8_encode($header);
return mail(
$mail_m,
mime_header_encode($subject_m),
str_replace("\r", '', $message_m),
"MIME-Version: 1.0\nContent-Type: text/plain; charset=UTF-8;
format=flowed\nContent-transfer-encoding: 8Bit\n" . $header_m
);
```

2. Conclusiones

Es preferible no cambiar el charset que Drupal usa, salvo que no quede otra alternativa, en tal caso los pasos enumerados son una guía para hacerlo. Particularmente no he encontrado hasta el momento algún otro punto de mejora, existirán seguramente, en caso de notar alguno o necesitar ayuda adicional puede enviarme un mail a mi dirección:

Referencias: [1] PHP Manual http://ar.php.net/utf8/_encode

Programación XML con .NET

Nombre: BORIS
País: PERÚ

Experiencia laboral: *desarrollador Independiente*
Conocimientos: *VB6 ,VB.NET, C #, Macromedia, SQL 7.0, SQL 2000*

XML y .NET

¿Alguna vez ha tenido la necesidad de que su programa interactué con información de configuración u otro tipo de datos grabados por el mismo sistema? (como la configuración para cada usuario, preferencias, referencias a archivos, etc.), una forma de resolver esto es mediante archivos planos, otra forma es creando archivos planos tipo .ini (que contienen información con formato), a los cuales hay que darles un tratamiento adecuado para grabarlos y recuperarlos.
Una opción igual de valida es la utilización de archivos XML, aprovechando el soporte que nos das el .Net Framework. En él se encuentra una jerarquía de clases para el tratamiento de archivos XML como detallare mas adelante.

Pero, ¿qué es XML?, son documentos estructurados para el manejo de información, estos datos están contenidos en formatos que son autodefinidos por medio de "etiquetas". Para mayor detalle al respecto puede consultar a wikipedia: http://es.wikipedia.org/wiki/XML .

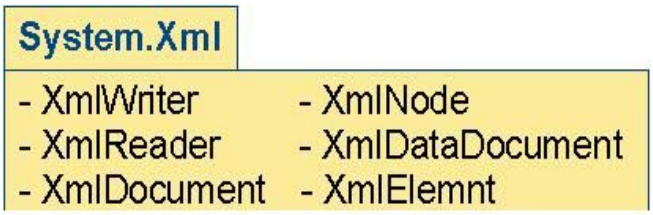
Un Ejemplo que llamaremos "probar.xml":
Queremos los datos contenga el nombre de un usuario y correo respectivos.

```
<?xml version="1.0" ?>
<listaNombres>
<usuario>
  <nombre>jose</nombre>
  <mail>jose@jose.com</mail>
</usuario>
<usuario>
<nombre>pedro</nombre>
  <mail>pedro@pedro.com</mail>
</usuario>
<usuario>
  <nombre>pablo</nombre>
  <mail>pablo@pablo.com</mail>
</usuario>
  </listaNombres>
```

Algo a tener en cuenta sobre los documentos XML es que estos deben estar bien formados y ser válidos. Un documento está bien formado si todas las Etiquetas de apertura cuentan con sus respectivas Etiquetas de cierre, cuenta con un solo elemento raíz en el cuál están incluidos todos los demás.

¿Como maneja Net los documentos XML? .Net Framework maneja los XML a través del namespace (jerarquía lógica de clases, agrupadas por temas en común) System.Xml, que contienen clases diseñadas para tareas de escritura, lectura, conversión entre otras.

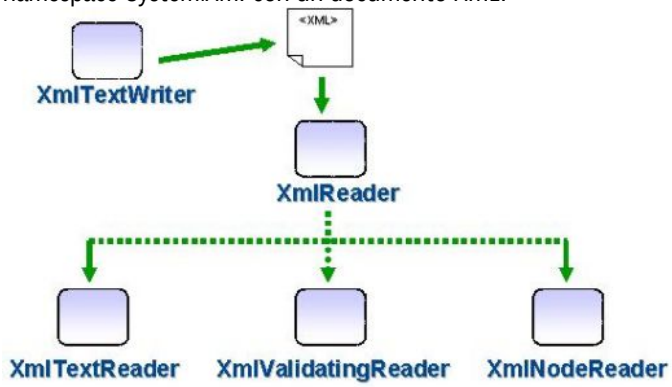
A continuación muestro el ámbito relacionado con XML que conforman System.XML:



Para leer de manera secuencial un documento XML, esto es nodo a nodo y elemento a elemento, tenemos a nuestra disposición las clases derivadas de XmlReader:

XmlReader
- XmlTextReader
- XmlValidatingReader
- xmlNodeReader

En la gráfica se muestra la interacción de las clases del namespace System.Xml con un documento XML:



A continuación construiremos un ejemplo de lectura en vb.Net, con salida en la consola (pantalla), de un archivo XML tomando como referencia el ejemplo anterior ("probar.xml") :

```
Imports System.Xml ' Espacio de nombre que se va utilizar
Module Module1
Sub Main()
      ' Obtenemos el documento XML desde el archivo, que se
encuentra en el sub directorio "Bin" del proyecto
Dim lector As New XmlTextReader("probar.xml")
While lector.Read() ' recorre todo el documento
           Select Case lector.NodeType
                Case XmlNodeType.Element ' Si es un elemento
                                  Console.Write("<{0}>", lector.Name)
                                  Console.WriteLine() 'salto de linea
               Case XmlNodeType.Text ' Si es un texto
                                  Console.Write(lector.Value) 'Imprime el
valor
                Case XmlNodeType.EndElement ' Si es el final del
elemento
                                  Console.Write("</{0}>", lector.Name)
                                  Console.WriteLine() 'salto de linea
            End Select
End While
Console.WriteLine() 'salto de linea
lector.Close() ' cerramos el lector
End Sub
```

'Nota: "<{0}>", lector.Name => lo utilizamos para dar el formato de salida del tìpo: < nombre_de_la_etiqueta >
End Module

Como puede ver con las clases derivadas de XmlReader es posible recuperar la información contenida en un documento Xml, pero en ningún caso facilita mecanismos para modificar el contenido de los nodos, eliminar, ó añadir elementos.

Para ello existe mecanismo como la clase XmlDocument, esta clase permite al documento Xml estar en memoria (genera un árbol jerárquico, compuesto por los nodos y elementos) y ofrece facilidades de navegación, lectura, modificación.

XmlDocument cuenta con Propiedades y métodos importantes para nuestros fines:
- **DocumentElemento** => obtendremos el primer elemento, el que representa la raíz de todos los demás
- **NodeType** => Contiene el tipo de Nodo.
- **Value**=> El valor de Nodo
- **ChildNodes**=> Recupera la lista de nodos hijos del nodo actual

A continuación construiremos un ejemplo que permite modificar el Archivo "probar.xml" anteriormente creado y grabar las modificaciones en un documento llamado "nueva_prueba.xml" con salida en la consola (pantalla) para ello hago uso de XmlDocument:

```
Imports System.Xml
Module Module1
Sub Main()
 Dim documento As New XmlDocument
 Dim nodo As XmlNode
 Dim mynombre, mycorreo As String
 documento.Load("probar.xml") ' Documento XML desde el archivo, que se
encuentra en el sub directorio "Bin" del proyecto
          For Each nodo In documento.DocumentElement.ChildNodes
' Recorrer los nodos
                    If nodo.Name = "usuario" Then ' si el nodo se llama captura
los nodos hijos de este
                              mynombre = nodo.ChildNodes(0).InnerText 'La
recuperacion es ordenada, ChildNodes ( 0 ) ,  ChildNodes ( 1 )
                             mycorreo = nodo.ChildNodes(1).InnerText
                    End If
                    If mynombre = "pedro" Then ' Aqui se va modificar un dato,
si es igual a "pedro" se va modificar por "Pedrito"
                              Console.Write("antes su nombre era => " &
mynombre)
                               Console.WriteLine()
                              mynombre = "Pedrito"
                              nodo.ChildNodes(0).InnerText = mynombre ' Aqui se
pasa el nuevo valor al nodo en cuestion
                     End If
          Console.Write("nombre: " & mynombre & " correo: " & mycorreo)
          Console.WriteLine()
           Next
documento.Save("nueva_prueba.xml") 'Aqui se guarda las modificaciones en
otro archivo
End Sub
End Module
..... Mas adelante mostrare como crear un documento Xml desde Net
 .....
```

Cómo hacer drag and drop usando javascript

Autor:mandm
mandm_mini@hotmail.com
País: MÉXICO

Más de alguna vez nos hemos encontrado con una página que use drag and drop, por lo que me di a la tarea de hacer una pequeña clase muy útil y éficaz.

Para hacer esto vamos a usar dos archivos.

archivo.html

```
<html>
   <head>
      <script src="drag.js"></script>
   </head>
   <body>
      <div id="drag" onmousedown="js_drag(event,this)"
style="width:300px; font-family:trebuchetms,arial,sans-serif;font-
size:11px;position:absolute;top:100px;left:100px;
cursor:move;background-color:#ccc;">Hola<br><br></div>
   </body>
</html>
```

drag.js

```
// Compatibilidad con el innombrable engendro de mocosoft
var is_ie = navigator.appName == 'Microsoft Internet Explorer';
// Compatibilidad con Opera
var is_op = navigator.appName == 'Opera' ? true : false;
// Compatibilidad con firefox o netscape
var is_ns = !is_ie && !is_op ? true : false;

// Función principal....

/*
   Esta función require dos parámetros
   el primero de ellos (e) es el evento
   el segundo es el elemento sobre el que se desea arrastrar y
soltar.
*/
function js_drag(e,elemento)
{
   // Por situaciónes de compatibilidad para ns es 'e' suficiente, en
cambio para IE e no basta sino window
   // aún no entiendo ¿por qué? acaso no se supone que TODO se
basa en el objeto window 8-)
   e||window.event;
   var e = e;
   // Creamos un nuevo Objeto
   var Obj = new Object();
   // Obtenemos el tag BODY, ( siempre hay uno de esos )...
   var body  = document.getElementsByTagName('body')[0];
   // El z-index ( el arrange , Hasta al frente, Hasta el fondo etc.. )
   Obj.zI = 0;
   // Ahora, el argumento 'elemento' puede ser un objeto o bien una
id del elemento
   // es decir js_drag(event,this) ó js_drag(event,'id')
   Obj.Elemento = typeof(elemento) == 'object' ? elemento :
document.getElementById(elemento);

   // Esta función obtiene la posición en la que está el elemento
HTML.
   js_position = function(ly,x,y)
   {
      /*
         Si es IE u Opera sumamos:
         clientX ( que es la posición del ratón en la ventana )
         document.documentElement.scrollLeft ( qué es la posición
del mouse en el elemento )
         body.scrollLeft ( que es el scroll que se le ha dado a la página
)
         Si es ns ( firefox, netscape, etcétera, )
         Sólo sumamos la posición del raton en la ventana y el scroll
que se le ha dado a la página.
      */
      x = is_ie||is_op ? e.clientX +
document.documentElement.scrollLeft + body.scrollLeft : e.clientX +
window.scrollX;
      y = is_ie||is_op ? e.clientY +
document.documentElement.scrollTop + body.scrollTop : e.clientY +
window.scrollY;
      // Guardamos la posición 'x' y 'y' inicial del elemento en una
variable ( contando el scroll ).
      Obj.startX=x;
      Obj.startY=y;
      // Guardamos la posición 'Left' y 'Right' inicial del elemento en
una variable ( sin contar el scroll ).
```

```
        Obj.startL=parseInt(Obj.Elemento.style.left,10);
        Obj.startT=parseInt(Obj.Elemento.style.top,10);
        Obj.startL=isNaN(Obj.startL) ? 0 : Obj.startL;
        Obj.startT=isNaN(Obj.startT) ? 0 : Obj.startT;
        // Aumentamos el z-index del objeto para enviarlo hasta el
frente ( aunque para IE esto no significa NADA )
        Obj.Elemento.style.zIndex = ++Obj.zI;

        /*
           js_addEvent() es una función propia, que añade al
primer argumento en este caso 'document'
           una función en este caso 'startdrag' que se ejecuta cada
segundo argumento en este caso 'mousemove'
        */
        js_addEvent(document,'mousemove',startdrag);
        // mouseup para cuando se 'suelte' el elemento
        js_addEvent(document,'mouseup',enddrag);
        // keypress para cuando se presione una tecla o se haga
click por cuestiones conocidas
        // ¿ realmente necesito explicar que es por IE ?
        js_addEvent(document,'keypress',enddrag);

        // Ahora prevenimos que los eventos que acabamos de
agregar se ejecuten inmediatamente
        if(is_ie){    e.cancelBubble = true;    e.returnValue =
false;    } else
        {
           e.preventDefault();
        }
    };

    startdrag = function(e)
    {
        // Esto ya lo expliqué arriba...
        var x, y;
        e||event;
        x = is_ie||is_op ? e.clientX +
document.documentElement.scrollLeft + body.scrollLeft :
e.clientX + window.scrollX;
        y = is_ie||is_op ? e.clientY +
document.documentElement.scrollTop + body.scrollTop :
e.clientY + window.scrollY;

        // Sumamos las posiciones guardardas y las actuales y ésa
es la posición actual ( a donde debe moverse )
        ILeft = ( Obj.startL + x - parseInt(Obj.startX)    );
        ITop = ( Obj.startT + y - parseInt(Obj.startY) );

        // js_moveTo esta función cambia la posición del elemento
cambiando el estilo css presizamente 'top' y 'left'
        js_moveTo(Obj.Elemento,ILeft,ITop);

        // Esto también lo expliqué arriba...
        if(is_ie){    e.cancelBubble = true; e.returnValue = false;    }else
        {
           e.preventDefault();
        }
    };

    enddrag = function (e)
    {    // Cuando se deje de arrastrar entonces eliminamos los
eventos que ya no nos sirven.
        js_detEvent(document,'mousemove',startdrag);
        js_detEvent(document,'mouseup',enddrag);
    };

    // Aquí inicializamos el arrastrar y soltar....
    js_position(Obj.Elemento,e.clientX,e.clientY);
};

js_moveTo = function(element,Left,Top)
{
    element.style.left = Left + "px";
    element.style.top  = Top + "px";
};

// Función que agrega los eventos
js_addEvent = function(Layer,eventype,func)
{
// addEventListener,attachEvent son propiedades para agregar
funciones a  eventos
    if( is_ns )
        Layer.addEventListener( eventype, func, true );
    else if( is_ie )
        Layer.attachEvent( "on" + eventype, func );
    else
// Opera simplemente lo usa como un array.
        Layer[ "on" + eventype ] = func;
};

// Igual que la función de arriba sólo que aquí quitamos las
funciones a los eventos.
js_detEvent = function(Layer,typef,func)
{
    if(is_ie)
        Layer.detachEvent("on" + typef, func);
    else if(is_ns)
        Layer.removeEventListener( typef, func, true);
    else
        Layer["on" + typef] = null;
};
```

Dudas y/o sugerencias al código gracias!!

Cómo hacer un formulario simple en Win32 con Visual Studio 6 y Visual C++

Autor:landanohr
landanohr@hotmail.com
País: ESPAÑA

Personalidad: Depende del momento: conciso, aplicado, atento,... o estrovertido, friki e incluso chiflado... | **Nivel de estudios:** Licenciatura o profesional | **Área de estudio:** Ingeniería en Informática | **Objectivo(s):** A corto plazo seguir mejorando en mi profesión. ¿Algún día? Entrar en el desarrollo y programación de juegos. | Meta(s): ¿Hay alguna verdadera meta en la vida que no sea la felicidad? | **Experiencia laboral:** [febrero 2005 - agosto 2005] en prácticas realizando tareas de programación de aplicaciones web usando Java, JavaScript, scriplet, JSTL, Struts, Postgre y Torque principalmente. [agosto 2005 - Mayo 2006] lo mismo, pero con rango de programador Junior y además algo de Oracle, Hibernate y xml. [Mayo 2006 - Junio 2006] ahora estoy con mis primeros pinitos en Cocoon... [Junio 2006 -] Se acabó el Cocoon, vuelvo con Java, JDBC y Oracle | **Actividades:** Aparte de trabajar, rolear con los colegas (Elric), WoW, Guild Wars | **Conocimientos:** Referentes a lenguajes de programación: - C, C++, con uso de las MFC , C#, con conocimiento avanzado en aplicaciones de escritorio ,Java, JavaScript, scriplet, JSTL, Struts, Hibernate , VBasic, VBScript , HTML, CSS, XML, XSLT, XUL , ASP, ASP.Net , Corba , SQL, Oracle, PostgreSQL , Otros: Lisp, Clips, Prolog, Other, Mace, OCL, ABAP 4

Buenas de nuevo, vamos a volver a las aplicaciones Win32 con Visual C++ con un ejemplo algo más complejo que el anterior... Por si no lo habéis visto, antes de leer este artículo os recomendaría dar un vistazo a este otro: "Cómo hacer una aplicación Win32 con Visual Studio y Visual C++", del que básicamente éste es la segunda parte.

Volviendo a lo importante, lo que vamos a hacer es un pequeño formulario para ver el funcionamiento de los controles básicos... y alguna otra cosa más.

Requisitos: tener una leve idea de cómo se crean aplicaciones Win32 en Visual Studio con Visual C++, y como es normal, el Visual a mano...

Pasos: como es de prever este apartado es más extenso, así que vamos por partes...

1-. Creación del proyecto

En el artículo anterior hemos visto que podemos crear una aplicación con una ventana de forma bastante simple, la aplicación "Hello World", y continuar a partir de ahí. Pues bien, en este caso eso no nos interesa, ya que queremos que la ventana principal de nuestra aplicación sea un formulario (típica ventana gris con controles), y no una ventana blanca como laque tendríamos en el caso anterior.

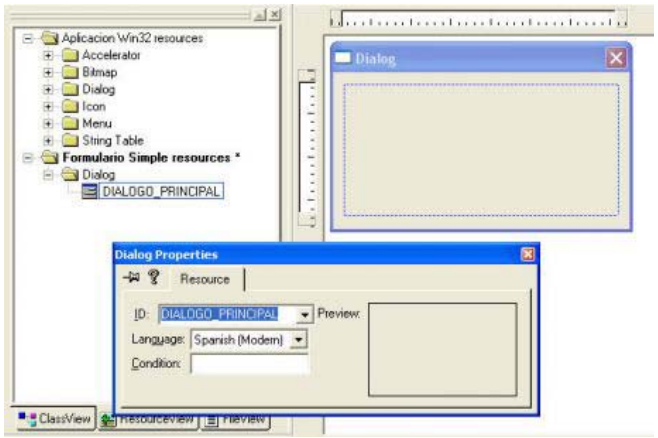
Vamos a crear por eso la aplicación desde cero, y ya de camino vemos cómo hacerlo. Empezamos: archivo -> nuevo -> proyecto, elegimos aplicación Win32 y ponemos el nombre que queramos, por ejemplo "Formulario Simple". Damos OK y elegimos una aplicación Win32 simple. De esta forma hemos creado una aplicación con varios ficheros, uno de ellos "Formulario Simple.cpp", que será al que demos contenido.

Lo que queremos hacer es que al ejecutar la aplicación aparezca nuestro formulario, y para ello necesitamos incluir algún código, pero antes hemos de crear el formulario.

2-. Creación del formulario

Antes incluso hemos de hacer algo más: crear el archivo de recursos. Para ellos insertamos un nuevo archivo en el proyecto: archivo ->nuevo -> script de recursos, ponemos el nombre adecuado, "Formulario Simple" y ok (aseguraos de que el archivo se va a incluir en nuestro proyecto). Una vez hecho esto aparece una ventana abierta, la cerramos y volvemos a abrir el archivo de recursos (Formulario Simple.rc). Tenemos entonces una vista de recursos como la de la aplicación anterior, solo que vacía.

Ya iremos incluyendo los recursos que nos hagan falta...Empezaremos por el cuadro de diálogo: segundo botón sobre el texto marcado-> insertar -> diálogo -> nuevo y... ya tenemos nuestro diálogo. Quitamos los botones, cambiamos el nombre para que sea un poco más identificativo y listo.



Bueno sí, es un poco soso, pero ya lo arreglaremos más adelante, ahora lo que queremos es que se muestre.

3-. Mostrando nuestro formulario

Lo primero, incluimos #include "resource.h", para que reconozca los recursos y los podamos usar.

Como ya vimos en el otro artículo, hace falta un manejador para el formulario, que será el encargado de responder a las acciones que hagamos en el mismo, como pulsar un botón o escribir texto. Por esto mismo incluimos un manejador escueto (antes de WinMain), que iremos completando a medida que lo necesitemos:

```
LRESULT CALLBACK Manejador(HWND hDlg, UINT message, WPARAM
wParam, LPARAM lParam)
{
    switch(message)
    {
        case WM_INITDIALOG:
            return TRUE;
        case WM_COMMAND:
            if(LOWORD(wParam) == IDCANCEL)
            {
                EndDialog(hDlg, LOWORD(wParam));
                return TRUE;
            }
            break;

    }
    return FALSE;
}
```

Sólo tratamos dos eventos, el de creación WM_INITDIALOG, para permitir que se cree el cuadro, y el de cierre IDCANCEL, para destruir el diálogo, ya que sino no podríamos salir de la aplicación.

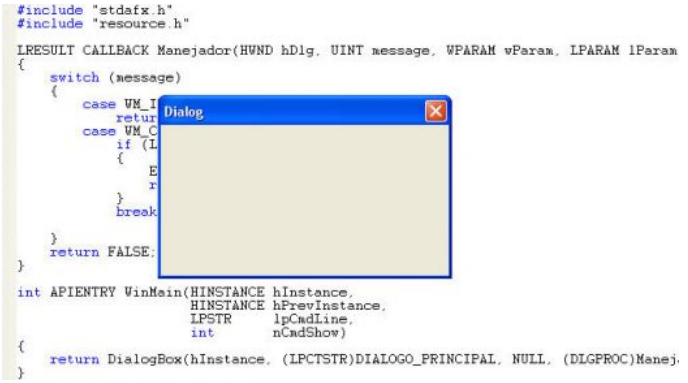
Además hemos de incluir en WinMain (que es el método inicial de la ejecución, al igual que el main en una aplicación de consola) el código necesario para la creación del cuadro de diálogo:

```
int APIENTRY WinMain(HINSTANCE hInstance,
                     HINSTANCE hPrevInstance,
                     LPSTR     lpCmdLine,
                     int       nCmdShow)
{
    return DialogBox(hInstance, (LPCTSTR)DIALOGO_PRINCIPAL, NULL,
(DLGPROC)Manejador);
}
```

Donde los parámetros pasados al método DialogBox (que crea el cuadro de diálogo) son:

hInstance-> Manejador de la aplicación
(LPCTSTR)DIALOGO_PRINCIPAL-> Cuadro de diálogo que ya hemos creado en recursos
NULL-> En principio ventana padre, pero como no queremos ninguna, nulo
(DLGPROC)Manejador-> Método que maneja los eventos del cuadro de diálogo

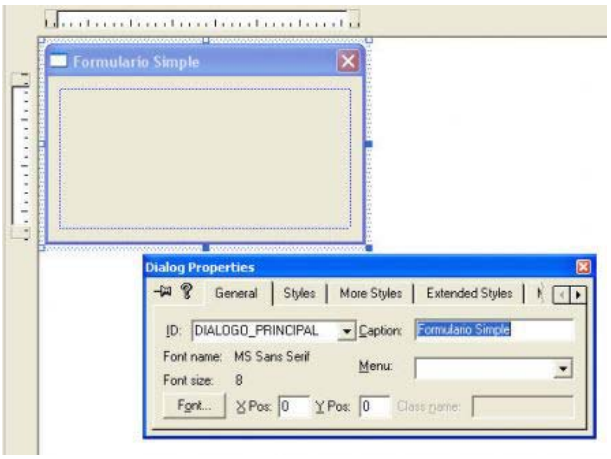
Ejecutamos la aplicación y:



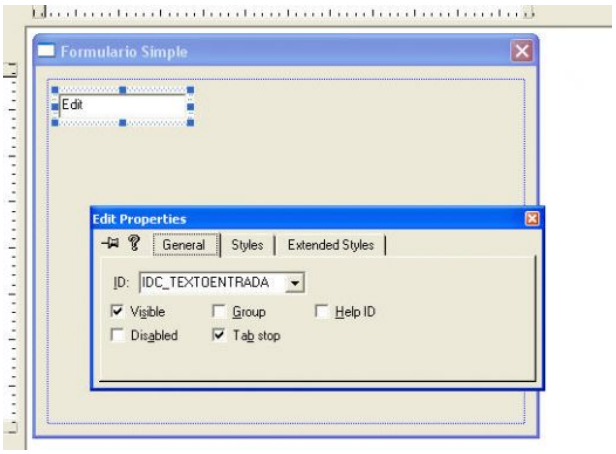
4-. Primeros controles

Pues bien, ya mostramos el formulario, así que va siendo hora de empezar a meterle contenido... Vamos ha hacer varias cosas:

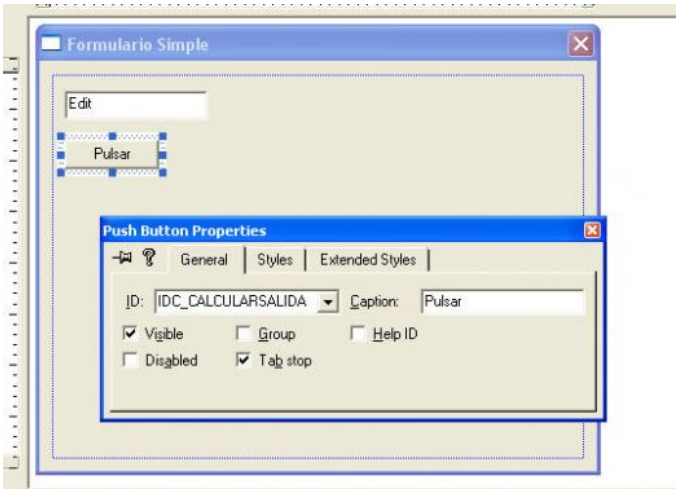
- Cambiamos el nombre del formulario



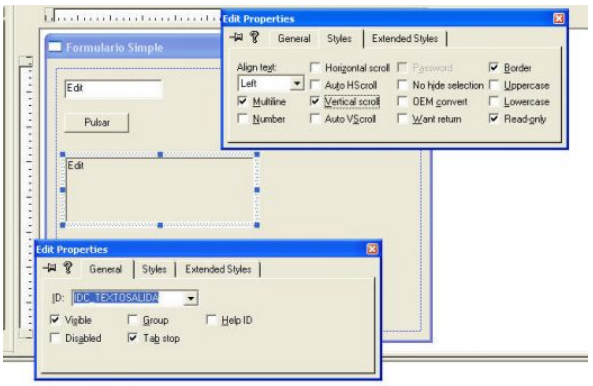
- Metemos un cuadro de texto



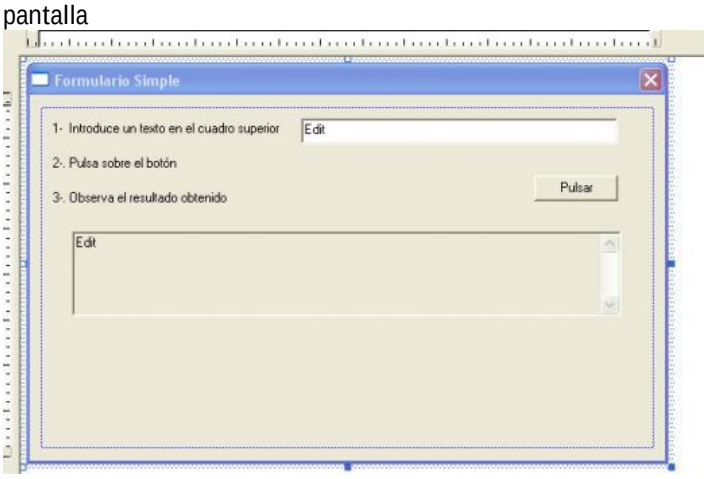
- Metemos un botón



- Un nuevo campo de texto



- Por último ponemos algún texto estático y ordenamos un poco la pantalla



Muy bonito, pero ahora viene la parte complicada (bueno, esperemos que no sea tanto), dar funcionalidad a los controles. Pero primero vamos a ver lo que queremos hacer: tenemos un texto de entrada, en el que el usuario introducirá un texto; también tenemos un texto de salida (un cuadro de texto de sólo lectura) en el que pondremos un texto dependiendo del texto introducido por el usuario. ¿Cuándo? Pues cuando se pulse el botón.

Manos a la obra pues. Como ya vimos en el otro artículo, para responder cuando se pulse un botón lo que tenemos que hacer es incluir un manejador para los eventos y hacer lo que queramos cuando se pulse el botón.

Por si no os acordáis ya pusimos un manejador para nuestro formulario, el método
LRESULTCALLBACK Manejador(...)
Además, como ya sabemos, para controlar las pulsaciones de botones sólo tenemos que incluir el código conveniente dentro de caseWM_COMMAND:

```
...
elseif(LOWORD(wParam) == IDC_CALCULARSALIDA)
{
/* lo que queramos hacer cuando se pulse el botón*/
}
```

¿Qué vamos a hacer? Eso según queráis, en mi caso voy a hacer un Cifrado César del texto introducido (sustituir cada letra por la

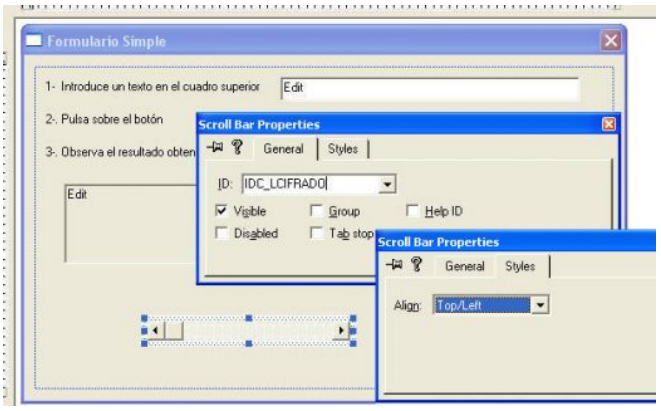
correspondiente en el abecedario a varias posiciones después). Tras un tiempo obtendremos el código que queramos, en mi caso quedaría:

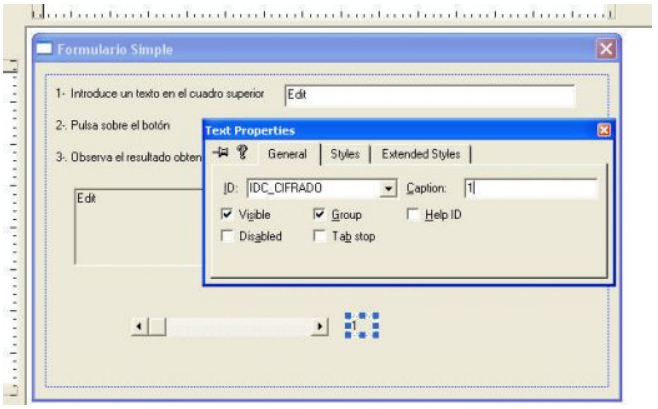
```
case WM_COMMAND:
{
    if(LOWORD(wParam)== IDCANCEL)
    {
        EndDialog(hDlg,LOWORD(wParam));
        return TRUE;
    }
    else if(LOWORD(wParam) == IDC_CALCULARSALIDA)
    {
        /* cogemos el texto de entrada*/
        LPTSTR entrada = new char[200];
        /* al método le pasamos el item que representa el cuadro de
texto,
          la variable donde queremos meter la cadena (ya inicializada),
          y la longitud máxima de la cadena.*/
        GetWindowText(GetDlgItem(hDlg, IDC_TEXTOENTRADA),
entrada, 200);
        /* calculamos la salida*/
        LPTSTR cadena = new char[400];
        LPTSTR aux = "Cifrado César del texto introducido: \r\n--------
---\r\n\r\n";
        int tam;
        int i;
        int longitudCifrado = 5;
        for(i= 0; true; i++)
        {
            char caracter = aux[i];
            if(caracter != '\0')
            {
                cadena[i] = caracter;
            }
            else
            {
                tam = i;
                break;
            }
        }
        for(i = 0; i < 200; i++)
        {
            int caracter = entrada[i];
            if(caracter != '\0' && caracter != ' ')
            {
                /* tratamiento para convertir sólo las letras permitidas
                 a-z, A-Z*/
                if(caracter > 63 && caracter < 92)
                {
                    /* A-Z */
                    caracter =(caracter - 65 + longitudCifrado)%26 +
65;
                    cadena[tam+i] = caracter;
                }
                else if(caracter > 96 && caracter < 123)
                {
                    /* a-z */
                    caracter = (caracter - 97 + longitudCifrado)%26 +
97;
                    cadena[tam+i] = caracter;
                }
                else
                {
                    /* carácter inválido*/
                    cadena[tam+i] ='_';
                }
            }
            else if(caracter == ' ')
            {
                cadena[tam+i] = ' ';
            }
            else
            {
                cadena[tam+i] = caracter;
                break;
            }
        }

        /* ponenos el texto correspondiente en la salida*/
        SetWindowText(GetDlgItem(hDlg, IDC_TEXTOSALIDA), cadena);
        return TRUE;
    }
    break;
}
```

5-. Añadiendo un control más

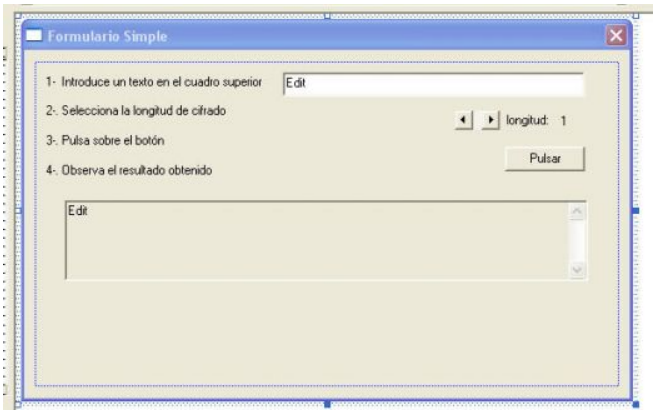
Dado que ya tenemos un primer formulario vamos a incluir un control más para dar más funcionalidad. En el código que he introducido (ya se que es un truño, pero bueno...) tenemos una variable, longitudCifrado, que se pone por defecto a 5; este valor representa la longitud de cifrado, podríamos hacer que fuera dinámico. Lo podemos hacer con una barra de scroll, de forma que seleccionemos el desplazamiento en ella.

Comenzamos insertando una barra de scroll y al lado un texto estático, donde pondremos el valor que tiene en cada momento la barra.





Lo ordenamos un poco, minimizamos el tamaño del scroll, ponemos algún texto estático más y quedará más o menos así:



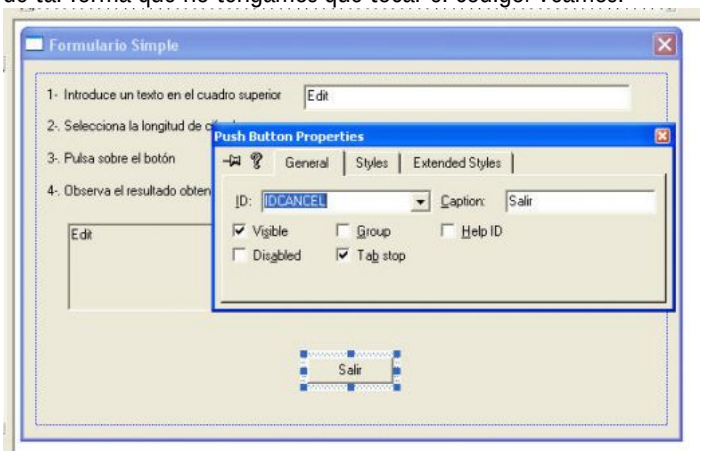
Vamos ahora a da la funcionalidad. Lo primero que tenemos que hacer es modificar el valor del texto estático que nos dice la longitud de cifrado cuando se desplace la barra; lo tendremos que hacer capturando el evento correspondiente en el manejador.

El evento que se provoca cuando movemos la barra de scrolles WM_HSCROLL, así que tendremos que incluir el nuevo case para la ocasión, además tendremos que modificar el case correspondiente a la inicialización para establecer el rango de desplazamiento del scroll, y tendremos que hacer global la variable longitudCifrado

```
int longitudCifrado=1;
...
case WM_INITDIALOG:
{
    /* marcamos el rango desde 1 a 50 */
    SetScrollRange(GetDlgItem(hDlg, IDC_LCIFRADO), 0, 1, 50, true);
    return TRUE;
}
case WM_HSCROLL:
{
    LPTSTR salida = new char[5];

    /* dependiendo de la flecha pulsada aumentamos o disminuimos el
valor,
       siempre dentro del rango*/
    if(LOWORD(wParam) == SB_LINEDOWN)
    {
        if(longitudCifrado < 50)
            longitudCifrado++;
    }
    else if(LOWORD(wParam) == SB_LINEUP)
    {
        if(longitudCifrado > 1)
            longitudCifrado--;
    }

    /* y mostramos el valor como contenido del texto estático*/
    _itoa(longitudCifrado, salida, 10);
    SetWindowText(GetDlgItem(hDlg, IDC_CIFRADO), salida);
    return TRUE;
}
```

6-. Punto y seguido

Por último vamos a añadir un botón para salir, pero lo vamos a hacer de tal forma que no tengamos que tocar el código. Veamos:



Con el identificador que hemos puesto al botón nos aseguramos que al pulsarlo el manejador lo controla como si se pulsase la X de cierre. Bueno, por ahora lo vamos a dejar aquí, que tanta letra cansa... espero que os sea de utilidad.

Si tenéis alguna duda, sugerencia o comentario, ponedlo aquí abajo o bien mandadme un mail a landanohr@hotmail.com

Creación de Gráficos en iReport

Cristóbal Vázquez
MÉXICO

***Área de estudio**: Sistemas de cómputo, Electrónica*
***Experiencia laboral**: Programador Java - Mapfre Tepeyac.*
***Experto en**: Swing, Análisis y diseño, modelado de sistemas con UML*
Actividades:
***Conocimientos**: Programación en lenguajes de alto nivel: C,C++, Java(J2SE). Programación en ensamblador: Intel, Motorola, Microcontroladores. Otros: Html, SQL, XML, Análisis y diseño de Sistemas digitales.*

JasperReports no maneja directamente gráficos: estos deben crearse independientemente como imágenes, incluso utilizando una de las numerosas librerías de código libre disponibles para la creación de gráficos. La imagen producida será mostrada usando un componente de imagen. La idea es realmente simple, pero la creación de un gráfico en tiempo de ejecución requiere de un buen conocimiento de la programación de JasperReports, y muchas veces es necesario utilizar scriptlets capaces de colectar los datos que se mostrarán en el gráfico.

A partir de la versión 0.4.0, iReport proporciona una herramienta para simplificar la construcción de un gráfico. Esta herramienta permite crear un gráfico configurando propiedades y datos principales que serán vistos de manera simple por el usuario final.

La creación de un gráfico se basa en una librería muy conocida de código libre llamada JFreeCharts desarrollada por David Gilbert de Object Refinery Limited. iReport soporta por ahora solamente un pequeño número de tipos de gráficos presentados en JFreeCharts, y pueden modificarse solamente algunas de las propiedades del gráfico, pero es posible aún así, crear gráficos limpios con un gran impacto a la vista.

Fuente: Documentación y Tutoriales de iReport en: *http://ireport.sourceforge.net/*

Después de la pequeña introducción, se mostrará la manera de crear un grafico en iReport.

La versión de iReport aquí utilizada será la 0.5.1, para versiones más recientes, la creación de los gráficos puede ser diferente; deben referirse a la documentación correspondiente de su versión.

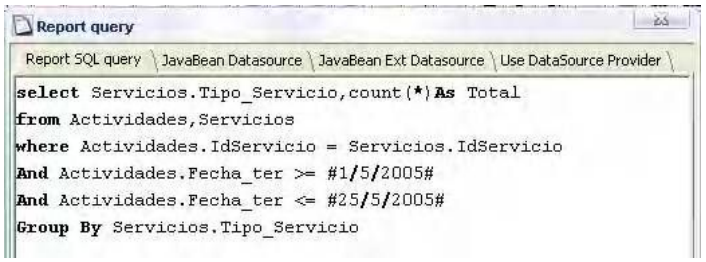
Supondremos que ya se cuenta con una configuración correcta del iReport y sus librerías, especialmente la librería JFreecharts, la versión que se inluye con iReport 0.5.1, es la jfreechart-1.0.0-rc1.

Además, se necesitará tener configurada una conexión a una base de datos, y por supuesto datos para poder establecer una consulta que alimentará con datos al gráfico.

A partir de los datos de las siguientes tablas, se creará el gráfico en cuestión.

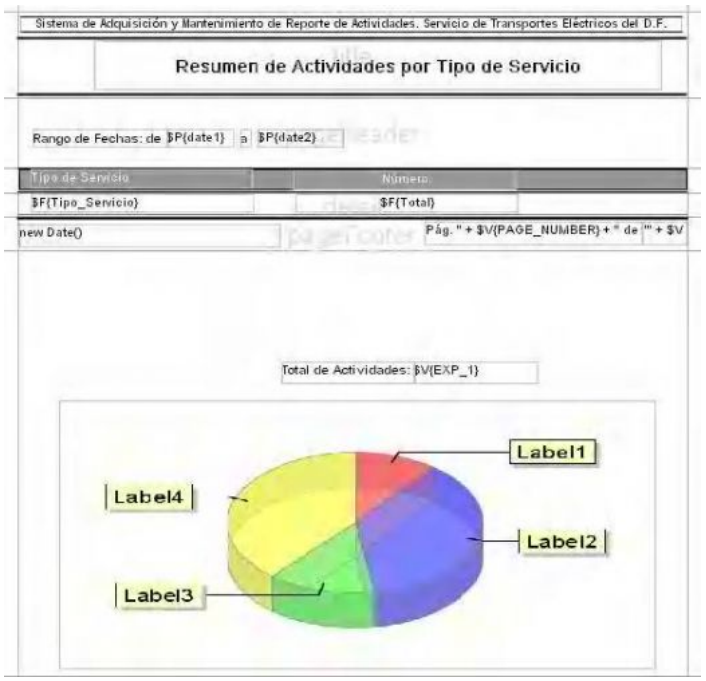
Las tablas anteriores muestran las actividades realizadas en una empresa. Cada una de las actividades se relaciona con un solo servicio. Cada actividad pertenece a un trabajador, que por simplicidad este campo no se muestra en este diseño de tablas.

Supongamos que se desea saber cuantas actividades se realizaron por servicio en un determinado rango de fechas, digamos en un mes. Se debe proceder a crear la consulta SQL correspondiente para obtener estos datos, más aún, podemos reflejarlos gráficamente, la consulta sería como la siguiente:

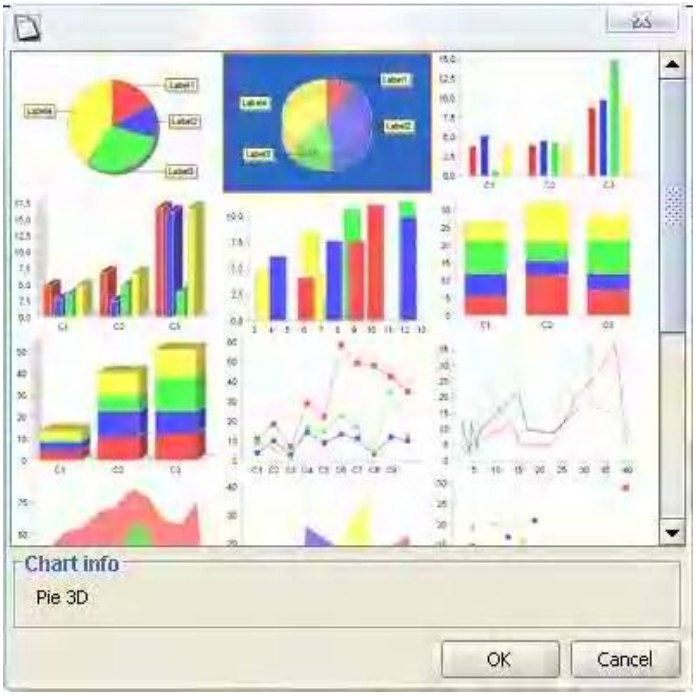


La consulta anterior agrupará las actividades realizadas por tipo de Servicio que se realizaron del 1 de mayo al 25 de mayo del 2005.

El diseño de reporte es el siguiente:

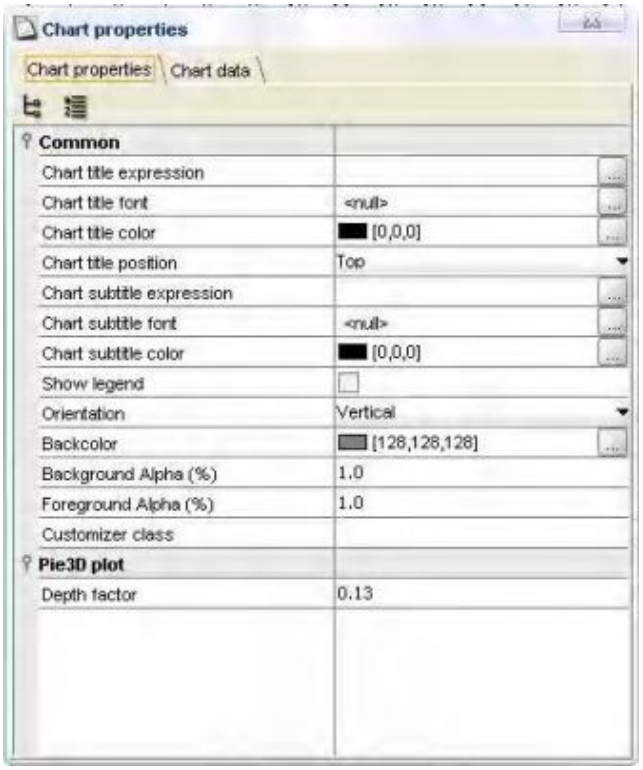


Para insertar un gráfico en un reporte de iReport, seleccione el objeto Chart tool de la barra de herramientas de iReport y dibuje el gráfico sobre la sección summary del reporte:



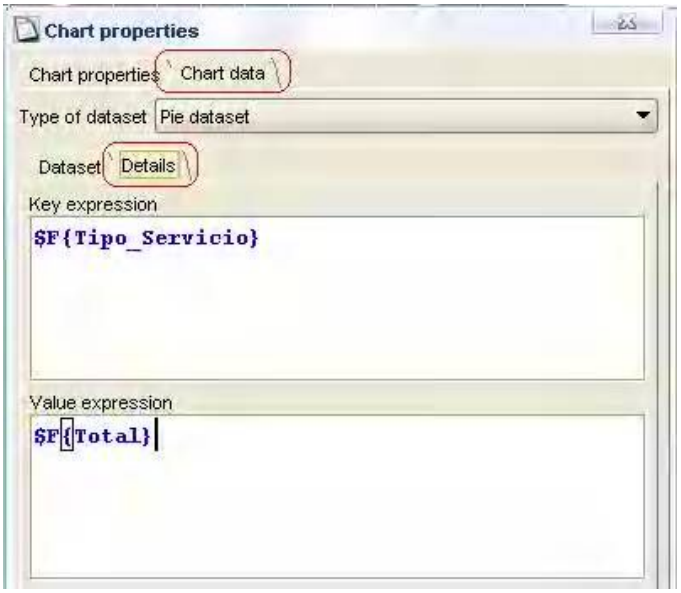
A continuación deberá seleccionar el tipo de gráfico deseado, para este ejemplo seleccionamos el tipo Pie 3D. Oprimir el botón OK y el componente que contendrá al gráfico ya ha sido creado, lo que resta es configurar las propiedades del mismo y los datos que mostrará.

Haciendo doble click sobre el componente del gráfico, se mostrará la pantalla de propiedades de este, sitúese en la pestaña Chart, a continuación oprima el botón Edit chart properties, deberá aparecer una pantalla como la siguiente:

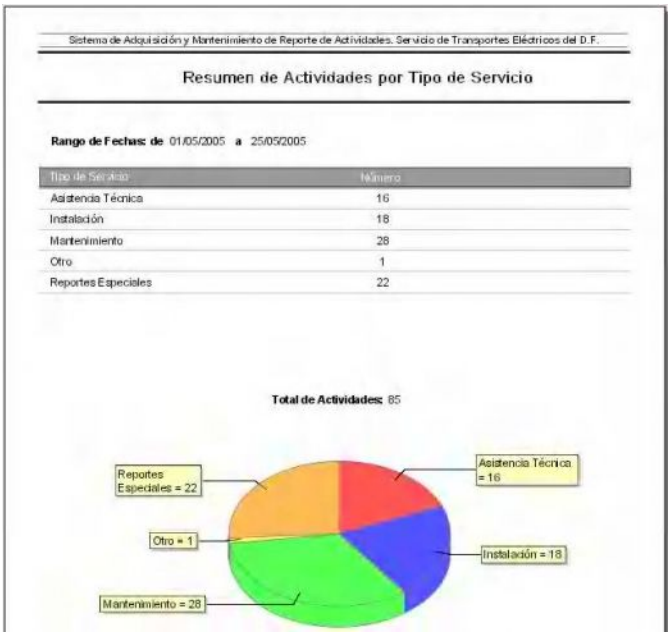


En la pestaña Chart properties de esta pantalla, se encuentran las propiedades que pueden modificarse para el gráfico en turno, como el nombre del gráfico, las fuentes, leyendas, ect. Puede dejar las propiedades actuales por ahora y modificarlas posteriormente. Ahora centraremos la atención en la manera de configurar los datos para el gráfico.

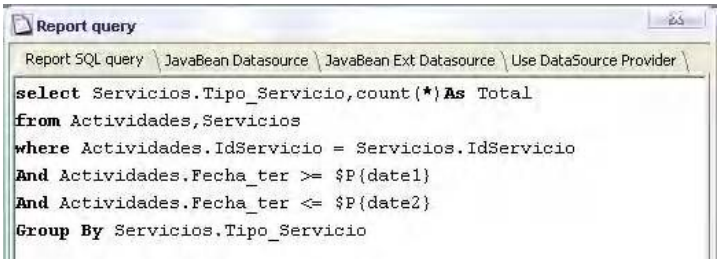
Debe situarse en la pestaña Chart data de la pantalla anterior y enseguida en la pestaña Details. En el apartado Key expression, coloque el campo $F{Tipo_Servicio} y en el apartado Value expresión coloque el campo $F{Total}. Estos campos son precisamente los que se obtienen de la consulta que se estableció anteriormente, estos a su vez se mostrarán en la sección detail del reporte.



Listo se han configurado los datos que necesita el gráfico. Al compilar y ejecutar el reporte con iReport el resultado puede ser parecido al siguiente:



Si se desea mostrar el gráfico anterior en tiempo de ejecución desde una aplicación Java, se procede de manera semejante a como se muestran otros reportes. En este caso deben determinarse los parámetros que se pasarán desde la aplicación java al reporte, por lo que la consulta se modifica como se muestra a continuación:



Lo que se pretende con la consulta anterior, es pasar como parámetros las fechas para las que se desea obtener el total de actividades agrupadas por servicio.

Para la versión 0.5.1 de iReport, solo debe compilarse el reporte para obtener el archivo Jasper que será llenado por la aplicación. En versiones anteriores o quizá recientes, es posible que se necesite incluir un scriplet para colectar los datos del gráfico.

Contando con el archivo Jasper del reporte, la manera en que se manda llenar desde una aplicación Java es la misma que para otros reportes, como se muestra en el siguiente fragmento de código:

```
...
//Ruta de Archivo Jasper
String fileName="C:\\proyecto\\Grafico.jasper";

//Obtner una conexión a la base de datos
conexion = new cConnection();
Connection con = conexion.mkConection();

//Pasamos parametros al reporte Jasper.
Map parameters = new HashMap();
parameters.put("date1",p_date1);
parameters.put("date2",p_date2);


//Preparacion del reporte (en esta etapa llena el diseño de reporte)
//Reporte diseñado y compilado con iReport
JasperPrint jasperPrint =
JasperFillManager.fillReport(fileName,parameters,con);

//Se lanza el Viewer de Jasper, no termina aplicación al salir
JasperViewer jviewer = new JasperViewer(jasperPrint,false);
jviewer.show();
...
```

Puede exportar el reporte a diferentes formatos de archivo directamente desde la aplicación sin pasar por el JasperViewer, para esto puede referirse a las API's de su versión correspondiente.

Programación scripts bash

Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com
ESPAÑA

***Área de estudio**: Administración de sistemas Informáticos*
***Experiencia laboral**: Reparación de ordenadores aparticulares, Clases de informática a particulares*
***Experto en**: Reparación de equipos informáticos*
***Actividades**: Estudiar, trabajar un poco y sacar adelante mis proyectos socio culturales de mi asociación (www.lalatina.org)*
***Conocimientos**: Redes; Sistemas operativos Windows (nivel Alto), Linux (nivel Medio); Programación (c/c++) nivel medio; Diseño de paginas Web (nivel medio -Alto); Uso de programas: photoshop, dreamweaver, virtual dj, atomix, office...etc*

Los scripts son simples ficheros de texto que contienen una serie de órdenes. Se pueden hacer con un editor vim.

#!/bin/bash identifica el fichero como un script; en el programa intérprete para la ejecución.

#comentario

Si se crea un script hay que asegurarse de que tiene permisos de ejecución para poder ejecutarlo. Una vez creado asigna el permiso de ejecución *$chmod u+x <fich script>*

Ejemplo:
[asi]$ vim ejemplo1

```
#!/bin/bash
#mensaje en pantalla
echo hola
sleep 10
echo mundo
```

[asi]$ chmod u+x ejemplo1
[asi]$ ejemplo1

El resultado es:

```
hola
mundo
```

Parámetros de los scripts
Los scripts pueden recibir y manipular parámetros. Estos parámetros se representan dentro de los scripts como $1, $2...
Ejemplo:

[asi]$ vim ejemplo2

```
#!/bin/bash
echo “cantidad de parámetros: $#”
echo “primer parámetro:$1”
echo “segundo parámetro:$2”
```

Para salir ZZ
[asi]$ chmod u+x ejemplo2
[asi]$ ejemplo2 p1,p2

El resultado es:

```
Cantidad de parámetros: 2
Primer parámetro: p1
Segundo parámetro: p2
```

Instrucciones de control

IF

```
Sintaxis: if [<condición>]
              then <comando>
          else
              <comandos>
          fi
```

Condiciones:

!condición	si condición es falsa
cond1 –a cond2	las dos condiciones son verdad
cond1 –o cond2	1 de las 2 es verdad
cadena	la cadena no está vacía
-z cadena	la cadena está vacía
cad1=cad2	las cadenas son iguales
cad1!=cad2	las cadenas son distintas
entero -eq entero	los enteros son iguales

FOR

```
Sintaxis: for <variable>in<lista>
              do <comandos>
          done
```

WHILE

```
Sintaxis: while <condición>
              do <comandos>
          done
```

Comprobación de ficheros (test)

Para evaluar expresiones condicionales test devuelve:

0 verdadero; 1 falso

Sintaxis: test <opciones> <fichero>

Opciones:

-e	fichero existe
-r	fichero si existe y es legible
-w	fichero existe y es modificable
-x	fichero existe y es ejecutable
-s	fichero existe y tiene tamaño>0
-d	fichero existe y es directorio

Ejercicios

1. Realiza un script de manera que automatice la creación de copias de seguridad de carpetas de manera que se le pase la ruta de una carpeta y éste haga la copìa de seguridad de la misma y la situe en una carpeta destinada al almacén de estas copias (situado por ejemplo en /home/$USER/seguridad)

$ vim ejer 6

```
#!/bin/bash
tar cfzv /home/$user/seguridad/fichero.tar.gz $1$ejer1
home/asi/alumno
```

2. Crea un script que reciba como parámetro un nombre de archivo e indique si el archivo es legible, modificable y ejecutable por el usuario

$ vim ejer2

```
#!/bin/bash
echo introduce fichero
read nombre fichero
if test –r nombre fichero → ó (if test –r $1)
then echo el fichero es legible
else hecho el fichero no es legible
fi
if test – w nombre fichero ó ($1)
then echo es modificable
else
echo no es modificable
fi
if test-x nombre fichero ó ($1)
then echo “el  fichero $nombre fichero es ejecutable”
else
echo no es ejecutable
fi
```

3. Crear un script que mueva todos los programas (archivo ejecutable) al directorio bin de la carpeta del usuario. Si esta carpeta no existe, la creará el script.

$ vim ejer3

```
#!/bin/bash
if test-x $1
then mv $1  /home/asi/bin

$ejer2 fich 1

$ vim ejer 2b
#!/bin/bash
for I in $*
do if test –x i
          then mv i -/bin
          else
          echo “si no es ejecutable”
          fi
done
$ejer2b f1 f2 f3 f4 ....
```

4. Realizar un script que permita copiar un archivo pasado como parámetro en un directorio cualquiera también pasado como parámetro, antes de copiar comprobar si el archivo se puede leer.

$vim ejer4

```
#!bin/bash
        If [ $#-eq 2 ]
        then
                If test-r $1
                then
                        If test-d $2
                        then
cp $1$2
                        else
          echo directorio inexistente
fi
else
echo archivo inexistente
fi
else
echo numero de parámetros incorrectos
        fi
```

5. Hacer un script que compare dos cadenas introducidas como parámetros, previamente comprobar si el número de parámetros es correcto.

$vim ejer5

```
#!bin/bash
If [ $#-eq 2 ]
        then
if test $1=$2
then
        echo las cadenas son iguales
else
        echo las cadenas no son iguales
fi
else
        echo parámetros incorrectos
fi
```

6. Hacer un script que visualice un menú de tres opciones, la primera borra un fichero leído por teclado, la segunda visualiza un fichero también leído por teclado y la tercera sale del programa

$vim ejer3

```
#!bin/bash
        while [ $#-et3 ]
        then
        do
        clear
                echo 1 borrar fichero leído por teclado
                echo 2 visualizar fichero leído por teclado
echo 3 salir
echo Introduce opción
read opción

if opción-eq1
then
        echo introduce fichero
        read $1
        run $1
fi
if opción-eq2
then
        echo Introduce fichero
read $1
        run $1
fi
if opción-eq3
then
        exit-1
fi
done
```

7. Script que acepta un fichero como parámetro, comprobar si se puede leer y visualizar su contenido

$vim ejer 7

```
#!bin/bash
        If [ $#-eq 1 ]
        Then
If test-r $1
        then
echo el archivo es legible
cat $1
else
echo archivo no legible
fi
else
echo no hay parámetro
```

8. Realizar un script que visualice si un usuario pasado como parámetro está conectado o no.

$vim ejer8

```
#!bin/bash
        echo Introduce el nombre del usuario
        read $1
who |Grep$1<dev/null
if ($?-eq 0)
then
echo conectado
```

```
else
echo no conectado
fi
```

9. Hacer un script que simule la orden cp. En este script pasamos dos parámetros que son ficheros, con el primer parámetro comprobamos si es de lectura y con el segundo comprobamos si existe y es de escritura. Pedir confirmación antes de sobrescribir el fichero.

$vim ejer9

```
#!bin/bash
        If test-r $1
                then
                if test-w $2
then
                        echo desea sobrescribir
read $3
if $3=S
                cp $1$1
if
fi
fi
```

10. Crear un script que acepte un número indefinido de parámetros (ficheros), en caso de existir se listan y al final del proceso se almacena en un fichero los nombres de los ficheros que se han podido listar y en otro los nombres de los que no se han podido listar. Después enviar un e-mail al usuario, diciéndole los ficheros que se han podido listar y los q no

$vim ejer10

```
#!bin/bash
for i in $
  If test-r $2
                        then
          echo $i>>mandados
else
          echo $i>> no mandados
fi

mail knoppix< mandados
mail knoppix< no mandados
```

11. Realizar un script que visualice un menú con 4 opciones:
-buscar un archivo
-cambiar permisos a un fichero
-buscar una cadena en un archivo
-salir

$vim ejer11

```
#!bin/bash
        Opcion=0
while [ $option –et4 ]
do
clear
echo 1 buscar archive
echo 2 cambiar permisos a un archivo
echo 3 buscar cadena en un archivo
echo 4 salir
echo Introduce opción
read opcion

if [opcion –eq1]
then
echo introduce fichero a buscar
read archive
find $archivo
fi

if [option –eq 2]
then
echo introduce el archivo
read archive
chmod (se indica los cambios) $archivo
fi

if [opcion –eq3 ]
then
echo introduce la cadena
read cadena
echo introduce el archivo
read archivo
grep $ cadena $archivo
fi

if [opcion –eq 4 ]
then
echo el programa se esta cerrando
break
fi
```

12. Utilizar un bucle while para repetir un número de veces un mandato.

$vim mandato

```
#!bin/bash
echo Introduce número de repeticiones
read $1
while [ option-lt $1]
        do clear
        $2 =4
```

```
echo $2
done
```

13. Utilizar en un script algunas variables y a continuación llamar a un segundo script permitiendo que algunas variables sean utilizadas por el segundo.

$vim ejer13

```
#!bin/bash

echo Introduce el nombre del usuario
read usuario
echo Introduce un fichero
read fichero
sh ejercicio 10-1 $usuario $archivo


$vim ejer 10-2
#!bin/bash
echo Enviando datos
mail $1<$2
```

14. Hacer un script que utilice un menú con tres opciones. Que son buscar, ordenar y salir con la primera opción llamamos a un segundo script que a su vez presenta un menú con:

Buscar por un campo determinado buscar por un dato salir o volver atrás con la segunda opción llama a otro script con dos opciones, una ordena ascendentemente y otra ordena descendentemente con la tercera opción sale del programa

$vim ejer14

```
#!bin/bash
        Opcion =0
while [ opcion –e 3]
do
clear
echo 1 buscar
echo 2 ordenar
echo 3 salir
read opcion

if [$opcion –eq 1]
then
sh ejer 11-2
fi

if [$ opcion –eq 2]
then
sh ejer 11-3
fi
done
```

```
$vim ejer11-2
#!bin/bash
echo  introduce archivo
read archivo

echo 1 ordenar ascendentemente
echo 2 ordenar descendentemente
echo elige opcion
read opcion

if [$ opcion –eq 1]
then
sort $ fichero
fi

if [$opcion –eq2 ]
then
sort –r $ fichero
fi


$vim ejer 11-3
#!bin/bash
clear
echo 1 buscar por un campo
echo 2  buscar dato
echo 3 salir
echo elige opcion
read opcion 2

if [$ opcion2 –eq 1]
then
echo introduce nombre del fichero
read fichero
echo introduce el campo
read campo
cut-f $ campo-d ``$ fichero
fi

if [$opcion2 –eq2 ]
then
echo introduce nombre del fichero
read fichero
echo introduce dato a buscar
read dato
grep $dato $fichero
fi
```

Resolución del problema de los frascos en Prolog

Autor:landanohr
landanohr@hotmail.com
País: ESPAÑA

Personalidad: Depende del momento: conciso, aplicado, atento, ... o estrovertido, friki e incluso chiflado... **| Nivel de estudios:** Licenciatura o profesional | **Área de estudio:** Ingeniería en Informática | **Objectivo(s):** A corto plazo seguir mejorando en mi profesión. ¿Algún día? Entrar en el desarrollo y programación de juegos. | **Meta(s):** ¿Hay alguna verdadera meta en la vida que no sea la felicidad? | **Experiencia laboral:** [febrero 2005 - agosto 2005] en prácticas realizando tareas de programación de aplicaciones web usando Java, JavaScript, scriplet, JSTL, Struts, Postgre y Torque principalmente. [agosto 2005 - Mayo 2006] lo mismo, pero con rango de programador Junior y además algo de Oracle, Hibernate y xml. [Mayo 2006 - Junio 2006] ahora estoy con mis primeros pinitos en Cocoon... [Junio 2006 -] Se acabó el Cocoon, vuelvo con Java, JDBC y Oracle | **Actividades:** Aparte de trabajar, rolear con los colegas (Elric), WoW, Guild Wars... | **Conocimientos:**Referentes a lenguajes de programación: - C, - C++, con uso de las MFC

Resolver un problema en Prolog puede llegar a ser una tarea más complicada de lo que se podría pensar en un primer momento dado la "simplicidad" del lenguaje. Para ilustrarlo vamos a ver cómo resolver el problema de los frascos con veneno.

1-. El problema

El Sr. Despistado, el químico, tiene seis frascos llenos de líquidos coloreados. Hay uno de cada color: rojo, anaranjado, amarillo, verde, azul y violeta. El señor Despistado sabe que algunos de esos líquidos son tóxicos, pero no recuerda cuales...

Sin embargo, sí recuerda algunos datos. En cada uno de los siguientes pares de frascos hay uno con veneno y otro no:

a) Los frascos violeta y azul
b) Los frascos rojo y amarillo
c) Los frascos azul y anaranjado

El Sr. Despistado recuerda también que en estos otros pares de frascos hay uno sin veneno:

d) el violeta y el amarillo
e) el rojo y el anaranjado
f) el verde y el azul

¡Ah! Casi lo olvido, añade el Sr. Despistado, el líquido del frasco rojo no es venenoso. ¿Qué frascos tienen veneno?

2-. Extraemos información

Lo primero que necesitamos para empezar a resolver el problema es diferenciar entre la información útil y el relleno que se añade para plantear el problema. En este caso no hay mucha dificultad en extraer la información que nos interesa:

1-. 6 frascos: rojo, anaranjado, amarillo, verde, azul y violeta

2-. Con veneno uno sí otro no:

a) Los frascos violeta y azul
b) Los frascos rojo y amarillo
c) Los frascos azul y anaranjado

3-. Uno del par no tiene veneno

d) el violeta y el amarillo
e) el rojo y el anaranjado
f) el verde y el azul

4-. El rojo no es veneno

3-. Planteamiento lógico

Antes de empezar a buscar predicados Prolog para resolver el problema suele ser bastante útil realizar un planteamiento más o menos lógico de cómo se podría llegar a la solución.

Supongo que si tenéis interés en Prolog ya tendréis unos conocimientos de lógica cuanto menos básicos, así que no perderemos tiempo en ello. El planteamiento que obtenemos es el siguiente:

Las variables que vamos a usar representan el conocimiento siguiente:

ro: el frasco rojo es venenoso
an: el frasco anaranjado es venenoso
am: el frasco amarillo es venenoso
ve: el frasco verde es venenoso
az: el frasco azul es venenoso
vi: el frasco violeta es venenoso

Traduciendo cada una de las condiciones anteriores tenemos las siguientes expresiones lógicas:

2-. Con veneno uno sí otro no:

a) los frascos violeta y azul	vi ↔ ¬az
b) los frascos rojo y amarillo	ro ↔ ¬am
c) los frascos azul y anaranjado	az ↔ ¬an

3-. Uno del par no tiene veneno

d) el violeta y el amarillo	¬vi v ¬am
e) el rojo y el anaranjado	¬ro v ¬an
f) el verde y el azul	¬ve v ¬az

4-. El rojo no es veneno ¬ro

Usando las expresiones podemos llegar a la solución. De forma simple:

¬ro
partiendo de ¬ro y usando ro ↔ ¬am obtenemos am
partiendo de am y usando ¬vi v ¬am obtenemos ¬vi
partiendo de ¬vi y usando vi ↔ ¬az obtenemos az
partiendo de az y usando az ↔ ¬an obtenemos ¬an
partiendo de az y usando ¬ve v ¬az obtenemos ¬ve

Con lo que tendríamos la solución:

- Los frascos venenosos son el amarillo y el azul
- Los frascos no venenosos son el rojo, el violeta, el anaranjado y el verde

4-. Modelando el problema en Prolog

Casi siempre, por no decir siempre, hay innumerables formas de modelar un problema en Prolog, normalmente alguna mejor que otra, pero indudablemente la mejor de todas es la que más clara veamos, porque es la que mejor entenderemos.

El modelado que he elegido para el problema no tiene porqué ser el mejor, pero es el que me ha parecido más correcto y el más intuitivo de ver. Veamos cómo es:

Lo que vamos a hacer es usar la base de conocimientos de Prolog, en la que iremos insertando información a medida que se resuelve el problema. Dicha información va a ser:

- Cuándo un frasco es venenoso
- Cuándo un frasco no es venenoso
- Cuándo hemos visitado una regla (nos servirá para no hacer uso varias veces de la misma regla)

Tendremos un predicado que será el encargado de incluir la información inicial en la base de conocimientos y de llamar al método que se encargará de procesar esa información resolver el problema.

Un apunte, para insertar la información usamos assert, que inserta la información al principio de la base de conocimientos.

Para cada una de las informaciones anteriores usaremos un predicado, e insertaremos en la base de conocimientos la información correcta (por ejemplo, inicialmente insertaremos no_venenoso (rojo)).

Además, inicialmente también insertaremos una información que nos diga que por defecto los predicados son falsos, ya que si preguntamos por ejemplo por venenoso (verde) y no tenemos esa información la respuesta que nos de tiene que ser falsa.
Por tanto el predicado principal sería de la forma:

```
resolver :-
    assert(no_venenoso(rojo)),
    assert(venenoso(X):-fail),
    assert(no_venenoso(X):-fail),
    assert(visitada_regla(X):-fail),
    procesar.
```

Incluimos un predicado de negación, que usaremos más adelante.

```
no(X) :-
    X,
    !,
    fail.
no(X).
```

Pasamos ahora al predicado procesar, que será el encargado de realizar el procesamiento de cada una de las reglas que hemos visto en el planteamiento lógico. En el caso de la primera regla vi ↔ ¬az obtenemos lo siguiente

% Regla 1

```
procesar :-
    venenoso(violeta),
    no(visitada_regla(1)),
    assert(no_venenoso(azul)),
    assert(visitada_regla(1)),
    procesar.

procesar :-
    no_venenoso(violeta),
    no(visitada_regla(1)),
    assert(venenoso(azul)),
    assert(visitada_regla(1)),
    procesar.

procesar :-
    venenoso(azul),
    no(visitada_regla(1)),
    assert(no_venenoso(violeta)),
    assert(visitada_regla(1)),
    procesar.

procesar :-
    no_venenoso(azul),
    no(visitada_regla(1)),
    assert(venenoso(violeta)),
    assert(visitada_regla(1)),
    procesar.
```

En cada una de las variaciones de la regla nos aseguramos de no haber visitado anteriormente la regla, ya que sino nos meteríamos en un bucle.

Por supuesto, tras ejecutar la regla la marcamos como visitada y seguimos procesando.

En concreto lo que se hace en la regla (al margen de controlar la visita) es ver si existe en la base de conocimientos, alguno de los valores posibles para sus variables, de forma que se pueda deducir el valor de la otra.

Por ejemplo, si tenemos en la base de conocimientos el predicado no_venenoso(violeta), podemos deducir venenoso(azul), por lo que lo incluimos.

De la misma forma, incluimos predicados para cada una de las reglas restantes, desde la regla 2 hasta la 6.

Vamos a obviar el código, ya que no aporta nada nuevo a la explicación, al final os pongo un enlace donde está la solución completa.

Y por último incluimos un predicado que haga terminar la ejecución, de forma que en la base de conocimientos tiene que quedar la solución al problema:

```
procesar:-
    write('fin del proceso').
```

Y como prueba de funcionamiento, obtenemos la solución que antes hemos deducido lógicamente:

```
1 ?- resolver.
fin del proceso
Yes

2 ?- venenoso(X).
X = amarillo ;
X = azul ;
No

3 ?- no_venenoso(X).
X = rojo ;
X = violeta ;
X = anaranjado ;
X = verde ;
No
```

Y listo, problema resuelto... El código completo de la solución lo podéis encontrar aquí: (http://www.mygnet.com/codigos/prolog/2/1708/ver/)

Bueno, eso es todo por ahora. Espero que os sirva tanta letra y si tenéis algún comentario o sugerencia ya sabéis, ponedlo aquí abajo o mándame un mail a landanohr@hotmail.com

Excepciones en VB.NET y C#

Juan Francisco Berrocal
berrocal239@hotmail.com
REPÚBLICA DOMINICANA

***Área de estudio**: Tec. En Programación y Operación de Microcomputadoras*
***Experiencia laboral:** Soporte IT/Software*
***Experto en**: VB,VB.NET*
***Actividades**: Bueno la única actividad que realizo es programar muchas Windows Application en lenguajes .NET (es mi pasión)*
***Conocimientos:** C/C++, HTML, VBScript, SQL, VB, VB.NET, C#.NET, VF*

En este articulo mostrare como evitar y manejar errores desde VB.NET utilizando los Bloques Try,Catch, Finally y la condicionante If..Then..Else.

Anteriormente cuando desarrollábamos una aplicación en VB6 tratábamos los errores o mejor dicho evitábamos un desborde de nuestra aplicación utilizando "On Error Resume Next" y esto nos ayudaba a que no se desbordara la aplicación.

Eso lo hacíamos más o menos así. (Ejemplo en VB6)

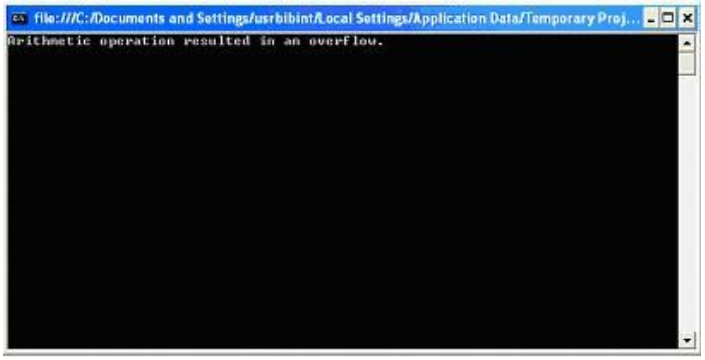
```
Private Sub cmdOk_Click( )

On Error Resume Next
If TextBox1.Text = 2 Then
   cmd.Write(TextBox1.Text)
End If

End Sub
```

Ciertamente aquí nos tiene que dar un error seguro, ya que "cmd.Write" no es parte de la sintaxis de VB6, en caso de que no hubiésemos tenido "On Error Resume Next" pues la aplicación sufriría un desbordamiento.

Aunque en .NET todavía podemos usar esta forma, lo que se nos aconseja es que utilicemos "Try Catch". Vamos a ver un ejemplo de una ConsoleApplication.

```
Sub Main()
      Dim i As Integer
      Dim j As Integer
      Try
         'Dentro de este bloque ponemos el codigo que
         'necesitamos evaluar
         i = 10
         j = 0
         Dim res As Integer
         res = i / j
         System.Console.WriteLine("El Resultado es:" & res)
      Catch ex As Exception
         'Aqui nos indicara el origen del error
         System.Console.WriteLine(ex.Message)
      Finally
         System.Console.ReadLine()
      End Try

   End Sub
```

Como podemos ver en el código (el cual esta comentado), se generara un error ya que estamos intentando dividir una cantidad por cero (0) y esto matemáticamente es imposible. Luego el Bloque "Catch" entra en función con el mensaje de excepción y nos presenta el siguiente mensaje en pantalla.



En caso de que sacáramos el codigo del "Try Catch" pasaria lo siguiente.

Nos aparece este mensaje de error el cual no nos dejara compilar nuestra aplicación.

Pero esto es con valores los cuales podemos controlar fácilmente porque lo ponemos nosotros mismos, pero que pasaria con una cantidad que introduzca el usuario del sistema, para ver este caso crearemos una WindowsApplication.

El Formulario se vera asi.

El mensaje de error como el del resultado de la operación (division) seran presentandos en un MessageBox.

Este seria el código de la aplicación.

```
Private Sub btnDividir_Click(ByVal sender As System.Object, _
    ByVal e As System.EventArgs) Handles btnDividir.Click

        'Declaramos y asignamos los valores de entrada
        'los cuales los definira el usuario
        Dim i As Integer = Val(Me.txtPR.Text)
        Dim j As Integer = Val(Me.txtSR.Text)

        Try
            'Declaramos la variable del resultado
            Dim res As Integer
            'Realizamos la operacion
            res = i / j
            'Mostramos el resultado de la operacion en pantalla
            MessageBox.Show("El Resultado es:" & res)
        Catch ex As Exception
            MessageBox.Show(ex.Message)
        End Try


    End Sub
```

La diferencia a simple vista no es mucha pero si nos fijamos esta vez el usuario definira la cantidad, pero con esto no es que todo esta hecho hay otras cosas que tenemos que tomar en cuenta, por ejemplo, si el usuario en vez de numeros introduce letras, la operación no se daria, esto lo podemos hacer utilizano "Not IsNumeric(objeto)" dentro de una condicion "If...Then...Else" la cual puede ir dentro del Bloque "Try Catch"

Veamos el Codigo.

```
Private Sub btnDividir_Click(ByVal sender As System.Object, _
    ByVal e As System.EventArgs) Handles btnDividir.Click

        'Declaramos y asignamos los valores de entrada
        'los cuales los definira el usuario
        Dim i As Integer = Val(Me.txtPR.Text)
        Dim j As Integer = Val(Me.txtSR.Text)

        Try

            'En caso de no sea numerico el dato introducido
            If Not IsNumeric(Me.txtPR.Text) Then
                MessageBox.Show("El Primer Rango debe ser
numerico", "Dato numerico")
                'Limpia la entrada
                Me.txtPR.Clear()
                'Enfoca para una nueva entrada
                Me.txtPR.Focus()
                'Con esto los que hago es dividir la ejecucion de cada
subrutina
                'para evitar una sobrecarga en la condicion
                Exit Sub
            ElseIf Not IsNumeric(Me.txtSR.Text) Then
                MessageBox.Show("El Segundo Rango debe ser
numerico", "Datos numerico")
                Me.txtSR.Clear()
                Me.txtSR.Focus()
                Exit Sub
            Else
                'Declaramos la variable del resultado
```

```
            Dim res As Integer
            'Realizamos la operacion
            res = i / j
            'Mostramos el resultado de la operacion en pantalla
            MessageBox.Show("El Resultado es:" & res)
        End If

    Catch ex As Exception
        MessageBox.Show(ex.Message)
    End Try
End Sub
```

La aplicación en caso de que utilicemos letras en lugar de números para realizar la operación matemática nos mostrara el siguiente error.

.

En caso de que el usuario haya introducido bien los datos, mostrara el resultado de la siguiente manera.

En conclusión, la diferencia que podemos constatar al realizar una WindowsApplication como una ConsoleApplication es que.

La ConsoleApplication: en esta el error es provocado por nosotros mismos y asi es demasiado facil predecir el error y evitarlo, aun sin tener que utilizar excepciones.

La WindowsApplication: aquí es diferente ya que los datos son introducidos por el usuario y de no utilizar las excepciones el programa nos daria un error de desbordamiento "muy feo" sacando al usuario del mismo.

Pues bien, esto es solo una parte de lo que es el tratamiento de errores en .NET, espero que este articulo les haya sido de utilidad, que esa es la intencion

Excepciones en c#

En otro articulo que escribí, hable sobre este mismo tema pero en Visual Basic .NET, ahora lo haré para C#.

En C#, se utilizan signos como (; { } [ ] !=) y demás..., así que lo recomendable es que conozcas un poco de C/C++ y porque no de JAVA, que al fin y al cabo es lo mismo en cuanto sintaxis. Pero como este no es curso de iniciación en C#, vamos a tratar el tema bien rapidito

Iniciaremos una ConsoleApplication y teclearemos el siguiente código. (Esta comentado)

```
static void Main(string[] args)
      {
         //Declaramos las variables de lugar
         int i;
         int j;

         //Iniciamos el Bloque "try"
         try
         {
            //Dentro de este bloque pondremos el codigo a evaluar
            i = 10;
            j = 0;
            int res;
            res = i / j;
            System.Console.WriteLine("El Resultado es:" + " " + res);
         }

         catch (Exception ex)
         {
            //Este bloque representa la excepcion y nos dara el error
            //en caso de que lo haya
            System.Console.WriteLine(ex.Message);
         }

         finally
         {
            //Aqui leeemos el resultado escrito en la consola
            //NOTA: este bloque es opcional
            System.Console.ReadLine();
         }
      }
   }
```

Como vimos en el codigo, cada bloque debemos iniciarlo con una llave de abertura "{" y otra que cierre "}" , cuando hablo de que el bloque "finally" es opcional, es que si quieres no lo pones y lo unico que tendrias que hacer es poner el metodo "ReadLine" fuera.

A diferencia de VB .NET, C# no da un "End Try", esta lo finaliza con la llave de cierre "}".

Como pudimos ver la diferencia de hacer esto en C# o en VB no es mucha, la diferencia son unos punto y coma (;) y unas cuantas llave ({ }).

Códigos fuentes del mes

Lenguaje Asp

Manejo de base datos

Crear Una Conexión Asp A Un Dsn Con Sql Server 2000

César Nava Camacho
nvcesar@yahoo.com.mx

Tamaño: 5 KB
Éste código conecta a un formulario asp con una base de datos en sql server a través de un dsn
http://www.mygnet.com/pages/down.php?cod=1722

.net

Ejecutar Url

Manuel Arturo Garcia Ramos
tenebris_luxperpetua@hotmail.com

Tamaño: 303 B
Con este código ejecuto un url en otro servidor diferente del ke contiene mi aplicación, este url que menciono es para procesar algunos datos y no lo podía hacer con response.redirect ni con server.transfer porke no se trata de \"ir\" a la página sino de ejecutar el mencionado proceso por medio de un url, les dejo el código bastante útil por si a alguien le sirviera hasta luego!!!
http://www.mygnet.com/pages/down.php?cod=1699

Lenguaje Bash

Método y comandos

Comando

Fructas
rcuellargtz@hotmail.com

Tamaño: 244 B
Ese comando me ha sido útil lo localice en Internet así que no es mió, pero se me hizo bueno para subir, para los master será una charada pero a mí me salvo de una. Simas allí esta es para copiar archivos pero concatenándole la fecha y hora en el nombre yo lo utilizo para auditorias.
http://www.mygnet.com/pages/down.php?cod=1731

Lenguaje C++

Varios

Ordenamiento Burbuja

Jose Gutierrez Saenz
bugsjard@hotmail.com

Tamaño: 834 B
Ordenamiento de datos por el método burbuja ascendente y descendente
http://www.mygnet.com/pages/down.php?cod=1728

Programillas En C++

Ugp –ulises–
gallardo_giva@yahoo.com.mx

Tamaño: 24 KB
Una leve recopilación de cpp's en un word sencillísimos pero que a alguien le han de servir. Hay de if else, for, do while, funciones, clases y un poco de herencia
http://www.mygnet.com/pages/down.php?cod=1727

Estructuras

Jose Gutierrez Saenz
bugsjard@hotmail.com

Tamaño: 701 B
Programa que registra alumnos y los imprime
http://www.mygnet.com/pages/down.php?cod=1719

Suma Pares E Impares

Osqui
osqui_3m@yahoo.es

Tamaño: 428 B
Este programa sumas los pares y los impares
http://www.mygnet.com/pages/down.php?cod=1704

Numero Perfecto

Osqui
osqui_3m@yahoo.es

Tamaño: 399 B
Muestra siun numero es perfecto
http://www.mygnet.com/pages/down.php?cod=1703

Cambia De Mayúscula A Minúscula
Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 346 B
Cambia de mayúscula a minúscula
http://www.mygnet.com/pages/down.php?cod=1695

Análisis numéricos

Adivinar Un Numero
Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 452 B
Programa que genera un numero aleatorio para ser adivinado y dice los intentos que se realizaron para obtenerlo.
http://www.mygnet.com/pages/down.php?cod=1696

Genera Un Numero Determinado De Números Primos
Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 379 B
Programa que genera un numero determinado
http://www.mygnet.com/pages/down.php?cod=1694

Máximo Común Divisor
Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 369 B
Máximo común divisor
http://www.mygnet.com/pages/down.php?cod=1693

Mínimo Común Múltiplo
Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 384 B
Minimo comun multiplo
http://www.mygnet.com/pages/down.php?cod=1692

Sistemas De Numeración ... Del Binario Hasta En Nonagésimo Sistema ...
Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 585 B
Sistemas de numeración... del binario hasta en nonagésimo sistema...
http://www.mygnet.com/pages/down.php?cod=1691

Juegos

Barco
Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 2 KB
Barco
http://www.mygnet.com/pages/down.php?cod=1707

Juego Del Ahorcado --colgado
Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 26 KB
Juego del ahorcado --colgado
http://www.mygnet.com/pages/down.php?cod=1690

Juego De Una Rana
Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 5 KB
Juego de una rana
http://www.mygnet.com/pages/down.php?cod=1689

Matrices y vectores

Serie
Osqui
osqui_3m@yahoo.es

Tamaño: 430 B
Genera la serie 1-2-4-7...n
http://www.mygnet.com/pages/down.php?cod=1702

Serie
Osqui
osqui_3m@yahoo.es

Tamaño: 426 B
Genera la serie 1-3-6-10...n
http://www.mygnet.com/pages/down.php?cod=1701

Par Impar
Osqui
osqui_3m@yahoo.es

Tamaño: 463 B
Verifica si existen pares o impares dentro de un vector
http://www.mygnet.com/pages/down.php?cod=1700

Punteros

Punteros
Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 418 B
Nombre matricula y asignaturas de n alumnos con estructura y punteros
http://www.mygnet.com/pages/down.php?cod=1717

Mayúscula, Minúscula O Digito

Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 380 B
//realizar un programa que determine cual de los siguientes caracteres leídos es una letra mayúscula, una letra minúscula, un digito o un carácter no alfanumérico
http://www.mygnet.com/pages/down.php?cod=1716

Descuentos En Productos Segun Cantidad

Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 335 B
Descuentos en productos segun cantidad 100 - 40% ente 25 y 100 25%
http://www.mygnet.com/pages/down.php?cod=1715

Cuenta Las Vocales

Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 502 B
Realiza un programa, que pida por teclado el nombre de una ciudad, y nos visualice el número total de vocales. (trabajar con punteros y con asignación dinámica de memoria)
http://www.mygnet.com/pages/down.php?cod=1714

Mayor De Dos Matrices Con Punteros

Evelyn Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 585 B
Mayor de dos matrices con punteros
http://www.mygnet.com/pages/down.php?cod=1698

Menu Con Punteros

Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 1 KB
Hacer un menu que permita dado un vector: ordenar, insertar, eliminar y buscar, y que sea repetitivo hasta pulsar la opcion salir con asignacion dinamica
http://www.mygnet.com/pages/down.php?cod=1697

Recuperar información

Multiplo De Un Numero

Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Tamaño: 235 B
Introducimos un numero y luego otro para comparar si uno es multiplo de otro o no
http://www.mygnet.com/pages/down.php?cod=1718

Lenguaje Css

Varios

Maquetando Con Css

Jorge Alberto Rojas Solórzano
rojasjorgealberto@gmail.com

Tamaño: 77 KB
Un código completo xhtml y css de como maquetar un sitio web, tan sencillo que hasta mi abuelita juana podría hacerlo!!!
http://www.mygnet.com/pages/down.php?cod=1753

Manipulación de imagen

Imagen De Sustitución Con Css

Jorge Alberto Rojas Solórzano
rojasjorgealberto@gmail.com

Tamaño: 70 KB
Un truco que se hace "supuestamente con javascript" pero he aquí un truco para hacerlo con dos simples imagenes + css
http://www.mygnet.com/pages/down.php?cod=1747

Barra de scroll

Scroll En Iexplore

Ugp –ulises–
gallardo_giva@yahoo.com.mx

Tamaño: 4 KB
Cambiar el color de las barras de desplazamiento
http://www.mygnet.com/pages/down.php?cod=1754

Graficación

Caja Bonita

Ugp –ulises–
gallardo_giva@yahoo.com.mx

Tamaño: 12 KB
Ejemplo de una caja con bordes diferentes, incluso, con esquinas no convencionales
http://www.mygnet.com/pages/down.php?cod=1721

Lenguaje Delphi

Monitorización

Codigo Para Grabar Un Log Con Las Aplicaciones

Daniel Serrano
darnaldo@hotmail.com

Tamaño: 446 B
Este codigo solo necesitan declararlo y el mismo creara dentro de la carpeta donde corran el aplicativo una de nombre log y grabará una con el nombre del día luego solo necesitaran declararla y

grabará lo que ustedes quieran que alamacen, tambien sirve para depurar. suerte!
http://www.mygnet.com/pages/down.php?cod=1734

Lenguaje Ensamblador

Fecha y hora

Reloj En Ensamblador

Diana Corrales Torres
dvct332@hotmail.com

Tamaño: 842 B
Programa que implementa un reloj en tiempo real, y cuenta las veces que se ha pulsado f10. el programa termina al pulsar esc.
http://www.mygnet.com/pages/down.php?cod=1750

Conexiones remotas

Modulo Usart De Pic16f877a

Daniel Enrique Velazquez Borja
dvelazquez@linuxmail.org

Tamaño: 1 KB
Programa que lee un byte de 8 bits sin bit de paridad con velocidad de recepcion a opcion del programador. el valor del byte leido acciona diferentes funciones en un segundo microcontrolador 16f84a que produce la accion correspondiente en los motores. se compila con mpasm de microchip por facilidad con los valores de include. el codigo para comunicacion con la pc lo encuentras en la seccion de lenguaje c.
http://www.mygnet.com/pages/down.php?cod=1706

Lenguaje FlashCom

Efectos y filtros

Kursores

Herick
trolmagic@hotmail.com

Tamaño: 64 KB
Unos kursores para su makina y no este tan monotona.
http://www.mygnet.com/pages/down.php?cod=1705

Lenguaje Fox pro

Animaciones

Marquesina En Vfp

Juan Francisco González Pinzón
jfpanchogp@gmail.com

Tamaño: 33 KB
Permite hacer marquesinas con opciones en vfp
http://www.mygnet.com/pages/down.php?cod=1744

Lenguaje J2se

Monitorización

Calidad Del Enlace

Ismael
elclon3000@hotmail.com

Tamaño: 302 KB
Este pequeño programa realizado en java, hace uso de un cierto numero de ping lanzado en windows , luego se calcula un promedio con el proposito de calcultar la calidad en el enlace a traves del reatardo obtenido, luego es guardado en una base de datos ping, con 2 tablas, para realizar su respectiva consulta, esta bdd esta hecha en mysql 4.01, usuario:root, psw: sistemasups. se debe ejecutar el archivo .jar para observar su ejecucion, o si desea tambien adjunto sus *.java, tomar en cuenta que debe importar la bdd q tambien esta en el comprimido
http://www.mygnet.com/pages/down.php?cod=1729

Lenguaje Java

Criptografía

Codificacion Y Decodificacion De Frases

Hugo
hugomora34@hotmail.com

Tamaño: 2 KB
El siguiente programa permite la codificación y decodificacion de frases. características: - la forma de codificación del programa es tomar la letra que le sigue cinco posiciones en el código ascii, por ejemplo: la primera letra es la 'a', que será reemplazada por la letra que le sigue cinco posiciones (a,b,c,d,e,f), es decir, la 'f'. el símbolo del espacio se sustituye por %, etc.
http://www.mygnet.com/pages/down.php?cod=1745

Matrices y vectores

Matriz Transpuesta, Matriz Inversa, Determinante De Una Matriz Y Sistemas De Ecuaciones

Hugo
hugomora34@hotmail.com

Tamaño: 2 KB
El siguiente programa permite obtener la matriz transpuesta de una matriz de mxn (m=filas, n=columnas) además se puede obtener la inversa de una matriz de mxm (filas=columnas). también se puede obtener el determinante de una matriz de orden mxm. solo se puede hallar el determinante y la inversa de una matriz cuadrada (el numero de filas es igual al numero de columnas). finalmente el programa permite obtener la solucion a un sistema de 3 ecuaciones con tres incognitas por el metodo de

determinantes. nota: si se modifica el codigo fuente se puede resolver un sistema de n ecuaciones por n incógnitas. el programa contiene un menú que permite una mejor interaccion entre el usuario y el programa. como dato adicional, este software está hecho usando librerías, la una contiene las operaciones y la otra contiene el ingreso de datos, todos los ingresos de datos están validados con la opción: try { }catch { } para ejecutar el programa se deben compilar las dos librerías y ejecutar el archivo trans_inv_det.java, ya que este archivo es el que contiene el main. espero que les sirva.
http://www.mygnet.com/pages/down.php?cod=1713

Lenguaje Javascript

Manipulación objetos

Opentag

Mandm
mandm_mini@hotmail.com

Tamaño: 2 KB
Función para crear elementos html en tiempo de ejecución, así como darles atributos.
http://www.mygnet.com/pages/down.php?cod=1723

Lenguaje Macros

Varios

Macros En Vb Para Excel Quiniela Alemania 2006.

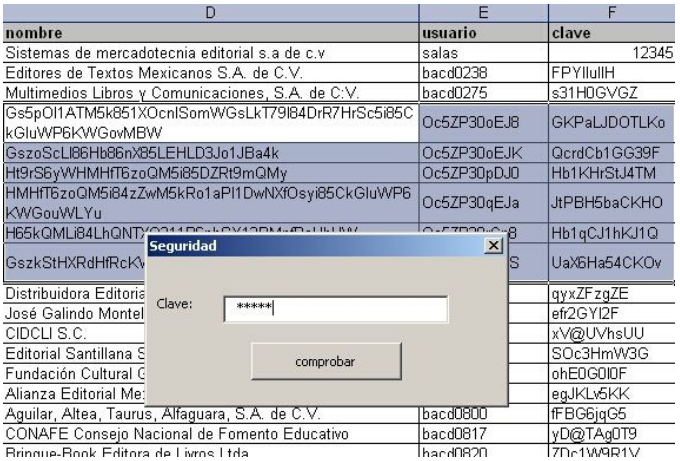
Martin R. Mondragón Sotelo
mygnet@gmail.com

Tamaño: 37 KB
Es un pequeño código hecho en macros para excel, para calcular los primeros lugares de los jugadores con aciertos más altos de los partidos de alemania 2006. hay tres hojas, la primera es para los participantes de la quiniela con sus pronósticos, la segunda es para los resultados de los equipos y la tercera muestra las posiciones según los aciertos de cada participante... se ejecuta la macro al hacer ctrl.+a. espero que este pequeño código sirva como base para hacer otras cosas interesantes...
http://www.mygnet.com/pages/down.php?cod=1725

Criptografía

Macro Para Cifrar Y Decifra En Base64

Martin R. Mondragón Sotelo
mygnet@gmail.com



Tamaño: 15 KB
Este es un pequeño codigo fuente en macros para excel, cifra y decifra en base 64, selecciona las celdas que hay que cifrar y presionamos ctr+e y aparece una venta que nos piede una contraseña: esta en texto plano: la contraseña es: yes01 y para decifrar es el mismo procedimiento.... ctr+d para decifrar...
http://www.mygnet.com/pages/down.php?cod=1738

Apis

Uso De Api Para Abrir El Diálogo De Archivos

Gustavo Alberto Rodriguez
gustavo@sasoft.com.ar

Tamaño: 48 KB
Archivo access con un formulario que permite buscar un archivo de imágen cuya ubicación se guarda en la base de datos. usa un módulo que se puede encontrar en http://www.mygnet.com/pages/down.php?cod=887
http://www.mygnet.com/pages/down.php?cod=1749

Datos externos

Macro Excel Vs Txt

Hans Abel
hansabel@hotmail.com

Tamaño: 8 KB
Pequeño macro que envia datos a un arhivo txt y viceversa
http://www.mygnet.com/pages/down.php?cod=1726

Lenguaje Matlab

Análisis numéricos

Integración Por El Método Simpson 1/3

Erik
erikalto@gmail.com

Tamaño: 491 B
Por este método puedes integrar la función que desees, poniendo los valores inicial y final y el número de trapecios a usar para el cálculo
http://www.mygnet.com/pages/down.php?cod=1746

Manipulación de imagen

Suma De 2 Imagenes

Patricio Villalobos R.
wothoti@hotmail.com

Tamaño: 103 KB
Sumar de 2 imagenes rgb y se crea una 3ra imagen con la fusion de las 2 imagenes, solo llaman a la funcion los nombres de las imagenes estan dentro del codigo de la función.
http://www.mygnet.com/pages/down.php?cod=1712

Cambia Imagen De Color A Escala De Grices

Patricio Villalobos R.
wothoti@hotmail.com

Tamaño: 253 B
Funcion para tranformar una imagen en colores rgb en escala de grices
http://www.mygnet.com/pages/down.php?cod=1711

Graficación

Grafica Con Movimiento

Erik
erikalto@gmail.com

Tamaño: 2 KB
Con este programa podrás graficar funciones trigonométricas, exponenciales y polinomiales dandoles moviento, asi como tambien series de fourier aunque estas sin movimiento.
http://www.mygnet.com/pages/down.php?cod=1748

Lenguaje Php

Formularios

Calculadora Básica En Php

Emanuel
emax_093@hotmail.com

Tamaño: 2 KB
Aquí les dejo el codigo de una simple calculadora hecha en php.
http://www.mygnet.com/pages/down.php?cod=1730

Lenguaje Prolog

Varios

Solución Al Problema De Los Frascos En Prolog

Landanohr
landanohr@hotmail.com

Tamaño: 1,016 B
Solución en polog al problema de los frascos venenosos del químico despistado.
http://www.mygnet.com/pages/down.php?cod=1708

Compiladores e intérpretes

Prolog Ejemplos

David Israel Silva
kaliumdavid@gmail.com

Tamaño: 3 KB
Buenos ejemplos de prolog que encontre en internet
http://www.mygnet.com/pages/down.php?cod=1709

Lenguaje Vb

Locker

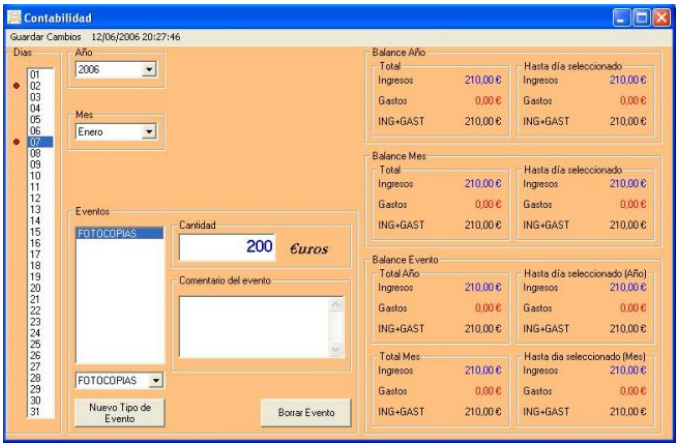
Giorgio Ivan Acosta Jaramillo
acosta_901106@hotmail.com

Tamaño: 15 KB
Es un programa no un codigo, lo publique aqui para que me puedan dar su opinon o sus comentarios. es un programa que yo acabo de hacer y lo que hace es pedir una contraseña y despues uno puede bloquear su computador, para mi es muy bueno sobre todo por la parte grafica.
http://www.mygnet.com/pages/down.php?cod=1732

Manejo de base datos

Contabilidad

José Manuel Acemel Gómez
acemel@hotmail.com



Tamaño: 16 KB
Para llevar comodamente y de manera visual las cuentas. gastos, ingresos, y llevar el control de cada evento
http://www.mygnet.com/pages/down.php?cod=1720

Cálculo y conversiones

Numeros A Nº Romanos

José Manuel Acemel Gómez
acemel@hotmail.com

Tamaño: 809 B
Eso, pasa un numero a numeros romanos no adjunto foto pq solo tiene 1commandbu tton y 2 textbox
http://www.mygnet.com/pages/down.php?cod=1724

Multimedia

Reproductor De Musica3

David Ordinola
davidordinola@yahoo.es

Tamaño: 17 KB
Y un ultimo codigo para musica, interesantes todos estos codigos
http://www.mygnet.com/pages/down.php?cod=1737

Reproductor De Musica2

David Ordinola
davidordinola@yahoo.es

Tamaño: 128 KB
Otro codigo interesante para cargar y escuchar musica
http://www.mygnet.com/pages/down.php?cod=1736

Reproductor De Musica1

David Ordinola
davidordinola@yahoo.es

Tamaño: 170 KB
Un codigo interesante para cargar y escuchar musica
http://www.mygnet.com/pages/down.php?cod=1735

Formularios

Mails Anonimos

David Ordinola
davidordinola@yahoo.es

Tamaño: 24 KB
Para que aprendas a enviar mails anonimos todo hecho en vb6
http://www.mygnet.com/pages/down.php?cod=1688

Lenguaje Vb.net

Manipulación objetos

Crear Una Dll En Net

David Ordinola
davidordinola@yahoo.es

Tamaño: 29 KB
Este codigo es bastante ilustrativo y bien util, pueden copiarlo para muchas cosas
http://www.mygnet.com/pages/down.php?cod=1743

.net

2ejemplo Xml Y .net

Boris
bormarduk@yahoo.com.ar

Tamaño: 13 KB
2er ejemplo complemento del articulo
http://www.mygnet.com/articulos/vb.net/744/
http://www.mygnet.com/pages/down.php?cod=1752

1ejemplo Xml Y .net

Boris
bormarduk@yahoo.com.ar

Tamaño: 14 KB
1er ejemplo complemento del articulo
http://www.mygnet.com/articulos/vb.net/744/ visual studio 2003
http://www.mygnet.com/pages/down.php?cod=1751

Condicionar Una Salida

Juan Francisco Berrocal
berrocal239@hotmail.com

Tamaño: 51 KB
Este codigo muestra como preguntar al usuario si desea salir de nuestro sistema, el cual podra elegir "si" o "no"
http://www.mygnet.com/pages/down.php?cod=1710

Seguridad informática Capitulo III: Aplicaciones Criptográficas

Autor:Gustavo Santiago L
gustavo@mygnet.com
País: MÉXICO

Personalidad: Me considero una persona, trabajadora, amigable, trato de ser optimista y de verlo lo mejor a la la vida. **| Nivel de estudios:** Licenciatura o profesional | **Área de estudio:** Sistemas Computacionales | **Objetivo(s):** Seguir mejorándome día a día y no quedarme estancado. | **Experiencia laboral:** 2001-2003 - Tecnológico en Computación premier. Profesor. 2003-2004.- Jefe de laboratorio de innovación informática de la SEP | **Actividades:** Programación de sistemas, Consultoría, Instalaciones y actualizaciones de servidores | **Conocimientos:** Diseño de base de datos relacionales. Programación en C++,VC++, Perl, PHP,ASP, VB, JavaScript,... | **Idioma(s):** ingles 85%

Seguridad informática Capitulo III: Aplicaciones Criptográficas

Hoy en día se dispone de algoritmos de cifrado que e consideran relativamente seguros, como DES, IDEA o RSA, por citar algunos ejemplos. Pero en que y como podemos utilizar este tipo de cifrado.

Procesos comunes, que se realizan durante un día, como por ejemplo cuando dos amigos quieren ir al cine pero no se ponen de acuerdo en que película ver, entonces utilizan un volado para poder tomar la decisión. Si están uno en frente del otro, no hay problema, pero que tal si esto sucede por medio de una conversación telefónica, no hay manera de verificar el volado en forma remota.

Los protocolos criptográficos son la solución a este tipo de situaciones.

Definición de protocolo

Un protocolo es un acuerdo entre dos o mas partes para realizar algo especifico.

Características de un protocolo:

- Resuelve un cierto problema o produce un cierto resultado.
- Consiste en una seria de pasos bien definidos. Bien definido significa que cubre todas las posibles situaciones que pueden surgir durante su ejecución. En todo momento debe ser claro lo que hay que hacer a continuación. Los pasos tienen que ser conocidos por anticipación, además el protocolo debe finalmente terminar.
- Involucra a dos o más partes.
- Todas las partes involucradas conocen el protocolo y están de acuerdo en seguirlo.
- Defina claramente lo que cada parte gana o expone con su ejecución.

Notación

No existe una notación para describir un protocolo en forma tal que todo el mundo lo entienda, así que denotaremos:

A Primer participante del protocolo
B Segundo participante
I Intruso malicioso que intenta atacar el protocolo, A → B o ambos.
S Tercera parte confiable que actúa como árbitro y en la que A y B confían.

Tipos de protocolos

Básicamente, existen tres tipos de protocolos: arbitrados, adjudicados y autoimplementados.

Arbitrados

Un protocolo arbitrado se basa en una tercera parte confiable para realizarse. El árbitro no tiene ningún tipo o forma de preferencia por ninguna de las partes involucradas.

Un ejemplo es cuando **A** quiere vender su auto a **B** y este desea pagar el auto con un cheque. **A** no conoce a **B** y no confía en que su cheque sea bueno. A no quiere dar el auto a **B** hasta que el banco no haya aprobado el cheque.

Por otro lado, **B** no confía en **A** y no quiere dar el cheque hasta no tener los papeles y las llaves del auto.
S puede ser un abogado que permite realizar la operación de compra venta del auto de forma segura entre **A** y **B**

El protocolo del ejemplo puede escribirse:

A entrega los papeles y las llaves del auto a **S**
B entrega el cheque a **A**
A deposita el cheque en el banco

Si el cheque es bueno, **S** entrega los papeles y las llaves del auto a **B**.
Si el cheque es malo, **S** regresa los papeles y las llaves del auto a **A**.
Desde luego, en caso de que el cheque sea malo, **A** tiene que mostrar pruebas de ello a **S**.

Adjudicados

Los protocolos adjudicados son una variante de los arbitrados. También se basan en una tercera parte confiable, pero esta parte, sin embargo no siempre es requerida.

Las parte involucradas tal como esta especificado. Si todas las partes respetan el protocolo, el resultado se logra sin ayuda de la tercera parte, usualmente llamada adjudicador.

Solo en el caso de que una de las partes involucradas piense o crea que las otras partes hacen trampa, se involucra el adjudicador como ayuda. El adjudicador analiza la disputa y las reglas y dice quien esta actuando bien y que es lo que se debe de hacer.

Ejemplo:

A entrega las llaves y los papeles a **B**
B entrega el cheque a **A**

Si el cheque no es bueno, o si los papeles son falsos, **A** y **B** comparecen ante un juez y ambos presentan sus evidencias. El juez juzga las evidencias y la parte que engaña es penalizada.
Una desventaja de este tipo de protocolos es que juzgar la disputa no siempre es sencillo por que dependen de la calidad de las evidencias, pero es tarea del protocolo producir buenas evidencias. Otro aspecto importante es la penalidad, la cual tiene que ser lo suficiente dura para desalentar la posibilidad de engaño.

Autoimplementados

Son los mejores protocolos. Se diseñan de tal manera que hacen virtualmente imposible el engaño. No requieren ni arbitro ni juez. Garantizan que cualquier participante en el protocolo hace un engaño, el engaño es descubierto inmediatamente por el otro u otos participantes.

En un mundo ideal, todos los protocolos deben ser autoimplementados, pero no todos los problemas tiene una solución de este tipo y, además, la mayoría de este tipo de protocolos requieren una cantidad de trabajo considerable para todos los participantes. Estas razones hacen que comúnmente se usen protocolos arbitrados y, sobre todo, adjudicados.

Protocolos criptográficos para implementar servicios de seguridad.

Una de las principales aplicaciones de la criptografía a la seguridad en cómputo y comunicaciones, es su capacidad de utilización para implementar servicios de seguridad tales como confidencialidad, autentificación, integridad y no repudio.

El servicio mas utilizado a lo largo del tiempo con técnicas criptográficas es la confidencialidad, después la autentificación, en estos dos servicios podemos usar criptografía simétrica o asimétrica.

Otro servicio fundamental es la verificación de integridad, las funciones Hash son las herramientas naturales para lograr esto. Para estos servicios es posible implementar soluciones que combinan dos o más técnicas criptográficas de la mejor manera para lograr seguridad y eficiencia.

El no repudio es un servicio que se implementa fundamentalmente utilizando una herramienta derivada de los esquemas de llave pública y privada conocida como firma digital.

Utilizando los algoritmos de cifrado para obtener los servicio de seguridad

DES

Confidencialidad con DES

Situación; **A** requiere enviar de manera secreta, el mensaje **M** a **B**

Para esta situación ocuparemos el algoritmo de criptografía simétrica DES, para ello se requiere que a y B compartan una llave de cifrado la cual nombraremos K_{ab}

Protocolo:

1. **A** cifra **M** usando DES con la llave K_{ab} y produce el texto cifrado **C**.
2. **A** envia **C** a **B**
3. **B** descifra **C** usando DES con la llave compartida K_{ab} y obtiene **M**.

Este protocolo funciona y es confiable por que nadie mas que **A** y **B** conocen la llave K_{ab} y, por tanto nadie mas puede leer el mensaje **M**.

Autentificación con DES

Otra situación es cuando **A** requiere enviar un mensaje **M** a **B**, pero de tal manera que **B** pueda estar seguro que solamente A pudo haber originado el mensaje **M**.

Para ello se requiere que **A** y **B** hayan acordado previamente una llave K_{ab}. El protocolo para resolver esta situación es el mismo que el anterior puesto que **A** y **B** comparten el conocimiento sobre la llave K_{ab}, **B** sabe que **A** es la única identidad que pudo haber generado **C**. este tipo de autentificación es unidireccional y directa entre dos partes.

Integridad con DES

A requiere enviar un mensaje **M** a **B**, pero de modo que **B** pueda estar seguro que **M** no fue modificado durante el trayecto.

Protocolo:

1. **A** cifra **M** usando DES con la llave K_{ab} y produce un texto cifrado **C**.
2. **A** cifra **M** usando DES con la llave K_{ab} y usando el modo CBC obtiene un MAC de 64 bits.
3. **A** envía **C** y el MAC de 64 bits a B.
4. **B** descifra **C** usando DES con la llave K_{ab} y obtiene **M**.
5. **B** cifra **M** usando DES con la llave K_{ab} y usando el modo CBC obtiene un MAC de 64 bits.
6. **B** compra los MAC's. si coinciden, verifica con ello la integridad de **M**.

B puede asegurar que **M** no fue modificado durante el trayecto por que los MAS's coinciden.

Problemas con la criptografía simétrica

El problema para implementar criptografía simétrica para implementar los servicios anteriores esta en que previamente hay que acordar una llave K_{ab} para cada pareja de usuarios. Esto se convierte en una pesadilla en cuanto al manejo de llaves, ya que para **n** usuarios se requieren n(n-1)/2 llaves.

Otro problema es la distribución de esas llaves compartidas, ya que se deben distribuir de manera segura tales como mensajería o correo certificado o alguna forma confiable. Otro problema lo constituye el hecho de que las llaves tienen que ser cambiadas frecuentemente, la razón es la cantidad de información útil que un criptoanalista obtiene, es proporcional al número y longitud de mensajes cifrados con la misma llave.

RSA

Confidencialidad con RSA

A desea enviar, de manera secreta el mensaje M a B pero ahora utilizando un algoritmo de llave de llave publica para cifrar.

Para ello se requiere que, previamente, cada parte haya generado su pareja de llaves (pública, privada) y que las llaves públicas de ambos sean públicamente accesibles.

Protocolo:

1. **A** cifra **M** usando RSA con la llave publica de **B** y produce un texto cifrado **C**.
2. **A** envía **C** a **B.**
3. **B** descifra **C** usando RSA y su propia llave privada para obtener **M**.

Proporciona confidencialidad por que nadie más que **B** puede descifrar **C** y obtener **M** puesto que solo **B** tiene su propia llave privada.

El problema es que, a diferencia de con la llave simétrica, **B** no puede estar seguro que el mensaje **C** haya sido originado por **A**, puesto que cualquiera pudo haber usado la llave publica de **B** para cifrar **M** y enviarlo. Este protocolo proporciona confidencialidad pero no autentificación.

Autentificación con RSA

A requiere enviar un mensaje M a B, pero de tal manera que B pueda estar seguro que solamente A lo pudo haber originado.

Protocolo:

1. **A** cifra **M** usando RSA con su propia llave privada y produce el texto cifrado **C**.
2. **A** envía **C** a **B**.
3. **B** descifra **C** usando RSA y la llave publica de **A** para obtener **M**

Este protocolo proporciona autentificación, ya que nadie más que **A** pudo haber cifrado **M** con la llave privada de **A** para obtener **C**, puesto que el único que conoce la llave privada de **A**, es precisamente **A**. es problema es que no proporciona confidencialidad puesto que cualquiera puede utilizar la llave publica de **A** para conocer **M**.

Ahora existirá un protocolo, o se podrá construir uno, que incluya los dos servicios, confidencialidad y autentificación en el mismo protocolo. La respuesta es si, y no solo eso también se puede agregar el servicio de integridad en el mismo protocolo.

Confidencialidad, autentificación e integridad con RSA

A desea enviar de manera secreta el mensaje **M** a **B**, pero de tal manera que **B** pueda estar seguro que solo **A** pudo haber originado el mensaje y, además, que el mensaje no haya sido alterado durante el trayecto.

Supóngase que tanto **A** como **B** han generado su pareja de llaves y las llaves públicas son públicamente accesibles. También se debe de asumir que ambas partes acuerdan el uso de la una función hash **h**, MD5 y que es públicamente disponible.

Protocolo:

1. **A** calcula el valor hash de **M**, **h**(**M**)
2. **A** cifra **h**(**M**) usando RSA con su propia llave privada y produce el equivalente a una firma **s** de **h**(**M**)
3. **A** cifra **M** con la llave publica de **B** y produce **C**
4. **A** envía **s** y **C** a **B**
5. **B** descifra **C** usando RSA con su propia llave privada, para obtener **M**
6. **B** calcula el valor hash de **M**, **h**(**M**)
7. **B** descifra s usando RSA y la llave publica de **A** para obtener el **h**(**M**) que genero **A** en el paso 1
8. **B** compara los resultados has, el que él calculo con el que recibió de **A**

Este protocolo proporciona confidencialidad, autentificación e integridad. Confidencialidad por que **M** viaja cifrado con la llave publica de **B** y nadie mas que **B** puede descifrarlo y leerlo, autentificación por que nadie mas que **A** pudo haber cifrado (firmado) **h**(**M**), ya que **A** es el único que posee la llave privada de **A**. integridad por que al recibir cifrados **M** y **h**(**M**), puede descifrarlos y hacer el mismo calculo sobre **M** y verificar los resultados hash. Si coinciden, esta seguro que el mensaje no ha sido alterado durante el trayecto.

Soluciones y problemas con la criptografía Asimétrica

Distribución de llaves

De alguna manera los sistemas de llave pública ayudan a resolver el problema del acuerdo de llaves de los sistemas simétricos, esto se debe a que:

- El número de llaves a distribuir en una comunidad se reduce significativamente cuando se usan este tipo de esquemas en lugar de esquemas de llave simétrica.
- Una comunidad de n entidades solo requiere n llaves publicas y n llaves privadas, es decir un total de 2n llaves, contra n(n-1)/2 que se requieren en los esquemas de llave simétrica.
- No se requiere confidencialidad en la distribución de las llaves públicas.

Problemas:

- El problema es el ataque conocido como hombre en medio el cual se logra sustituyendo la llave publica de la persona a ser atacada (**B**), así al enviar algo con una llave falsa a otra persona (**A**) este creerá que es del destinatario correcto (**B**) y cuando quiera enviar un mensaje privado lo enviará con la llave cambiada (**I**) y entonces el intruso podrá ver el mensaje secreto.

Consideraciones:

Los algoritmos de llave simétrica como DES, IDEA son mucho mas rápidos que los de llave asimétrica como RSA. Entonces como aprovechamos las ventajas de la criptografía de llave asimétrica para la distribución de llaves y de la criptografía simétrica para el cifrado masivo. La respuesta es usar esquemas híbridos como el PGP.

Sistemas híbridos

Estos sistemas combinan la criptografía de llave simétrica con la de llave asimétrica, cada una tiene una funcionalidad en el diseño y operación del protocolo:

- Se usa un algoritmo de llave publica para cifrar (y descifrar) una llave compartida (como una llave DES)
- Se cifra un mensaje con esa llave compartida
- El mensaje cifrado y la llave compartida se cifran con la llave pública y se envían.
- El receptor usa el algoritmo de llave publica acordado para descifrar la llave compartida y luego usa esa llave descifrada para descifrar el mensaje.

Firmas Digitales

Las transacciones de dinero son muy comunes en la vida real pero como pasamos eso al mundo digital, se podría hacer con un cheque digital. De forma convencional un cheque tiene las siguientes características:

- Es un objeto tangible que autoriza una transacción bancaria.
- La firma del cheque confirma la autenticidad, por que solo el firmante legitimo puede producir esa firma.
- En caso de falsificación, una tercera parte puede intervenir para juzgar la autenticidad.
- Un cheque puede ser cancelado, de tal modo que no se pueda usar.
- El papel de un cheque es inalterable; la mayoría de las alteraciones son detectables con facilidad.

Los objetos tangibles no existen para transacciones en computadoras, por lo que la autorización de pagos por computadora requiere un modelo distinto.

La transacción en un mundo digital podría ser la siguiente:

- **A** envía a su banco un mensaje autorizando una transferencia para **B**.
- El banco de **A** debe ser capaz de verificar y probar que el mensaje viene de **A**, para protegerse de que mas tarde **A** puede negar haber enviado el mensaje.
- El banco también desea asegurarse que el mensaje es íntegramente el que **A** envió, es decir, que no haya sido alterado durante el viaje.
- **A** desea asegurarse que el banco no pueda falsificar el mensaje.
- Ambas partes, **A** y el banco, desean asegurarse que el mensaje es nuevo, que no es un reuso de un mensaje previo y que no ha sido alterado durante la transmisión.

La naturaleza electrónica de las señales en lugar de papel, hace difícil esa transacción. El problema aquí consiste en como implementar digitalmente el equivalente al concepto de firma autógrafa con las características que esta tiene:

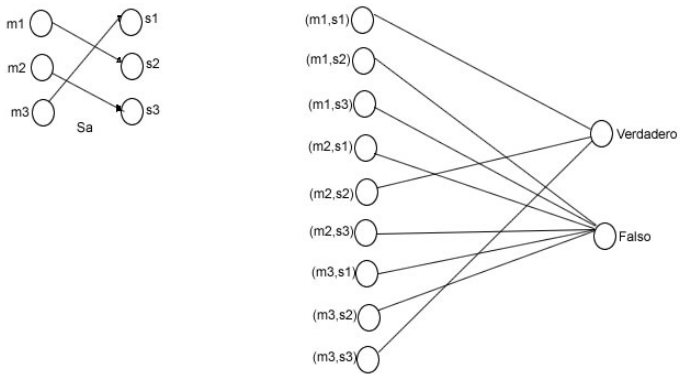
- **Autentica**.- convencer al receptor del documento firmado que el firmante deliberadamente firmó el documento.
- **Infalsificable**.- probar que el firmante, nadie mas, firmó el documento.
- **No reusable**.- la firma es parte del documento no se puede mover a otro.
- **Inalterable**.- después de firmado el documento, no puede alterarse.
- **No repudiada**.- el firmante no puede negar la firma.

En el mundo de las computadoras surgen problemas adicionales: los archivos y documentos son fáciles de copiar, el texto se puede cortar y pegar en otro documento, los archivos y documentos son fáciles de modificar, etc.

Pasar estas características al mundo digital fue un problema sin solución hasta la aparición de la criptografía de llave pública en 1972.

Al comprender a fondo las implicaciones de los esquemas de llave pública; el problema parece sencillo: los esquemas de llave pública involucran dos llaves, una publica y otra privada, donde la primera puede ser conocida por cualquiera y la segunda solo la debe conocer el dueño de ella; es decir, esta ultima es un elemento propio del poseedor de la llave. Las transformación de cifrado relaciona de manera única el texto en claro, la función de cifrado y la llave, que solo puede ser "destransformado" por medio de otro elemento único que es la otra llave.

De acuerdo a lo anterior, una firma digital consiste en una transformación, por medio de una función de firma, que relaciona de forma única el documento o archivo con esa función de firma y un elemento propio de la identidad del firmante que es la llave de firma (esta llave debe ser privada).



Funcion de firma y verificacion para un esquema de firma digital

La firma digital consiste de dos procesos: el proceso de firma y el de verificación de la firma. Una vez aplicada la transformación de firma al documento, se obtiene como resultado la firma digital. Esta se envía, junto con el documento, a la parte interesada, que es quien debe verificar la validez de la firma digital usando la otra llave (la

llave pública). Si la verificación es valida, la firma se acepta como buena; de lo contrario, se rechaza.

El proceso de verificación se realiza aplicando una función de verificación a la firma por medio de una llave de verificación (la llave pública). Como resultado de esa verificación debe obtenerse sólo uno de dos posibles valores: verdadero o falso.

Los proceso de firma y verificación pueden resumirse de la siguiente manera:

Proceso de firma:

- **A** (el firmante) crea una firma digital **s** para un mensaje **M**, de la siguiente manera:
  - **A** calcula $s=S_A(M)$, donde s es la firma de **A** sobre el mensaje **M** con la función de firma S_A.
  - **A** envía a **B** la pareja (**M**,**s**)

Proceso de verificación

- **B** (el verificador) verifica que la firma s sobre el mensaje **M** haya sido creada por **A**, de la siguiente manera:
  - Obtiene la función de verificación V_A de **A**
  - Calcula $v=V_A(M,s)$
  - Acepta la firma como creada por **A** si **v**=verdadero, y la rechaza si **v**=falso.

Las funciones S_A y V_A se caracterizan por una llave: existen algoritmos de firma y verificación públicamente conocidos identificados cada uno por una llave. Normalmente S_A se caracteriza por una llave privada que mantiene en secreto y V_A por una llave pública, conocidas como llaves de firma y verificación, respectivamente.

La fortaleza de seguridad de estos esquemas de firma digital es que es computacionalmente infactible para cualquier entidad distinta de **A**, hallar algún mensaje **M** y una firma s tal que se cumpla que $V_A(M,s)$=verdadero.

Aunque la firma digital se basa en esquemas de llave publica, la transformación o función de firma no tiene por que ser una transformación de cifrado, ni la función de verificación tiene que se una de descifrado. Aunque es posible utilizar la misma pareja de llaves para criptografía de llave publica que para firma digital. Se recomienda que no sea así. Lo recomendable es tener parejas distintas y esto es para evitar ataques de hombre en medio.

Una firma digital es entonces un protocolo que produce el mismo efecto que una firma autógrafa: es una marca que solo el firmante puede hacer (por que solo el posee la llave privada), pero otros pueden fácilmente reconocer (por que todos pueden la llave pública correspondiente) como perteneciente a la firma.

Una firma digital es un medio de relacionar información con la identidad de su originador. Los principales servicios de seguridad que proporciona la firma digital son: autentificación de identidad y de origen de datos, integridad y no repudio.

Una diferencia fundamental de la firma digital con respecto a la firma autógrafa es que esta ultima es independiente del mensaje es decir la misma firma se usa para firmar distintos documentos. La firma digital por el contrario, es dependiente del documento.

Firmas digitales y funciones Hash

Como se ha visto en los procesos de firma y verificación, al obtener la firma digital s, esta se envía al verificador junto con el documento **M** para ser verificada y, en su caso, aceptada como valida o rechazada como falsa.

El proceso de firma del documento **M** puede ser muy costoso en términos de proceso computacional y eficiencia. Por esta razón, lo que normalmente se firma y envía, es el resultado hash o valor de dispersión **h** de **M**, denotado como **h**(**M**). Desde luego, previamente las partes tienen que acordar, tanto las funciones de firma y verificación como la función de dispersión **h**.

De esta manera, un protocolo típico para que **A** firme digitalmente y envié a **B** la firma del documento **M**, usando la función de firma **S**, la función de verificación **V**, y la función de **h**, es el siguiente:

1. **A** calcula la función de dispersión del documento **M**, **h**(**M**).
2. **A** firma con su llave para firma (llave privada) el resultado **h**(**M**). es decir, obtiene $s=S_k(h(M))$.
3. **A** envía a **B** el documento y la firma. Envía **M** y **s**.
4. **B**, al recibir **M** y **s**, calcula **h**(**M**) y le aplica la función de verificación **V** a **s** usando la llave publica de **A**. calcula $v=V_K(s) = V_K(S_K(h(M)))$. Si **v** es el verdadero, acepta la firma **s** como valida; si **v** es falso, la rechaza.

Algoritmo Elgamal

Este algoritmo, que es el algoritmo en que se basa el estándar para firma digital, requiere que el mensaje a firmar **M** sea convertido a una cadena de bits de longitud arbitraria, utiliza una función de dispersión **h** y un numero primo **p** grande (mas de 512 bits).

Generación de llaves para Elgamal

- Cada parte debe crear una pareja de llaves pública y privada.
- **A** debe de generar un numero primo grande **p** y un generador α del grupo multiplicativo **Zp**.
- **A** debe seleccionar un numero entero aleatorio **a** tal que $1 \leq a \leq p-2$.
- **A** debe calcular el valor $y = \alpha^a \pmod p$
- La llave publica de **A** es (**p**, α, **y**). la llave privada de **A** es **a**.

Una vez realizado el proceso de generación de llaves anterior, los procesos de firma y verificación son los siguientes:

Proceso de firma para Elgamal

A debe hacer lo siguiente:

1. Seleccionar un número entero aleatorio y secreto **k**, tal que $1 \leq a \leq p-2$ de tal manera que el máximo común divisor de **k** y **p**-1 sea igual 1.
2. calcula el numero $r = \alpha^K \pmod p$
3. calcular $k^{-1} \pmod{p-1}$
4. calcular $s = k^{-1}(h(M)-ar) \pmod{p-1}$
5. La firma de **A** para el mensaje **M** es la pareja (**r**,**s**)

Proceso de verificación para Elgamal

Para verificar la firma (**r, s**) de **A**, el verificador **B** debe hacer lo siguiente:

1. Obtener la llave publica de **A**, (p, α, y)
2. Verificar que $1 \leq a \leq p-1$, si no se cumple esto rechaza la firma.
3. calcula $V_1 = y^r r^s \pmod p$
4. calcula $h(M)$ y $V_2 = \alpha^{(h(M))} \pmod p$
5. Acepta la firma como valida si y solo si $V_1 = V_2$

Para probar que la verificación es correcta se debe observar que, si la firma fue generada por **A** entonces:

$s = k^{-1}(h(M)-ar) \pmod p$

Si se despeja $h(M)$ y se tome como exponente de α, se obtiene lo siguiente:

$\alpha^{h(M)} = \alpha^{ar+ks} = (\alpha^a)^r (r)^s \pmod p$

de esta manera se observa que, en efecto, $V_1 = V_2$, ya que

$\alpha^{ar+ks} = \alpha^{ar}\, \alpha^{ks} = (\alpha^a)^r\, (\alpha^k)^s = (y)^r\, (r)^s$

Ejemplo de Elgamal:

Generación de llaves

- **A** escoge **p**=2357 y un generador $\alpha = 2$ de **Zp**
- **A** escoge su llave privada **a**=1751
- **A** calcula $y = \alpha^a \pmod p = 2^{1751} \pmod{2357} = 1185$
- La llave publica de **A** es: (**p**=2357, α=2, **y**=1185)

Generación de la firma

Para simplificar los mensajes serán enteros de **Zp** y $h(M) = M$. Para firmar el mensaje **M**=1463.

- **A** escoge un numero entero aleatorio **k**=1529
- **A** calcula $r = \alpha^k \pmod p = 2^{1529} \pmod{2357} = 1490$
- $K^{-1} \pmod{p-1} = 245$
- **A** calcula $s = 245\{1463-1751(1490)\} \pmod{2356} = 1777$
- La firma de **A** para **M**=1463, es la pareja (**r** =1490, **s** =1777)

Verificación de la firma

- **B** calcula $V_1 = y^r r^s \pmod p = (1185^{1490})(1490^{1777} \bmod 2357) = 1072$
- **B** calcula $h(M) = 1463$
- **B** calcula $V_2 = \alpha^{h(M)} \pmod p = 2^{1463} \pmod{2357} = 1072$
- **B** acepta como valida la firma de **A**, ya que $V_1 = V_2 = 1072$

Algoritmo DSA

Se ha convertido en el estándar Federal de procesamiento de información (FIPS 186) de Estados Unidos conocido como el estándar de firma digital (DSS), y es el primer esquema de firma digital reconocido por cualquier gobierno. Es una variante del esquema Elgamal.

Requiere de una función hash **h**: {0,1}→ **Zq** para un entero **q**. El DSA requiere de un algoritmo de hash seguro como el **SHA-1**.

Generación de llaves con DSA

Cada entidad debe generar su pareja de llaves. La entidad **A** debe hacer lo siguiente:

1. Seleccionar un numero primo **q** tal que $2^{159} < q < 2^{160}$
2. Escoger **t** tal que $0 \leq t \leq 8$, y seleccionar un numero primo p donde $2^{511+64t} < p < 2^{512+64t}$, con la propiedad que **q** divida a (**p**-1).
3. Seleccionar un generador α del grupo cíclico único de orden **q** en **Zp**
4. Seleccionar g ε Zp y calcular $\alpha = g^{(p-1)/q} \bmod p$
5. Si $\alpha = 1$, entonces regresar al paso 3.
6. Seleccionar aleatoriamente un entero a tal que $1 \leq a \leq q-1$
7. Calcular $y = \alpha^a \bmod p$.
8. La llave publica de A es (p, q, α, y). la llave privada de A es **a**.

Nota: en el algoritmo anterior, se debe seleccionar primero el numero primo **q** y entonces intentar hallar un numero primo **p** de tal manera que **q** divida a (**p**-1).

Generación de firma y verificación con DSA

La entidad **A** firma una cadena de binaria de longitud arbitraria que representa el mensaje **M**. La entidad **B** puede verificar esta firma usando la llave pública de **A**.

Generación de la firma.- La entidad **A** debe hacer lo siguiente:

1. Seleccionar aleatoriamente un número entero secreto **k**, tal que $0 < k < q$.
2. Calcular $r = (\alpha^k \bmod p) \bmod q$
3. Calcular $k^{-1} \pmod q$
4. Calcular $s = k^{-1}\{h(M) + ar\} \pmod q$
5. La firma de **A** para el mensaje **M** es la pareja (**r, s**)

Verificación de la firma. Para verificar la firma (**r, s**), de **A** sobre el mensaje **M**, el verificador **B** debe hacer lo siguiente:

1. Obtener la llave publica de **A**, (**p**, **q**, α, **y**)
2. Verificar que 0 < **r** < **q** y que 0 < **s** <**q**. Si no, rechaza la firma.
3. Calcular **w** = s^{-1} (mod **q**) y **h**(**M**)
4. Calcular u_1= **w** **h**(**M**) (mod **q**) y u_2= **rw** (mod **q**)
5. Calcular v = (α^{u1} y^{u2} mod **p**) mod **q**
6. Aceptar la firma si y solo si **v** = **r**

Para probar que la verificación es correcta se debe observar que si (r, s) es una firma legitima A, entonces debe cumplirse:

K s = **k** k^{-1} { **h**(**M**) + **ar**}(mod **q**)

h(**M**) = -**ar** + **ks** (mod **q**)

Multiplicando ambos lados de la igualdad anterior por w y arreglando terminus, se obtiene:

w – **h**(**M**) + **aw** = **k** (mod **q**) por que **w** = s^{-1}(mod **q**)

Pero esto es simplemente: U_1 + aU_2 = **k** (mod **q**)

Elevando α a ambos lados de esta ecuación, se obtiene:

($\alpha^{U1 + aU2}$ mod **p**) mod **q** = (α^{k} mod **p**) mod **q**
((α^{U1})(α^{a})^{U2} mod **p**)mod **q** =(α**k** mod **p**)mod **q**
(α^{U1} y^{U2} mod **p**) mod **q** = (α^{k} mod **p**) mod **q**

Y de aquí se tiene que que v = r, como efectivamente se requiere.

Ejemplo práctico con DSA

Generación de llaves

A selecciona los números primos **p**= 124540019 y **q**= 17389 tal que **q** divida a (**p**-1). De aquí (**p**-1)/**q**=7162.

A selecciona aleatoriamente un elemento **g**= 110217528 ε **Zp** y calcula α = g^{7162} (mod **p**)= 10083255. ya que $\alpha \neq 1$, α es un generador del unico subgrupo ciclico de orden **q** en **Zp**.

A selecciona aleatoriamente un número entero **a** = 12496 que satisface $1 \leq a \leq q - 1$

A calcula **y** = α^{a} (mod **p**) = 10083255^{12496} (mod 124540019) = 119946265

La llave publica de **A** es (**p**=124540019, **q**=17389, α=10083255, **y**=119946265)

La llave privada de **A** es **a**=12466

Generación de la firma

Para frimar **M, A** selecciona aleatoriamente un número entero **k** = 9557, y calcula **r** = (α^{k} mod **p**)(mod **q**) = (10083255^{9557} mod 124540019)(mod 17389)=27039929 (mod 17389)=34

A calcula k^{1} (mod **q**) = 7631, **h(M)**=5246 (el valor hash ha sido inventado para este ejemplo) y finalmente **S** =(7631){5246+(12496)(34)}(mod **q**)=13049

La firma de **A** para **M** es la pareja (**r** =34, **S**=13049)

Verificación de la firma

B calcula **w** =S^{-1} (mod **q**) =1799, U_1= **w h(M)**(mod **q**) = (5246)(1799)(mod 17389) =12716, y U_2 = **rw**(mod **q**)=(34)(1799)(mod 17389)=8999.

B calcula **V**= (α^{U1} y^{U2} mod **p**)(mod **q**)=(10083255^{12716} 119946265^{8999} mod 124540019)(mod 17389)= 27039929 (mod 17389)= 34

Ya que **V**= **r**, entonces **B** acepta la firma de **A** como valida.

Protocolos para la utilización de firmad digitales

Firmas múltiples

Una situación muy común es cuando se requiere que varias personas firmen un documento, en el caso de la firma autógrafa esto se resuelve juntado a las personas para que firmen el documento pero el la firma digital ¿como es que se resuelve este problema?, esto se logra a través de un protocolo arbitrado, es decir, un protocolo que utilice una parte confiable que actué como juez o autoridad entre las partes y que se encargue de verificar las firmas de cada uno.

Supóngase que los firmantes del documento **M** son **A** y **B**, la parte confiable o juez es **J**, y que utilizan la función de dispersión **h** para optimizar la firma. Entonces, el protocolo a implementar seria:

1. **A** firma el resultado has del documento
2. **B** firma el hash del documento
3. **B** envía a **A** su firma **s**
4. **A** envía a **J** el documento, su firma y la firma de **B.**
5. **J** verifica las firmas.

Firmas digitales con cifrado

Una situación común con las firmas autógrafas es que después de firmar un documento, ya sea por una o varias personas, se guarde en un sobre y se selle para proteger el documento de miradas indiscretas no autorizadas. El equivalente a esta situación con las firmas digitales seria, que después del proceso de firma, se tenga la capacidad de ocultar la firma, es decir, la capacidad de cifrar la firma.

El protocolo para esta situación seria el siguiente:

1. **A** firma el documento **M** con su llave privada para firma.
2. **A** cifra la firma con la llave publica, para cifrado de **B** y lo envía a **B**.
3. **B** descifra la firma con su llave privada para cifrado
4. **B** verifica la firma con la llave pública, para firma, de **A**.

De analizar este protocolo surge una pregunta, ¿es mejor firmar antes de cifrar o al revés?, para comprender mejor la pregunta imaginemos a que equivaldría esto con firmas autógrafas; firmar y después cifrar equivale a firmar el documento y luego ponerlo en el sobre; en el caso contrario equivale a primero poner el documento en el sobre y después firmarlo.(esto ultimo desde luego que se puede hacer con las firmas autógrafas si usamos un papel carbón, pero seria como una copia de la firma que no tendría validez.)

Firmas digitales y no repudio

Una situación que se puede presentar en firmas digitales es que alguno de los firmantes niegue haber firmado el documento. Esta situación es hipotética por que si la firma se puede verificar como perteneciente al firmante, eso significa que el único que pudo haber firmado es el dueño de la firma verificada, garantizándose con ello el servicio de no repudio de la firma.

Supóngase el siguiente protocolo.

1. **A** firma el mensaje **M**
2. **A** genera un encabezado con su identificación y concatena este encabezado con su firma de **M**, firma de nuevo todo y esto lo envía a **J**.
3. **J** verifica la firma exterior y confirma la identificación de **A**. **J** agrega una lectura de reloj local (timestamp) al mensaje firmado de **A** y a la identificación. **J** firma todo eso y lo envía a **A** y a **B**.
4. **B** verifica la firma de **J**, la identificación y la firma de **A**.
5. **A** verifica el mensaje que **J** envió a **B**. si no coincide con el original que **A** envió a **J**, habla rápidamente para avisar de la no coincidencia.

Certificados digitales

El término certificado hace referencia a un documento público verificable, que contiene información acerca de su propietario y es avalado por una tercera entidad confiable. Su autenticidad es garantizada por el hecho que solamente un organismo oficial puede crearlo.

En el mundo digital un certificado de llave pública es un identificador que funciona como un medio para probar la identidad en transacciones electrónicas. Estos certificados relacionan la llave pública de una entidad con algunos de sus atributos.

Típicamente un certificado contiene información referente a la llave publica del dueño, nombre, fecha de expiración, nombre del emisor (autoridad certificadora que genero el certificado), numero de serie y la firma digital del emisor. Esta firma es la que garantiza su autenticidad.

Un certificado digital puede ser emitido para una persona, un dispositivo de hardware o un proceso de software. Para emitir el certificado, las autoridades certificadoras validad previamente la identidad de solicitante. Durante el proceso de generación del certificado, se encuentran involucrados algoritmos criptográficos para la generación de las firmas digitales. Estos mecanismos hacen imposible la falsificación, ya que para ello, el falsificador necesita conocer la llave privada de la autoridad certificadora.

Con los certificados digitales se pueden implementar servicios como; identificación y autentificación, también pueden ser utilizados para la distribución segura de llaves publicas en comunidades grandes. Sin embargo la confianza de un certificado depende de que confiable es la autoridad certificadora.

Autoridades certificadoras

La naturaleza de un certificado requiere la intervención de una tercera parte confiable que pueda confirmar los datos proporcionados por los suscriptores y emitir los certificados. A estas entidades se les denomina Autoridades certificadoras (AC).

Obtención del certificado

Para obtener un certificado el usuario llena una solicitud y la envía a la autoridad certificadora. La información que el usuario debe proporcionar depende principalmente del tipo de certificado que se solicite; sin embargo, en cualquiera de los casos, deberá incluir su llave publica y alguna información para identificación.

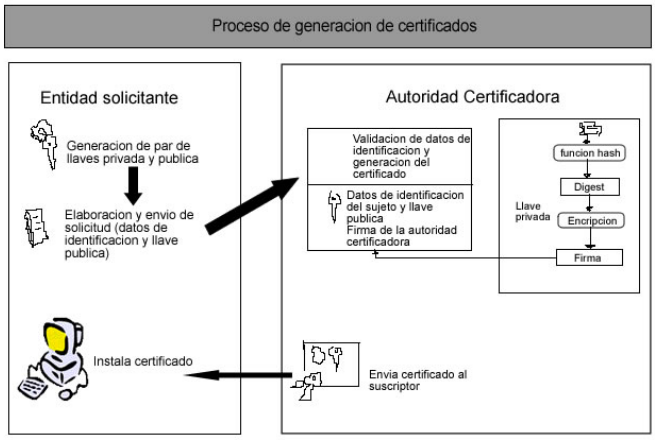
La generación del par de llaves pública y privada y la transmisión segura de la llave publica a la autoridad certificadora, son pasos muy importantes durante la elaboración de la solicitud para el certificado. El suscriptor puede generar un par de llaves en el sistema local, almacenar de una forma segura la llave privada y mandar la llave publica junto con la solicitud a la autoridad certificadora.

El almacenamiento seguro de la llave privada puede lograrse mediante el cifrado de la misma con una contraseña, o bien, almacenando la llave en una tarjeta inteligente.

Validación de certificados

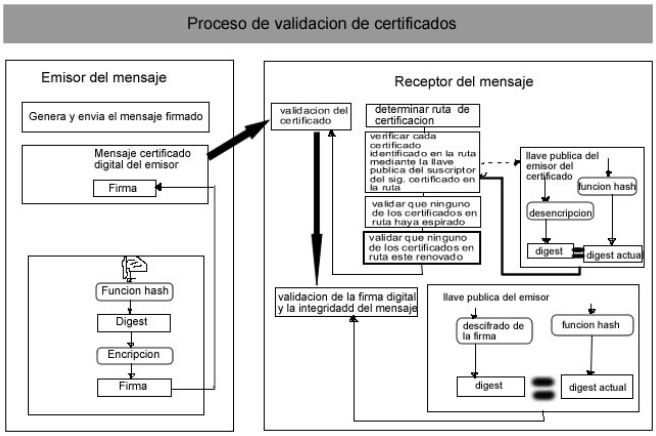
Las aplicaciones que utilizan certificados solamente pueden establecer confianza en los certificados recibidos cuando estos son validados. Para tal efecto, las aplicaciones deben ejecutar el siguiente proceso.

1. determinar la ruta de validación
2. verificar cada certificado identificado en la ruta mediante la llave publica del suscriptor del siguiente certificado en la ruta. Si el certificado es el último de la ruta, este debe ser verificado con la llave publica de la autoridad certificadora raíz.
3. validar que ninguno de los certificados en al ruta haya expirado.
4. validar que ninguno de los certificados este revocado.
5. verificar que las extensiones criticas de cada certificado sean reconocidas y procesadas.



Determinación de la ruta de Certificación

Una ruta de certificación es una secuencia de uno o mas nodos conectados entre los suscriptores y una autoridad certificadora raíz, e indica la forma en que la aplicación que utiliza los certificados puede generar la confianza en el certificado del suscriptor.



Estándares PKCS

En el ámbito de los certificados digitales, adicionalmente a los entandares de firma digital, existen varios elementos que han sido sujetos a estandarización. A saber:

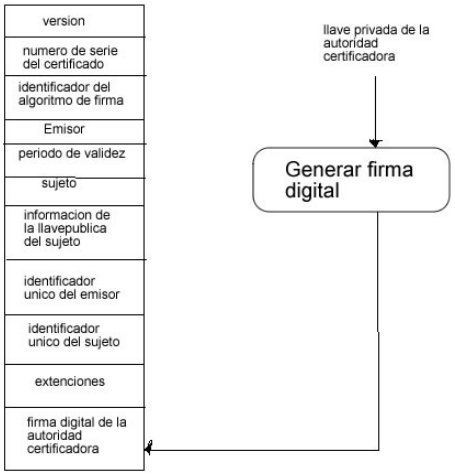
- Solicitudes de certificados (PKCS #10)
- Formato de certificados (X.509)
- Formato para enviar el certificado al solicitante (PKCS #7)
- Formato para transferir y almacenar el certificado junto con su respetiva llave privada (PKCS #12)

Certificados X.509

Un certificado digital es representado como una estructura de datos definida por el estándar X.509. este estándar fue publicado por primera vez en 1988 por ITU-T e ISO. En 1996, se publico la version 3, la cual es utilizada actualmente.

El certificado X.509 V3 esta formado por los siguientes campos.

- Versión
- Numero de serie del certificado
- Identificador del algoritmo de firma
- Nombre del emisor
- Periodo de validez
- Nombre del sujeto
- Información de la llave publica del sujeto
- Identificador único para el emisor
- Identificador único del sujeto
- Extensiones
    - Restricciones básicas
    - Política del certificado
    - Uso de la llave



Listas de Revocación

Los certificados X.509 tienen un periodo de validez, el cual típicamente dura desde unos pocos mese hasta algunos años. Una vez que el certificado caduca, este se convierte en no valido, locuaz implica que no es seguro para una aplicación seguir confiando en el.

El término de periodo de vigencia no representa la única razón por la que un certificado deja de ser considerado valido. También se puede revocar cuando la llave privada del sujeto o de la autoridad certificadora se compromete. O bien cuando hay un cambio de características registradas del sujeto.

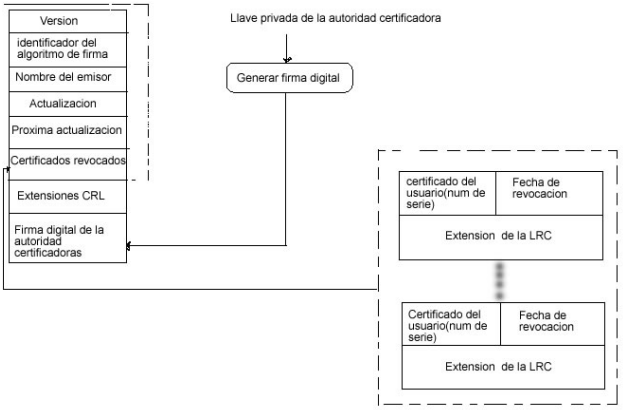
Las listas de revocación de certificados (LRC) son los mecanismos que una autoridad certificadora usa para publicar y difundir entre las aplicaciones que usan certificados, información sobre los certificados revocados.

Una LRC es una estructura de datos firmada digitalmente por la autoridad certificadora que la emite, dicha estructura contiene la fecha y la hora de la publicación de la LRC, el nombre de la autoridad certificadora y los números de serie de todos los certificados revocados que aun no han expirado.

Una aplicación que utiliza certificados deberá obtener la más reciente LRC publicada por la autoridad certificadora y asegurarse que los números de serie de los certificados que reciba no se encuentren contenidos en el LRC.

Al igual que los certificados digitales, existe un formato estándar X.509 para las LRC, cuya primera versión fue publicada en 1988. Conforme a dicho estándar, los campos de una LRC son:

- Versión
- Firma
- Nombre del emisor
- Actualización
- Próxima actualización
- Certificado de usuario
- Fecha de revocación



Aplicaciones de los certificados digitales

Debido a su versatilidad y características los certificados digitales pueden ser utilizados en una amplia gama de aplicaciones como son:

- Correo electrónico seguro
- Sistemas de autentificación para transacciones bancarias
- Código firmado

Código firmado

En el mundo del Internet es muy común que muchas personas descarguen aplicaciones a sus computadoras sin estar seguras que estas aplicaciones sean seguras y confiables, este es un grave problema al cual nos enfrentamos y que podemos combatir con el uso de certificados digitales, para lograr esto se debe hacer lo siguiente:

1. El desarrollador del software debe obtener un certificado digital que sea valido para firmar código.
2. Una vez que lo tiene firma su código usando su llave privada, Luego coloca en una misma estructura de datos el código, la firma digital y el certificado correspondiente y lo publica en su sitio Web.
3. cuando al browser descarga el código firmado, éste verifica la firma digital para asegurarse que el código descargado no ha sido alterado.
4. el browser valida la firma extrayendo la llave publica del certificado de la persona que publico el software, descifra esta firma y compara el resultado con el valor de dispersión del código, que es calculado por el browser en ese momento. Si el valor de dispersión calculado por el browser con coincide con el del creador del software alertara d esto para que se tomen las medidas necesarias.

Esto ya lo vemos más seguido en páginas de software serias que ponen la liga del programa a descargar y su correspondiente valor de dispersión (MD5).

Correo electrónico seguro (S/MIME)

Para garantizar la seguridad de un correo electrónico en una red abierta es necesario contar con seguridad desde el emisor hasta el lector, de forma que el mensaje sea protegido desde le momento en que éste sale de la herramienta de correo del remitente hasta que llega a la herramienta de correo del destinatario.

Existen muchos protocolos que implementan seguridad en el envió de correo electrónico como son:

- Privacy Enhanced Mail (PEM)
- X.400
- Pretty Good Privacy (PGP)

Sin embargo, existe un protocolo que ha sido reconocido e impulsado comercialmente debido a su compatibilidad con el correo de Internet, y esta siendo utilizado ampliamente en el mercado. Este protocolo es conocido como S/MIME (Secure Multipurpose Internet Mail Exchange).

S/MIME está basado en dos estándares de llave pública PKCS#7 y PKCS#10, es decir aplica las firmas digitales y cifrado de mensajes, implementa los siguientes servicios de seguridad:

- Autentificación del origen del mensaje (firma digital)
- Integridad del mensaje (firma digital)
- No repudio del origen (firma digital)

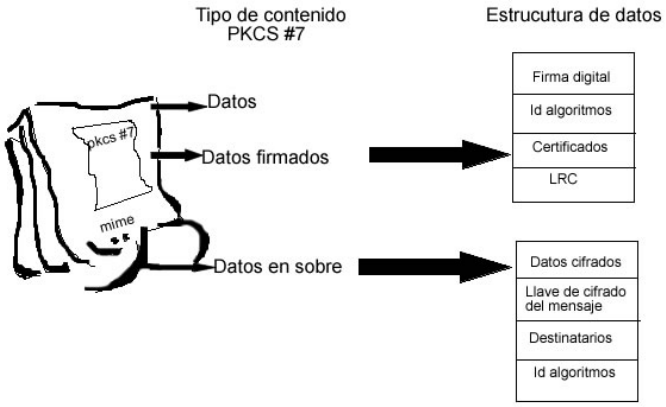
- Confidencialidad del mensaje (Cifrado)

Se mime se basa en el estándar PKCS#7 para definir el formato y sintaxis necesarios para envolver un mensaje MIME dentro de un objeto PKCS#7. el cual es, a su vez, envuelto en un mensaje MIME para ser transportado a los destinatarios. El receptor extrae el objeto PKCS de la entidad MIME que lo transporto, lo desenvuelve y recupera el mensaje MIME original.

Tipos de contenidos PKCS#7 usados por S/MIME:

- Datos
- Contenido firmado
- Sobre digital

En la siguiente imagen se puede observar gráficamente la composición de un mensaje S/MIME.



Mensaje Firmado en S/MIME

Los servicios de autentificación del origen, integridad y no repudio de origen del mensaje, se implementan en S/MIME mediante las firmas digitales y el proceso para firmar un mensaje es el siguiente:

1. se convierte la entidad S/MIME que contiene el mensaje en claro, a una forma canónica que sea única y no ambigua tanto en el ambiente como fue generada la firma como en el que esta es validada. Por ejemplo, para entidades MIME de texto, el proceso de canonización implica convertir los caracteres de fin de línea y cambiarlos por el correspondiente en el código de caracteres elegido, si esto no se hace se corre el riesgo que su representación cambie en el camino, y cuando el destinatario calcule el valor de dispersión del documento, este difiera del que ampara la firma.
2. Se hace la transformación del mensaje a un código basado en 7 bits. Esto se debe a que, aun cuando algunos segmentos de red pueden manejar datos binarios y código de 8 bits, la mayor parte de la infraestructura de SMTP puede manejar únicamente texto de 7 bits.
3. Se obtiene l valor de dispersión del mensaje.
4. se cifra el valor de dispersión obtenido con la llave privada del emisor del mensaje.
5. La firma digital, los identificadores de algoritmos usados y los certificados del emisor, son empaquetados en un objeto "Signed PKSC#7"
6. El objeto PKCS#7 es transformado a Base64, para que pueda ser transmitido como un objeto binario.
7. el objeto PKCS#7 resultante es insertado dentro de un mensaje MIMEque contiene el mensaje original
8. el mensaje se envia.

El receptor verifica la firma descifrando el valor de dispersión del mensaje con la llave publica del firmante, la cual se encuentra en el certificado digital adjunto al mensaje.

Mensaje en sobre (cifrado) en S/MIME

La implementación del servicio de confidencialidad, se logra mediante el cifrad del mensaje. S/MIME lleva a cabo el siguiente proceso:

1. Se convierte la entidad MIME que contiene el mensaje a una forma canónica.
2. Se lleva a cabo la transformación del mensaje a un código de 7 bits.
3. El agente S/MIME del emisor del mensaje, genera una llave secreta aleatoria y con ella cifra el mensaje.
4. El agente S/MIME cifra la llave secreta con RSA, usando la llave publica certificada por el destinatario.
5. El mensaje cifrado , la llave secreta cifrada y los identificadores de algoritmos usados son empaquetados en un objeto "Envoloped-data PKCS#7"
6. El objeto PKCS#7 es transformado a Base64, para que pueda ser transmitido como un objeto binario.
7. El objeto PKCS#7 resultante es insertado dentro de un mensaje S/MIME.
8. El mensaje se envia.

Mensaje firmado y cifrado S/MIME

Para crear un mensaje firmado y cifrado, el agente S/MIME puede firmar el mensaje primero y luego anidarlo en un mensaje cifrado (sobre), o bien, puede cifrarlo primero y luego firmarlo.

Protocolos de acuerdo de intercambio de llaves

Algoritmo Diffie-Hellman

Este algoritmo permite a dos o mas partes acordar una llave, aun cuando los intercambios previos al acuerdo sean públicos. La idea fundamental del algoritmo es el siguiente:

- **A** inventa un numero N_A , aplica una transformación **f** a ese numero y transmite el resultado $f(N_A)$, a **B.**
- **B** inventa su propio número N_B, aplica la transformación **f** a ese numero y transmite el resultado, $f(N_B)$ a **A**.
- **A** calcula la llave de la sesión utilizando N_A y $f(N_A)$
- **B** calcula la llave de la sesión utilizando N_B y $f(N_B)$

Solo hay que establecer las siguientes cosas; que significa "inventar" un número, de que tipo y tamaño, en que consiste la transformación **f** y que propiedades tiene y que tipo de calculo tiene que hacer **A** y **B** sobre N_A y N_B.

El fundamento de todo lo que se requiere para satisfacer estas dudas es la matemática y en particular la Teoría de Números.

Ejemplo:

- **A** y **B** tiene conocimiento previo, se puede pactar públicamente, de 2 números: el número **n** que es un número primo grande (mayor de 512 bits) y el número **g** de tal manera que $1 \leq g \leq n$.
- A y B generan o seleccionan aleatoriamente un número grande y lo mantienen en secreto. Supóngase que **A** selecciona el número **x** y **B** selecciona un numero **y**.
- **A** calcula $X=g^x \pmod n$
- **B** calcula $Y=g^y \pmod n$
- **A**y **B** intercambian los resultados **X** y **Y** de tal manera que **A** conozca **Y** y que **B** conozca **X**.
- **A** calcula la llave de sesión $k=Y^x \pmod n$
- **B** calcula la llave de sesión $k'=X^y \pmod n$
- Las llaves de sesión **k** y **k'** son idénticas e iguales a $g^{xy} \pmod n$

La fortaleza en seguridad del algoritmo de Deffie-Hellman radica en la imposibilidad matemáticas de calcular g^{xy} a partir del conocimiento de $g^x \pmod n$ y $g^y \pmod n$.

Protocolo de intercambio de llave con Criptografía Simétrica

El siguiente ejemplo muestra un protocolo arbitrado para el intercambio de llave de sesión usando criptografía simétrica.

- **A** envía a **S** una petición de llave para comunicarse de modo seguro con **B**.
- **S** genera aleatoriamente la llave de sesión **k**. **S** cifra dos copias; una usando **PA** como llave y la otra utilizando **PB** como llave. **S** envía ambas copias a **A**.
- **A** usa **PA** para descifrar su copia y conocer **k**. **A** envía la otra copia cifrada a **B**.
- **B** usa **PB** para descifrar su copia y conocer **k**.

Al término ambas partes **A** y **B** conocen **k** y pueden usarla como llave de un algoritmo simétrico.

Protocolo de intercambio de llave con Criptografía Asimétrica

Ejemplo de protocolo autoimplementado para intercambio de llave de sesión usando criptografía asimétrica:

- **B** genera su pareja de llaves (publica y privada) y envía a **A** su llave pública.
- **A** genera una llave de sesión **k** y utiliza la llave pública de **B** para cifrar **k** y enviarla a **B**.
- **B** utiliza su llave privada para descifrar el mensaje y conocer **k**.

Así como esta, este protocolo es susceptible a ataques por hombre en medio ya que un atacante **I** puede sustituir la llave pública de **B** y poner su propia llave publica y con esto engañar a **A** , esto se puede evitar certificando las llaves publicas.

Protocolo para distribución de llave secreta

Las partes **A** y **B** acuerdan una llave secreta K_S para ser usada después con criptografía simétrica. Este protocolo logra confidencialidad en los paquetes intercambiados y autentificación. El protocolo asume que las llaves públicas de **A** y **B** han sido intercambiadas por un método seguro.

- **A** envía a **B** un requerimiento cifrado con un algoritmo de llave publica, usando como llave de cifrado la llave publica de **B**, y que consiste en: un número aleatorio N_A, que previamente genera, y su identidad (la de **A**).
- **B** descifra el paquete utilizando su llave privada y conoce N_A y la identidad del solicitante. Después **B** genera su propio numero aleatorio N_B, lo concatena con el numero que recibió de **A**, N_A y lo cifra con un algoritmo de llave pública usando como llave de cifrado la llave pública de **A**. envía este mensaje a **A**.
- **A** recibe el paquete cifrado y lo descifra utilizando su llave privada y conocen N_A y N_B. verifica que el número que envió antes sea N_A. si coincide, está seguro que **B** recibió y descifro el paquete y es quien envía el nuevo paquete cifrado. Después de esto, **A** genera la llave secreta k_s, la cifra con su llave privada; al resultado le concatena N_B y el nuevo resultado lo cifra con la llave publica de **B** y se lo envía a **B**.
- Al recibir el paquete **B** descifra el cifrado exterior con su llave privada y conoce N_B. Verifica que sea el mismo N_B que envió antes. Si es así, esta seguro que **A** recibió el paquete enviado antes, que lo pudo descifrar y es quien envía este nuevo paquete. luego usa la llave publica de **A** para descifrar el cifrado interior y obtener k_s.

Noticias del mes

Microsoft Robotics Studio

Juan Francisco Berrocal
berrocal239@hotmail.com

En la **RoboBusiness Conference and Exposition 2006**, Microsoft, ha mostrado las últimas novedades para crear aplicaciones robóticas para una amplia variedad de plataformas de computación. las primeras compañías adaptadoras, universidades e institutos de investigación han ofrecido demostraciones, proporcionando el apoyo de la nueva plataforma desarrollada: **Microsoft(R) Robotics Studio**.

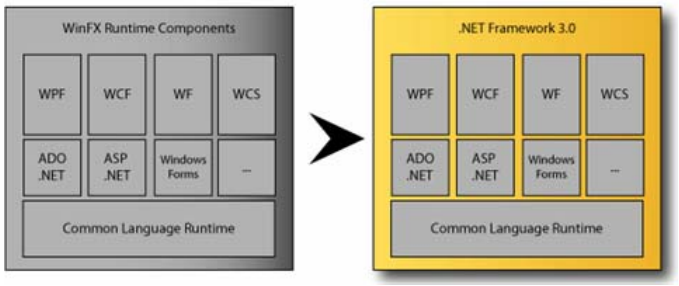
La buena noticia es que, de cara a la programación, los lenguajes serán los propios de .NET, según dice el comunicado ofial textualmente: "*se pueden desarrollar utilizando una selección de lenguajes de programación, incluyendo los de los lenguajes Microsoft Visual Studio 2005 y Microsoft Visual Studio Express (Visual C# y Visual Basic .NET), JScript y Microsoft IronPython 1.0 Beta 1*". En el sitio Web asociado, puede descargarse, además, la presentación oficial en formato PowerPoint. Para los relamente interesados, puede que les apetezca ver el vídeo de una entrevista con el equipo de desarrollo que publicaba hace poco **Channel9**.

Fuente: *http://www.elavefenix.net*

Se Anuncia La Estructura De .net Framework 3.0

Juan Francisco Berrocal
berrocal239@hotmail.com

Para evitar más confusiones, en la última entrada de su



bitácora, **Soma Somasegar**, uno de los principales responsables de herramientas de desarrollo en Microsoft, anunciaba oficialmente las características que tendrá la nueva **versión 3.0 de .NET Framework**, (que en realidad, son las API's sobre las que se basa el nuevo sistema operativo Windows Vista, como puede apreciarse en el grabado adjunto. La última de las "bautizadas", WCS, corresponde a **Windows CardSpace**, que se une a las librerías base ya existente, y se complementa con ADO.NET, ASP.NET y Windows Forms. Esta versión aparecerá con Windows Vista, tal y como estaba previsto. Solo se trata de una aclaración de nomenclatura (resumiendo, WinFX,pasa a llamarse .NET Framework 3.0, como era de esperar). Para más detalles, ver la nota: .NET Framework 3.0 , con interesantes comentarios, como el de **Bryant Longley** (ver los últimos comentarios).

Además, en otra nota anterior, Somasegar también revela las características del nuevo **MSDN Wiki**, un sistema de ayudas interactivo, que ya dispone de su propia bitácora, donde se explica su funcionamiento, y donde los usuarios podrán participar en la elaboración y corrección de contenidos..

Fuente: *http://www.elavefenix.net*

El Banco Mundial Estudia Apoyar Los Ordenadores 'prepago' De Microsoft

Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

WASHINGTON.- El Banco Mundial, a través de su rama dedicada al sector privado, apoya la idea de Microsoft de **vender ordenadores** más baratos para países menos desarrollados **a cambio de micropagos por tiempo de uso**, a través del programa FlexGo. Una de las modalidades de pago de estas máquinas será la **fórmula 'prepago'**, que tanto éxito ha tenido en la telefonía móvil.

La institución internacional **sopesa financiar en parte el proyecto** del gigante de Redmond, el cual sostiene que **la flexibilidad en los pagos puede ser la clave del éxito**.El director gerente de mercados emergentes de Microsoft, Craig Fiebig,identificó el 'prepago' como una de las herramientas que explican eléxito de los móviles.

Microsoft estima que hay en el mundo 1.370 millones de familias que no tienen ordenador en casa, por lo que deduce que **la base de un mercado de ordenadores 'baratos' puede situarse entre los 300 y los 400 millones de hogares**.

Brasil ha sido el banco de pruebas de este proyecto de Microsoft. "Si puedes hacerlo funcionar allí, puedes hacer que funcione en cualquier otro lugar", comentó Fiebig.

Esta semana se han puesto a la venta 1.000 ordenadores en dicho paíspor un precio de 600 dólares, de los que los consumidores pagan 200 alprincipio, y el resto viene financiado por HSBC Holding.

En lugar de abonar cuotas mensuales, los usuarios compran tarjetasque activan sus ordenadores por tiempo, o en función de

lasherramientas utilizadas, hasta completar el precio de la máquina. **"Se trata de comprar tiempo, aquí el tiempo realmente es dinero"**, dijo Xavier Jordan, especialista financiero del Banco Mundial.

La próxima fase del proyecto se producirá después del verano, cuandosaldrán a la venta en Brasil entre 30.000 y 50.000 PC de este tipo.

Mientras que el banco Mundial afina el mecanismo de riesgofinanciero, Microsoft ya planea lanzar ordenadores personales consistema de tarjetas 'prepago' en países como China, la India, México yRusia.

http://www.elmundo.es

Autodesk Presentará Autocad 2007 En Argentina

Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

La compañía presentará la nueva plataforma el 7 de julio en el Hotel Hilton

La empresa Autodesk anunció su evento "Accelerate your Ideas" para presentar al público argentino su nueva plataforma AutoCAD 2007 y las versiones actualizadas de sus productos para los mercados de arquitectura, ingeniería, construcción, manufactura e infraestructura.

Tal como anunció la compañía, dicho encuentro se realizará el próximo viernes 7 de julio a las 8 hs. en el hotel Hilton Buenos Aires.

Según comunicó Autodesk, la nueva línea de productos 2007 contiene las más recientes versiones de sus soluciones, "con mejoras que economizan el tiempo y los costos de los proyectos".

De acuerdo con la empresa, las nuevas versiones permitirán administrar, editar y compartir datos de proyectos, anotaciones y revisiones, para mejorar los resultados y cumplir con los plazos previstos. Así, según Autodesk, la línea 2007 combina los comandos e interfaz de usuario de AutoCAD con un ambiente de diseño conceptual para ayudar al usuario a darle forma a sus ideas.

La inscripción para participar en el evento es gratuita y se debe realizar con antelación ingresando a:
www.accelerateautodesk.com/arg

http://www.tectimes.com/secciones/notas.asp?codnota=18940

La Nueva Java Platform Enterprise Edition 5

Gustavo Alberto Rodríguez
gustavo@sasoft.com.ar

En la última conferencia mensual JavaOne, Sun lanzó la Java Platform Enterprise Edition 5, la actualización más importante a la tecnología Java para empresas en seis años. Java EE 5 es la primer plataforma industrial para la creación y desarrollo de servicios web para empresas y ha sido establecida, dentro de la comunidad de desarrollo Java, como la elección mas popular para la tecnología Java y el desarrollo de servicios web. La Enterprise Java Platform ha tenido más de cinco millones de descargas.

Obtenga ahora el Java EE 5 SDK:
http://java.sun.com/javaee/downloads/

Fuente:
https://communications.sun.com/sunSat/c/ECNL13_EC_0606insidetech.html?email=san_antonio_soft%40hotmail.com&mid=1096144012&pid=389732&cid=12838074964

Google Deberá Indemnizar Con 300.000 Euros A Louis Vuitton

Gustavo Alberto Rodriguez
gustavo@sasoft.com.ar

Un tribunal francés condenó al buscador por imitación de marca

PARIS (AFP) - Un tribunal francés condenó a Google a abonar a la sociedad Louis Vuitton unos 300.000 euros en concepto de daños y perjuicios por imitación de marca, anunció Vuitton en un comunicado.

Este veredicto obliga asimismo a Google a pagarle 60.000 euros de gastos legales, además de los 15.000 euros a los que ya fue condenado en 2005.

La sentencia agrava una sanción anunciada en primera instancia contra Google y su filial francesa, condenados en febrero de 2005 a indemnizar a la compañía de productos de marroquinería con 200.000 euros por imitación de marca, competencia desleal y publicidad engañosa.

La Justicia considera que Google cometió una infracción al proponer un servicio publicitario que asociaba palabras claves (como imitación, réplica o copia) a los términos Louis Vuitton o Vuitton

Link corto: *http://www.lanacion.com.ar/819026*

Nuevo Flash 9

Gustavo Alberto Rodriguez
gustavo@sasoft.com.ar

La empresa Adobe presentó Flash 9, la última versión de su player paraaplicaciones multimedia. Según la compañía, el software fue reescritopara mejorar su rendimiento, interactividad y "expresividad". Laaplicación se puede descargar de manera gratuita, tanto para Windowscomo para Mac OS X. La empresa

también lanzará una versión para Linux,aunque todavía no se adelantó una fecha concreta.

Deacuerdo con el comunicado de la compañía, el nuevo Flash Player lograprocesar el lenguaje ActionScript hasta 10 veces más rápido que laversión anterior. De esta manera, el soft incorpora una nueva "máquinavirtual" que posee un compilador que traduce instantáneamente el códigode programación de Flash a lenguaje de máquina, para permitir así unamáxima velocidad de ejecución.

Junto con la edición de Flash9, Adobe introdujo Flex 2, la nueva versión de su software paradesarrolladores destinado a crear aplicaciones similares a las delentorno AJAX. Como la estrategia de Adobe es fomentar la adopción deFlex por parte de los programadores, la empresa ofrece gratuitamente unkit de desarrollo básico. La versión completa tiene un valor de 500dólares en Estados Unidos. Tal como informó la compañía, el objetivo deAdobe es que entre 2009 y 2012 existan un millón de desarrolladores queutilicen Flex.

Esta herramienta comercial de Adobe está basadaen el entorno abierto Eclipse y permite desarrollar aplicacionescorporativas multiplataforma que integran textos, interactividad,gráficos, animación y video. Con ella se pueden crear desde cursos deentrenamiento multimedia hasta mapas interactivos y solucionesfinancieras.

Según Adobe, la nueva versión está diseñada parafacilitar la tarea de los desarrolladores ya que incorpora galerías decomponentes creados previamente, y aprovecha al máximo las ventajas deActionScript 3.0, la última versión del lenguaje de programación de lacompañía. De acuerdo con ejecutivos de Adobe, las herramientas de Flexpermitirán que los autores de software creen interfaces dinámicas muchomás rápido que si se utilizaran otros sistemas, por ejemplo HTML.

Secalcula que distintas versiones de Flash Player están instaladas en másde 600 millones de computadoras de todo el mundo. El nuevo plugin sepuede descargar de *www.adobe.com/go/getflashplayer.*

Fuente: *www.tectimes.com*

Google Lanza Su Propio Servicio De Pagos A Través De Internet

Martin R. Mondragón Sotelo
mygnet@gmail.com

Google lanzó hoy, jueves, su esperado sistema de transacciones online, que bajo el nombre de Checkout ha sido diseñado por la compañía californiana para facilitar a sus usuarios la compra de productos o servicios a través de internet.

Los consumidores que tengan una cuenta de Google podrán ingresar una sola vez la información de su tarjeta de crédito y dirección de entrega en Checkout, para posteriormente pagar con "un click" en sitios web que integren esta plataforma, señaló a News.com el vicepresidente de administración de productos en la compañía, Salar Kamangar.

El sistema puede ser integrada en sitios de venta en línea y ofrecido como una alternativa a Paypal y otros sistemas que permiten realizar transacciones comerciales usando tarjetas de crédito. En todo caso, Google Checkout está pensado para ser implementado por empresas más que para transacciones entre personas, como sucede con la alternativa usada por eBay.

Hace al menos un año que la compañía estaba usando esta solución para recibir pagos por versiones premium de servicios como Google Earth, Google Video y Picasa, según informó Kamangar.

Microsoft Intenta Competir Con Sourceforge

Martin R. Mondragón Sotelo
mygnet@gmail.com

Microsoft ha dado a conocer una web de desarrollo open source.

La web Codeplex permite a los desarrolladores "crear nuevos proyectos para compartir con compañeros desarrolladores de todo el mundo, unirse a otros que ya hayan empezado sus nuevos proyectos o utilizar aplicaciones del site e proporcionar comentarios."

No hay logos de Microsoft en el site, excepto por el copyright en letra pequeña al final de la página. La compañía parece asumir que su logo no sienta muy bien dentro de la comunidad open source.

Esta web parece un intento desesperado de entrar en contacto con la comunidad open source más que una manera de resolver problemas reales del mundo. Además, Codeplex parece más bien un clon del proyecto SourceForge.

Eso es lo que lo convierte en un producto típico ed Microsoft: toman la idea de otro y la reclaman como propia.

Fuente original:

http://www.siliconvalleysleuth.com/2006/06/microsoft_launc.html#more

http://sourceforge.net/
http://codeplex.com/

Las Computadoras Fallan Menos Que Antes

Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Un estudio afirma que el porcentaje de computadoras con problemas se redujo en el último año

Las computadoras se han vuelto más confiables en los último años. De todos modos, una de cada seis notebooks necesita ser reparada dentro del primer año de compra. Así lo undica un estudio de la consultora Gartner que también afirma que las mejoras se deben a la incorporación de mejores diseños por parte de los fabricantes.

Según el estudio, la cantidad de fallas de los equipos nuevos disminuyeron en el período 2005-2006 en comparación con los años 2003-2004. Actualmente, sólo el 5% de las computadoras de escritorio necesitan algún componente de repuesto durante el primer año, en comparación con el 7% de hace 2 años.

Por otro lado, la probabilidad de necesitar una reparación 4 años después de la compra es en la actualidad del 12%. En 2003-2004 ese indicador era del 15%.

En cuanto a las notebooks, estos porcentajes son más elevados. Se calcula que el 15% de las unidades evaluadas en el último período necesitaron una reparación antes del año de compra. Este número era del 20% hace dos años.

De acuerdo con la consultora, el 50% de todas las fallas de las notebooks están relacionadas con problemas del motherboard o del disco rígido.

http://www.tectimes.com/secciones/notas.asp?codnota=1893

Symantec Contra El "phishing"

Gustavo Alberto Rodríguez
gustavo@sasoft.com.ar

La modalidad de estafa online conocida como "phishing" es uno de los principales problemas de seguridad para empresas y usuarios finales. Con Microsoft como un jugador recién llegado al campo de la seguridad informática, muchas de las compañías especializadas se apuran a lanzar aplicaciones que combatan este tipo de amenazas.

En el caso de Symantec, la compañía acaba de presentar Norton Confidential, un paquete de seguridad –aún en beta- que tiene por objetivo que los usuarios recuperen la confianza en las transacciones electrónicas vía Web.

Según Enrique Salem, Presidente de Productos y Soluciones para el Consumidor de Symantec, "en un contexto en que Internet presenta una gran cantidad de sitios y amenazas de estafa electrónica que roban información con fines económicos, la confianza de los clientes para realizar negocios en línea se ha erosionado". De esta manera, la empresa afirma que su nuevo producto ofrecerá protección de la información personal "en el punto de mayor riesgo: durante una transacción, al inicio de sesión o al enviar datos confidenciales a un sitio Web".

De acuerdo con Symantec, Norton Confidential combina las tradicionales listas de bloqueo con nuevas tecnología heurísticas que protegen a los consumidores de amenazas que aún no han sido expuestas públicamente. Según la empresa, esta protección del tipo "hora-cero" es crucial, ya que los ataques están diseñados para ser efímeros y -por lo tanto- difíciles de detectar. De hecho, según el Anti-Phishing Group, un sitio de estafa electrónica está en línea sólo unos cinco días antes de que sea desmontado y remplazado por un nuevo sitio Web fraudulento.

En cuanto a las transacciones online, Symantec asegura que el nuevo producto ayudará al usuario a distinguir fácilmente entre los sitios seguros y aquellos que son fraudulentos. De esta manera, cuando el usuario visite un sitio genuino del tipo SSL, Norton Confidential advertirá al consumidor que puede proceder tranquilamente al mostrar una clave visual especial.

Por otro lado, el nuevo software también añade protección heurística para otras amenazas como keystroke loggers, troyanos, y otros códigos maliciosos que atacan las contraseñas y captan información confidencial de los consumidores.

Tal como informó la compañía, el nuevo Norton Confidential estará disponible para Windows en septiembre y para Macintosh en octubre.

Los usuarios interesados pueden registrarse como beta testers del nuevo software en

http://www.symantec.com/home_homeoffice/transactsafely/overview.jsp

Fuente: *www.tectimes.com*

IBM Construye Transistor 100 Veces Más Rápido

Alfredo De Jesús Gutiérrez Gómez
neojag@hotmail.com

IBM ha construido un transistor que corre aproximadamente 100 veces más rápido que los chips actuales, un desarrollo que puede pavimentar la vía para computadores ultra rápidos y redes inalámbricas. Este record se logró construyendo un transistor de silicio mezclado con germanio. El transistor obtuvo una velocidad de 500 GHz, más de 100 veces más rápido que los chips para PC vendidos hoy, y aproximadamente 250 veces más rápido que el chip de un teléfono móvil. Aunque estas velocidades fueron obtenidas trabajando a temperaturas cercanas al cero absoluto, se estima que correrán a 300GHz a temperatura ambiente. Se espera que los beneficios de este desarrollo aparezcan en productos en un par de años, probablemente en chips para crear redes inalámbricas muy rápidas que puedan mover una película con calidad de DVD en menos de cinco segundos.

Intel Recortaría Hasta 60% El Precio De Sus Chips

Alfredo De Jesús Gutiérrez Gómez
neojag@hotmail.com

Según algunas fuentes del mercado, Intel decidió recortar el precio de sus procesadores Pentium hasta 60% y en 15% los chips de doble núcleo. Si bien este movimiento puede obedecer a la necesidad de reducir inventarios - la empresa está preparando lanzamientos agresivos para los próximos meses - lo cierto es que el objetivo principal es frenar el aumento de participación de mercado de su rival AMD. Las rebajas comenzarían a fines de julio.

El Office 2007 Se Puede Probar En Línea

Gustavo Alberto Rodríguez
gustavo@sasoft.com.ar

Microsoft lanzó una versión de pruebas de lo que será su nueva suite de herramientas Office 2007 , con la particularidad de que no se necesita descargar ningún software para utilizarla dado que está íntegramente basada en Internet.

Bajo el lema "pruébelo antes de comprarlo", la firma de Bill Gates ofrece a cualquier internauta la posibilidad de examinar las nuevas opciones que formarán parte de las clásicas aplicaciones que componen la suite.

De momentos, el servicio se encuentra con una alta demanda por lo que los tiempos de espera para el acceder a las pruebas son elevados.

Según la compañía, más de 2,5 millones de personas utilizan la Beta 2 del sistema lanzada el mes pasado.

Para probar el Office 2007 en línea, visite:
http://www.microsoft.com/office/preview/beta/testdrive.mspx

Link corto: *http://www.lanacion.com.ar/818460*

Intel Dice Que Comenzará A Servir El Chip De Doble Núcleo Xeon De Inmediato

Martin R. Mondragón Sotelo
mygnet@gmail.com

Intel, el mayor fabricante de semiconductores del mundo, ha dicho que planea comenzar a enviar esta semana nuevos procesadores para servidores, tratando de frenar una ofensiva de su rival Advanced Micro Devices (AMD).

Las nuevas series de procesadores de doble núcleo Xeon, que previamente llamó Woodcrest, son los primeros de una gama de productos con un diseño más eficaz. Intel ha dicho que el diseño permitirá un mejor funcionamiento y un menor consumo de energía.

AMD, que una vez estuvo relegado a copiar los avances de su rival, ha dado la vuelta a la situación en los últimos años con innovaciones como poner dos núcleos de procesamiento en un solo chip, lo que permite realizar multitareas de forma más eficiente.

Microsoft Podría Comprar Yahoo

Juan Francisco Berrocal
berrocal239@hotmail.com

Mientras Google consolida su posición dominante en el mercado de búsquedas en Internet, parece cada vez más probable que Microsoft adquiera una gran empresa de la red como Yahoo, dijo ayer el banco de inversión Merrill Lynch.

Una eventual decisión de Microsoft de adquirir Yahoo aceleraría los intentos del gigante del software de construir su negocio de búsquedas, impulsar su presencia en Asia y eliminar un rival, según el informe.

El texto, escrito por el analista de Merrill Lynch, Justin Post, llega en un momento crítico para la compañía Microsoft.

La firma, cuyo sistema operativo Windows está presente en el 90% de las computadoras personales del mundo, lucha por hallar fuentes de crecimiento más allá de su negocio tradicional de producción de software.

Además, el fundador Bill Gates dijo a principios de este mes que en los próximos dos años tiene pensado abandonar el trabajo del día a día en la empresa.

Las presiones sobre Microsoft, que ha sufrido la caída de un 10% de su valor accionario en el último año, han hecho crecer las especulaciones de que podría considerar una gran adquisición como Yahoo o eBay.

"Microsoft ha ido tarde en Internet y, dada la significativa inversión financiera que ha afectado al precio de las acciones de Microsoft, el nuevo equipo administrativo tendrá una mayor presión para competir eficazmente con los líderes de Internet", escribió Post, de Merrill Lynch.

"Una eventual adquisición (...) reduciría los riesgos y el horizonte de tiempo para que Microsoft reconduzca sus acciones y haga rentable su unidad MSN", dijo.

Fedora Core 6 Test 1

Moises Perez
moy456xx@gmail.com

Ya está disponible para su libre descarga el test 1 del Core 6 de Fedora, que viene a sustituir a la versión libre de Red Hat. Recordemos que Fedora es el nombre clave del proyecto que ha tomado las riendas de la versión gratuíta de Red Hat Linux.

Fedora es una distribución íntegramente basada en software libre y desarrollada por la comunidad.

http://download.fedora.redhat.com/pub/fedora/linux/core/test/5.90/

Lanzamiento Oficial De Windows Live Messenger

Gustavo Alberto Rodríguez
gustavo@sasoft.com.ar

Después de varios meses en versión beta, Microsoft lanzó la versión final de Windows Live Messenger, la aplicación que eventualmente reemplazará a su mensajero MSN.

Según Microsoft, entre las funcionalidades que posee el nuevo software se encuentran: telefonía IP mejorada, conversaciones con video incorporado, la posibilidad de compartir carpetas entre los usuarios, el envío de mensajes de texto a celulares, una nueva libreta de direcciones y alertas de Windows Live. También se incluyen varios juegos interactivos y la posibilidad de enviar mensajes aunque el receptor no esté conectado.

De acuerdo con la empresa, próximamente los usuarios de Windows Live Messenger podrán intercambiar mensajes con personas que utilicen el mensajero de Yahoo!

El nuevo software sólo puede correr desde equipos que cuenten con Windows XP Service Pack 2 o tengan instalada la beta 2 de Windows Vista.

El link para descargar el nuevo software es: *http://imagine-msn.com/messenger/launch80/default.aspx?locale=es-us&source=msncommessenger*

Fuente: *www.tectimes.com*

Firefox Sincronizado

Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Google lanzó un plugin que permite sincronizar las preferencias del navegador entre varias PCs

La empresa Google lanzó una extensión para Firefox que permite sincronizar seteos como favoritos, historial, cookies y passwords entre distintas PCs. Las preferencias de los navegadores que utilicen este sistema se almacenarán en los servidores de Google, y estarán encriptadas bajo una clave única para impedir accesos no autorizados.

La nueva funcionalidad resultará especialmente útil para aquellos usuarios que utilizan múltiples computadores, por ejemplo una laptop y una PC. Así cualquier cambio introducido en el navegador, como el añadido de un nuevo favorito, será trasladado inmediatamente al otro equipo. Además, Firefox "recordará" las pestañas que estaban abiertas en una de las máquinas durante la última sesión, y las reabrirá en la computadora alternativa.

Como el navegador necesita contactarse con Google cada vez que se inicia, la compañía advirtió que este proceso podría incrementar el tiempo de arranque del programa. Sin embargo, Google también comunicó que se encuentra trabajando para minimizar este problema.

El plugin trabaja con Firefox 1.5 o versiones posteriores. La URL de descarga es:
http://www.google.com/tools/firefox/browsersync/index.html
http://www.tectimes.com/secciones/notas.asp?codnota=18897

La Tecnología Wi-fi Avanza En España

Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

Madrid posee más 800.000 usuarios de este sistema inalámbrico

La tecnología inalámbrica avanza rápidamente en la península Ibérica, con más de seis millones de usuarios. Según el estudio 'V Informe del Observatorio Wireless' elaborado por la empresa Iber Band Exchange, Madrid con cuenta con 805.556 personas que utilizan Wi-Fi, seguida por Barcelona con 708.333; Valencia, con 319.444; Sevilla, con 250.000; y Bilbao, con 152.778

De acuerdo con el informe, el avance se apoya en la proliferación de puntos de acceso ('hot spots') en las principales ciudades

Según el sitio CDT Internet, las cinco ciudades citadas en el informe cuentan con un total de 2.450 puntos comerciales de acceso Wi-Fi a Internet, de los que el 52% pertenecen al sector de la hotelería, y están situados principalmente en bares, hoteles y discobares.

Madrid cuenta ya con 17.150 puntos de acceso, de los que 16.520 son privados y los 630 restantes comerciales. Barcelona, aunque es la segunda en número de usuarios, es la ciudad con mayor número de puntos de acceso inalámbrico a Internet, un total de 20.610, de los que 19.615 son privados, y 995 comerciales.

El 19 % de los puntos de acceso comerciales corresponden al sector servicios, mientras que un 17 % se encuentran al aire libre, y otro 12 % se encuentran en centros de enseñanza. Bilbao es la única ciudad que cuenta con más 'hot spots' de uso libre que en los sectores comerciales.

Según el informe, el perfil de los usuarios de tecnología Wi-Fi está compuesto por personas mayores de 25 años, de clase media alta, ejecutivos de alto poder adquisitivo, y turistas

http://www.tectimes.com/secciones/notas.asp?codnota=18915

Opera 9 Ya Está Aquí

Gustavo Alberto Rodríguez
gustavo@sasoft.com.ar

Fuente: *www.tectimes.com*

Finalmente, después de algunos meses en beta, la empresa Opera Software lanzó oficialmente la versión 9 de su navegador. De esta manera, la compañía noruega desafía abiertamente a sus principales rivales, Explorer de Microsoft y Firefox de la Fundación Mozilla.

La nueva versión fue lanzada en 25 idiomas, y con compatibilidad con las plataformas Windows, Linux y Mac OS X. Entre las nuevas características de Opera 9 se encuentran la incorporación de Widgets y el soporte para descargar archivos a través del protocolo BitTorrent.

Tal como sucede en otros tipos de software, los widgets son aplicaciones muy livianas que pueden ser utilizadas para proveer servicios e información al usuario. En el caso de Opera, los widgets están basados en lenguajes como JavaScript y DHTML. Según la compañía, los nuevos widgets podrán ser usados para lectores de noticias, juegos, y funcionalidades multimedia.

Según el CEO de Opera Software, Jon S. von Tetzchner, la empresa “trabajó duro para traspasar los límites de lo que los usuarios esperan de un navegador web, con mayor velocidad, mayor soporte de estándares y características innovadoras como los widgets y el soporte de BitTorrent” Según el sitio Beta News, esta última funcionalidad será muy útil para aquellos usuarios que quieran descargar archivos BitTorrent sin tener que recurrir a una aplicación externa. Los usuarios también podrán rastrear este tipo de contenidos gracias al buscador integrado al navegador.

La presencia de esta herramienta podría ser resistida por los defensores de los derechos de propiedad intelectual, ya que habitualmente el sistema BitTorrent es utilizado para descargar películas de forma “ilegal”. Sin embargo, existen usos menos controvertidos para este tipo de funcionalidades, como la distribución de software de código abierto, o todo aquel contenido que necesite ser distribuido rápidamente a gran escala.

Por otro lado, Opera 9 también incorpora un bloqueador para limitar el acceso a determinadas publicidades e imágenes de la web. Además, dentro de la nueva barra de seguridad se ofrece protección contra el phishing y otros delitos de robo de identidad. Otra nueva función es la vista previa que aparece al pasar el mouse sobre determinada pestaña cerrada.

Para promocionar su nuevo navegador, la empresa creó una campaña de marketing llamada “tu web, tu elección” que pone el foco sobre la capacidad para optar por un navegador distinto al predeterminado de Windows, es decir Internet Explorer. Para resaltar la campaña, la compañía también creó una compleja animación en la home page de su sitio web, en la que las nuevas características de Opera 9 están representadas por distintos personajes que bailan en una fiesta.

Al igual que la versión anterior, Opera 9 es de descarga gratuita.

www.opera.com

Stallman: "el 'software' Que No Es Libre Trata De Prohibir La Solidaridad Social"

Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

SAN SEBASTIÁN.- **Richard M.Stallman** ha estado de nuevo en España. El considerado como el padre del 'software' libre defendió en San Sebastián este tipo de sistemas **frente a los privativos**, impulsados por grandes corporaciones informáticas como Microsoft que, en su opinión, lo que quieren es **"prohibir la cooperación y la solidaridad social"**.

Stallman, en San Sebastián. (Foto: EFE)

Stallman, quien participó en unas jornadas organizadas por la Cátedra Sánchez Mazas de la Universidad Pública del País Vasco, detalló a los periodistas las **ventajas del 'software' libre que respeta, en todo caso, la "voluntad del usuario"**. Explicó que el usuario puede ejecutar el programa como desee, cambiar el código fuente y distribuir copias y versiones modificadas.

Todos los usuarios deben tener estas libertades, ya que lo contrario sería "injusto", enfatizó Stallman, quien abogó por "eliminar el mal social" que acarrea el 'software' privativo, que pretende "prohibir la solidaridad" y "castigar" a los que comparten. La meta es "liberar completamente el ciberespacio y a todos sus habitantes", ironizó este licenciado en Física por la Universidad de Harvard.

Tras precisar que 'software' libre **no es sinónimo de gratuito sino que implica que se puede copiar, modificar y distribuir con libertad**, Stallman dijo que hay miles de programas que cumplen estos requisitos con los que se puede hacer "todo" en un ordenador sin ser tentado a abandonar la libertad.

También en la música

"No queremos imponer la cooperación" sino dar la posibilidad de compartir siempre que se desee, añadió Stallman, quien comentó que su filosofía puede aplicarse a **otros ámbitos, como es el caso de la música**.

Recordó una anécdota que le ocurrió en una de sus primeras visitas al País Vasco cuando fue obsequiado con un disco

compacto que se vio obligado a devolver tras comprobar que **era un objeto "corrupto" producido para "no ser leído libremente"**.

Resumió su proyecto como una "lucha por la libertad que se puede perder o ganar", pero que trata de ir contra un sistema "injusto" que además genera "impotencia".

http://www.elmundo.es/navegante/2006/06/20/softlibre/1150789354.html

Crear Un Virus Para Buscar Empleo

Pedro
Linux1982@gmail.com

"Soy el autor del virus Yamanner que fue descubierto el 12 de junio (...), he de decir que no me gusta molestar a nadie. Como vivo en Irán conseguir trabajo en una buena compañía informática es muy difícil y sólo quería probar que tengo habilidades de programación". Es parte del mensaje que varias compañías de seguridad han recibido de una persona que dice ser la responsable del gusano que durante la última semana ha castigado miles de cuentas de correo de Yahoo! Sea o no cierto que es el responsable del ataque, su extraña solicitud de empleo ha sido rechazada. También de Irán proviene el nuevo responsable de seguridad de Microsoft, Ben Fathi, que según informa Kriptópolis se desvincula de la seguridad del sistema operativo Windows Vista en sus primeras declaraciones.

Adios Billi!

Pedro
Linux1982@gmail.com

NUEVA YORK (AFP) - Ray Ozzie, que entró en Microsoft en 2005, sucederá a Bill Gates como jefe de ingenieros de sistemas en momentos en que el dominio de Microsoft en el mundo informático debe adaptarse a internet.

Microsoft anunció el jueves que su fundador, Bill Gates, abandonará progresivamente sus funciones en la dirección operativa hacia julio de 2008, cuando se mantendrá solamente a la cabeza del consejo de administración. Su título de arquitecto jefe de informática, nombre que se le da en la firma al jefe de desarrollo de productos, recae inmediatamente sobre Ray Ozzie, quien en la primavera de 2005 había asumido las funciones de director técnico, cuando Microsoft compró Groove Networks. Ozzie, de 50 años, había fundado en 1997 ese grupo especializado en programas informáticos de trabajo a distancia en tiempo real. Los analistas se mostraban escasamente preocupados el viernes por ese cambio al frente de Microsoft, insistiendo en que se trataba de una sucesión bien preparada por Bill Gates (que ya había cedido en 2000 su cargo de presidente a Steve Ballmer) y en la buena reputación de Ray Ozzie. Antes de sus inicios en Groove Networks, Ozzie había creado en los años 80 los programas de mensajería para profesionales Lotus Notes (desarrollados luego por IBM), y pasa por ser uno de los mejores programadores de aplicaciones profesionales del mundo. Los inversores parecían tener dificultades para recuperar la confianza tras los fiascos vinculados al dubitativo arranque estos últimos meses de la consola de videojuegos Xbox 360 y, sobre todo, a la salida retardada de Windows Vista, el nuevo sistema operativo de Microsoft. La acción del grupo perdió más de un 20% de su valor desde fines de enero.

Gusano Vía Msn Messenger

Martin R. Mondragón Sotelo
mygnet@gmail.com

Se trata de un gusano que se propaga a través de Microsoft MSN Messenger y que ya ha producido diversas incidencias.

PandaLabs, laboratorio de la empresa de software de seguridad Panda Software, advierte sobre la propagación de la nueva variante del gusano BlackAngel, en este caso la versión B. Hasta el momento, PandaLabs ha recogido diversas incidencias de usuarios afectados por los efectos de este gusano.

Este gusano utiliza para propagarse la herramienta de mensajería **Microsoft MSN Messenge**r. Para ello, envía mensajes a la lista de direcciones del usuario, haciéndose pasar por un video con el título “Fantasma”. El usuario receptor, si lo abre, verá en pantalla una imagen con el texto “En el 1er día te espantas, en el 2º te desesperas, en el 3º buscas ayuda y en el 4º mueres”.

Una vez abierto el archivo, el código de BlackAngel.B llevará a cabo varias modificaciones en el sistema, entre las que destacan el cierre de distintas aplicaciones de seguridad (antivirus, firewalls, etc.) con el fin de evitar ser detectado. Además, intenta cerrar distintas ventanas para que el usuario no pueda usar las herramientas de configuración del sistema operativo. Estas ventanas son

- Administrador de tareas de Windows
- Panel de control
- Editor del Registro
- Utilidad de configuración del sistema
- Restaurar sistema

Para propagarse a los contactos de **MSN Messenger**, bloquea una ventana de esta aplicación y evita que el usuario pueda acceder a ella. Desde esta ventana inicia una conversión con los contactos en la que envía mensajes como “jaja look a that” o “mira este video” y una dirección web desde la que descargar el gusano para infectar otro ordenador.

Este gusano de nueva creación ha sido detectado y neutralizado proactivamente por las **Tecnologías TruPrevent™**, aún sin conocerlo con anterioridad. De este modo, los usuarios de soluciones Panda Software han estado protegidos desde el primer momento.

Sobre PandaLabs

Desde 1990, tiene como misión analizar las nuevas amenazas lo antes posible para mantener seguros a nuestros clientes. Varios equipos especializados en cada tipo concreto de malware (virus, gusanos, troyanos, spyware, phishing, spam, etc.) trabajan 24x7 ofreciendo una cobertura global. Para ello, se apoya en las **Tecnologías TruPrevent™**, un auténtico sistema global de alerta temprana formado por sensores estratégicamente distribuidos, que neutraliza nuevas amenazas y las envía a PandaLabs para su análisis en profundidad. De acuerdo con Av.Test.org, actualmente, PandaLabs es el laboratorio más rápido de la industria en proporcionar actualizaciones completas a los usuarios (más información en www.pandasoftware.es/pandalabs.asp/).

Para más información: *http://www.pandasoftware.es/virus_info/*

Microsoft Despide Win 98

Pedro
Linux1982@gmail.com

El próximo 11 de julio finalizar el soporte oficial de Microsoft a las versiones 98 y Millenium de Windows.

A partir de esa fecha las actualizaciones mensuales de seguridad de Microsoft para estos usuarios desaparecerán así como el soporte técnico y por lo tanto los usuarios pueden enfrentarse a riesgos importantes.

Por supuesto, Microsoft aconseja actualizar las versiones a la más reciente y a aquellos que prefieran seguir usando 98 y tengan acceso a internet, filtren el tráfico procedente del puerto TCP 139. Un mal menor... pero suficiente para dejar al menos equipo un poco más protegido.

Google Saca En Beta Un Servicio 'on Line' Similar A Excel De Microsoft, Pero Gratis

Evelyn Elizabeth Llumitasig Alvarez
evelyneli86@gmail.com

SAN FRANCISCO (EEUU).- El buscador estadounidense Google ha puesto en marcha un servicio una versión experimental de una nueva aplicación en línea para crear hojas de cálculo, accesible completamente gratis a través de Internet. Nace una dura competencia para programas tan populares como Excel, que pertenece a la 'suite' Office, de Microsoft.

De momento, este programa está en pruebas en Google Labs, aunque a disposición de un número limitado de internautas para que realicen pruebas con esta aplicación para gestionar datos en forma de tablas.

Con esta nueva herramienta Google vuelve una vez más a jugar en un terreno que tradicionalmente ha sido el reino del gigante Microsoft, el mayor fabricante de 'software' del mundo. Su célebre programa Excel cuenta ahora con una aplicación similar, completamente gratis y en la Red.

Según algunos analistas de la firma Jupiter Research, Google está posicionándose para luchar directamente contra Microsoft, pero se muestran algo escépticos. "El público en general no utiliza tablas, y particularmente no creo que los directores técnicos de las empresas abandonen Excel por una aplicación gratis accesible a través de Intenet", comentó el analista David Card.

http://www.elmundo.es/navegante/2006/06/07/empresas/1149666877.html

Desmantelada Una Red De Falsificación De Tarjetas De Crédito [20-05-06]

Alfredo De Jesús Gutiérrez Gómez
neojag@hotmail.com

Desmantelada una red de falsificación de tarjetas de crédito

La Guardia Civil ha desmantelado en Cáceres una red internacional que se dedicaba a la falsificación de tarjetas de crédito. En la operación "Ala ancha", han sido detenidas nueve personas de nacionalidad cubana, una de las cuales fue arrestada en Madrid. Estos delincuentes podrían haber estafado cerca de 2 millones de euros en compras realizadas en establecimientos comerciales.

La operación se inició a finales del pasado mes de enero, cuando los agentes sospecharon de varias personas que estaban realizando compras por importantes cantidades de dinero en distintos establecimientos comerciales de la localidad de Navalmoral de la Mata (Cáceres) y su comarca, utilizando para ello tarjetas de crédito expedidas a un mismo nombre.

Posteriores investigaciones permitieron constatar que al menos ocho personas diferentes utilizaban la misma tarjeta en puntos diferentes y, en algunos casos, al mismo tiempo, en las provincias de Badajoz, Cáceres, Toledo, Madrid, Ávila, Burgos e incluso Portugal. Una vez que la Guardia Civil pudo comprobar que se habían utilizado 32 tarjetas de crédito duplicadas, el objetivo se centró en la localización y detención de las personas que integraban el grupo delictivo.

Según las investigaciones se pudo identificar al cabecilla de la organización, que previo pago de una cierta cantidad de dinero, duplicaba tarjetas de crédito para su uso fraudulento por parte de otras personas que conseguían de forma ilegal la información bancaria necesaria.

La clonación de las tarjetas de crédito se realizaba mediante la obtención de los datos de las bandas magnéticas de las víctimas, utilizando para ello unos pequeños lectores que utilizaban en connivencia con empleados de algunos comercios. Estos empleados cobraban a los clientes pasando la tarjeta por el terminal de venta (TPV), y seguidamente la pasaban una segunda vez por un lector que almacenaba los datos en su memoria para un posterior uso ilícito.

Estos datos obtenidos se volcaban sobre la banda magnética

virgen de una tarjeta nueva, troquelando posteriormente el nombre de la persona ficticia que se ampararía bajo un pasaporte o una licencia de conducir falsos. Las tarjetas se utilizaban para adquirir determinados bienes, preferentemente electrodomésticos, televisores de plasma, equipos informáticos, teléfonos móviles de última generación, joyas, ropa de marca y productos de perfumería.

El fraude realizado al propietario legal de la tarjeta duplicada, oscilaba entre los 1.800 y 8.500 euros, aprovechando los primeros días de cada mes cuando tenían constancia del ingreso de la nómina.

Symantec Exige Detener El Desarrollo De Windows Vista

Juan Francisco Berrocal
berrocal239@hotmail.com

A través de una demanda presentada en los tribunales estadounidenses, la firma de seguridad alega que Microsoft utiliza en forma indebida una tecnología de almacenamiento cuya propiedad intelectual adquirió en 2005. El requerimiento también afecta a Windows XP y Windows 2003 Server.

La disputa entre ambas multinacionales surge de un acuerdo firmado en 1996 entre Microsoft y la empresa Veritas para que Windows pudiera beneficiarse con su tecnología de almacenamiento por volúmenes. Sin embargo, tras la adquisición de Veritas por Symantec el año pasado, ésta alegó que los términos del contrato habían sido violados.

Ésto es así, alegan, porque el mismo prohibe a Microsoft desarrollar productos que compitan con los de Veritas, algo que en opinión de Symantec ocurre por la forma en que Vista almacena datos y administra sus unidades de disco. "Lo que pedimos es remover la tecnología, porque nos pertenece", afirmó un representante de la empresa a PCWorld.

Por su parte, Microsoft emitió un comunicado donde reafirma su derecho a utilizar la tecnología de Veritas. "El contrato de 1996 nos dio la posibilidad de comprar tanto los derechos como el código y la propiedad intelectual, lo que hicimos en 2004", establece.

Symantec hizo sus exigencias el mismo año, cuando obtuvo detalles de un lanzamiento previo del sistema en la Conferencia de Ingeniería en Hardware de Windows. Ahora, el requerimiento aumenta las tensiones entre ambas empresas, ya afectadas por el ingreso de Microsoft al mercado de la seguridad informática.

Apple Pierde El Juicio Contra Los Weblogs

Juan Francisco Berrocal
berrocal239@hotmail.com

El Juez de la Corte de Apelación de California acordó que la confidencialidad de las fuentes de los periodistas de los sitios de noticias esta protegida por la primera enmienda de la constitución estadounidense.

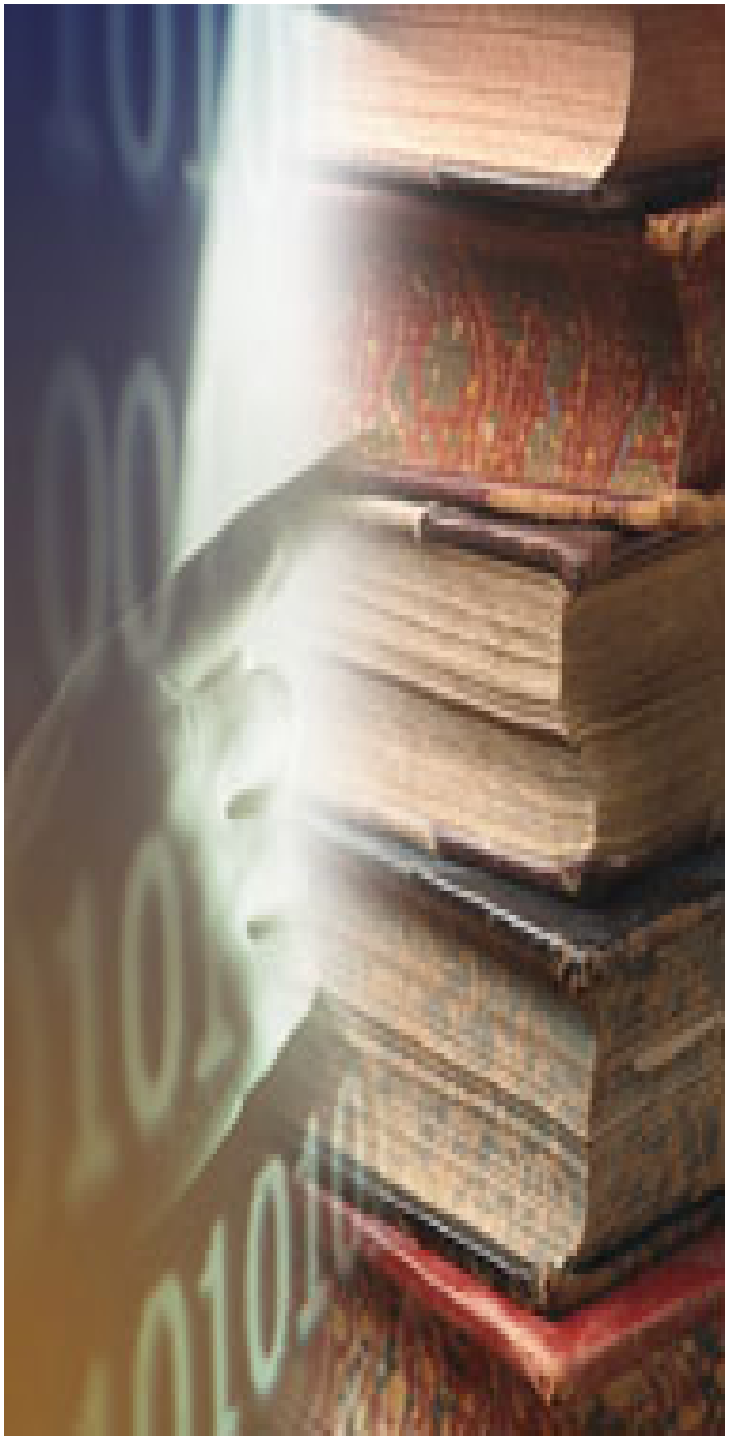
Apple ha sufrido un importante revés en el frente que mantiene con aquellos sitios de internet que publican noticias y rumores sobre proyectos de la empresa. La firma informática inició una demanda para procesar a unos individuos no identificados que habían contado información sobre un producto en fase de desarrollo (**Asteroid**) a periodistas de PowerRage.com y Appleinsider.com.

En su demanda, Apple exigía que ambas publicaciones online divulgaran cuales eran sus fuentes para poder proceder en su contra. Apple insistía que las informaciones publicadas eran no legitimas al no contar con la autorización de la firma para ser divulgadas.

El juez dió la razón a los abogados de PowerPage e AppleInsider al considerar que es imposible identificar cuales son las noticias legitimas de las ilegitimas y que cualquier distinción en este terreno entraría en confrontación con la libertad de información que protege la primera enmienda de la Constitución estadounidense. También acordó que la confidencialidad d las fuentes, incluso en el caso de publicaciones digitales, esta protegida por la primera enmienda.

Para la EFF, esta decisión judicial "*es una victoria clara para los periodistas online y offline, y el publico en general*", dijo su abogado **Kurt Opsahl**. Éste insistió que la "*Corte garantizó la protección y la libre circulación de la información para la prensa y de la prensa hacía el público*".

Manuales del mes



Fox pro

Método y comandos

Fox-pro

Lupita Alamilla Garcia
lupita_neil@hotmail.com
Tamaño: 61 KB
Este manual es una descripción en general del uso de foxpro
http://www.mygnet.com/pages/down.php?man=874

Formularios

Números a palabras en un form de visual fox pro 1-

Juan
aldevaran_527@hotmail.com
Tamaño: 7 KB
Form de ejemplo para deletrear números a palabras desde visual fox pro . instrucciones: descomprimir en c:\ va a autocrear un directorio paso1 asi c:\paso1 luego llamar desde el visual fox pro ubicando esta carpeta en c:\ author :aldevaran_527@hotmail.com
http://www.mygnet.com/pages/down.php?man=890

Hardware

Discos duros

Jose Gutierrez Saenz
bugsjard@hotmail.com
Tamaño: 20 KB
Malual sobre discos durpos
http://www.mygnet.com/pages/down.php?man=887

Linux

Construccion de un vehiculo explorador

Daniel Enrique Velazquez Borja
dvelazquez@linuxmail.org
Tamaño: 653 KB
Es el reporte del vehiculo explorador que hice para la clase de micros i, por ahi en la seccion de c y en ensamblador estan los codigos por separado. se trata de controlar una nave terrestre via internet
http://www.mygnet.com/pages/down.php?man=878

Java

P2p y jxta

Douglas Quintero Vinces
djquintero83@yahoo.com
Tamaño: 185 KB
Este pdf son uno slides que explican de una manera breve todo acerca de la jxta y de las aplicaciones p2p
http://www.mygnet.com/pages/down.php?man=891

Guia de programacion de jxta

Douglas Quintero Vinces
djquintero83@yahoo.com
Tamaño: 968 KB
Esta la guia de programacion de jxta muy buena para comenzar tu desarrollo
http://www.mygnet.com/pages/down.php?man=889

Linux

Linux

Linux

Pedro
linux1982@gmail.com
Tamaño: 269 KB
Manual, de linux para principiantes....espero sea de ayuda
http://www.mygnet.com/pages/down.php?man=880

Macros

Macros en excel

Hans Abel
hansabel@hotmail.com
Tamaño: 375 KB
Manual sencillo con lo básico para empezar a realizar macros en excel
http://www.mygnet.com/pages/down.php?man=885

Matlab

Guide matlab

Oscar Ramiro
starrider2_007@hotmail.com
Tamaño: 793 KB
Manual para realizar una interfaz con el matlab, para calcular la derivada I aintegral y la serie de furier
http://www.mygnet.com/pages/down.php?man=884

Mysql

Biblia de mysql

Enrique
fatcorona@hotmail.com
Tamaño: 6 MB
La biblia de mysql en inglés
http://www.mygnet.com/pages/down.php?man=898

Manejo de base datos

Mysql con clase

Alejandro Benavides
abenavidescr@gmail.com
Tamaño: 259 KB
Manual de referencias para utilizar mysql (muy bueno)
http://www.mygnet.com/pages/down.php?man=900

Manual de mysql

José Edgardo Mendoza Mayén
edgardo.mayen@navegante.com.sv
Tamaño: 145 KB
Este es un manua para un ayudarte en la configuración de tu mysql y cargar tus tablas espero que te ayuda
http://www.mygnet.com/pages/down.php?man=886

Ninguno

Seguridad

Jesús Morphi Gonza Lex
soul_angel13@hotmail.com
Tamaño: 174 KB
Seguridad
http://www.mygnet.com/pages/down.php?man=897

Comandos basicos de linux

Pedro Calderon
linux1982@gmail.com
Tamaño: 29 KB
En este manual, conseuiras casi todos lo comandos, de la consola de linux, esta en formato odb, que es el fomato de documentos de openoffice... apoyemos el moviento opensource
http://www.mygnet.com/pages/down.php?man=881

Cálculo y conversiones

Mathematicas 5.0

Christian Mora
christmo_99@yahoo.com

Tamaño: 1 MB
Es un completisimo tutor, para el mejor manejo del programa de cálculo mathematicas 5.0... disfrutenlo!!!
http://www.mygnet.com/pages/down.php?man=877

Multimedia

Infraestructura para servicios multimedias 02

Douglas Quintero Vinces
djquintero83@yahoo.com
Tamaño: 3 MB
Segunda parte del archivo pdf donde veras la infraestructura que debe tener un servicio multimedia
http://www.mygnet.com/pages/down.php?man=876

Infraestructura para servicios multimedias 01

Douglas Quintero Vinces
djquintero83@yahoo.com
Tamaño: 1 MB
Primera parte del archivo pdf donde veras la infraestructura que debe tener un servicio multimedia
http://www.mygnet.com/pages/down.php?man=875

Oracle

Manejo de base datos

Iniciacion a oracle

Ehooo
web.ehooo@gmail.com
Tamaño: 580 KB
Curso de iniciacion aoracle 8
http://www.mygnet.com/pages/down.php?man=899

Php

Php biblia español

Stig Sæther Bakken, Editado Por Rafael Martínez
fatcorona@hotmail.com
Tamaño: 3 MB
La binblia de php en español
http://www.mygnet.com/pages/down.php?man=896

Apache y php

Pedro
linux1982@gmail.com
Tamaño: 22 KB
Sencillo tutorial de apache y php
http://www.mygnet.com/pages/down.php?man=882

Redes

Fundamentos de tcp-ip

Jose Gutierrez Saenz
bugsjard@hotmail.com
Tamaño: 443 KB
Fundamentos tcp-ip
http://www.mygnet.com/pages/down.php?man=883

Varios

Tipos de redes

Pedro
linux1982@gmail.com
Tamaño: 6 KB
Breve manualiio de los tipos de redes
http://www.mygnet.com/pages/down.php?man=888

Seguridad

Cifrado

Douglas Quintero Vinces
djquintero83@yahoo.com
Tamaño: 109 KB
Este pdf nos muestra las tecnicas de cifrado mas comunes
http://www.mygnet.com/pages/down.php?man=895

Software

Diseño de sistemas de informacion

Douglas Quintero Vinces
djquintero83@yahoo.com
Tamaño: 184 KB
Buen manual con lo que se debe saber acerda del desarrollo de un diseño para un sistema de informacion
http://www.mygnet.com/pages/down.php?man=894

Modelos de requisitos

Douglas Quintero Vinces
djquintero83@yahoo.com
Tamaño: 127 KB
Este archivo muestra un buen modelo a seguir en la fase de peticion de requisitos del desarrollo de un producto de software
http://www.mygnet.com/pages/down.php?man=893

Vb.net

Fundamentos de la programacion

Gregor Flavio Conde Vilca
flavgregor@hotmail.com
Tamaño: 301 KB
Aprenda sobre que es fundamentos de programacion
http://www.mygnet.com/pages/down.php?man=879

Enlaces del mes

Asp.net

Descarga visual web developer express edition

Enviado por Juan Francisco Berrocal

Descarga la versión Express de visual Web Developer y a crear aplicaciones Web utilizando asp.net 2.0

http://www.microsoft.com/spanish/msdn/vstudio/express/vwd/default.mspx

Curso de desarrollo Web con visual Studio 2005

Enviado por Juan Francisco Berrocal

En este curso se tratan todas las cuestiones fundamentales que le permitirán crear aplicaciones Web con visual Studio 2005. al final del curso sabrá todo lo necesario para crear sus propias aplicaciones Web orientadas a datos y con multitud de características avanzadas

http://www.desarrollaconmsdn.com/msdn/cursos/curso_desarrollo_web_con_visual_studio_2005/index.html

Diseño Gráficos

Inkscape

Enviado por Gustavo Alberto Rodriguez

Inkscape es un editor de gráficos vectoriales de código abierto, con capacidades similares al illustrator, freehand, coreldraw o xara x, usando el estándar de la w3c: el formato de archivo scalable vector graphics (svg).

http://www.inkscape.org/

Diseño Web

La técnica raid

Enviado por Alfredo De Jesús Gutiérrez Gómez

Explica que es esta técnica.

http://www.desarrolloweb.com/faq/497.php

Utilizar información pública para realizar una web

Enviado por Alfredo De Jesús Gutiérrez Gómez

Muestra la utilidad de crear Web publicas y como

http://www.desarrolloweb.com/articulos/2468.php

J2ee

Manual de websphere 6 español

Enviado por Jose

Manual de administración websphere 6 en español. uso de wsadmin con ejemplos

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp

Varios

Articulo sobre diseño

Enviado por Douglas Quintero Vinces

Esto un buen articulo para aquellos que se dedican al diseño de soluciones de software

http://www.programacionextrema.org/articulos/designdead.es.html#tth_sec1

Jxta.org

Enviado por Douglas Quintero Vinces

Esta la pagina oficial de jxta

http://www.jxta.org/

Sistemas operativos de tiempo real orientado a componentes

Enviado por Douglas Quintero Vinces

Este es un artículo con ligera introducción y aplicaciones de los sistemas de tiempo real orientados a componentes

http://www.pablin.com.ar/electron/info/portos/

Php

Utilidad de los includes en php

Enviado por Alfredo De Jesús Gutiérrez Gómez

Muestra la forma en que se pueden crear plantillas utilizándolas con includes en php

http://www.desarrolloweb.com/articulos/2472.php

Software

Entrevista con richard stallman

Enviado por Ismael Utitiaj

Una entrevista realizada a Richard stallman sobre el software libre

http://ia300135.us.archive.org/3/items/invasioninvasionstallman/stallmaninterview.mp3

Unix

Alternativas al software de pago

Enviado por Ehooo

Esta es una página donde hay multitud de programas de software libre y lo comparan con otros programas de pago

http://alts.homelinux.net/index.php

Vb

The vb source code site

Enviado por Filiberto Ugarte Castañeda

Extenso sitio en inglés con códigos fuente para vb, vb.net, asp y asp.net

http://www.a1vbcode.com

Vrml

Tutorial de vrml97

Enviado por Filiberto Ugarte Castañeda

Escrito por narcís parés burguès. Incluye una recopilación de recursos, clientes vrml, exportadores, aplicaciones de autoría y vínculos.

http://www.iua.upf.es/~npares/docencia/vrml/tutorial_e.htm