SIBOS

Universo 07

www.sibos.com.mx

3er. Congreso

Tecnologías de Información y Comunicación

Expandiendo tus ideas

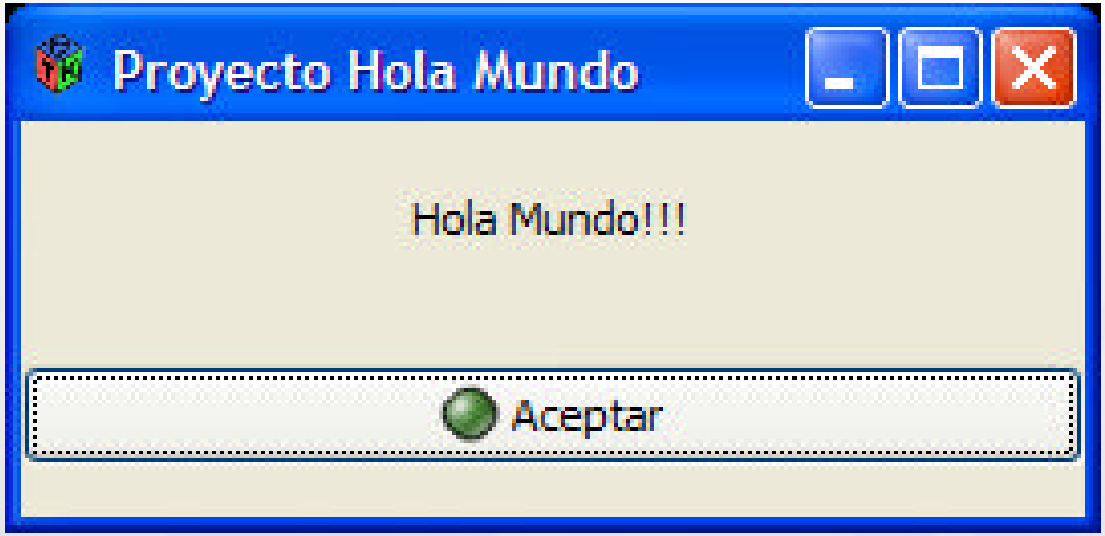
Realizado en la semana del 28 de mayo al 1ro. de Junio del 2007

FCC - BUAP

Memorias del Congreso

monodevelop

Ejemplo “Hola Mundo”



El mismo archivo compilado, se ejecuta sobre Windows.

monodevelop

Desarrollando con MonoDevelop (Mono, C# y Gtk#)

Ponente:
Alejandro García González

Tecnologías Involucradas

monodevelop

Proyecto Mono
http://www.mono-project.com/

Mono una una libre implementación de la plataforma de desarrollo **.Net**, enfocada principalmente a sistemas Unix, y con el propósito de brindar puentes de migración de Windows hacia Linux.

monodevelop

Tecnologías Involucradas

Proyecto Mono
http://www.mono-project.com/

- Máquina Virtual (Runtime)
- Biblioteca de Clases
- Compilador
- Common Language Runtime (CLR)
- Common Intermediate Language (CIL)

monodevelop

Tecnologías Involucradas

C#

C Sharp

Lenguaje de programación orientado a objetos desarrollado y estandarizado por Microsoft como parte de su plataforma .NET, que después fue aprobado como un estándar por la ECMA e ISO.

Mono cuenta con un compilador de C# que soporta la sintaxis de la versión 2.0

Tecnologías Involucradas

C#

C Sharp (Ejemplo)

```
using System;

namespace HolaMundo
{
  class MainClass
  {
    static void Main()
    {
      Console.WriteLine("Hola Mundo!!!");
    }
  }
}
```

```
[nexus@Develop ~]$ mcs holamundo.cs
[nexus@Develop ~]$ ./holamundo.exe
Hola Mundo!!!
```

monodevelop

Tecnologías Involucradas

Gtk# (GIMP toolkit Sharp)
http://www.gtk.org/
http://www.mono-project.com/GtkSharp

Conjunto de librerías para el desarrollo de Interfaces Gráficas de Usuario (GUI), usado principalmente en Gnome, pero con una naturaleza **Multiplataforma**.

Gtk# brinda un API sencillo y de gran desempeño para el desarrollo GUI de aplicaciones gráficas.

Tecnologías Involucradas

monodevelop

Bases de Datos

http://www.mysql.com/

http://www.postgresql.org/

Existe una gran gama de motores de bases de datos a las cuales podemos conectar nuestras aplicaciones, entre ellas destacan MySQL y PostgreSQL, quienes cuentan con “drivers” funcionando para .Net.

MySQL: Connector/Net

PostgreSQL: Npgsql

Nacimiento MonoDevelop

monodevelop

#Develop (SharpDevelop)
http://www.icsharpcode.net/OpenSource/SD/

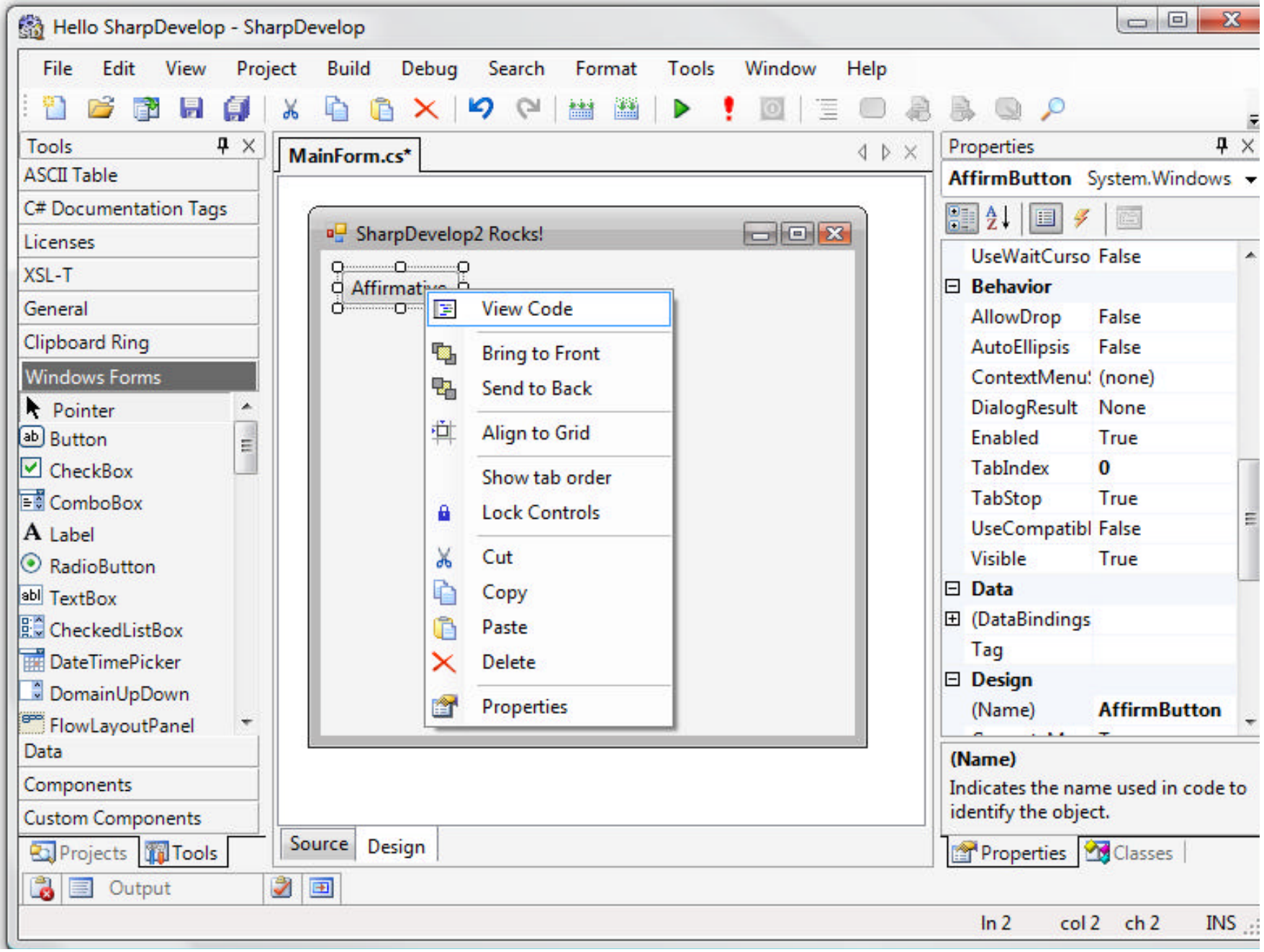
#Develop es un producto libre y gratuito realizado por la empresa “ic#code” para el desarrollo gráfico de aplicaciones con C# y VB.Net en la plataforma .Net sobre Windows.

Es una excelente alterativa a Visual Studio .Net

monodevelop

Nacimiento MonoDevelop

#Develop (SharpDevelop)



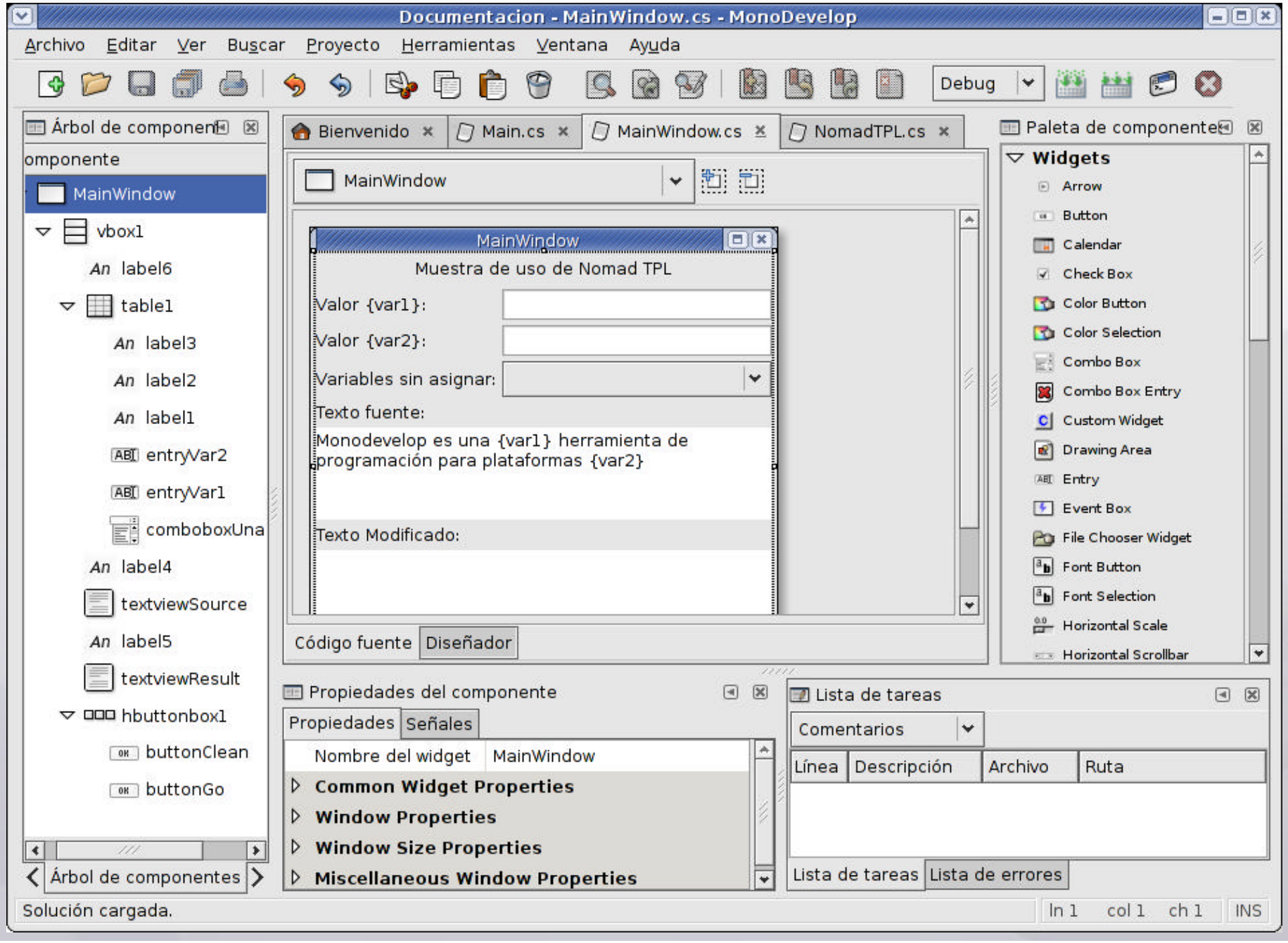
MonoDevelop
http://www.monodevelop.com/

MonoDevelop es un IDE para GNOME diseñado para programar en C# y otros lenguajes .NET

Actualmente se encuentra en la versión 0.13 y cuenta con una gran cantidad de características que deben ser tomadas en cuenta para un proyecto de tan corta edad.

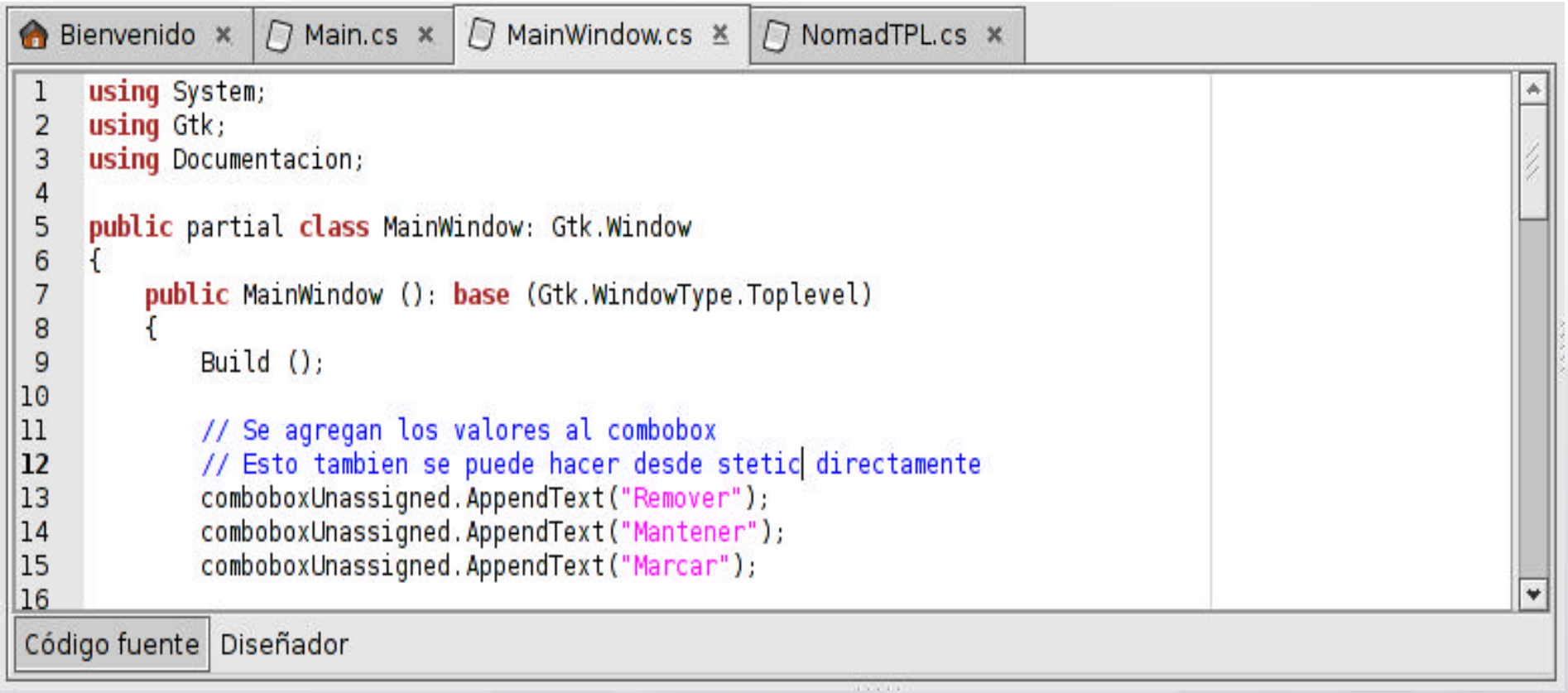
monodevelop

MonoDevelop



monodevelop

Editor de Código



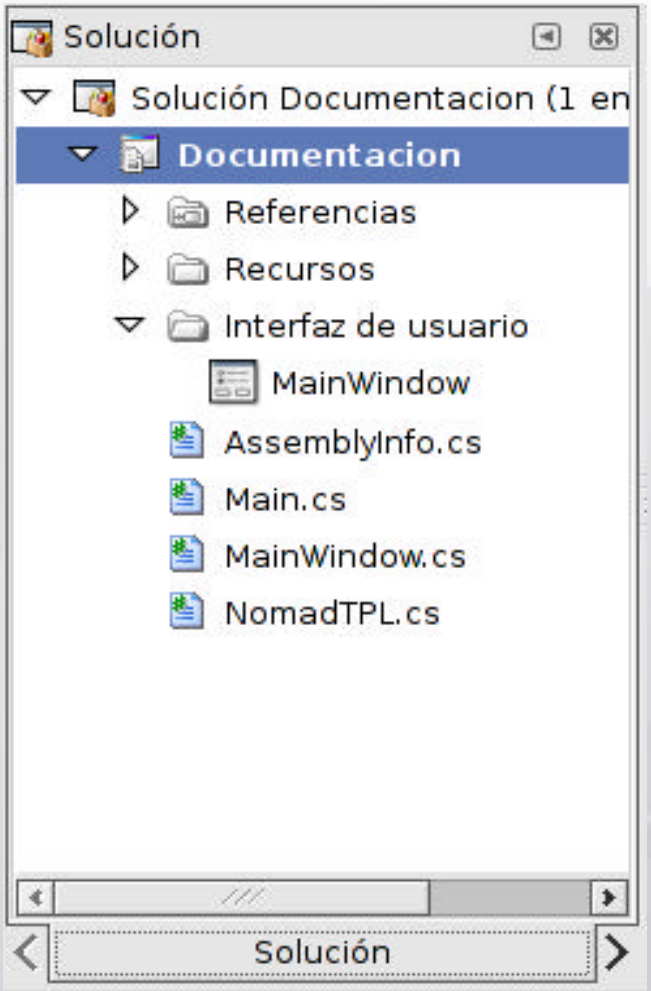
- Resaltado de Sintaxis
- Completado de código Inteligente
- Code Shortcuts

monodevelop

Soporte de Proyectos

Módulo de Árbol de la Solución; todas las partes que incluyen un proyecto.

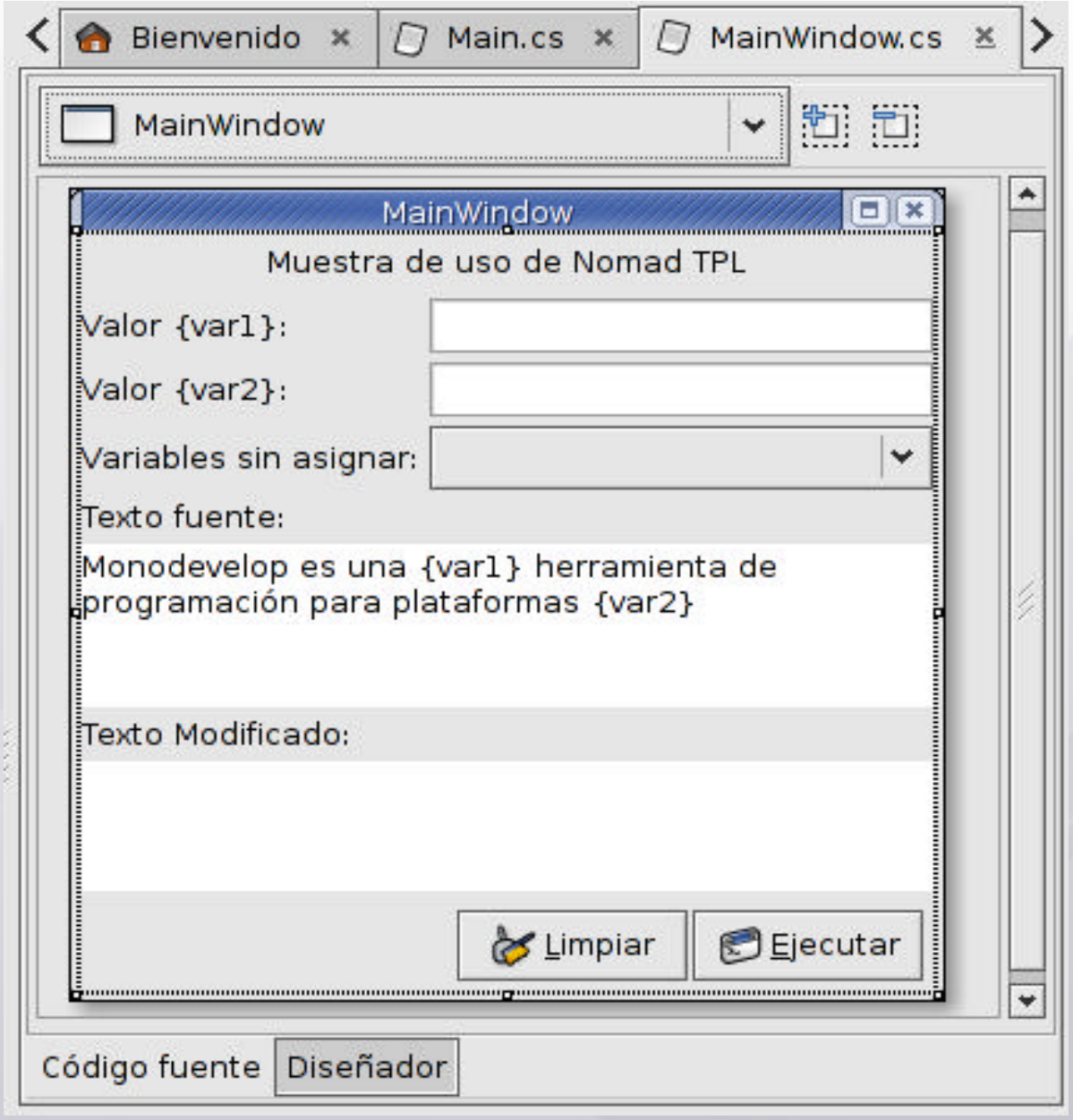
Al igual que en otros IDE's, desde esta ventana es posible agregar/modificar la estructura y contenidos.



monodevelop

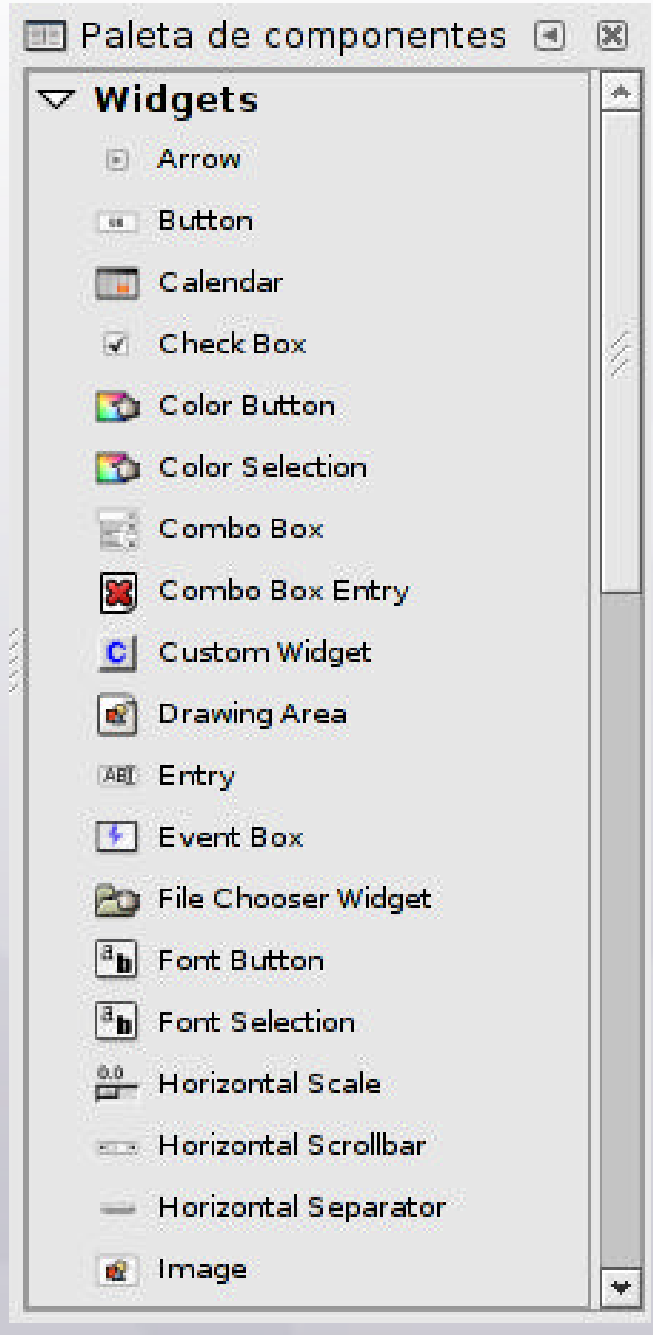
Diseño de Formularios

Área para el Diseño de Formularios (RAD) intuitivo y de fácil uso.



monodevelop

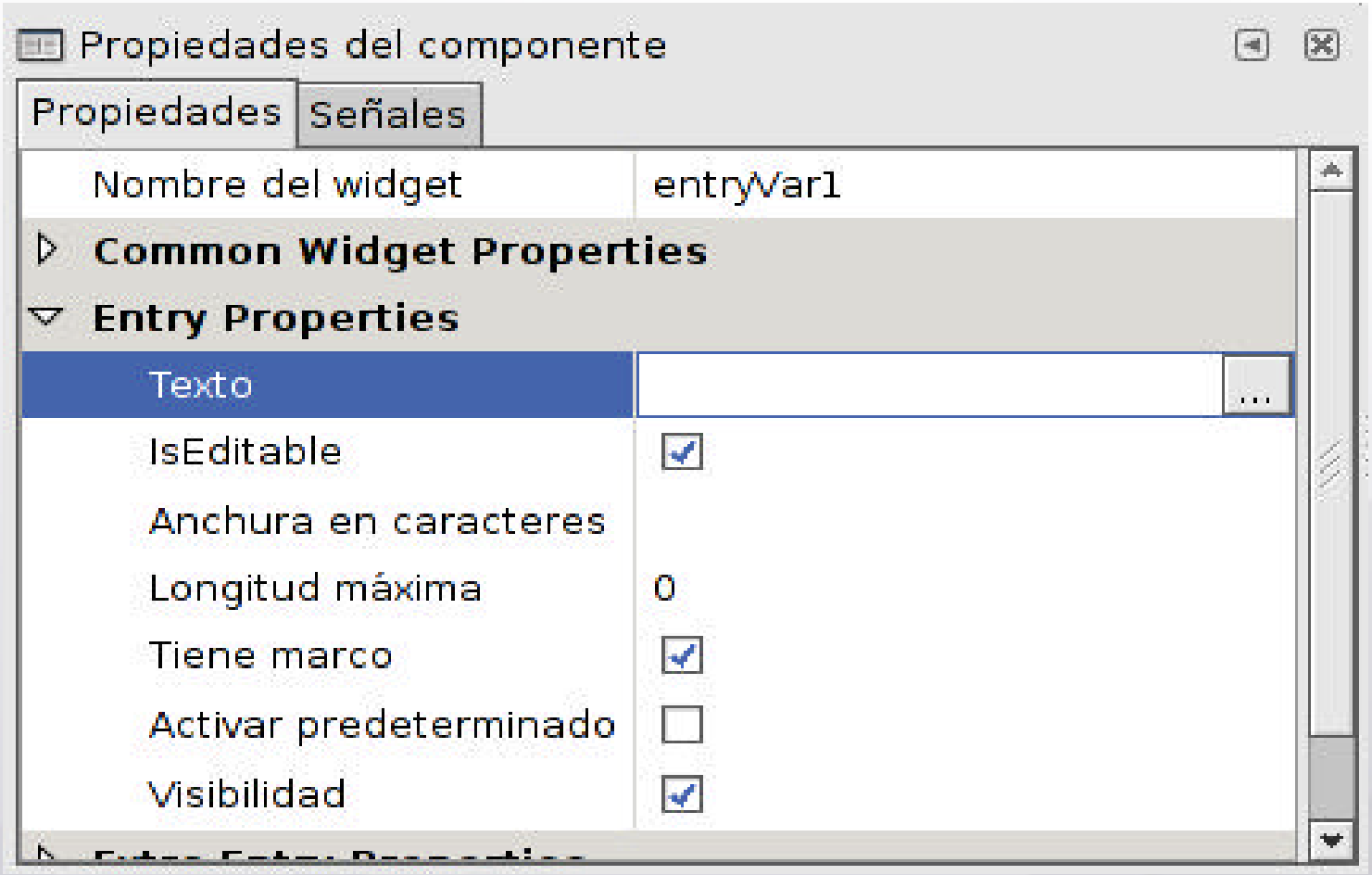
Paleta de Widgets



Complementando el área de diseño de formularios se encuentra la paleta de componentes, desde donde es posible pulsar y arrastrar los Widgets que se usarán en el proyecto.

monodevelop

Propiedades del Widget

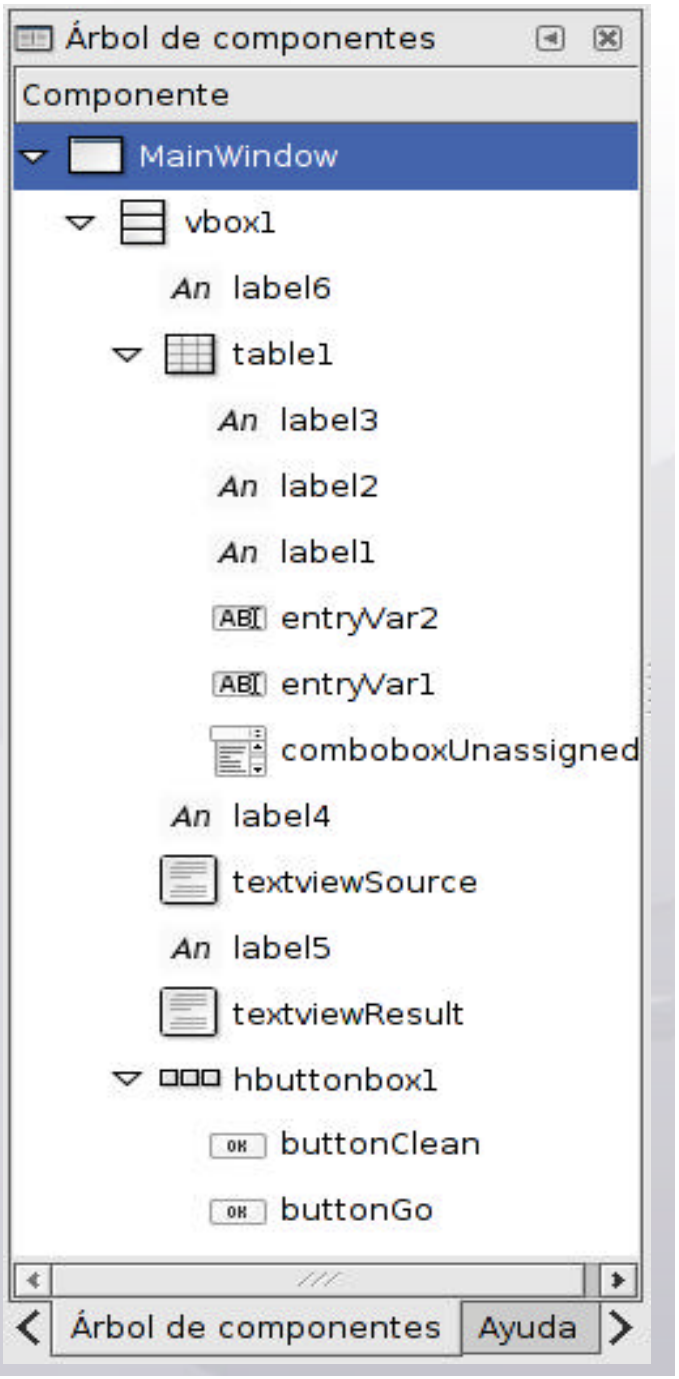


Listado de las propiedades de cada uno de los Widgets disponibles.

monodevelop

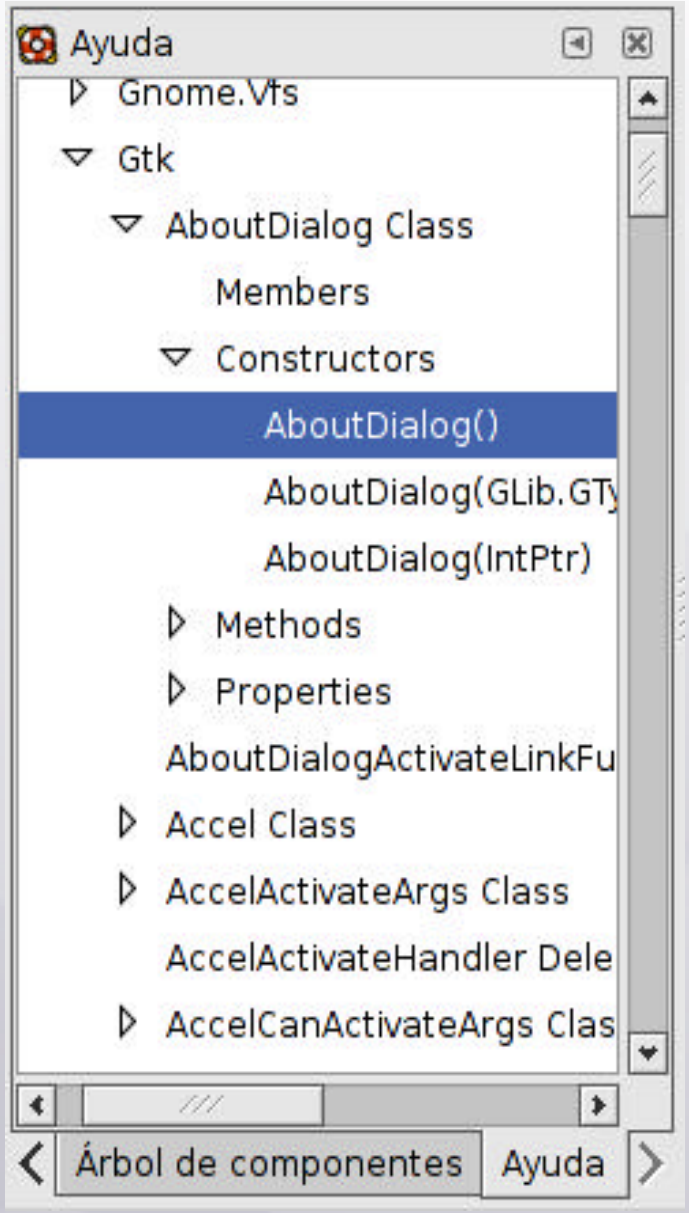
Árbol de Componentes

Estructura de los Widgets usados en el proyecto. Sumamente útil debido a la necesidad de usar Vbox, Hbox y TableBox.



Ayuda MonoDoc

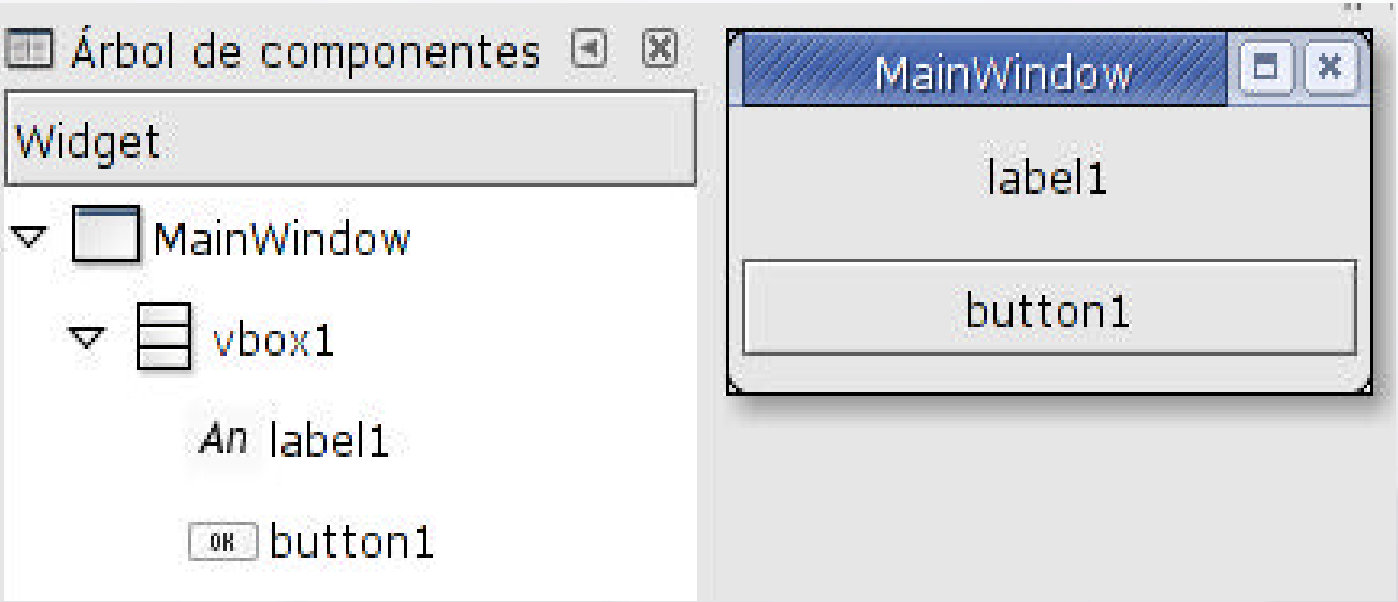
monodevelop



MonoDoc incorporado para la búsqueda y referencia rápida de los “namespaces” y sus clases.

monodevelop

Ejemplo “Hola Mundo”



Se dibuja el formulario

monodevelop

Ejemplo “Hola Mundo”

Se crea la señal (evento)

monodevelop

Ejemplo “Hola Mundo”

```
protected virtual void boton_Clicked(object sender, System.EventArgs e)
{
  texto.Text = "Hola Mundo!!!";
}
```

Se escribe el código

monodevelop

Ejemplo “Hola Mundo”

Se compila y Ejecuta sobre GNU/Linux

Aprendizaje en Redes Neuronales Wavelet Aplicado en la Eliminación de Ruido.

Hugo Adrián García Elías, José Federico Ramírez Cruz
Instituto Tecnológico de Apizaco, Avenida Instituto Tecnológico S/N 90300
Apizaco, Tlaxcala, A. P. 19, México
hugoage@gmail.com, framirez@itapizaco.edu.mx

Resumen- **En este trabajo se ejemplifica el aprendizaje en Redes Neuronales Wavelet, la red implementada en el presente trabajo es entrenada con un grupo de espectros estelares, que son las señales elegidas para este proyecto, los espectros fueron alterados con un tipo de ruido aleatorio del mismo tipo para cada espectro, suponiendo que fueron adquiridos en el mismo lugar y con el mismo instrumento, después de obtener los parámetros de aprendizaje durante el entrenamiento, se prueba la red para filtrar un espectro estelar y eliminar el ruido presente en esté con los parámetros aprendidos previamente en la etapa de entrenamiento por la Red Neuronal Wavelet, demostrando la capacidad de aprendizaje de las Redes Neuronales Wavelet y la aplicación de este tipo redes en la eliminación de ruido, los resultados obtenidos en los experimentos fueron satisfactorios.**

Palabras Clave- Aprendizaje, Redes Neuronales Wavelet, RBF, RNW.

I. INTRODUCCION

Las redes neuronales artificiales de manera general son modelos computacionales que imitan la manera de procesar la información del cerebro humano. Una red neuronal artificial posee la importante característica de "aprender de la experiencia" lo que le permite resolver problemas desde un punto de vista diferente al de las computadoras actuales. Asimismo, las wavelets son una nueva familia de funciones, las cuales combinan importantes propiedades, tales como localización en tiempo y frecuencia, ortogonalidad y soporte compacto. El análisis a base de wavelets, al igual que el análisis de Fourier, se basa en el concepto de aproximación de señales usando superposición de funciones.

En la teoría de wavelets, se pueden seleccionar diversas funciones prototipo, para formar diferentes funciones base de la Transformada Wavelet, dicha capacidad de selección permite obtener diferentes características de localización, tanto en el tiempo como en la escala, se introduce la noción de escala como una alternativa a la noción de frecuencia. Entonces la señal es mapeada dentro de un plano escala-tiempo. Esta característica hace de la Transformada Wavelet la herramienta adecuada para el análisis de señales no estacionarias.

Las Wavelets han generado un tremendo interés tanto en las áreas teóricas como en las aplicadas, especialmente en el procesamiento de señales como en [1]. Particularmente, durante la década pasada, las Transformadas Wavelet han emergido como una herramienta matemática muy importante para el análisis de series de tiempo (ver por ejemplo [2], [3], [4]). Las redes neuronales se han utilizado en la eliminación de ruido en señales como en [5], en [6] y [7] se utilizan algoritmos de aprendizaje para análisis y cancelación de ruido en espectros estelares. Dos son principalmente las líneas de investigación que combinan la teoría de wavelets con la teoría de redes neuronales artificiales. Ambas con un sólido fundamento teórico: La primera se basa en los trabajos de Zhang y Benveniste [8], [9] quienes proponen una red del tipo propagación hacia adelante con una y media capas de neuronas, las cuales utilizan Wavelets como funciones de activación.

Dicho modelo utiliza para su entrenamiento el método tradicional conocido como algoritmo de propagación hacia atrás. El segundo grupo de investigación, propone una estructura similar a las redes de funciones base radial (redes RBF), cuyas funciones de activación son wavelets [4] [10] [11]. Pero dado que, a grandes rasgos, este tipo de redes son simplemente la ecuación de síntesis de la transformada wavelet discreta expresada en forma de red neuronal, no requiere de un algoritmo de aprendizaje iterativo. El aprendizaje de este tipo de redes puede entenderse como la correspondiente expansión en funciones wavelet.

Las redes neuronales wavelet son una nueva y poderosa clase de redes neuronales artificiales que emplean wavelets como funciones de activación en sus neuronas. Éstas incorporan las ventajas de la descomposición de señales mediante wavelets con las propiedades de generalización y de aproximación universal de las redes neuronales tradicionales. En años recientes este tipo de redes han sido ampliamente investigadas como un modelo alternativo a las redes neuronales tradicionales basadas en funciones sigmoide. Sin embargo, los modelos de redes neuronales wavelet existentes, de manera general se restringen al uso de wavelets continuas y diferenciables. Cabe mencionar que la mayoría de familias de wavelets más utilizadas en el procesamiento de señales no cumplen con dicha propiedad.

II. DESARROLLO

En las redes neuronales tradicionales, comúnmente son utilizadas dos tipos de funciones de activación: las funciones globales, utilizadas en las redes de propagación hacia delante; y las funciones locales, utilizadas en las redes RBF. Cada una de estas redes posee especiales propiedades de aproximación, y dado un número suficiente de neuronas, ambas redes son capaces de aproximar cualquier función continua con una precisión arbitraria [12] [4]. Con las funciones de activación globales, la adaptación y el aprendizaje son lentos, debido a la interacción de todas las neuronas de la red, por lo que la convergencia no siempre está garantizada. Además, las funciones globales no permiten el aprendizaje local ni la manipulación de la red. Estos problemas son superados en las redes con funciones de activación locales. Pues en ellas, cada función de activación se centra en el aprendizaje de sólo una parte del domino de la superficie mapeada por las entradas y las salidas. Las redes neuronales wavelet (RNW) surgen de la idea de combinar las redes neuronales tradicionales con las funciones base empleadas en la teoría de wavelets. Por lo anterior en [3] se define a las RNW como "*una red neuronal de propagación hacia delante, constituida por una sola capa oculta de neuronas, cuyas funciones de activación son seleccionadas de una familia de wavelets ortonormales"*.

Las RNW son una nueva y poderosa clase de redes neuronales que incorporan las más importantes ventajas de la descomposición de señales mediante wavelets de acuerdo con [13] y [14] con las propiedades de aprendizaje y aproximación universal de las redes neuronales tradicionales [15].

El Aprendizaje Maquina o Computacional trata sobre los programas de computadora que automáticamente son capaces de mejorar o adaptarse a nuevas situaciones, teniendo a la experiencia como herramienta para ello.

Este trabajo consiste en un método de aprendizaje en Redes Neuronales Wavelet, para eliminar ruido en espectros estelares que son las señales elegidas por nosotros para efectos de este proyecto, el cual consiste en: Entrenar a la Red Neuronal Wavelet con un conjunto de espectros estelares, considerados como ruidosos, el conjunto de espectros de entrenamiento es alterado con un tipo de ruido aleatorio para cada uno de los espectros estelares del conjunto de entrenamiento, asumiendo que fueron tomados en el mismo lugar y con el mismo instrumento, después de entrenar la Red Neuronal Wavelet, su realizan pruebas para filtrar otro conjunto de espectros de entrada y eliminar el ruido presente en ellos, de acuerdo a los parámetros aprendidos por la Red Neuronal Wavelet, los resultados obtenidos

fueron satisfactorios probando la capacidad de este tipo de redes en el filtrado de datos ruidosos.

La arquitectura de la red neuronal Wavelet en este proyecto se diseño como estructura de tres capas, una capa de entrada, una capa oculta y una capa de salida, cada capa puede contener uno o mas nodos, en la Figura II.1 se muestra un diagrama esquemático de las Redes Neuronales Wavelet de tres capas.

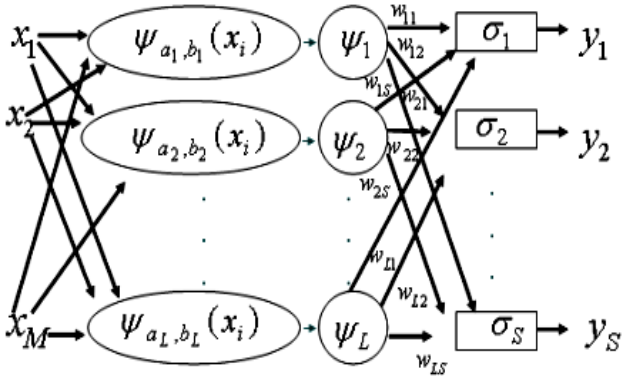


Figura II.1. Red Neuronal Wavelet

Como se ilustra en la Figura II.1, el vector que almacena el espectro con ruido se conecta con los nodos de entrada de la red. Las funciones de activación de los nodos Wavelet en la capa oculta se derivan de una Wavelet Madre $\psi(x)$. La función wavelet Morlet se selecciono como Wavelet madre en esta red y se define en (1):

$$\psi(x) = \cos(1.75x)e^{-(1/2)x^2} \tag{1}$$

La función Wavelet Morlet se vuelve la función de activación con escala a_l y traslación b_l, Por consiguiente, la función de activación del l nodo wavelet $l = 1,2...,L$ se calcula con (2):

$$\psi_{a_l,b_l}(x) = a_l^{-1/2}\cos(1.75(\frac{x-b_l}{a_l}))e^{-1/2(\frac{x-b_l}{a_l})^2} \tag{2}$$

Entonces, la salida del l nodo wavelet con m variables de entrada $x_i, i = 1,2,...,M$, se calcula con (3):

$$\psi_l(x) = \sum_{i=1}^{M}\psi_{a_l,b_l}(x_i) \tag{3}$$

Cada salida de los nodos Wavelet en la capa oculta se multiplica por un valor de peso apropiado determinado por la capa oculta. En la figura 2 los pesos w_{ls} que conectan el nodo Wavelet l con el nodo de salida s están indicados por el vector de pesos $w_l = [w_{l1},...w_{ls},...,w_{lS}]$ para $l = 1,2...,L$ y $s = 1,2...,S$ y S es el numero total de nodos de salida. La función sigmoide es seleccionada como la función de activación σ de los nodos de salida en la capa de salida. Y el valor final calculado como valor del nodo de salida es calculado con (4):

$$y_s(x) = \sigma(\sum_{l=1}^{L} w_{ls}\psi_l(x)) \tag{4}$$

Notablemente, la salida $y_s(x)$ en (4) contiene, implícitamente, los parámetros de ajuste de la red: los pesos de conexión (w_{ls}) y los parámetros de escala (a_l) y traslación (b_l) en cada nodo Wavelet. Los parámetros de escala se inicializan con (5):

$$a_l = 2^{-l} \tag{5}$$

Y los parámetros de traslación se inicializan con (6):

$$b_l = x_i a \tag{6}$$

Los pesos w_{ls} se pueden actualizar con (7):

$$w_{ls}(k+1) = w_{ls}(k) + \Delta w_{ls}(k) + \delta_w[w_{ls}(k) - w_{ls}(k-1)] \tag{7}$$

$$\Delta w_{ls} = \xi\frac{\partial e}{\partial w_{ls}} \tag{8}$$

Donde ξ_w es la tasa de aprendizaje y δ_w es el factor de momento correspondiente.

Del mismo modo se pueden actualizar los coeficientes de escala (a_l) y traslación (b_l) con (9) y (11) :

$$a_l(k+1) = a_l(k) + \Delta a_l(k) + \delta_a[a_l(k) - a_l(k-1)] \quad (9)$$

$$\Delta a_l = \xi_a \frac{\partial e}{\partial a_l} \quad (10)$$

Donde ξ_a es la tasa de aprendizaje y δ_a es el factor de momento correspondiente.

$$b_l(k+1) = b_l(k) + \Delta b_l(k) + \delta_b[b_l(k) - b_l(k-1)] \quad (11)$$

$$\Delta b_l = \xi_b \frac{\partial e}{\partial b_l} \quad (12)$$

Donde ξ_b es la tasa de aprendizaje y δ_b es el factor de momento correspondiente.

El error en los nodos de la capa de salida puede ser calculado con (13):

$$e = y(s) - y^d(s) \quad (13)$$

Y

$$E = \frac{1}{2}e^2 \quad (14)$$

Donde $y^d(s)$ es la salida deseada, y $y(s)$ es la salida obtenida y E es el error cuadrático en la salida.

III. RESULTADOS

La primera parte del experimento consiste en entrenar a la Red Neuronal Wavelet con un conjunto de espectros estelares consideraos como ejemplos de entrenamiento, los cuales se muestran en las figuras III.1, III.2, III.3 y III.4.

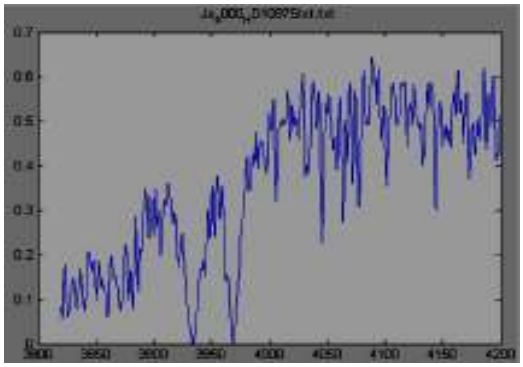


Figura III.1 Espectro de Entrenamiento 1.

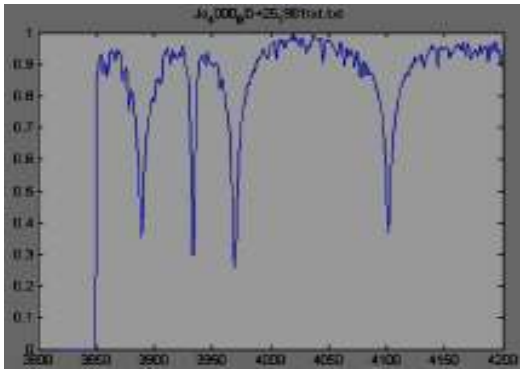


Figura III.2 Espectro de Entrenamiento 2.

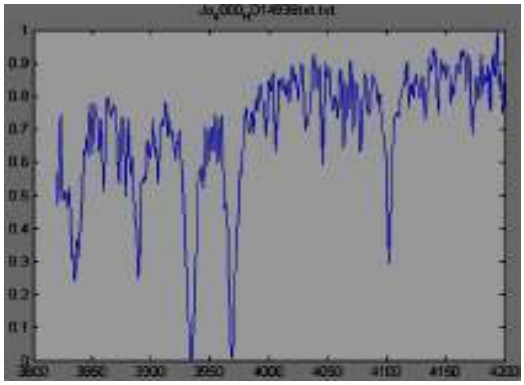


Figura III.3 Espectro de Entrenamiento 3.

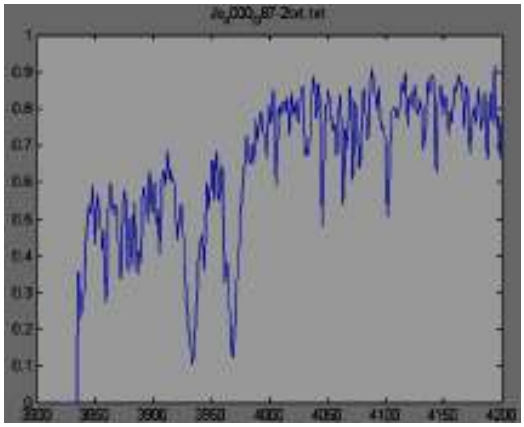


Figura III.4 Espectro de Entrenamiento 4

Los espectros aprendidos como resultado en la etapa de entrenamiento se muestran en la figura III.5.

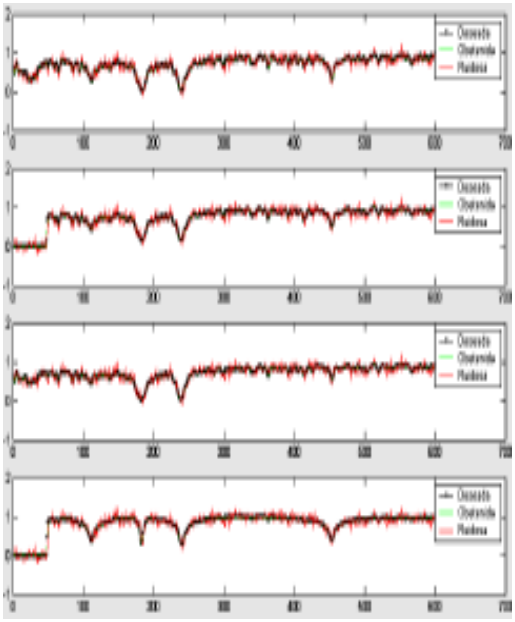


Figura III.5 Espectros Aprendidos por la Red Neuronal Wavelet.

Como se observa en la Figura III.5 los espectros aprendidos por la Red Neuronal Wavelet son los mismos que los espectros deseados, se muestran también en la imagen el espectro con ruido.

El siguiente paso en el experimento es proporcionar a la Red Neuronal Wavelet un espectro estelar para ser filtrado y eliminar el ruido presente en el espectro, el espectro a ser filtrado se observa en la Figura III.6.

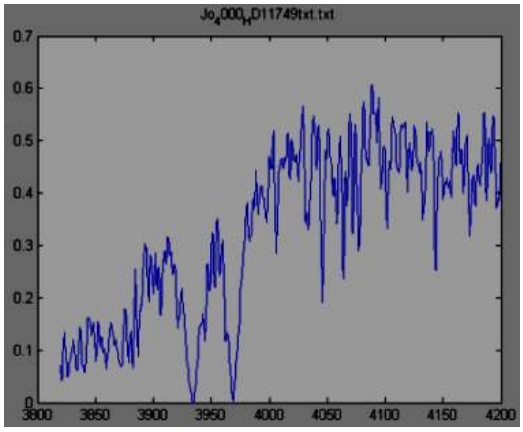


Figura III.6 Espectro a filtrar en la Red Neuronal Wavelet

En la Siguiente Figura (Figura III.7) se observa el Espectro ruidoso de entrada (VERDE), el espectro obtenido o filtrado por la Red Neuronal Wavelet (ROJO), El espectro deseado (NEGRO), y la grafica del Error medio cuadrático (AZUL).

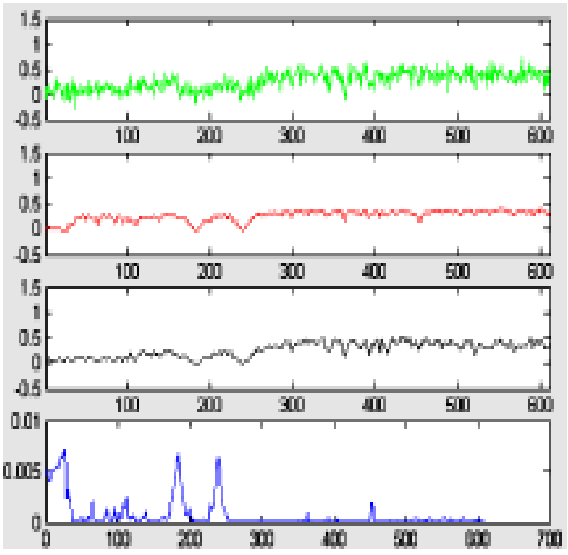


Figura III.7 Resultados obtenidos por la Red Neuronal Wavelet.

Como se observa en la Figura III.7 los valores del error son muy pequeños (AZUL), se observa que el espectro filtrado tiene una apariencia no ruidosa (ROJO) en comparación con la salida deseada (NEGRO) y el espectro de entrada (VERDE).

V. CONCLUSIONES

Las RNW han probado sus ventajas sobre los esquemas tradicionales en muy variados problemas de aplicación, pero particularmente en lo que respecta a problemas de aproximación y predicción de funciones, en este proyecto se prueba también su enorme utilidad en la eliminación de ruido, se realizaron pruebas filtrando diferentes espectros estelares, obteniendo valores de error mínimos y resultados satisfactorios en el filtrado de datos ruidosos. Sin embargo, el procedimiento de aprendizaje utilizado por RNW actuales, tiene sus fundamentos en la posibilidad de diferenciación de una función wavelet continua. Desafortunadamente, la mayoría de las wavelets más utilizadas en el procesamiento de señales, no satisfacen dicha propiedad.

RECONOCIMIENTOS

Agradezco al Instituto Tecnológico de Apizaco por las facilidades otorgadas para la realización de este proyecto, a la Dirección General de Educación Superior Tecnológica y a COSNET por la Beca Otorgada para el proyecto denominado: “Detección de Ruido En espectros Estelares Mediante Redes Neuronales y Ondeletas”. Clave: 042005065.

REFERENCIAS

[1] B. Jawerth, and W. Sweldens. "An overview of wavelet based multiresolution analyses" , SIAM, 1994.
[2] O. Rioul, and M. Vetterli, “Wavelets and Signal Processing”, IEEE SP Magazine, Octubre 1991.
[3] Sitharama Iyengar, E.C. Cho, and Vir V. Phoha, "Foundations of Wavelet Networks and Applications", Chapman & Hall/CRC. U.S.A. 2002
[4] B. R. Bakshi, G. Sthepanopoulos, "Wavelets as Basis Functions for Localized Learning in a Multiresolution Hierarchy", Laboratory for Intelligent Systems in Process Engineering, Department of Chemical Engineering. Massachusetts Institute of Technology, Cambridge, MA 02139, 1992
[5] Hernández Montero, Fidel Ernesto y Falcón Urquiaga, Wilfredo (1999) “Cancelación de Ruido a través de Técnicas Neurales” Proceedings of the IV Brazilian Conference on Neural Networks pp. 001-006, July 20-22, 1999 - ITA, São José dos Campos - SP – Brazil
[6] Ramirez. J. Federico and Fuentes Olac. “A Hybrid algorithm for spectral analysis” experimental astronomy, 2003. Kluwer academic publishers. Printed in the Netherlands.
[7] Escalante, H. Jair. And Fuentes Olac (2004), “Noise Elimination with a Re-Sampling Algorithm” Workshop on Machine Learning for Scientific Data Analysis, pp. 307-316, Copyright Iberamia 2004
[8] Q. Zhang, A. Benveniste, "Wavelet Networks", IEEE Transactions on Neural Networks. Vol 3. No 6. July 1992.
[9] Q. Zhang. "Wavelet network: the radial structure and an efficient initialization procedure", In European Control Conference (ECC), Groningen, Pays-Bas, 1993.
[10] K. Bakshi y Stephanopoulos, “Wave-Nets: Novel Learning Techniques, and the Induction of Phisically Interptetable Models” SPIE vol. 2242, pp. 637-648, 1994
[11] A. A. Safavi, and J. A.Romagnoli, "Application of Wave-nets to Modellling and Optimisation of a Chemical Process", Proceedings., IEEE International Conference on Neural Networks, 1995.
[12] K. Hornik, “Multilayer FeedForward Networks are Universals Approximators”, IEEE Neural Networks No 2, 359-366, USA 1989.
[13] S. G. Mallat, "A theory for Multiresolution Signal Decomposition: The Wavelet Representation", IEEE Transactions on Pattern Analysis and Machine Intelligence. Vol II. No 7. July 1989.
[14] I, Daubechies. "Ten Lectures on Wavelets", New York. SIAM. 1992.
[15] V. Alarcón-Aquino, E. S. García-Treviño, R. Rosas-Romero, J.F. Ramírez-Cruz, (2005) "Learning and Approximation of Chaotic Time Series Usign Wavelet Networks". Proceedings of the Sixth Mexican International Conference on Computer Science (ENC’05), México 2005
[16] Luo Zhi Yong and Shi Zhong Ke “Wavelet Neural Network Method For Fault Diagnosis Of Push-Pull Circuits**”.** Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, China 18-21 August 2005.
[17] E. S. García Treviño, V. Alarcón Aquino. “Chaotic Time Series Approximation Using Iterative Wavelet-Networks” Proceedings of the 16th IEEE International Conference on Electronics, Communications and Computers (CONIELECOMP 2006).
[18] Dian-chun Zheng , Chun-xi Zhang, Guo-qing Yang , Xue-yong Sun. “An Experiment Study of Partial Discharge Pattern Recognition Method Based on Wavelet Neural Networks”. Proceedings of the Conference Record of the 2006 IEEE International Symposium on Electrical Insulation.
[19] E. S. Garcia-Treviño., V. Alarcón-Aquino, J.F. Ramírez-Cruz, “Improving Wavelet-Networks Performance with a New Correlation-based Initialization Method and Training Algorithm”. Proceedings of the 15th IEEE Computer International Congress (CIC 2006), México, November 2006.

SIBOS

Universo 07

www.sibos.com.mx

3er. Congreso

Tecnologías de Información y Comunicación

Expandiendo tus ideas

Realizado en la semana del 28 de mayo al 1ro. de Junio del 2007

FCC - BUAP

Memorias del Congreso

AJAX, Navegador NO recargado

Dasaev Cerqueda Pérez

Nuvek LLC.

Introducción

¿Qué es AJAX?

- **TECNICA** de desarrollo web
- Combinación de tres tecnologías existentes
- Herramienta para creación de Aplicaciones web interactivas
- Herramienta de comunicación entre máquina cliente y servidor

¿Qué NO es AJAX?

- Un Lenguaje de Programación
- Una tecnología
- Un invento de Google (Jesse J. Garret, Microsoft)
- La solución de todos los problemas en la comunicación cliente servidor

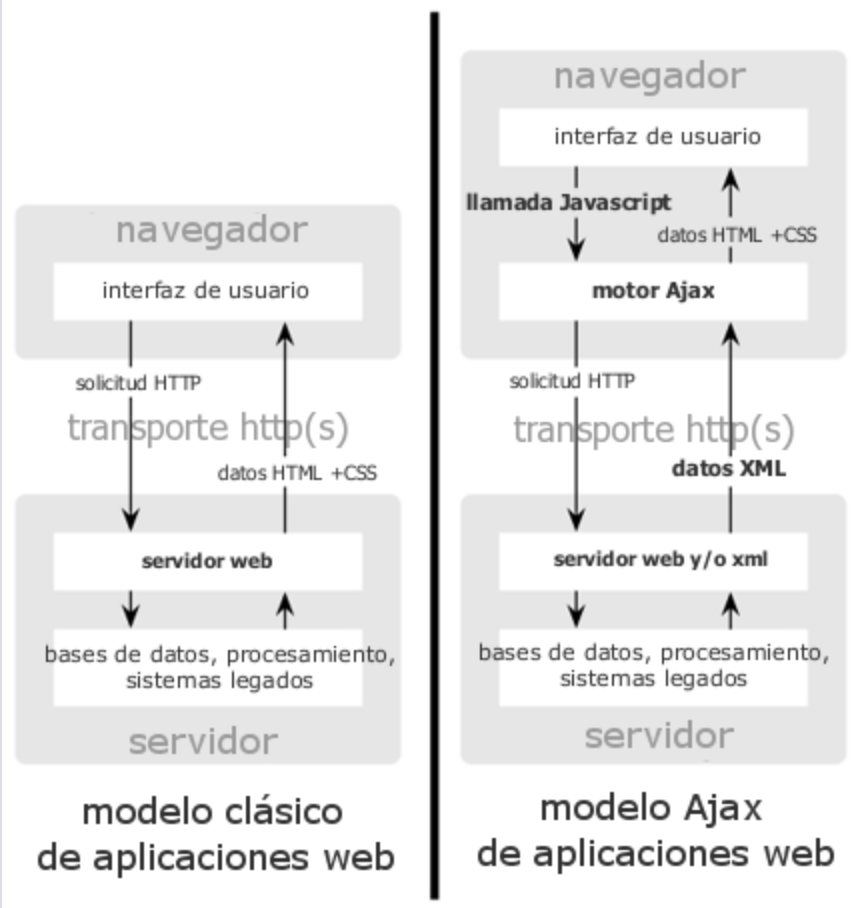
Conociendo AJAX

- Significa Asynchronous Javascript and XML (Extensible Markup Language)
- Las 3 tecnologías que la conforman:
  - XHTML (ó HTML) y Hojas de Estilo en Cascada (CSS)
  - JavaScript: implementación del Objeto XMLHttpRequest, manipulación de peticiones y respuestas
  - XML: Formato usado comúnmente para recepción de datos

Un poco de Historia

- Hace 10 años comenzó la propuesta de Microsoft con su Scripting Remoto
- Desarrollo de Técnicas de carga remota
  - Carga mediante el atributo src
    - Iframe (Internet Explorer 3, 1996)
    - Elemento Layer (Netscape 4, 1997)
  - Applet JAVA
    - Microsoft's Remote Scripting MSRS (Microsoft y Netscape, 1998)
  - Javascript:
    - Librería JSRS (2000)
    - Técnica imagen/cookie
    - Javascript on Demand (2002)
    - XMLHttpRequest (2002)

Modelo Clásico vs Modelo AJAX



¿Qué puedo hacer con AJAX?

- Enviar datos al servidor sin recargar la página
- Manipular los datos de respuesta del servidor
- Cambiar estados de componentes web
- Mostrar información en tiempo “real”

¿Qué NO puedo hacer con AJAX?

- Enviar información confidencial
- Enviar archivos
- Cambiar el comportamiento del navegador
- Acceder al Hardware
- Interactuar con el SO

¿Quién y quién no soporta AJAX?

- Navegadores que permiten AJAX:
  - Navegadores basados en Gecko
  - Microsoft Internet Explorer para Windows versión 5.0 y superiores, y los navegadores basados en él
  - Navegadores con el API KHTML versión 3.2 y superiores implementado
  - Opera versión 8.0 y superiores
- Navegadores que no permiten AJAX
  - Opera 7 y anteriores
  - Microsoft Internet Explorer para Windows versión 4.0 y anteriores
  - Dillo
  - Navegadores basados en texto
  - Navegadores para incapacitados visuales

Desventajas

- Sobrecarga del Navegador
- Deshabilitación de JavaScript por parte del usuario
- Falta de integración con el botón retroceder
- Cambio del estado de los links
- El usuario común no sabe que se está cargando información

Nuestro amigo XMLHttpRequest

Propiedades

- **onreadystatechange [function]**: manejador de eventos que se dispara en cada cambio de estado
- **readyState [integer]**: Estado del Objeto
  - 0: no inicializado
  - 1: cargando
  - 2: cargado
  - 3: interactuando
  - 4: completo
- **responseText [String]**: datos regresados como una cadena de texto
- **responseXML [XMLObject]**: datos regresados en formato DOM-compatible
- **status [integer]**: código numérico de estado regresado por el servidor. Ejemplo 400 para “Not Found” o 200 para “OK”
- **statusText [String]**: Mensaje que acompaña al código de estado

Métodos

- **abort**: detiene la petición en curso
- **getAllResponseHeaders [String]**: regresa la colección completa de encabezados regresado por el servidor en una sola cadena de Texto
- **getResponseHeader [String]**: regresa el valor de un solo encabezado regresado por el servidor
- **open(“método", "URL"[, bandera Asíncrona[, “Nombre de usuario"[, “contraseña"]]])**: Asigna la ruta de destino, método y otros atributos opcionales a una petición pendiente
- **send(contenido)**: transmite la petición, opcionalmente con cadena posteable u objeto DOM
- **setRequestHeader(“etiqueta”, “valor”)**: Asigna un par etiqueta/valor a el encabezado que será enviado con la petición

Creando el Objeto XMLHttpRequest

```
<script>
  <!--
  /*Rutina para crear el objeto XmlHttpRequest*/
  function createAjaxObject(){
    var xmlhttp=null; //Inicializamos la variable como nula

   //código para Internet Explorer, dependiendo de la versión MSXML instalada
    try {
      xmlhttp = new ActiveXObject("Msxml2.XMLHTTP");
    } catch (e) {
      try {
        xmlhttp = new ActiveXObject("Microsoft.XMLHTTP");
      } catch (E) {
        xmlhttp = null;
      }
    }

    //Código para Mozilla y otros navegadores
    if (!xmlhttp && typeof XMLHttpRequest!='undefined') {
      xmlhttp = new XMLHttpRequest();
    }

    return xmlhttp;
  }
  //-->
</script>
```

Llamando al Objeto XMLHttpRequest (Ejemplo)

```
…
<script>
<!--
function executeRequest(){
  //mandamos a crear el objeto AJAX
  var ajaxObject = createAjaxObject();

  if( ajaxObject != null ){ //validamos que el objeto no sea nulo

    ajaxObject.open("GET", "ejemplo.txt", true); //abrimos la conexión
    ajaxObject.onreadystatechange = function(){ //verificamos los estados de la conexión
      if( ajaxObject.readyState == 4 || ajaxObject.readyState == 'complete' ){ //ya hay respuesta
        if( ajaxObject.status == 200 ){ //hay una respuesta válida
          alert( ajaxObject.responseText );
        }else{
          alert( "Petición denegada por el servidor, Mensaje: " + ajaxObject.status + "\n" + ajaxObject.statusText );
        }
      }
    }
    ajaxObject.send( null ); //esta linea es muy importante, sin ella no hay comunicación
  }else{ //el navegador no soporta AJAX, mandamos un mensaje

    alert( "El navegador no soporta AJAX" );

  }
}
//-->
</script>
<!-- llamamos a la funcion executeRequest -->
<a href="javascript:executeRequest()">P&uacute;lsame</a>
…
```

ejemplo.txt

```
Ejemplo práctico del uso de AJAX
Esto es solo el comienzo, el uso
de la propiedad responseText
permite manejar el resultado de
la petición como una cadena JavaScript
mediante el uso de la función eval()
```

Llamando al Objeto XMLHttpRequest (Ejemplo XML)

```
<script>
<!--
function executeRequest(){
  //mandamos a crear el objeto AJAX
  var ajaxObject = createAjaxObject();

  if( ajaxObject != null ){ //validamos que el objeto no sea nulo

    ajaxObject.open("GET", "ejemplo.xml", true); //abrimos la conexión
    ajaxObject.onreadystatechange = function(){ //verificamos los estados de la conexión
      if( ajaxObject.readyState == 4 || ajaxObject.readyState == 'complete' ){ //ya hay respuesta
        if( ajaxObject.status == 200 ){ //hay una respuesta válida
          xmlData = ajaxObject.responseXML; //recuperamos el XML
          xmlDoc = ( xmlData.XMLDocument ) ? xmlData.XMLDocument  :  xmlData; //obtenemos la estructura XML si no existe
          itemsXML = xmlDoc.getElementsByTagName( 'materia' ); //Obtenemos los nodos llamados "materia"
          mensaje = ""; //Inicializamos la variable mensaje
          for( countItems = 0; countItems < itemsXML.length; countItems++ ){
            nomMateria = itemsXML[ countItems ].attributes.getNamedItem('nombre').value;
            reprobe = itemsXML[ countItems ].attributes.getNamedItem('reprobe').value;
            mensaje += (( reprobe == "true" ) ? "-reprobé " : "-aprobé ") + nomMateria;
          }

          alert( mensaje );
        }else{
          alert( "Petición denegada por el servidor, Mensaj
        }
      }
    }
    ajaxObject.send( null ); //esta linea es muy importante
  }else{ //el navegador no soporta AJAX, mandamos un mensaj

    alert( "El navegador no soporta AJAX" );

  }
}
//-->
</script>
…
<!-- llamamos a la funcion executeRequest -->
<a href="javascript:executeRequest()">P&uacute;lsame</a>
```

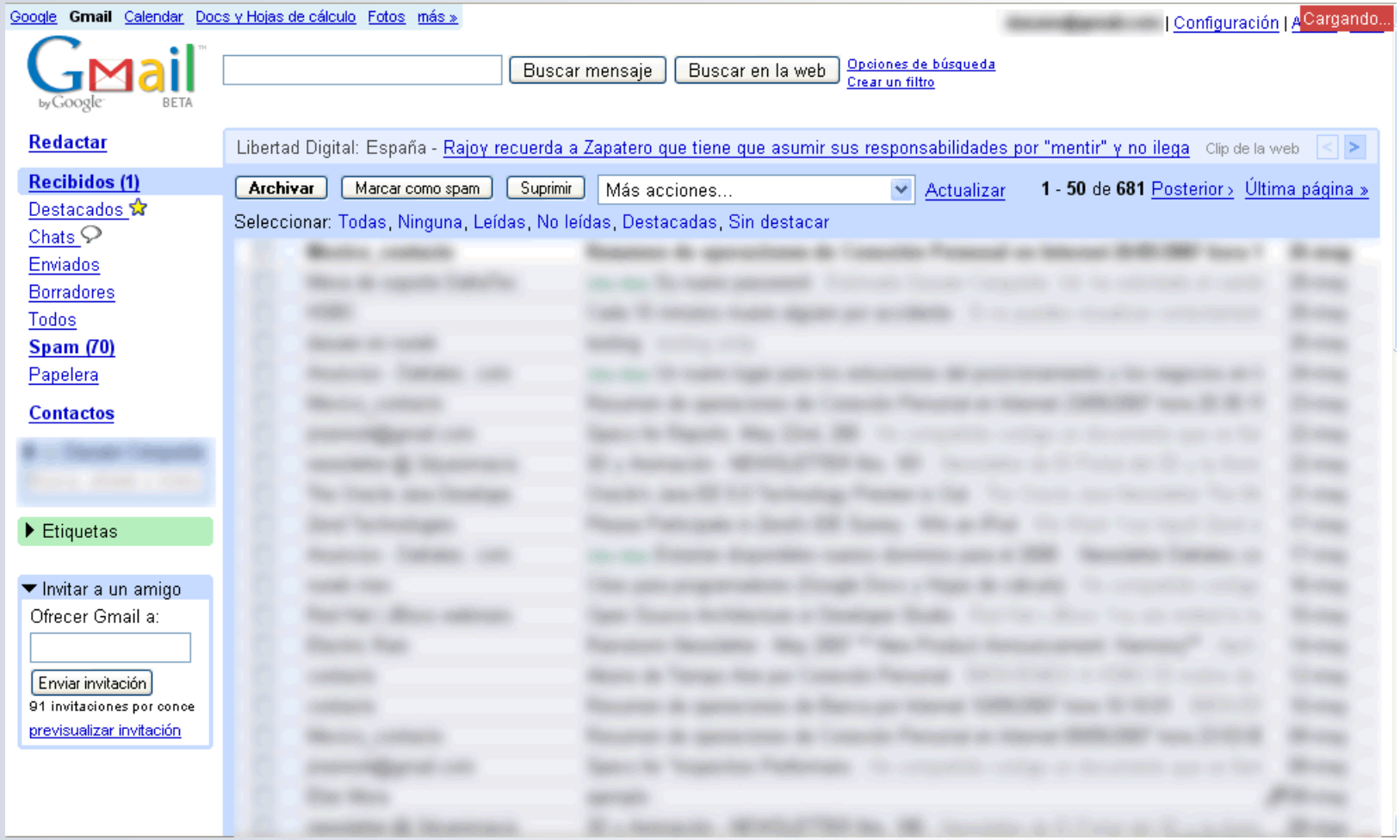
ejemplo.xml

```
<?xml version="1.0" encoding="utf-8"?>
<materias>
  <materia nombre="Calculo Diferencial" reprobe="true"/>
  <materia nombre="Calculo Integral" reprobe="true"/>
  <materia nombre="Programación" reprobe="false"/>
  <materia nombre="Etica y Práctica" reprobe="false"/>
  <materia nombre="Arquitectura de Computadoras" reprobe="true"/>
  <materia nombre="CAD" reprobe="false"/>
  <materia nombre="Imágenes Digitales" reprobe="false"/>
</materias>
```

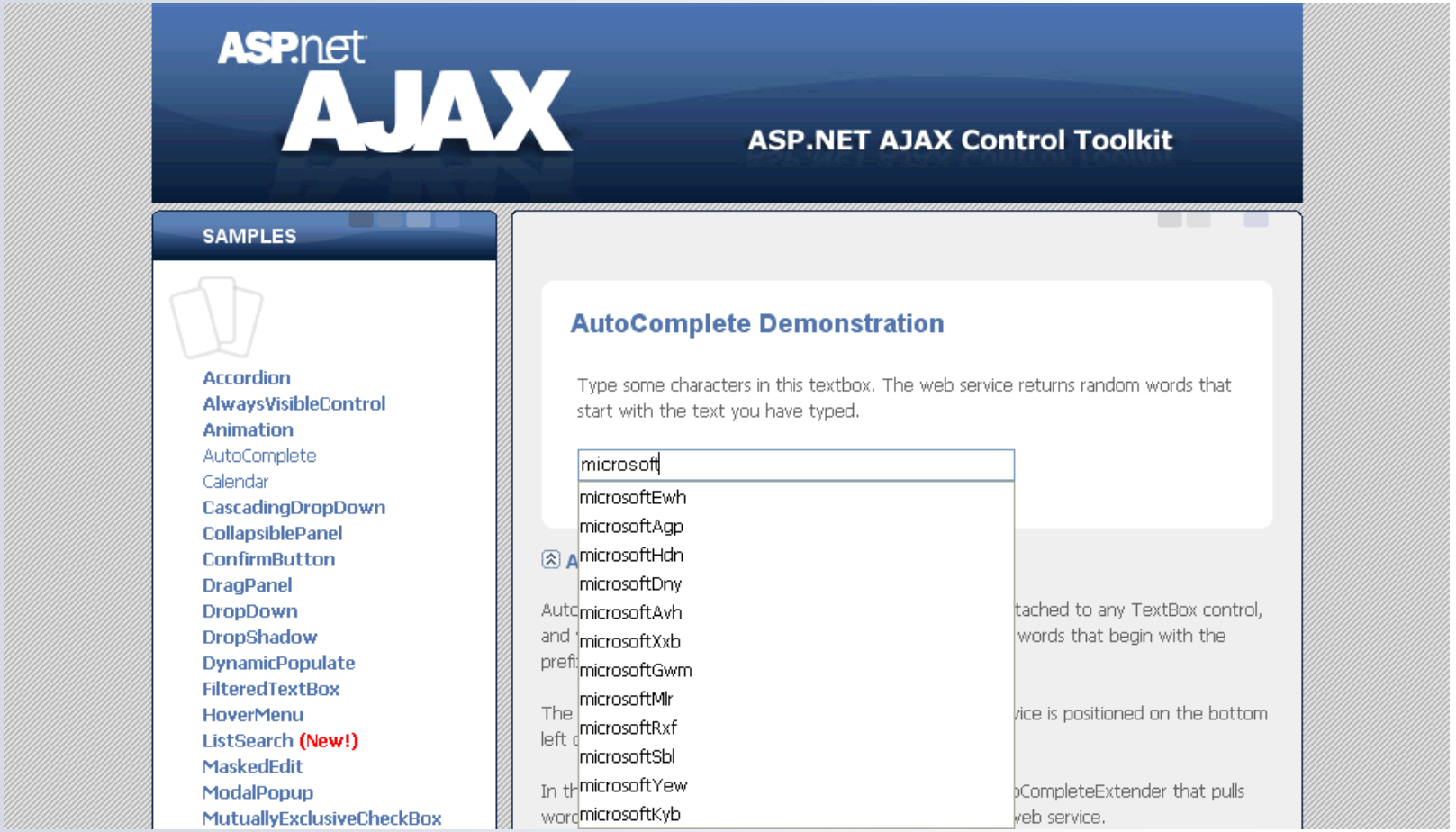
¿Y.....?

¿Quién lo usa?

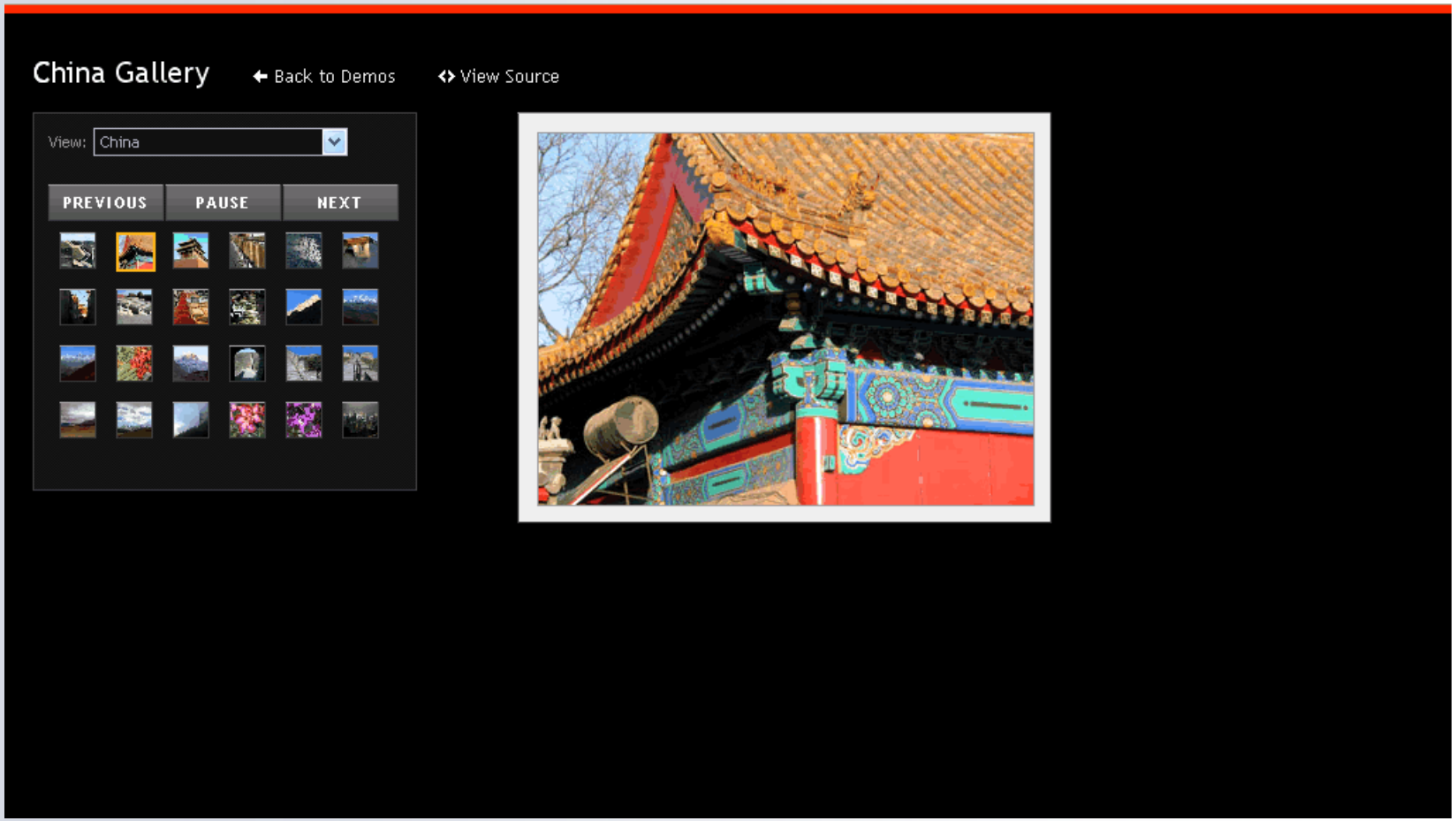
Google


Google Gmail Calendar Docs y Hojas de cálculo Fotos más »
Configuración
Cargando...
Gmail by Google BETA
Buscar mensaje
Buscar en la web
Opciones de búsqueda
Crear un filtro
Redactar
Recibidos (1)
Destacados
Chats
Enviados
Borradores
Todos
Spam (70)
Papelera
Contactos
Etiquetas
Invitar a un amigo
Ofrecer Gmail a:
Enviar invitación
91 invitaciones por conce
previsualizar invitación
Libertad Digital: España - Rajoy recuerda a Zapatero que tiene que asumir sus responsabilidades por "mentir" y no llega
Clip de la web
Archivar
Marcar como spam
Suprimir
Más acciones...
Actualizar
1 - 50 de 681 Posterior › Última página »
Seleccionar: Todas, Ninguna, Leídas, No leídas, Destacadas, Sin destacar

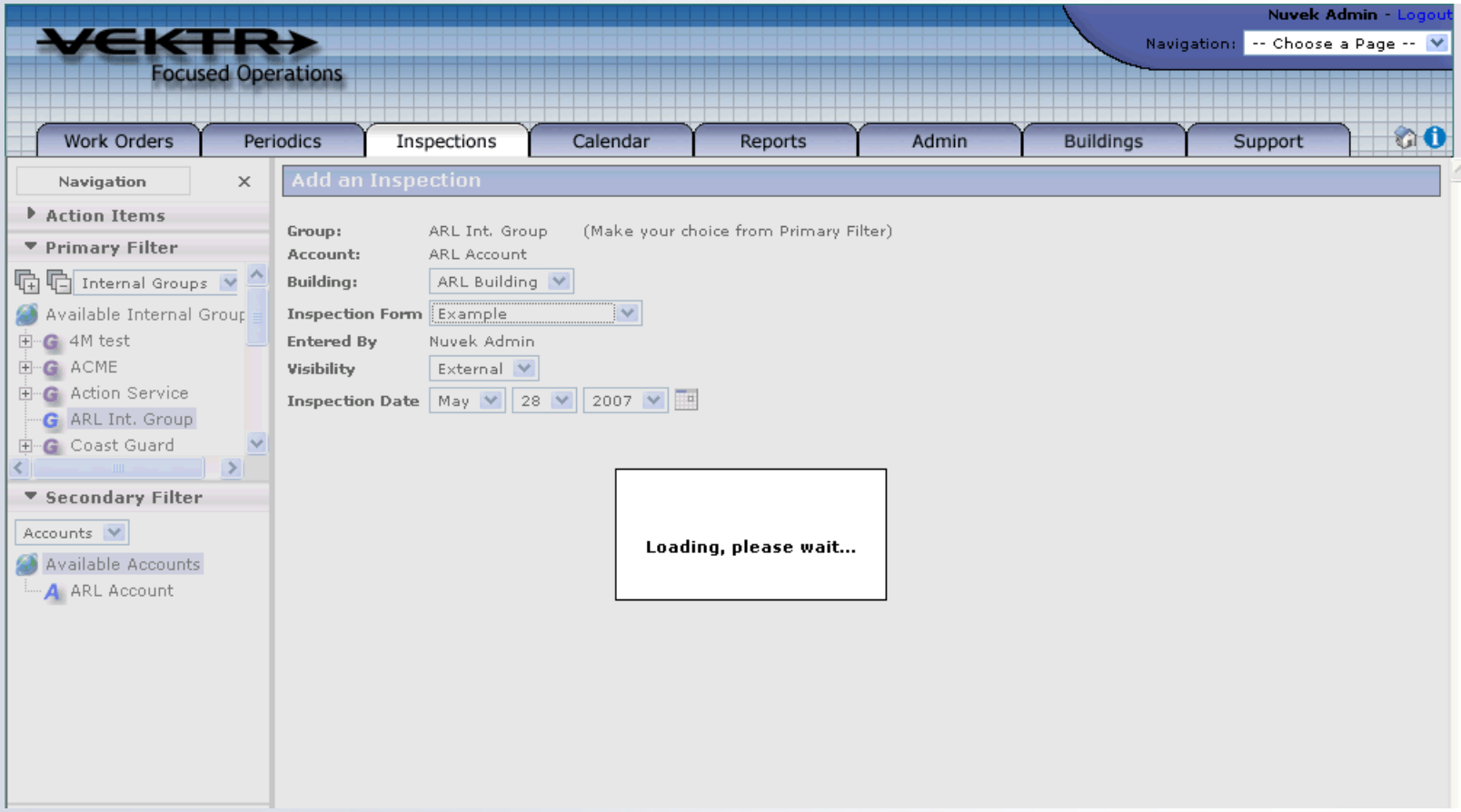
Microsoft


ASP.net
AJAX
ASP.NET AJAX Control Toolkit
SAMPLES
Accordion
AlwaysVisibleControl
Animation
AutoComplete
Calendar
CascadingDropDown
CollapsiblePanel
ConfirmButton
DragPanel
DropDown
DropShadow
DynamicPopulate
FilteredTextBox
HoverMenu
ListSearch (New!)
MaskedEdit
ModalPopup
MutuallyExclusiveCheckBox
AutoComplete Demonstration
Type some characters in this textbox. The web service returns random words that start with the text you have typed.
microsoft
microsoftEwh
microsoftAgp
microsoftHdn
microsoftDny
microsoftAvh
microsoftXxb
microsoftGwm
microsoftMlr
microsoftRxf
microsoftSbl
microsoftYew
microsoftKyb

Macromedia


China Gallery
Back to Demos
View Source
View:
China
PREVIOUS
PAUSE
NEXT

Y por supuesto... Nuvek



Frameworks y Librerías

- AjaxCFC: ColdFusion framework
- AjaXSLT: Implementación XSL-T para AJAX de Google
- FJAX: AJAX para Flash
- JSON, AJAX sin XML: formato ligero para el intercambio de datos
- Open Ajax: proyecto impulsado por varias empresas para crear un estándar para AJAX
- Sajax: Colección de herramientas simples de AJAX
- Xajax ajax for PHP: Biblioteca AJAX de código abierto para PHP

Enlaces y Recomendaciones

- http://es.wikipedia.org/wiki/AJAX
- http://www.uberbin.net/archivos/internet/ajax-un-nuevo-acercamiento-a-aplicaciones-web.php
- http://www.cristalab.com/tutoriales/162/tutorial-de-ajax
- http://www.baluart.net/articulo.php?id_art=55

La Importancia de las Herramientas de V&V

Christian A. Martínez
Instituto Tecnológico y de Estudios Superiores de Monterrey Campus Puebla
pinkejo@acm.org

***Resumen*—El presente artículo explica brevemente algunas técnicas de Verificación y Validación que se utilizan en la fase de V&V del ciclo de vida de desarrollo del software. Propiamente con referencia al artículo, muestro la diferencia entre inspecciones simples e inspecciones técnicas formales, así como la metodología de peer review para proyectos de extreme programming.**

***Palabras Clave*—Verificación y Validación (V&V), Technical Reviews, Inspecciones Técnicas Formales, Peer Review.**

I. Introducción

Actualmente existen todavía empresas desarrolladoras de software que no toman con importancia la fase de Verificación y Validación (V&V). Seguramente son empresas que no se encuentran calificadas en algún nivel de certificación de CMM. Los clientes que buscan aplicaciones de software para sus negocios o empresas piensan que el costo de V&V es muy alto, pero la realidad y los múltiples casos de fracaso en proyectos de software hacen ver que el cliente termina pagando más del doble si omite esta fase de desarrollo en su producto. Technical Reviews, Inspecciones Técnicas Formales y Peer Review son algunas herramientas que aseguran la calidad en el proceso de desarrollo de software y las describiré brevemente citando algunas de sus ventajas y su importancia en la época tecnológica actual.

II. Technical Reviews (Inspecciones Simples)

Las inspecciones sirven para evaluar un producto de software a través de un equipo de personal calificado para determinar su confiabilidad con respecto a sus propósitos de uso e identificar discrepancias en relación con estándares [1]. Con esto se puede llevar la administración de evidencias para confirmar:

Manuscrito presentado en Frebrero 19, 2007, para la materia Verificación y Validación de Software (TC3008). Revisión por M.C. Alma Ríos Flores.

C.A. Martínez es Ingeniero en Tecnologías Computacionales con el plan ITC01 en curso 8vo. Semestre, Departamento de Tecnologías de Información del Instituto Tecnológico y de Estudios Superiores de Monterrey, Puebla, Pue., (e-mail:pinkejo@acm.org).

a) Si el producto de software es acorde con sus especificaciones.
b) Si el producto de software se ajusta a regulaciones, estándares, guías, planes y procedimientos aplicables al proyecto.

c) Si los cambios del software se han implementado satisfactoriamente y afectan solamente aquellos módulos del sistema identificadas en la especificación de cambios.

Asimismo, pueden surgir en este tipo de inspecciones recomendaciones para examinar o explorar diferentes alternativas en el diseño o especificación que se esté inspeccionando que requieran importancia.

Algunos de los productos que pueden evaluarse pueden ser: Software Requirement Specification, Software Design Description, Vision and Scope Document [3], Software User Documentation, entre otros.

Para las “Technical Reviews” deben definirse roles de: tomador de decisiones, líder de revisión, escriba y personal técnico de staff, que en mi opinión pienso son los roles mínimos necesarios para este tipo de inspección. Cabe mencionar que estas revisiones no son formales pero tienen gran importancia en la actualidad porque permite a los autores y diseñadores tener un retroalimentación con recomendaciones para la mejora de su producto, sin embargo, considero necesario que después de una o más technical reviews, deben realizarse inspecciones técnicas formales que aseguren la calidad del producto de software que se está desarrollando, pero eso lo veremos más adelante en el presente artículo.

La realización de una inspección requiere siempre de cinco aspectos de relevancia para llevarse acabo: conjunto de objetivos de la inspección, el producto de software que se examinará, plan de administración del proyecto de software, las anomalías actuales del software y la documentación de los procedimientos de revisión. Si alguna de estas características falta, hay que tomar en cuenta que puede haber problemas con respecto a la administración global del proyecto, es mejor siempre cumplir con ellas. No obstante, existen documentos extra que pueden servir para conformar una inspección, pueden ser como ejemplo: diagramas, reportes de revisión relevantes o estándares que se hayan utilizado.

Después de concluir con éxito una inspección, existen varios criterios de salida entre los que se encuentran: la revisión del proyecto, la revisión del software, lista de anomalías del software resueltas e inconclusas, y otros.

III. Inspecciones Técnicas Formales

A diferencia de las inspecciones rápidas, las inspecciones técnicas formales tienen una importancia mucho mayor en cuanto a verificación y validación se refiere. Este tipo de inspecciones permiten a los desarrolladores de software tener una revisión con mucho más detalle y por consiguiente, un aseguramiento de calidad que aumenta la plusvalía de su producto.

Hedberg e Iisakka las definen como métodos bien conocidos para detectar defectos en artefactos producidos en cualquier fase del desarrollo de software [2], *"es una evaluación sistemática de un producto de software por un equipo de personas calificado que examinan la confiabilidad del producto de software para la intención a la que se quiere utilizar e identifica discrepancias en especificaciones y estándares".* Siguiendo la opinión de Hedberg e Iisakka en su artículo de Calidad del Software, aseveran que la definición tiene dos ideas clave a su punto de vista: la inspección formal se lleva acabo por un equipo, lo que muestra que el autor no puede hacer una inspección formal por si mismo y que se realiza para un producto, no para un draft o prueba del producto. A estas palabras puedo inferir que cuando se solicita una revisión técnica formal es porque los autores han terminado ya su producto y el propósito es revisar si se necesitan reparaciones o modificaciones. Mientras el autor escribe su producto, como Vision and Scope Document [3], no hay chequeo, i.e. los verificadores no participan en la preparación.

A diferencia de una inspección sencilla, las inspecciones técnicas formales brindan una retroalimentación con mayores fundamentos y profundidad para los autores que la solicitan. Con este tipo de inspección puede mostrarse evidencia para verificar que el software satisface sus especificaciones, atributos de calidad, estándares, planes y procedimientos. Aunado a esto, permite también saber si existen desviaciones de estándares y utiliza los datos de ingeniería de software recabados para mejorar el proceso de inspección y su documentación.

Con respecto a las entradas, requiere más documentos que una inspección sencilla, como lo son: checklist de lo que se evaluará, especificaciones del hardware ó lista de errores ortográficos (typo list), y al ser formal no puede llevarse acabo si falta alguno de los miembros del equipo de inspección, si falta algún documento o si alguna de las personas relacionadas no ha revisado a detalle lo que se va a evaluar.

Pienso que las revisiones técnicas formales deberían tomarse en cuenta por todas las empresas desarrolladoras de software pues aquellas que no llevan una fase de verificación y validación a detalle, terminan gastando más en la corrección de errores que aquellas que la implementan. Es bien sabido que esta fase es de las más caras del ciclo de vida, pero no lo es tanto como el pago que debe hacerse si existe su omisión.

TABLA 1

Benefits \ Reference	Barnard & Price	Briand et al.	Chatzigeorgiou & Antoniadis	Gilb & Graham	Grady & van Slack	Porter et al.	Wiegers
Knowledge sharing and education		x		x			x
Increased project awareness and tracking	x	x	x	x			x
Process improvement	x	x	x	x			x
Finding more defects				x		x	x
Finding defects earlier and faster				x	x	x	x
Reduced development costs	x	x		x	x		x

Beneficios de las Peer Reviews

IV. Peer Reviews Aplicadas al Peer Programming

A. ¿Qué son y para qué sirven?

Desde el punto de vista científico, *"peer review es la evaluación científica en la búsqueda o propósitos para la competencia y originalidad por expertos calificados que buscan crear productos de la misma forma (peers)"* [4].

El peer programming es un método de desarrollo de software clasificado en los métodos ágiles, entre los que figura
también el extreme programming. Estos tipos de desarrollo implican poco tiempo en la elaboración de un producto y por consiguiente podemos deducir que su modelación y diseño deben ser rápidos y precisos para tener un producto final de calidad. Las revisiones técnicas diseñadas para métodos ágiles, por lo regular deben llevarse acabo por dos personas. Sin embargo, los métodos ágiles no son similares en este aspecto. Algunos métodos las incluyen, mientras que otros no. A su vez, las principales actividades de control de calidad en procesos ágiles se evalúan a través de pruebas de código y retroalimentación del cliente. Típicamente estas metodologías muestran que las revisiones del proceso de desarrollo y productos pueden reemplazarse por inspecciones informales y con esto hay que señalar que existen pocos métodos ágiles que las envuelven.

Aunque he explicado que existen varias metodologías, enfoquémonos a las limitaciones de esta investigación. Peer review en peer programming es un método de revisión paradójico. La idea es que dos desarrolladores trabajen juntos escribiendo el mismo código. Naturalmente, este doble trabajo cuesta. Los defensores dicen que este trabajo se compensa parcialmente desde el punto de vista que doble programador tiene un desarrollo más rápido con una densidad de defectos de código menores.

En general, el aseguramiento de la calidad en métodos ágiles como el peer programming recae en las pruebas de código en parejas y la interacción del cliente. Usualmente, deben existir este tipo de pruebas peer, pero son informales.

Pocas compañías de software consideran que las peer reviews tienen importancia en la calidad de sus productos. Sin embargo, han ajustado el método a sus recursos limitados. Sin importar cuánto pueden aportar en la cadena de valor, puedo decir que la técnica brinda una detección de defectos eficiente.

B. Beneficios y Desventajas

Las revisiones son unas de las pocas técnicas de aseguramiento de calidad en el desarrollo de software. Veamos en la tabla I [5] algunos de los beneficios encontrados en esta técnica y revisemos las desventajas en la tabla II [5]. Como podemos ver existen puntos de vista muy diferentes para esta técnica de verificación, pero yo creo que todo depende del producto de software que se debe desarrollar y el fin para el que se utilizará.

V. CONCLUSIÓN

Los métodos de prueba de software deben ser siempre conocidos y aplicados en las empresas de desarrollo de software que quieren asegurar una calidad alta en sus productos. Con Technical Reviews para revisiones rápidas en el producto, Inspecciones Técnicas Formales en la verificación de documentos de diseño y especificaciones del software ó con el uso de Peer Reviews, podrán mostrar siempre una evidencia tangible de que los productos que brindan han llevado un proceso correcto en su elaboración.

Aunque los clientes de ayer y hoy piensan que la aplicación de este tipo de herramientas eleva demasiado el costo de lo que compran, ya sea una aplicación estándar o un producto hecho a la medida, existen casos reales que muestran totalmente lo contrario.

En nuestro país ya existen empresas certificadas por CMM que para calificar con un nivel de madurez en desarrollo de software debieron haber mostrado técnicas de verificación en el proceso, involucrando algunas de las que se mostraron en esta investigación.

Yo creo que lo más importante, independientemente del método seleccionado, es que los desarrolladores y autores se complementen en trabajo en equipo empatizando en una selección de técnica correcta que sea acorde con el producto final. Inspecciones Técnicas Formales mínimo para la especificación del SRS en proyectos no muy grandes o su aplicación en todo el diseño para el desarrollo de productos mayores con el apoyo de Technical Reviews entre los documentos finales, pueden llevar al desarrollo de una aplicación al éxito. O bien, el uso de éstas últimas combinadas con las Peer Reviews en casos extremos de desarrollos que impliquen poco tiempo y buena calidad.

TABLA 2

Obstacle \ Reference	Chroust & Lexen	Ciolkowski et al.	Glass	Johnson	Laitenberger et al.	O'Neill	Shepard & Kelly
Lack of time	x	x	x	x		x	x
Lack of human resources	x				x		
Cost		x		x	x		x
Laboriousness			x	x			
Complexity or inadequate training	x	x		x			x
Resistance to change	x						
Inefficiency				x			x

DESVENTAJAS DE LAS PEER REVIEWS

Es necesario que nosotros como Ingenieros de Software intentemos mostrar esta importancia con nuestros clientes, pues sabemos que la naturaleza intangible de nuestro producto final, hace más difícil convencer que lo que hacemos implica mucho trabajo, muchas personas y mucha calidad.

Ayudémonos con las evidencias que dejan estas metodologías de prueba y otras más para convencer que nuestro trabajo debe ser bien remunerado y que sin duda, la falta de la aplicación de la tecnología computacional en la actualidad no permitirá tener una buena competencia en cualquier sector de mercado de hoy en día.

REFERENCIAS

[1] IEEE, IEEE Standard for Software Reviews IEEE Std 1028-1997. New York, NY 1997., Proceedings of the IEEE 1998.

[2] Hedberg, H., Iisakka, J., Technical Reviews in Agile Development: Case Mobile-DTM. Beijing, China Oct. 2006 Page(s): 347 – 353., Six International Conference.

[3] Wiegers, K.E. Vision and Scope Template. 1999.

[4] Brown T, Peer Review and The Acceptance of New Scientific Ideas. London May. 2004 Page 7.

[5] Harjumaa, L.; Tervonen, I.; Huttunen, A., Peer reviews in real life - motivators and demotivators. Oulu Univ., Finland, 19-20 Sept. 2005 Page(s): 29 – 36. Fifth International Conference.

SIBOS

Universo 07

www.sibos.com.mx

3er. Congreso

Tecnologías de Información y Comunicación

Expandiendo tus ideas

Realizado en la semana del 28 de mayo al 1ro. de Junio del 2007

FCC - BUAP

Memorias del Congreso

Herramientas de Monitoreo y Detección de Intrusos en Servidores Linux

Hilda María Chablé Martínez
Asesor de tesis:
Dr. Arturo Díaz Pérez

Centro de Investigación y Estudios Avanzados del I.P.N.
Departamento de Computación
México. D.F.

Tabla de contenidos

1 Resumen

2 Introducción

3 Sistemas de Detección de Intrusos

4 Sistema Híbrido de Monitoreo y Detección de Intrusos

5 Consola de Eventos y Visualización de Resultados

6 Conclusiones y Trabajo Futuro

Resumen

Resumen

- El propósito de este trabajo es usar conjuntamente diversas técnicas de supervisión de bitácoras de uso para un servidor Linux y extraer patrones de acceso que determinen comportamientos anormales y combinar esta información con la extracción estadística del tráfico en una red.

Introducción

Las actividades maliciosas en contra de un sistema informático son cada vez más comunes y sofisticadas; por esta razón, el tema de la seguridad en sistemas operativos y redes ha sido un factor a tener muy en cuenta por cualquier responsable o administrador de sistemas informáticos.

Introducción

Las actividades maliciosas en contra de un sistema informático son cada vez más comunes y sofisticadas; por esta razón, el tema de la seguridad en sistemas operativos y redes ha sido un factor a tener muy en cuenta por cualquier responsable o administrador de sistemas informáticos.

Mecanismos de seguridad

Actualmente existen varios mecanismos de seguridad para proteger los recursos informáticos de un sistema:

- Cortafuegos y listas de control de acceso.
- Sistemas de Detección de Intrusos (SDI).

Introducción

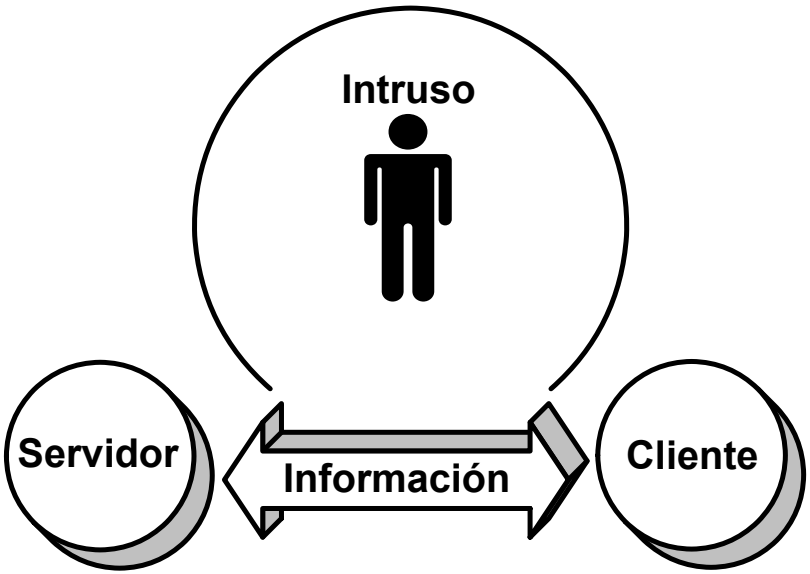
Las actividades maliciosas en contra de un sistema informático son cada vez más comunes y sofisticadas; por esta razón, el tema de la seguridad en sistemas operativos y redes ha sido un factor a tener muy en cuenta por cualquier responsable o administrador de sistemas informáticos.

Mecanismos de seguridad

Actualmente existen varios mecanismos de seguridad para proteger los recursos informáticos de un sistema:

- Cortafuegos y listas de control de acceso.
- Sistemas de Detección de Intrusos (SDI).

Seguridad informática



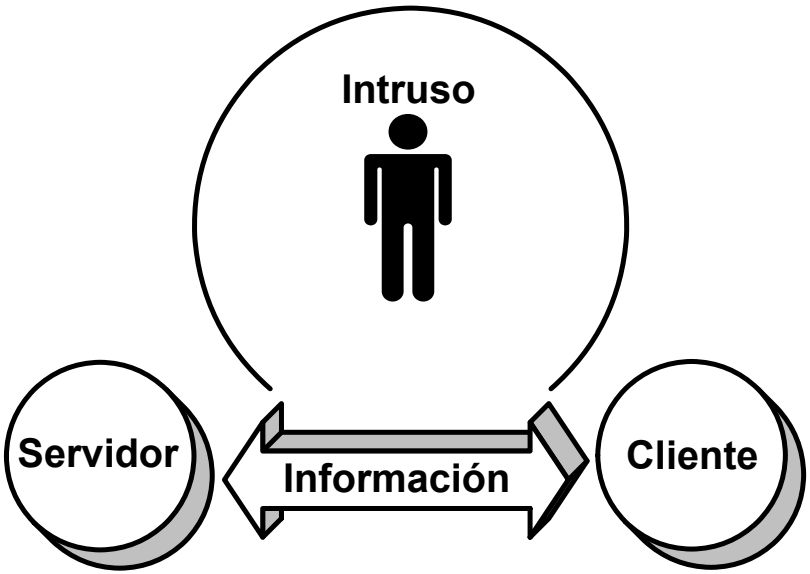
Tipos de ataques:

- Ataques pasivos.
- Ataques activos.

Tipos de intrusos:

- Intrusos curiosos.
- *Crackers*.
- Intrusos remunerados.

Seguridad informática



Tipos de ataques:

- Ataques pasivos.
- Ataques activos.

Tipos de intrusos:

- Intrusos curiosos.
- *Crackers*.
- Intrusos remunerados.

Herramientas de seguridad informática

Mecanismos de prevención:

- Mecanismos de control de acceso
- Cortafuegos

Herramientas de seguridad informática

Mecanismos de prevención:

- Mecanismos de control de acceso
- Cortafuegos

Mecanismos de recuperación:

- Antivirus

Herramientas de seguridad informática

Mecanismos de prevención:

- Mecanismos de control de acceso
- Cortafuegos

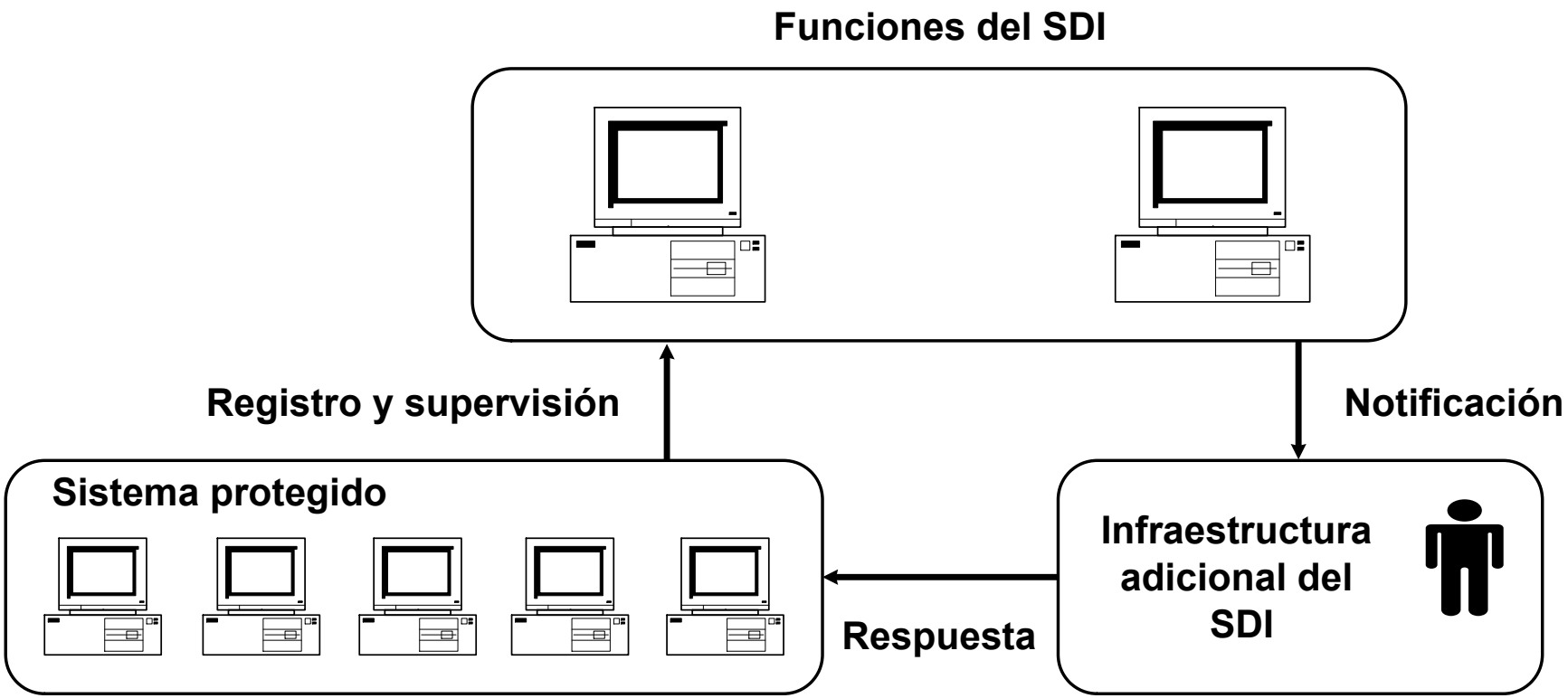
Mecanismos de recuperación:

- Antivirus

Mecanismos de detección:

- Sistemas de Detección de Intrusos

¿Qué es un Sistema de Detección de Intrusos (SDI)?



Tipos de SDI

Con base en:	Tipo de SDI
Modo de análisis	Detectores de usos indebidos
	Detectores de anomalías
Tipo de sensor	De red
	De huésped
Tiempo de ejecución	Periódicos
	De tiempo real
Tipo de respuesta	Pasivos
	Activos
Arquitectura	Centralizados
	Distribuidos

Objetivo y Motivación

Objetivo

Usar diversas técnicas de supervisión de bitácoras de uso para un servidor Linux para extraer patrones de acceso que determinen comportamientos anormales y combinar esta información con la información extraída de un análisis estadístico de tráfico.

Objetivo y Motivación

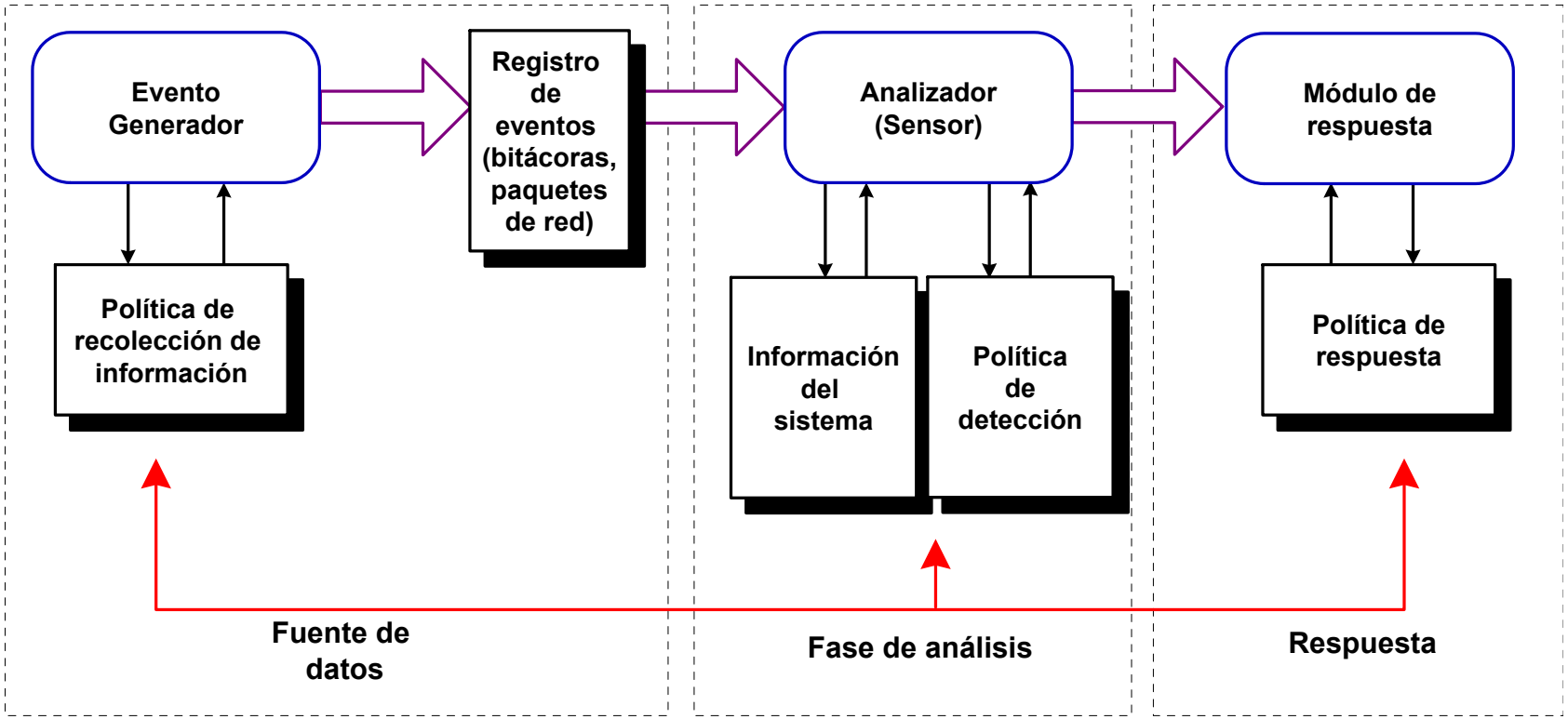
Objetivo

Usar diversas técnicas de supervisión de bitácoras de uso para un servidor Linux para extraer patrones de acceso que determinen comportamientos anormales y combinar esta información con la información extraída de un análisis estadístico de tráfico.

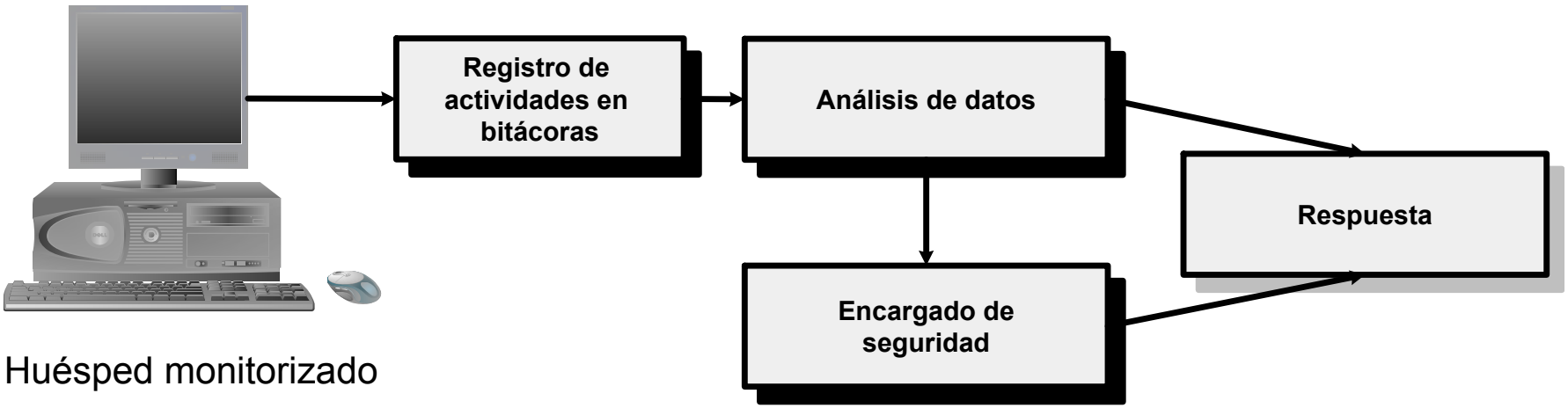
Motivación

Desarrollar un SDI híbrido que supervise las actividades de cada servidor de una red a nivel del sistema operativo, añadiendo la capacidad de supervisar el tráfico de entrada y salida de esta red.

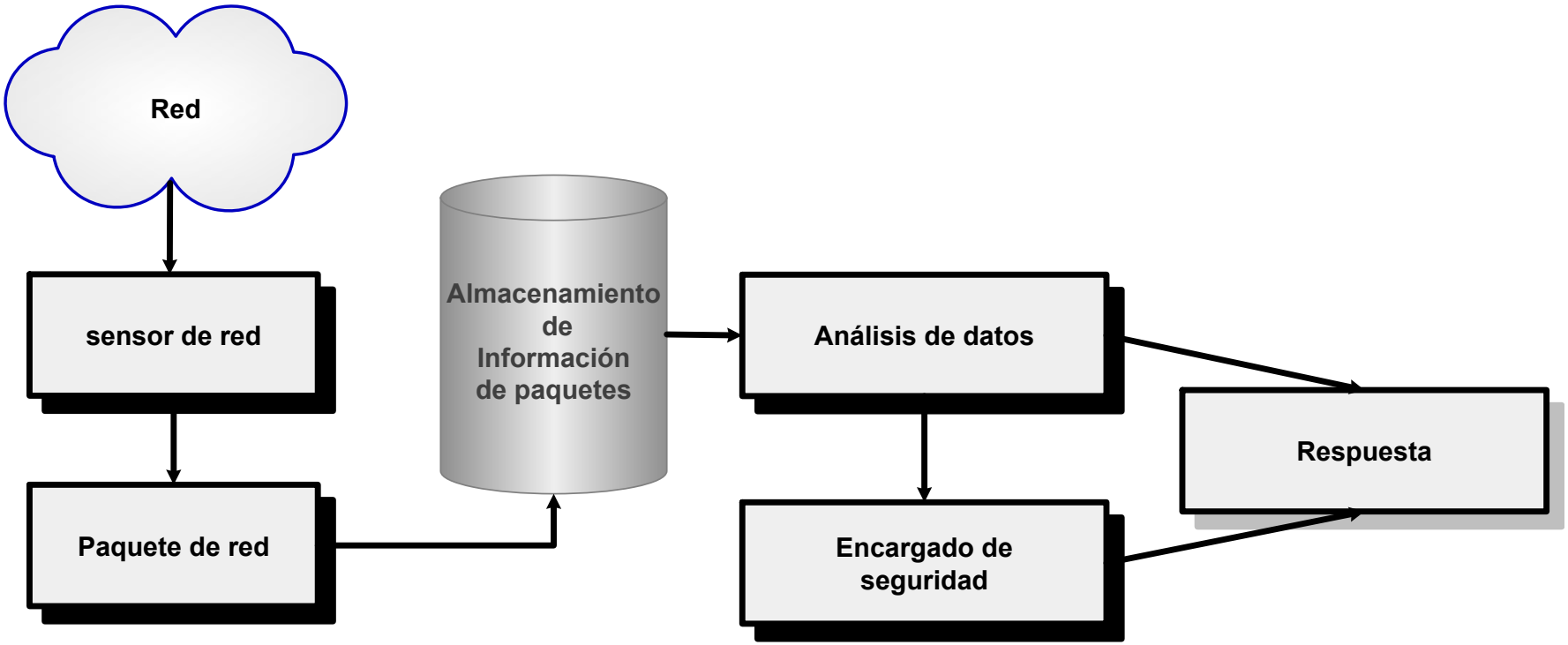
Sistemas de Detección de Intrusos (SDI)



SDI basado en huésped (SDIh)



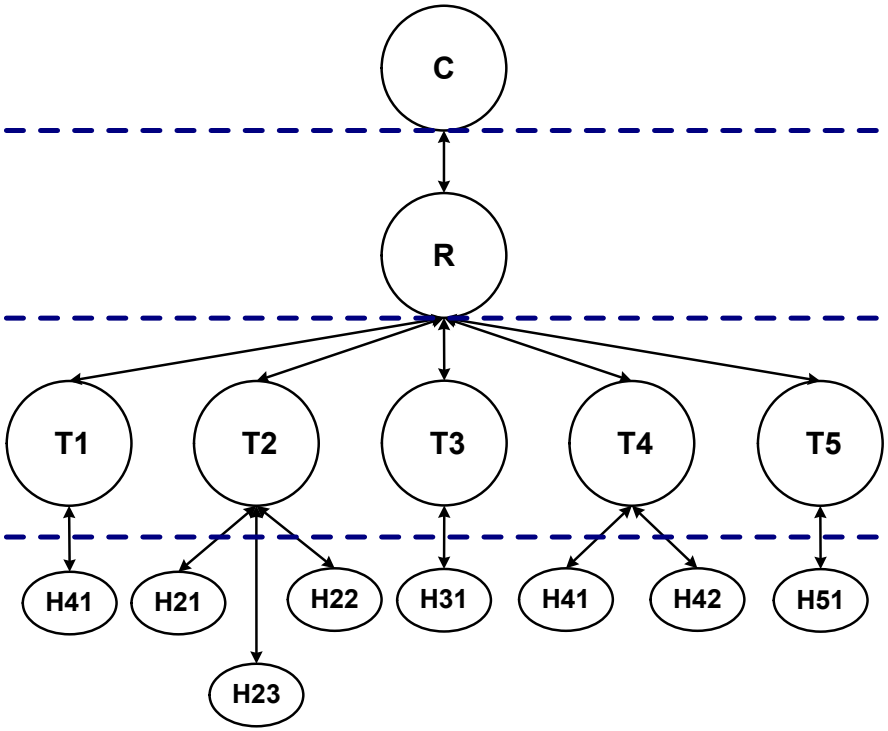
SDI basado en red (SDIr)



Diferencias entre los SDIh y los SDIr

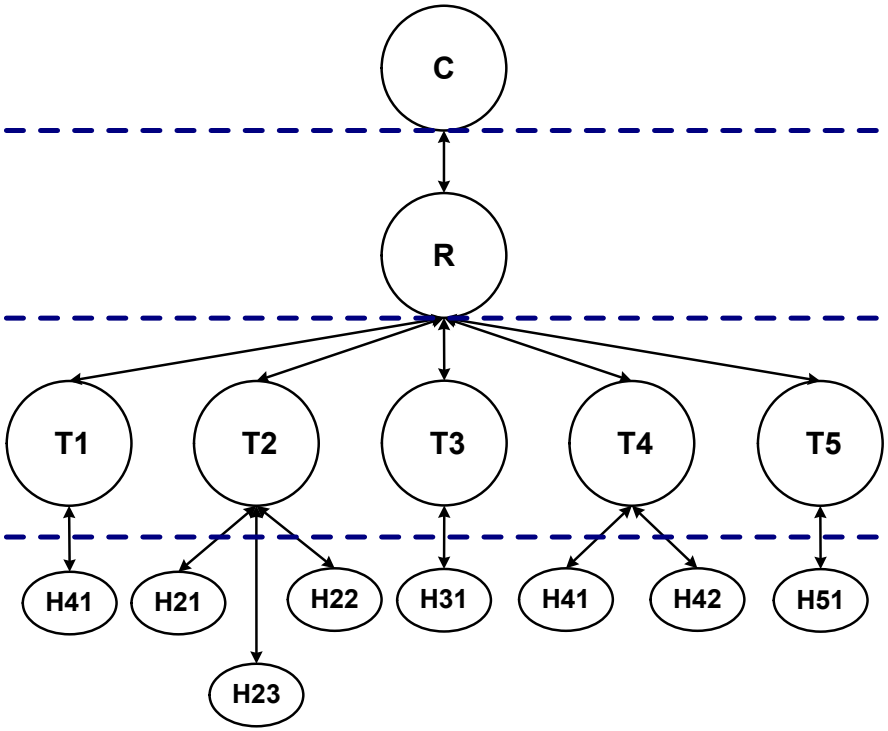
Característica	*SDIr*	*SDIh*
Visibilidad	Todo un segmento de red	Un único equipo
Nivel de operación	Diferentes capas de red	Eventos a nivel del Sistema Operativo y aplicativo
Recursos necesarios	Requiere de un equipo adicional a los sistemas protegidos con suficiente capacidad.	Utiliza los mismos recursos del sistema que protege

SDI híbrido (SDIh&r)



Componentes de un SDIh&r:

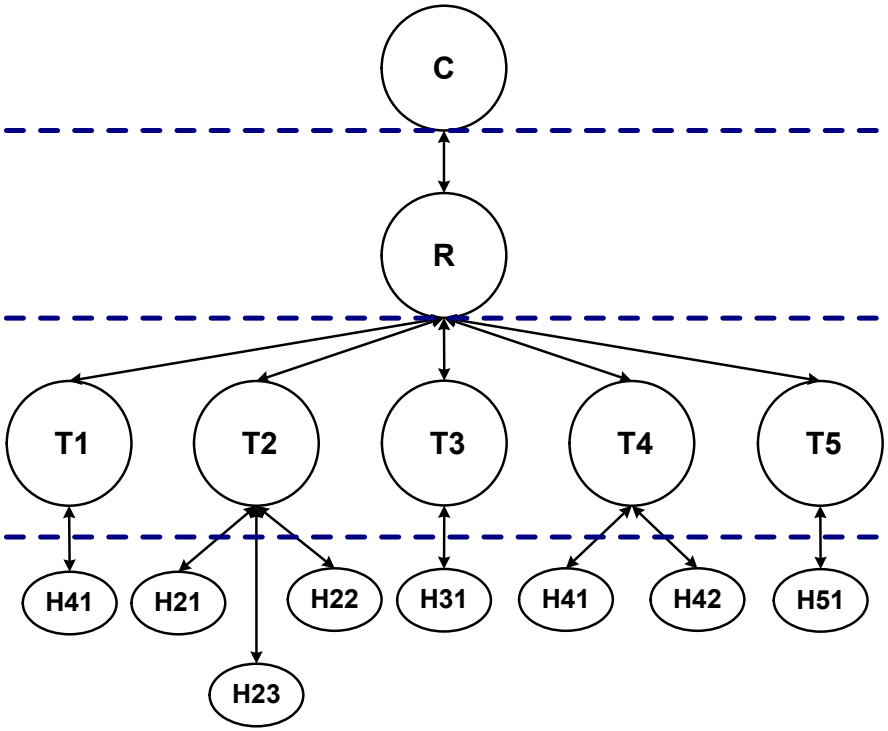
SDI híbrido (SDIh&r)



Componentes de un SDIh&r:

- Agentes de huésped.
- Agente de red.
- Tranceptores.
- Consola de eventos.

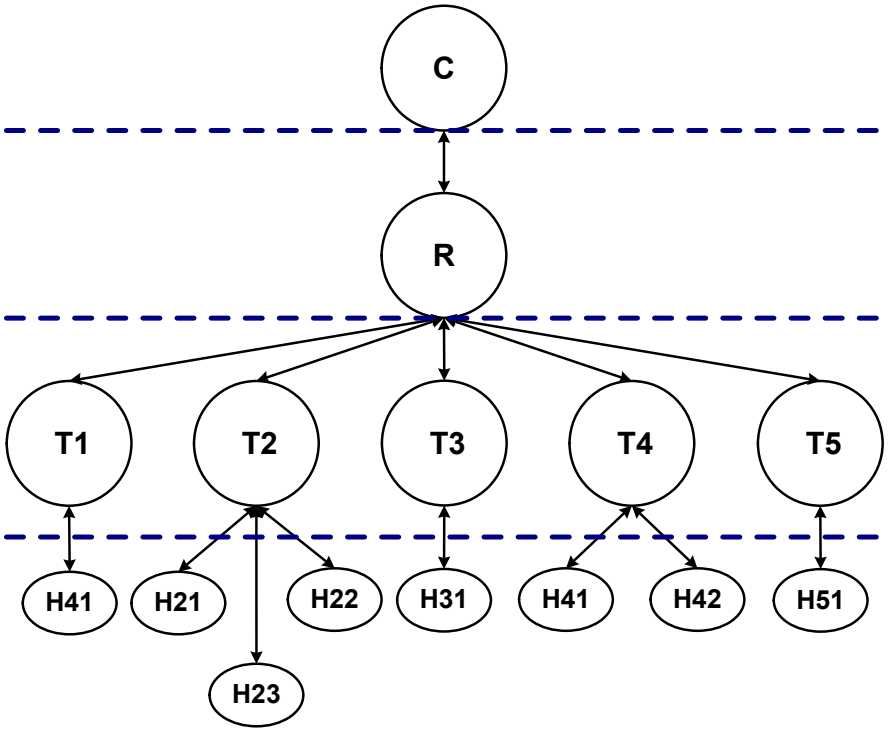
SDI híbrido (SDIh&r)



Componentes de un SDIh&r:

- Agentes de huésped.
- Agente de red.
- Tranceptores.
- Consola de eventos.

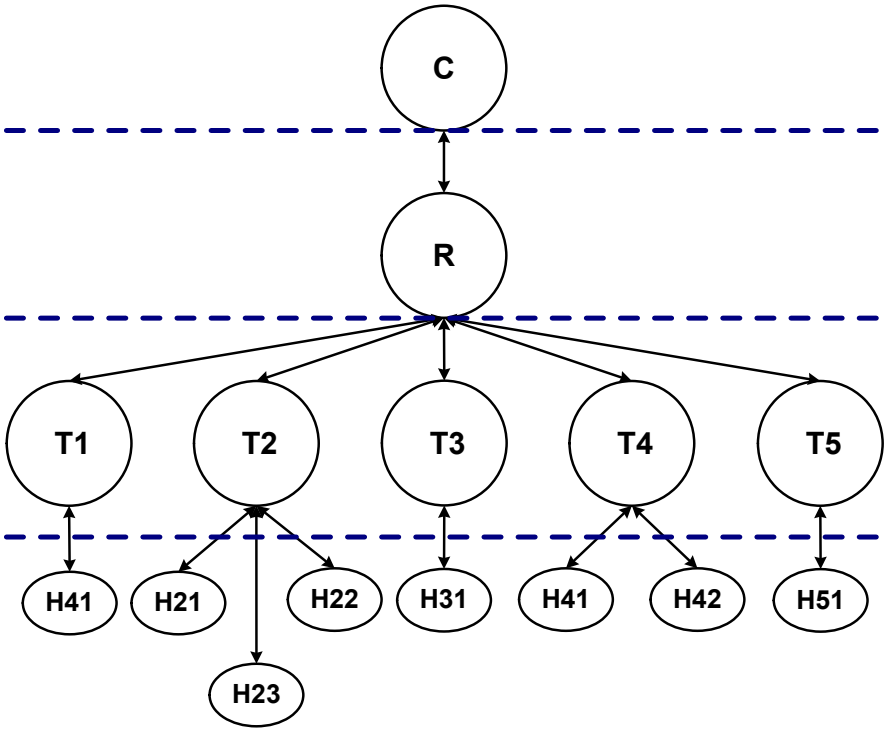
SDI híbrido (SDIh&r)



Componentes de un SDIh&r:

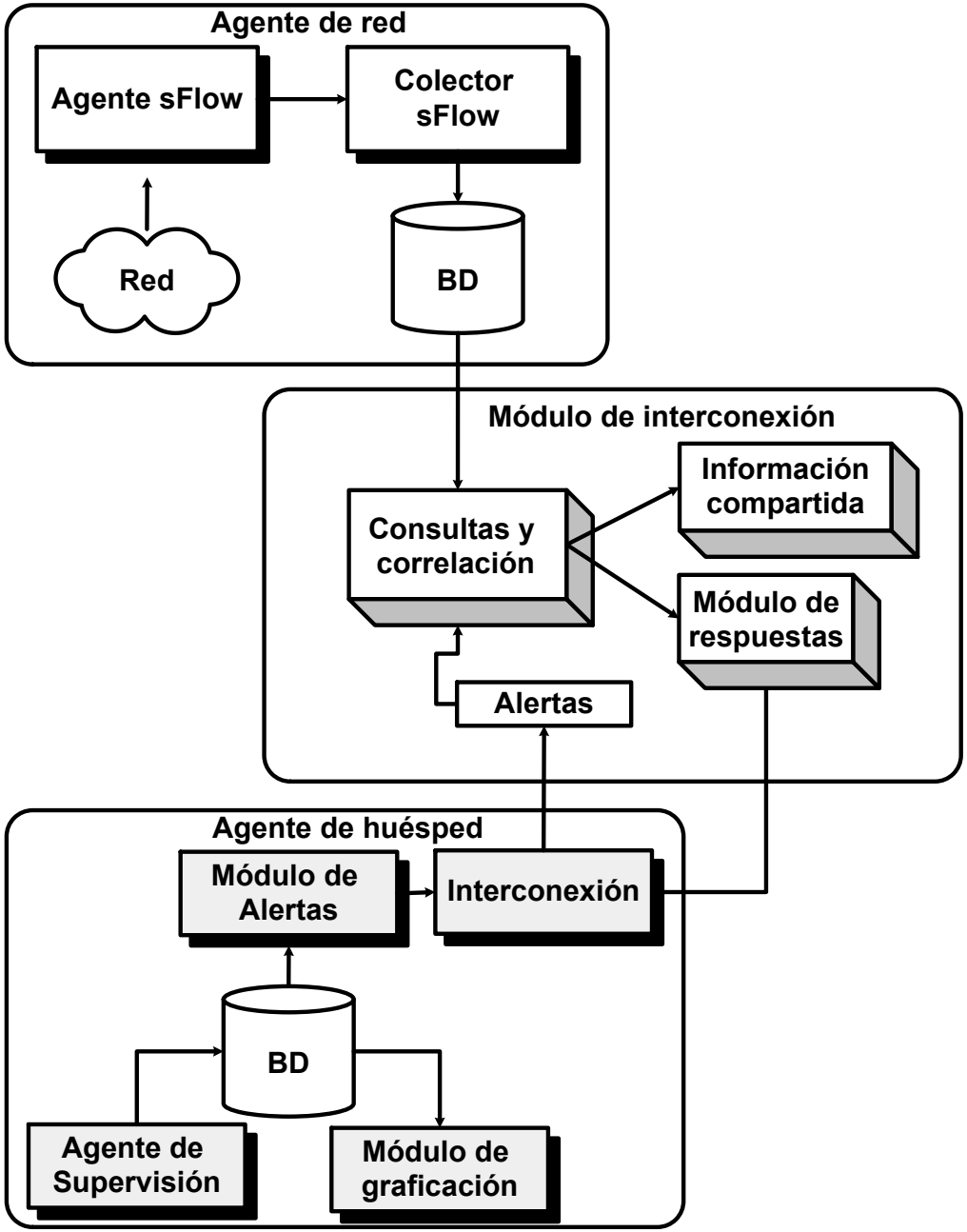
- Agentes de huésped.
- Agente de red.
- Tranceptores.
- Consola de eventos.

SDI híbrido (SDIh&r)

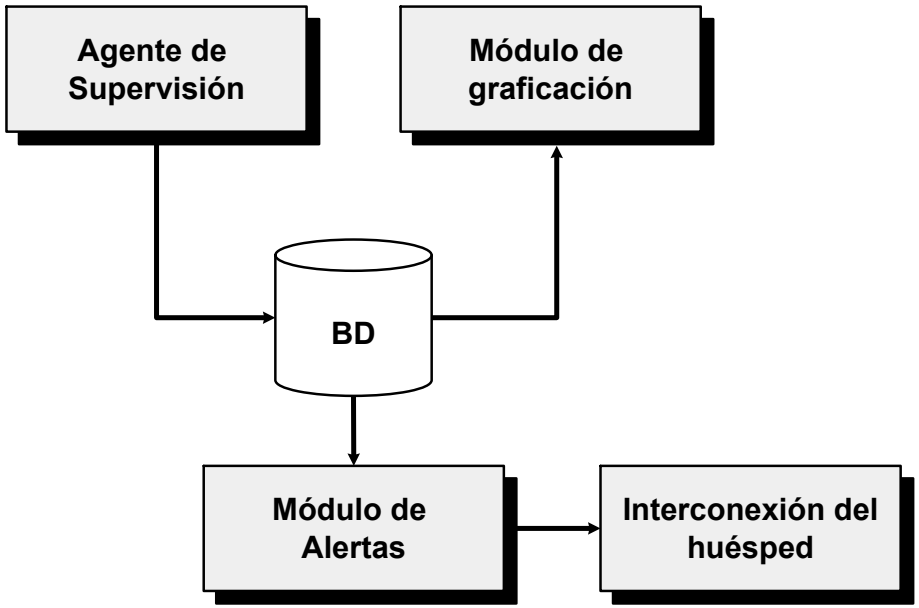


Componentes de un SDIh&r:

- Agentes de huésped.
- Agente de red.
- Tranceptores.
- Consola de eventos.

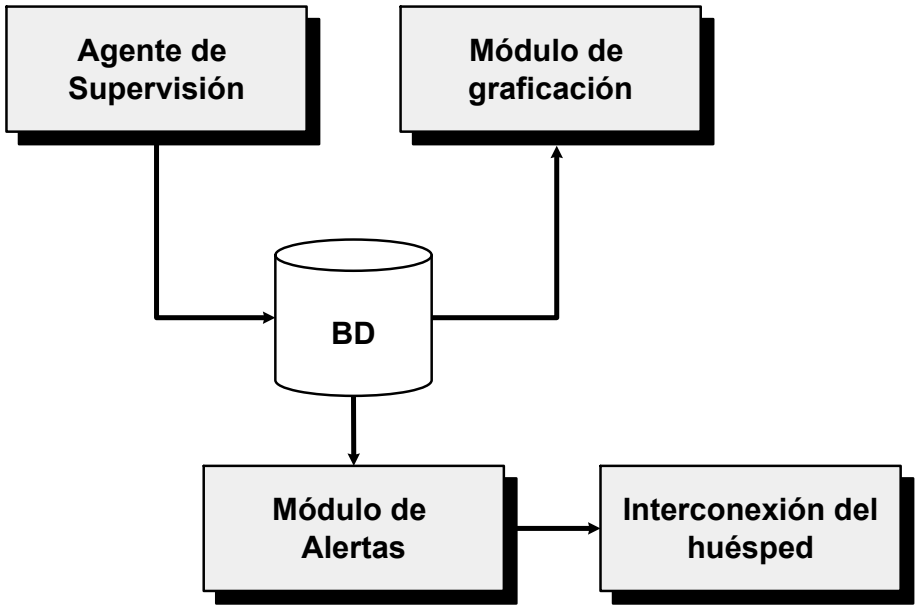

Agente de red
Agente sFlow
Colector sFlow
Red
BD
Módulo de interconexión
Información compartida
Consultas y correlación
Módulo de respuestas
Alertas
Agente de huésped
Módulo de Alertas
Interconexión
BD
Agente de Supervisión
Módulo de graficación

Agente de huésped



Módulos del SDIh:

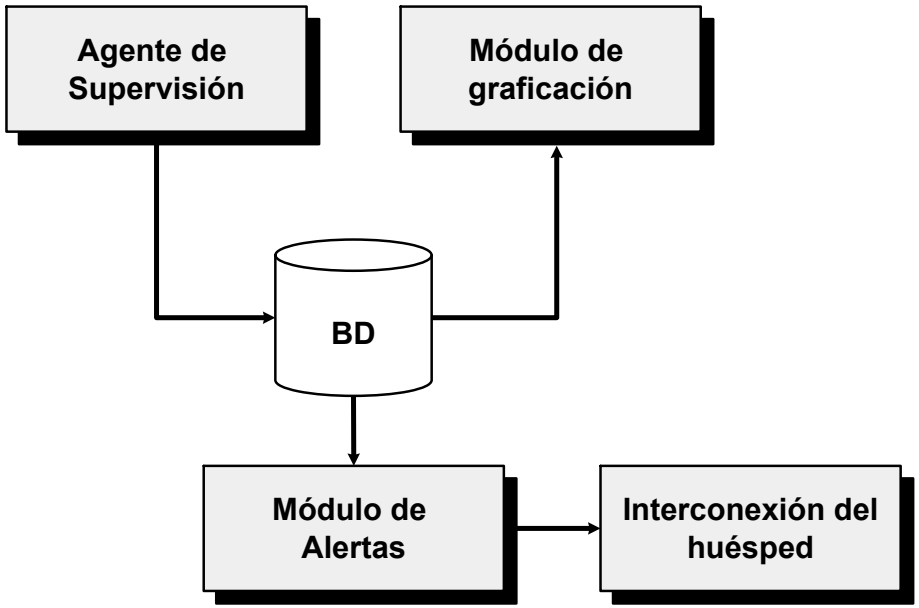
Agente de huésped



Módulos del SDIh:

- Agente de supervisión.
- Módulo de graficación.
- Módulo de alertas.
- Módulo de interconexión del huésped.
- Base de datos del huésped.

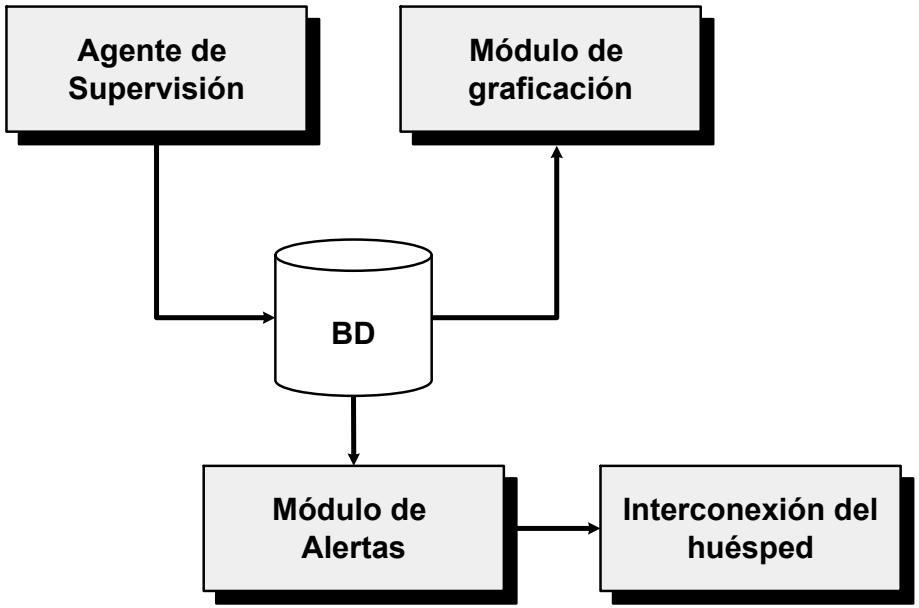
Agente de huésped



Módulos del SDIh:

- Agente de supervisión.
- Módulo de graficación.
- Módulo de alertas.
- Módulo de interconexión del huésped.
- Base de datos del huésped.

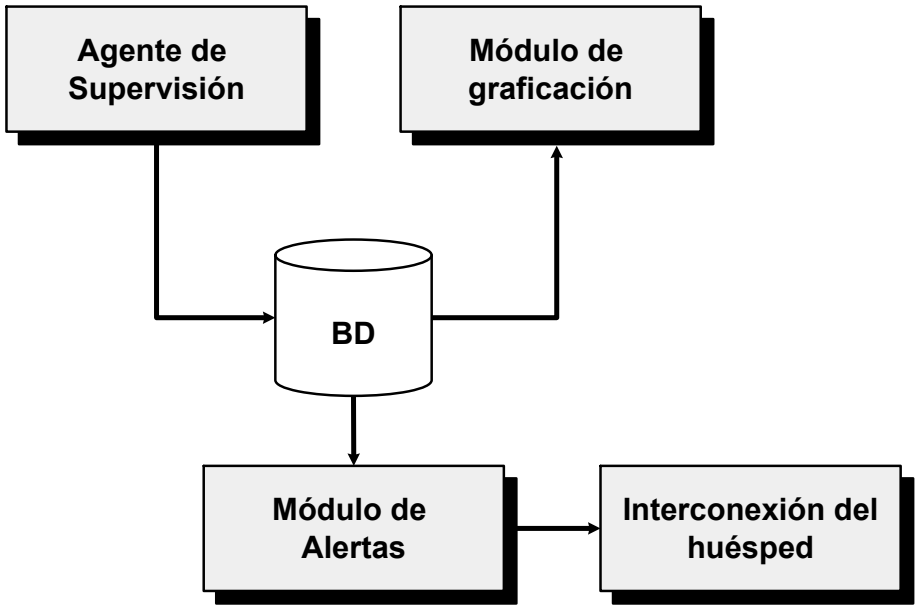
Agente de huésped



Módulos del SDIh:

- Agente de supervisión.
- Módulo de graficación.
- Módulo de alertas.
- Módulo de interconexión del huésped.
- Base de datos del huésped.

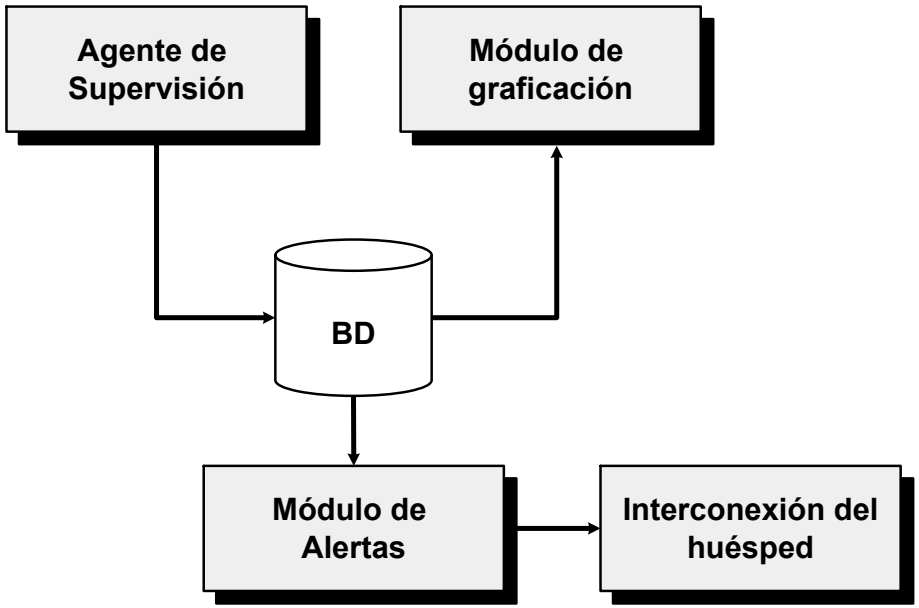
Agente de huésped



Módulos del SDIh:

- Agente de supervisión.
- Módulo de graficación.
- Módulo de alertas.
- Módulo de interconexión del huésped.
- Base de datos del huésped.

Agente de huésped



Módulos del SDIh:

- Agente de supervisión.
- Módulo de graficación.
- Módulo de alertas.
- Módulo de interconexión del huésped.
- Base de datos del huésped.

Agente de supervisión

Preprocesamiento:

Variable	Bitácora
Accesos con nombres de usuarios inexistentes	*secure*
Accesos con contraseñas incorrectas	*secure*
Correos enviados desde/hacia el servidor	*maillog*
Tamaño de los correos	*maillog*
Accesos a páginas inexistentes	*error_log*
Visitas a páginas del servidor	*acces_log*
Número de sesiones activas	*messages*

Módulo de alertas

En este trabajo se consideran tres alertas:

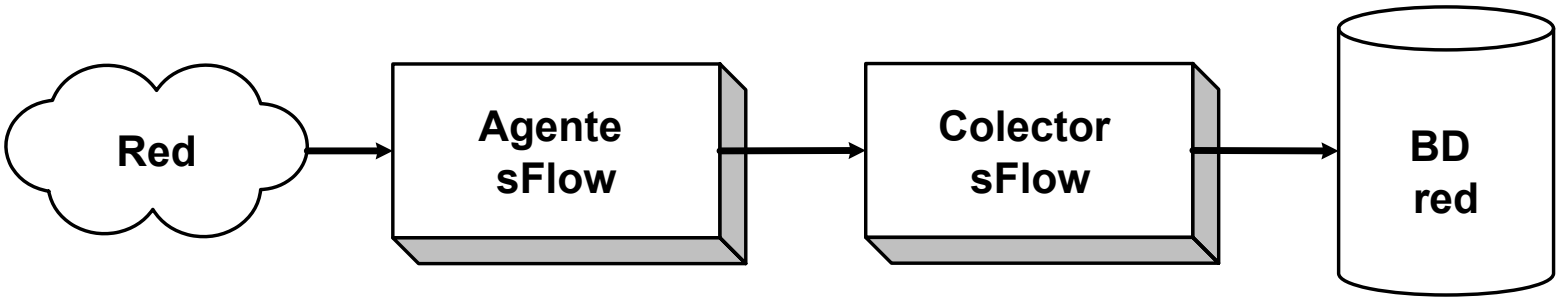
- Estado normal.
- Estado preventivo.
- Estado crítico.

Función de generación de alertas

$$f_{alerta}(c) = \begin{cases} 0, & \text{Si} \quad c < \text{Umbral}_a \\ 1, & \text{Si} \quad \text{Umbral}_a \leq c < \text{Umbral}_r \\ 2, & \text{Si} \quad \text{Umbral}_r \leq c \ . \end{cases}$$

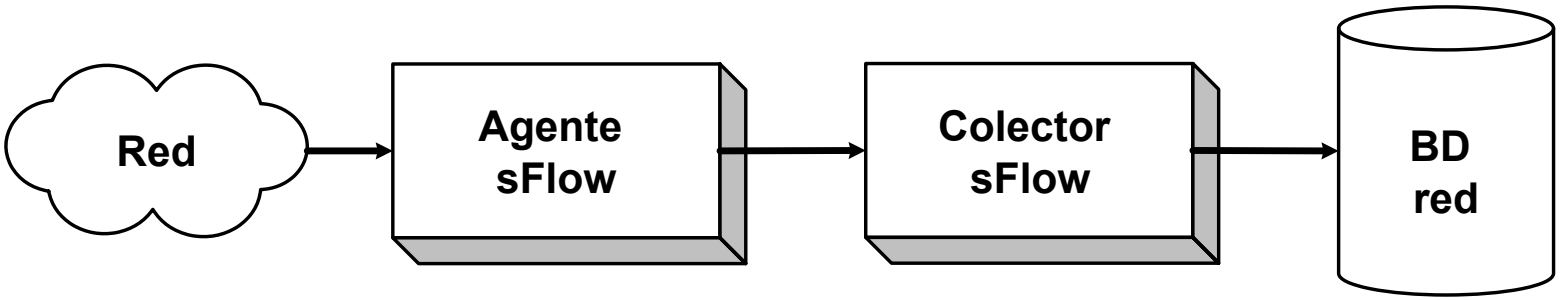
donde:
c es el contador de cada variable,
0 es una alerta verde,
1 es una alerta amarilla,
2 es una alerta roja.

Agente de red



Componentes del agente de red

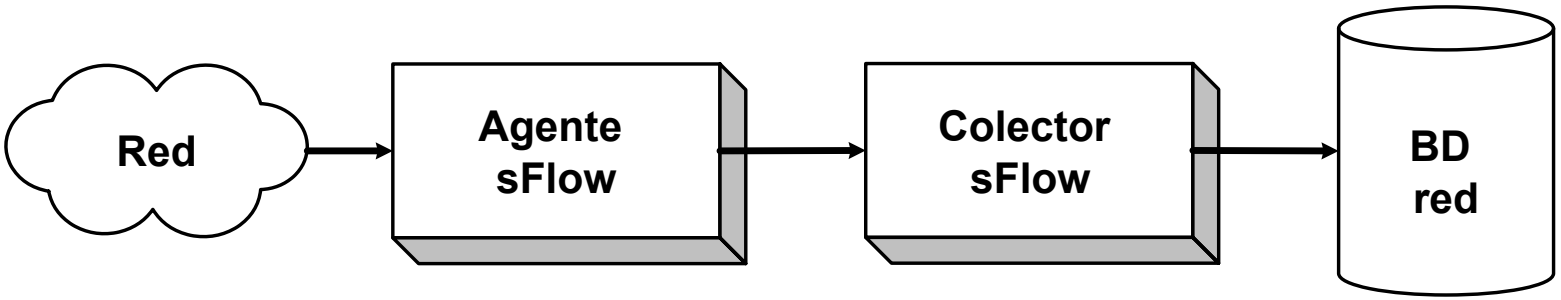
Agente de red



Componentes del agente de red

- Agente sFlow.
- Colector sFlow.
- Base de datos de red.

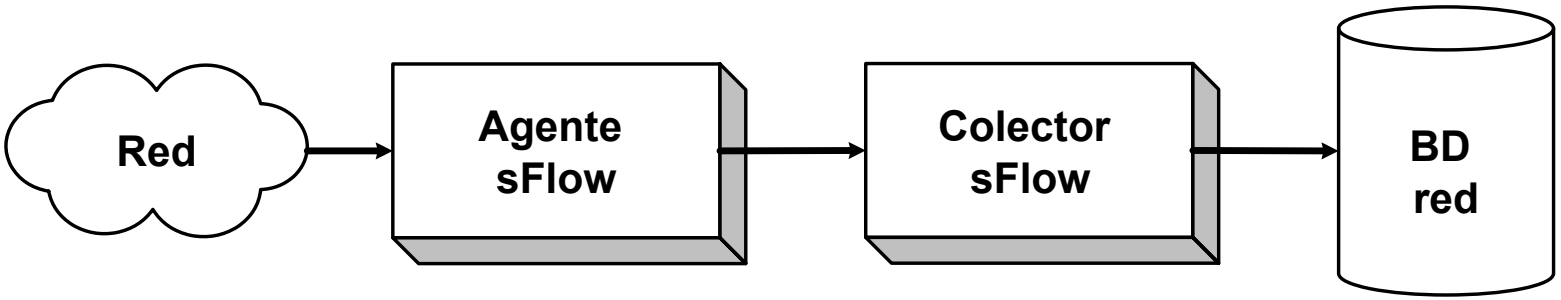
Agente de red



Componentes del agente de red

- Agente sFlow.
- Colector sFlow.
- Base de datos de red.

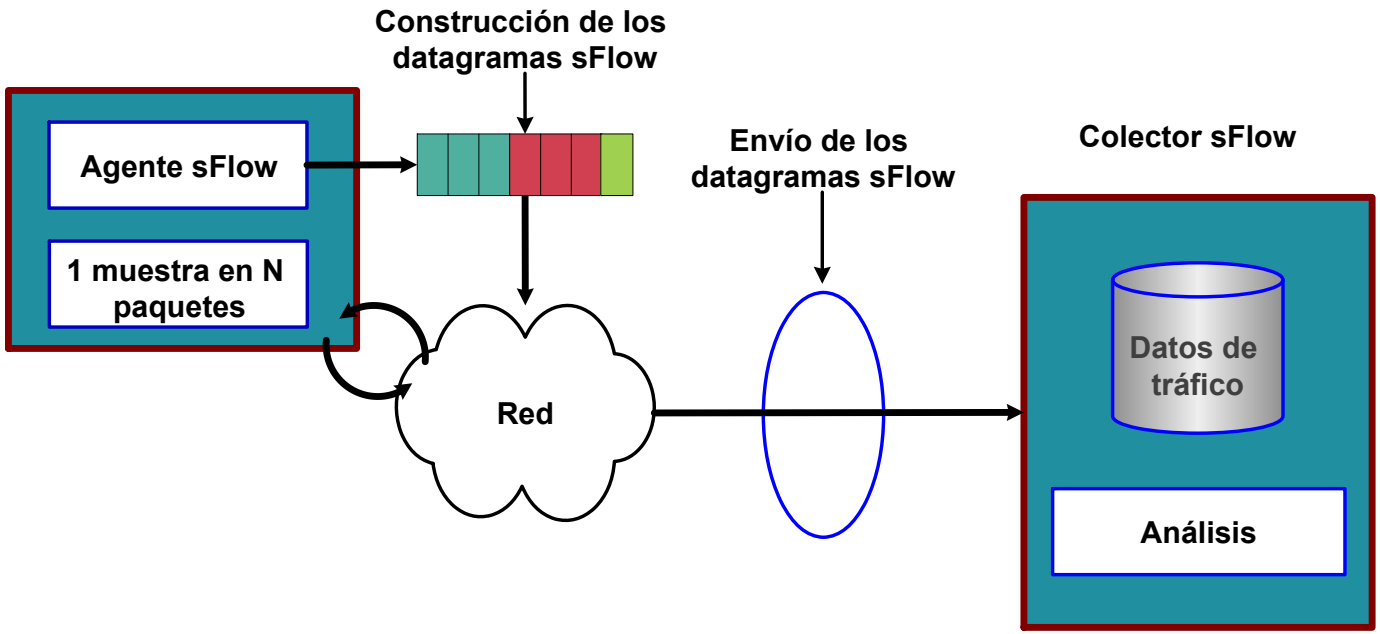
Agente de red



Componentes del agente de red

- Agente sFlow.
- Colector sFlow.
- Base de datos de red.

Componentes sFlow

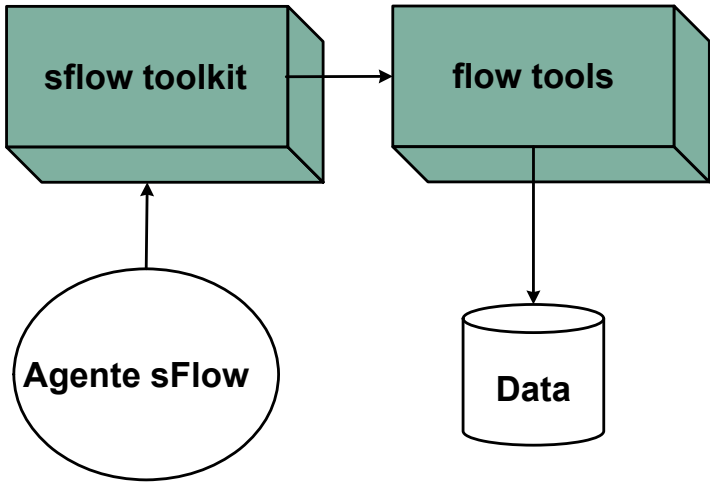


Agente sFlow

Agente sFlow

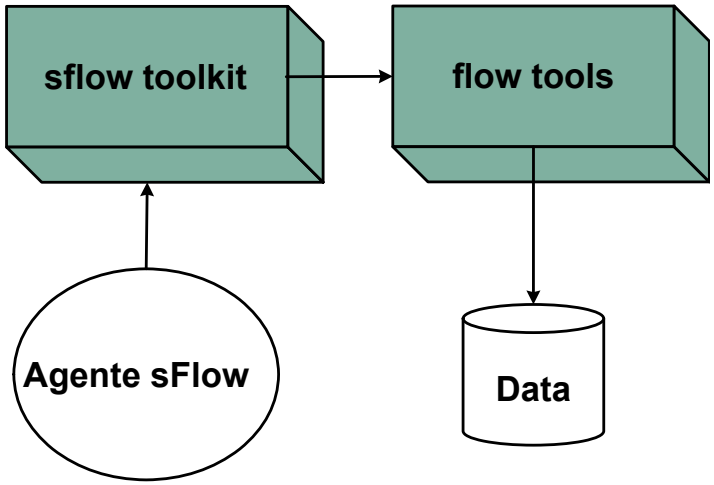
- El agente sFlow empaqueta datos dentro de datagramas sFlow que son inmediatamente enviados a través de la red a un colector sFlow.

Colector sFlow



Colectores usados:

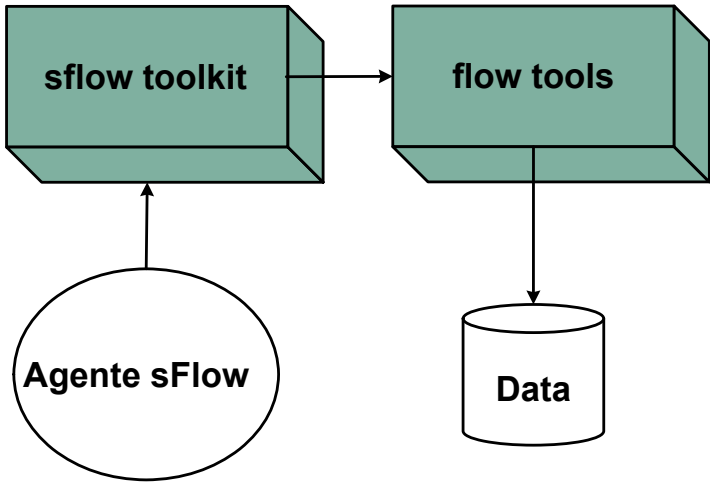
Colector sFlow



Colectores usados:

- sFlow Toolkit.
- Flow-tools (Colector Netflow).

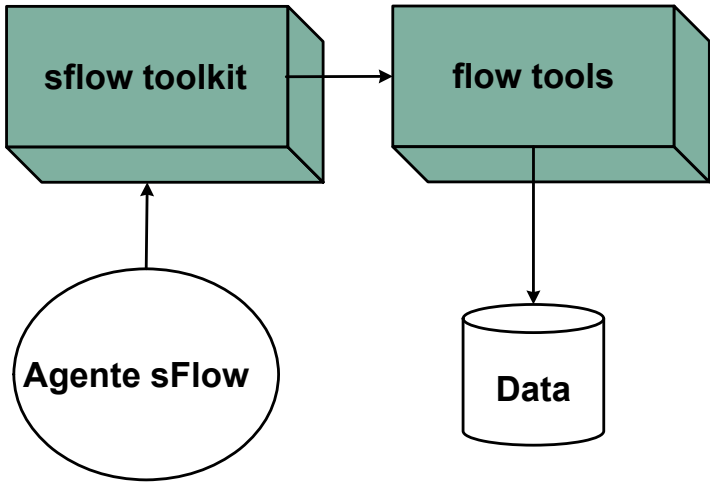
Colector sFlow



Colectores usados:

- sFlow Toolkit.
- Flow-tools (Colector Netflow).

Colector sFlow



Colector:

Algoritmo 3. Algoritmo colector de tráfico

Entrada: Archivo de flujo generado por flow-capture.
Salida: Base de datos de red actualizada.
1. *Datos* ← flow-export(Archivo de flujo)
2. for cada línea del archivo *Datos* **do**
3. Obtener cada cadena delimitada por una coma
4. Insertar cadenas en la base de datos de red
5. end for

Base de datos de red

Estructura de la base de datos de red

Campo	*Descripción*
Hora	Hora exacta en segundos en que ocurrió el evento
Protocolo	Protocolo usado en la transmisión
IPFuente	Dirección IP origen
IPDestino	Dirección IP destino
PtoFuente	Puerto origen
PtoDestino	Puerto destino
Paquetes	Tamaño en paquetes de los datos transmitidos en la sesión
Bytes	Tamaño en bytes de los datos transmitidos en la sesión

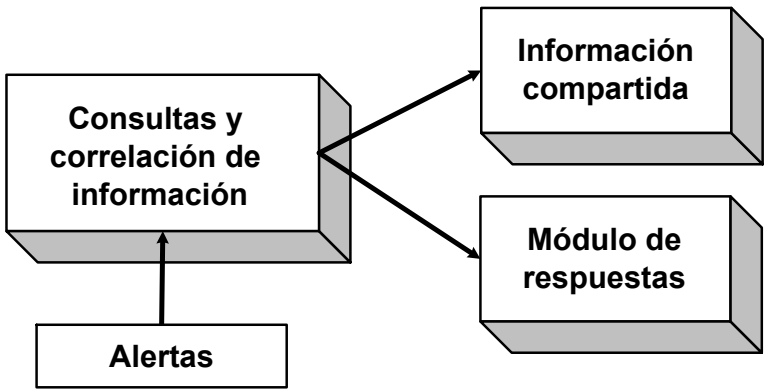
Detección de patrones de red

Hora	*IP Fuente*	*IP Destino*	*Pto Fuente*	*Pto Destino*
11:10	148.247.10.1	192.168.10.157	8080	2030
11:10	—	—	—	2031
11:10	—	—	—	2032
11:10	—	—	—	.
11:10	—	—	—	.
11:10	—	—	—	.
11:10	—	—	—	2039
11:10	—	—	—	2040
11:10	—	—	—	2041

Patrones de red:

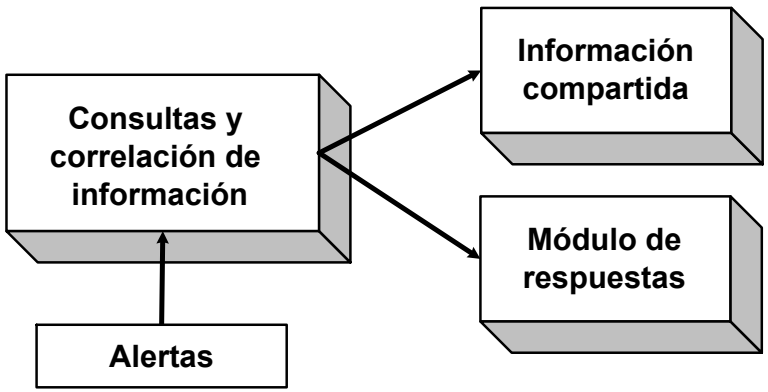
- Exploración de puertos.
- Exploración de direcciones IP.

Módulo de interconexión



Módulos del módulo de interconexión:

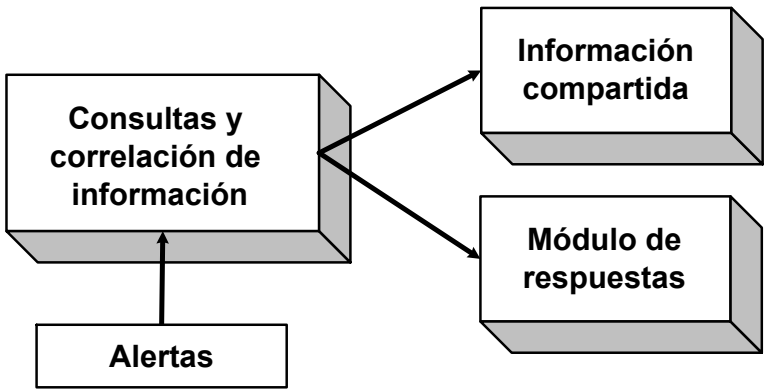
Módulo de interconexión



Módulos del módulo de interconexión:

- Monitor de alertas.
- Módulo de correlación de información.
- Información compartida.
- Módulo de respuestas.

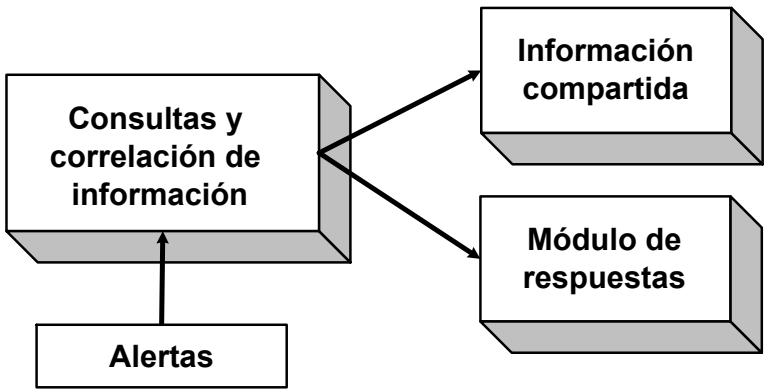
Módulo de interconexión



Módulos del módulo de interconexión:

- Monitor de alertas.
- Módulo de correlación de información.
- Información compartida.
- Módulo de respuestas.

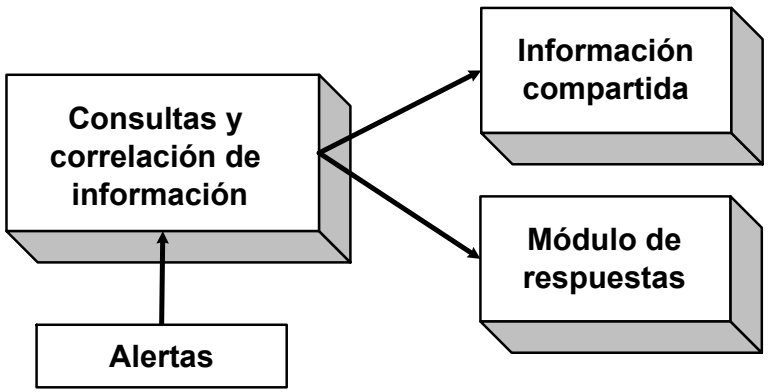
Módulo de interconexión



Módulos del módulo de interconexión:

- Monitor de alertas.
- Módulo de correlación de información.
- Información compartida.
- Módulo de respuestas.

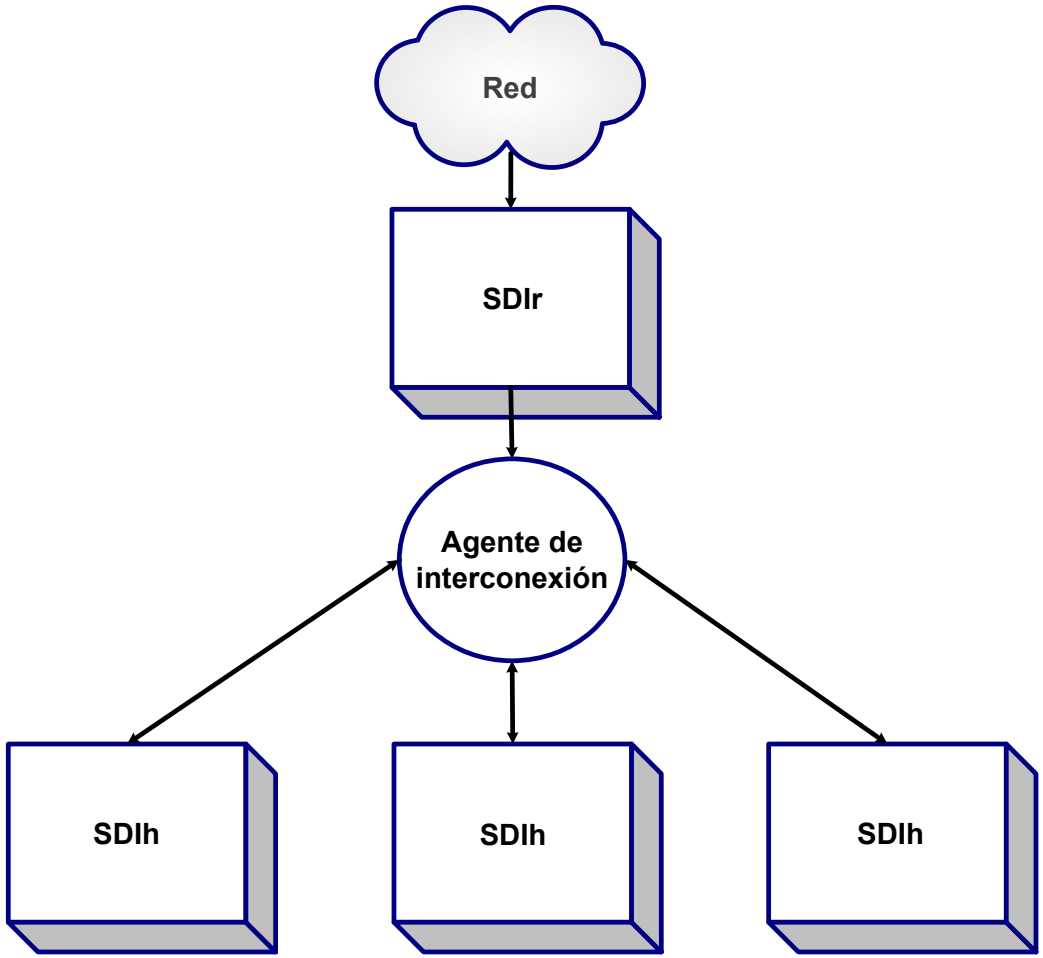
Módulo de interconexión



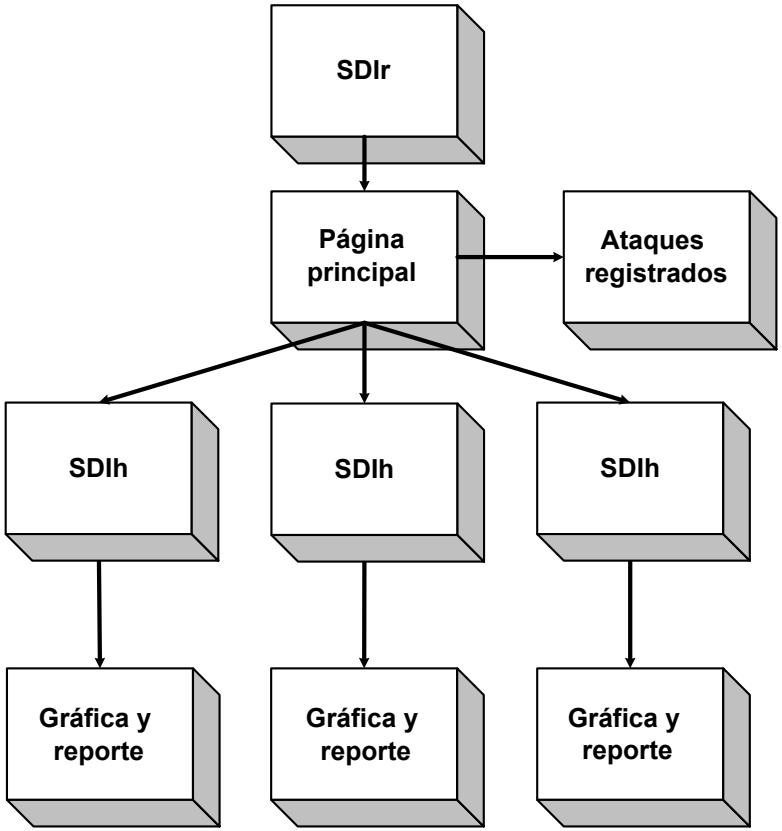
Módulos del módulo de interconexión:

- Monitor de alertas.
- Módulo de correlación de información.
- Información compartida.
- Módulo de respuestas.

Funcionamiento del sistema de monitoreo y detección de intrusos



Mapa del sitio web del sistema



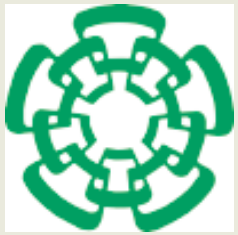
Sitio web del sistema:

- Página principal.
- Página de información compartida.
- Sitio web del SDIh.
- Sitio web del SDIr.

Estructura básica del sitio web

Página principal

Página principal



Monitoreo de archivos de bitácora

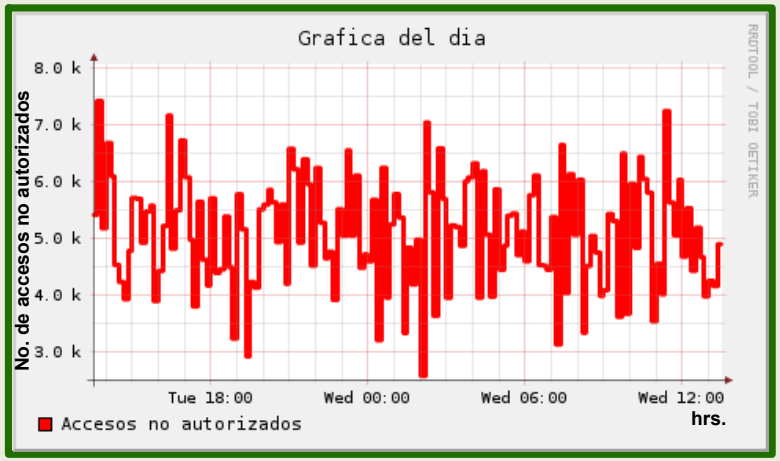
Intento de acceso con nombres de usuario inexistentes	(Alerta verde)	Umbrales:3,5	Periodo:10 min
Intento de acceso con passwords incorrectos	(Alerta verde)	Umbrales:3,15	Periodo:10 min
Correos enviados al servidor	(Alerta roja)	Umbrales:5,15	Periodo:10 min
Correos enviados desde el servidor	(Alerta amarilla)	Umbrales:10,15	Periodo:10 min
Conexiones perdidas con el servidor de correo	(Alerta verde)	Umbrales:4,8	Periodo:10 min
Correos enviados a usuarios inexistentes	(Alerta verde)	Umbrales:10,15	Periodo:10 min
Tamaño de los correos	(Alerta roja)	Umbrales:15,25	Periodo:10 min
Intento de acceso a páginas inexistentes	(Alerta verde)	Umbrales:20,35	Periodo:10 min
Intento de acceso a directorios prohibidos	(Alerta verde)	Umbrales:3,5	Periodo:10 min
Visitas a páginas del servidor	(Alerta roja)	Umbrales:10,15	Periodo:10 min
Número de sesiones activas	(Alerta verde)	Umbrales:10,15	Periodo:10 min

Estructura básica del sitio web

Estructura de los resultados

Visualización de resultados

<<Mensaje de alerta>>

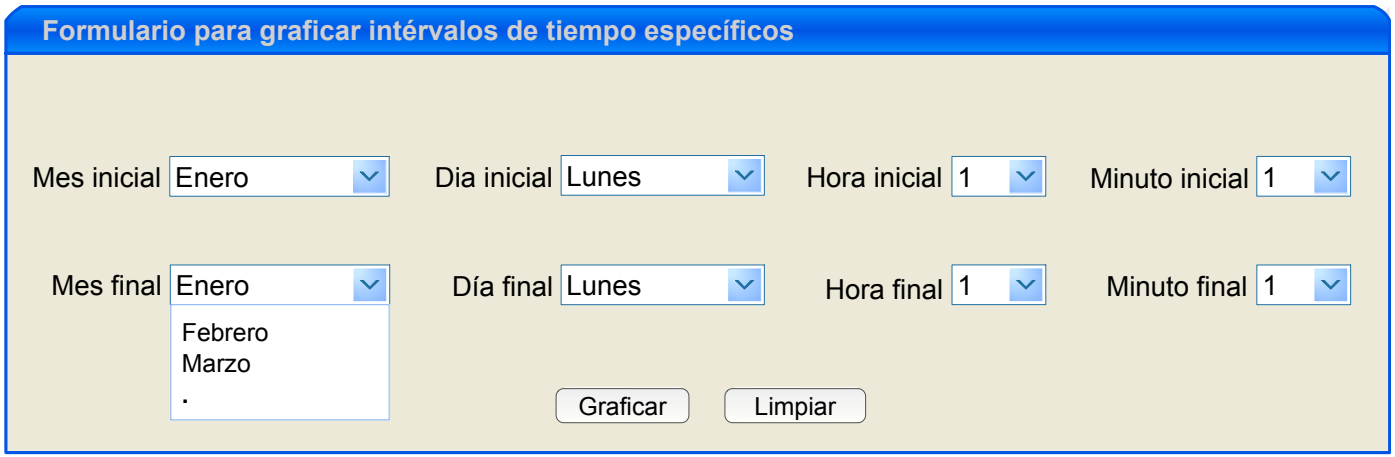


Hora	Fuente	Destino	Tipo de ataque
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.

Estructura básica del sitio web

Gráficas por fechas y configuraciones

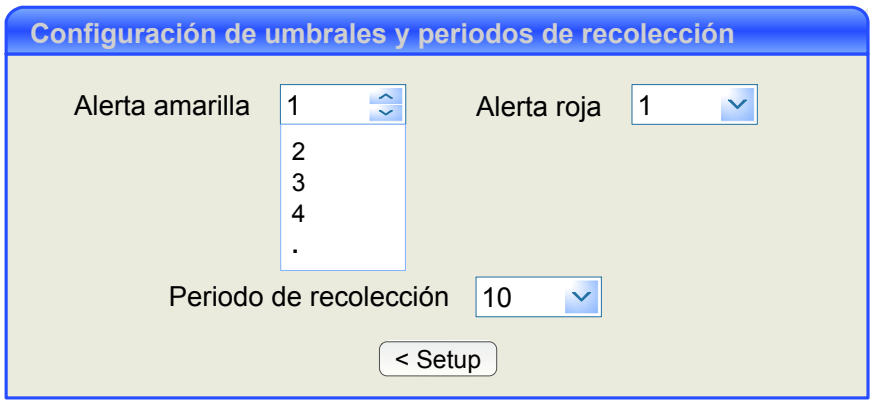
Gráficas por fechas específicas



Estructura básica del sitio web

Gráficas por fechas y configuraciones

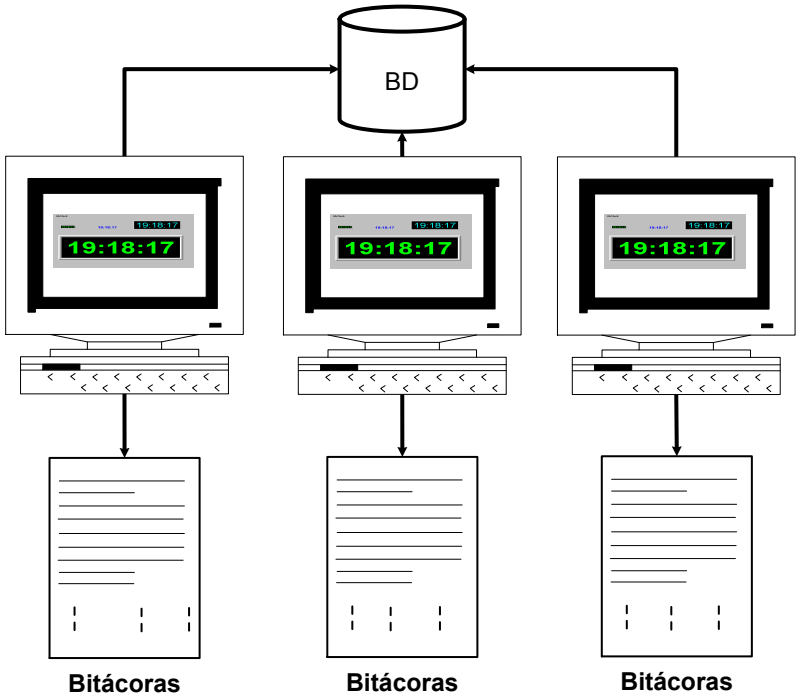
Configuración de umbrales y periodos de recolección



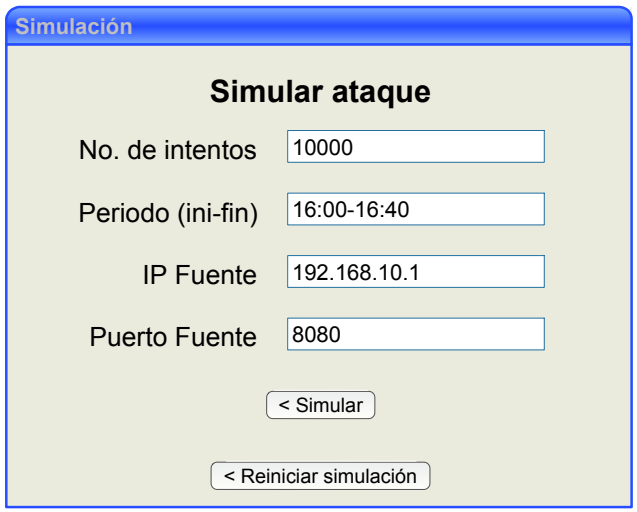
Modo de simulación

Componentes del sistema en modo de simulación

- Un reloj que consiste en un archivo que se actualiza cada *N* segundos.
- Los datos que se procesan son generados por el usuario de manera aleatoria o inducida.



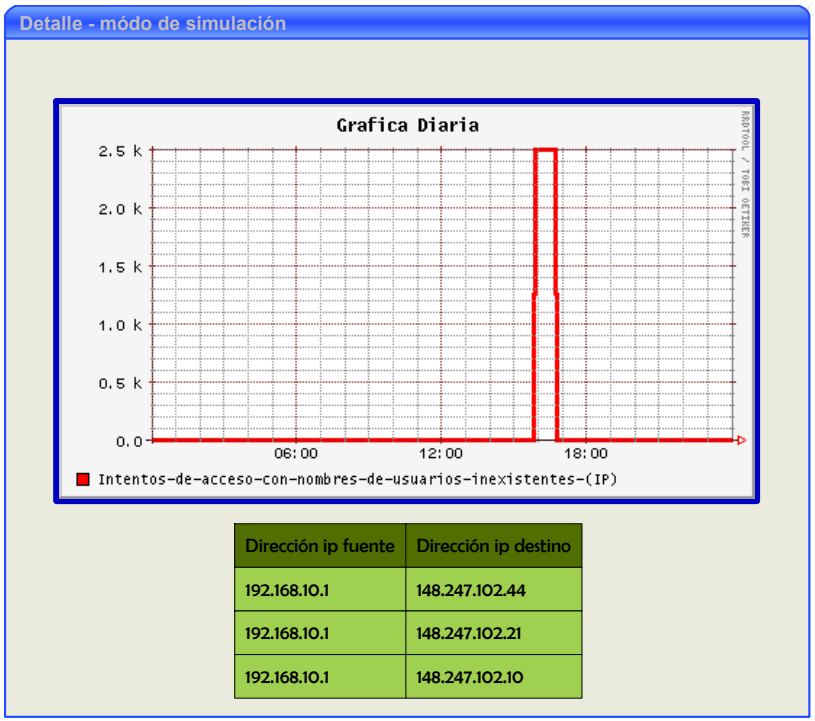
Sitio web en el modo de simulación



Elementos del sitio web en modo de simulación:

- Formulario para generar ataques.
- Resultados en forma de gráficas y reportes.

Sitio web en el modo de simulación



Dirección ip fuente	Dirección ip destino
192.168.10.1	148.247.102.44
192.168.10.1	148.247.102.21
192.168.10.1	148.247.102.10

Elementos del sitio web en modo de simulación:

- Formulario para generar ataques.
- Resultados en forma de gráficas y reportes.

Discusión

SDI existentes

SDI	Análisis	Sensor	Ejecución	Respuesta	Arquitectura	Distribución
Tripewire	A	Huésped	Periódico	Pasivas	Centralizado	Comercial
OSSEC	A	Huésped	T. Real	Activas	Distribuido	Libre
RealSecure	UI	Red	T. Real	Activas	Distribuido	Comercial
Snort	A&UI	Red	T. Real	Activas	Centralizado	Libre
Prelude	UI	Híbrido	T. Real	Activas	Distribuido	Libre
DIDS	UI	Híbrido	T. Real	Activas	Centralizado	No disponible
S. Híbrido	A	Híbrido	Periódico	Pasivas	Distribuido	—

Donde:
A - Basado en Anomalías.
UI - Basado en Usos Indebidos.
A&UI - Basado en Anomalías y en Usos Indebidos.

Conclusiones

Conclusiones

- El sistema implementado en este trabajo de tesis consiste de tres módulos principales: un agente de huésped, un agente de red y un módulo de interconexión.
- El sistema está diseñado como una solución robusta para detectar intrusos en un sistema, con la capacidad de supervisar servidores y redes.
- Este sistema presenta una arquitectura distribuida capaz de proveer exactitud en las detecciones. Por un lado el agente de red proporciona al sistema información general de un ataque, mientras que el agente de huésped proporciona el rastro del origen del ataque.

Trabajo Futuro

Trabajo Futuro

- Aumentar el número de patrones en los dos agentes —huésped y red—.
- Añadir métodos automáticos e inteligentes para la definición de umbrales.
- Usar métodos para el módulo de interconexión que analicen los ataques detectados por el sistema y obtener estadísticas de éstos.
- El módulo de respuestas puede generar respuestas activas.

SIBOS

Universo 07

www.sibos.com.mx

3er. Congreso

Tecnologías de Información y Comunicación

Expandiendo tus ideas

Realizado en la semana del 28 de mayo al 1ro. de Junio del 2007

FCC - BUAP

Memorias del Congreso

Conferencia : Project Management

Manuel Rivera, PMP

T · · Systems ·

Contenido

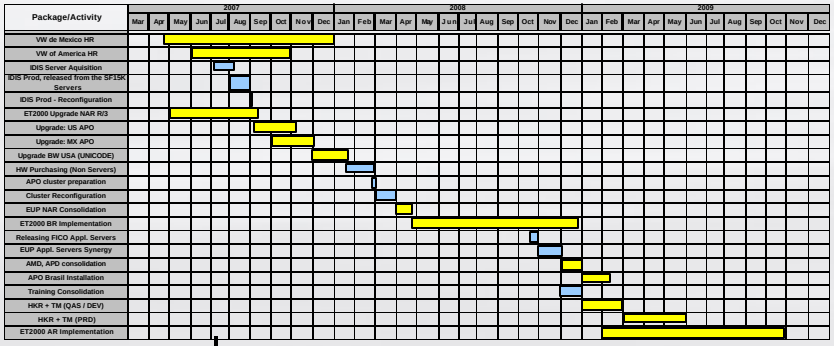
- Que es Project Management?
- Que pasa si no se utiliza PM….
- Conceptos básicos PM
- PM en Puebla
- Recomendaciones
- Propuesta

Que es PM (Project Management) ?

- Es el arte o ciencia para manejar o gestionar Proyectos.
- Es una nueva especialidad o carrera profesional a nivel mundial
- Actualmente hay 250,000 PMPs certificados en todo el mundo.
- Se aplica en cualquier tipo de industria
- Inicia en los ’50s

Metodologías
y Mejores prácticas

Proyectos = PMI



Servicio o Mantenimiento

ITIL

Sistema Calidad
ISO
Kaizen

Metodología : CMMI (ISO)

Desarrollo SW
Implementación SW-STD o HW

Que es un Proyecto?

- "…una misión temporal que se realiza para producir un único producto, servicio o resultado.
- Se realiza por única vez
- Con un inicio y fin definido
- Con un presupuesto definido
- Con un alcance definido
- Con la calidad esperada

Que es PMI?

- Project Management Institute (PMI®)
- Creado en 1969
- Certifica Líderes experimentados como PMP® s
- Ofrece credenciales a nivel asociados -> Ruta CAPM ®. (Sin experiencia laboral)
- Crea el PM-BOK® (2004)
- Certifica productos y PgMP

Cuando se debe usar PM?

- Competencia
- Los trabajos son complejos?
- Existen consideraciones dinámicas del ambiente?
- Existen fuertes restricciones?
- Existen varias actividades a integrar?
- Se requiere atravesar fronteras funcionales?

Que es un PMP ?

- Project Manager Professional
- Liderazgo
- Capacitación Formal
- Certificado mundial
- 5,000hrs o 7,000hrs como LP
- Código de Etica PMI®

Que es un CAPM ?

- Capacitación Formal 23 hrs

o

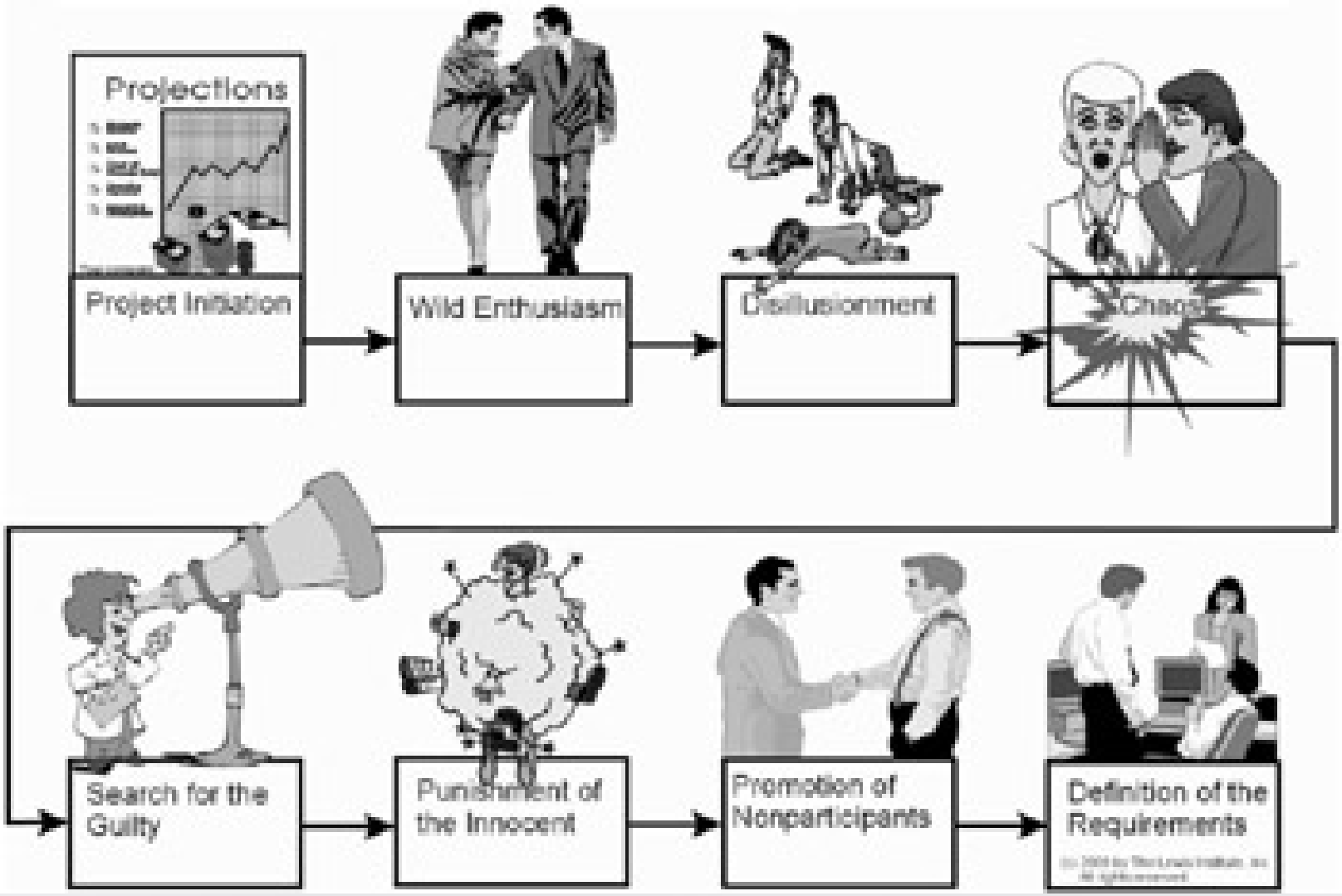
- 1500 hrs en proyectos
- Nivel preparatoria o carrera no terminada.
- Código de Etica PMI®
- Faculta como :

  Miembro Equipo o PMjr

Que pasa si no se utiliza PM?

- 80% de proyectos fracasan….
- Éxitos gracias a ‘’Héroes’’ o suerte…
- Dificil replicar éxitos….
- Desviación tiempo y costo….
- Desmotivación del personal…
- *Fuera de mercado*….

Ejemplo de un proyecto que no usa PM



Skills requeridos de un PMP?

1. Habilidades Técnicas

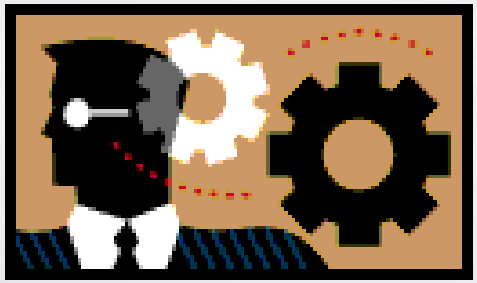
2. Habilidades Personales

Skills Personales

- Flexibilidad
- Liderazgo
- Comunicación (90%)
- Disciplina
- Organización
- Decisión
- Negociación

Porqué Skills Personales?

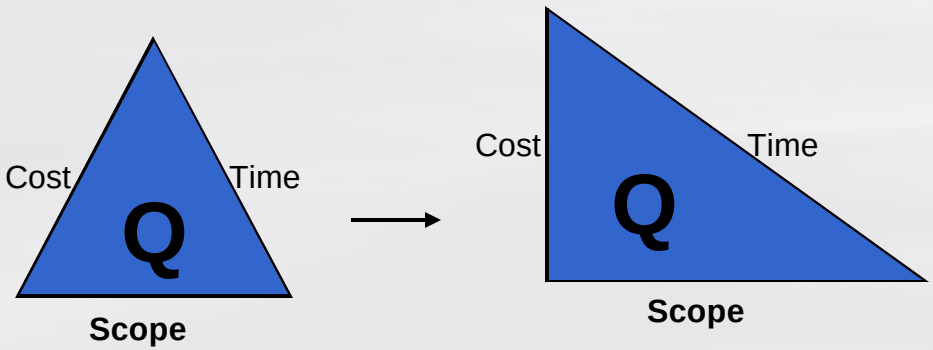
- Organizaciones Matriciales (Roma)
- Recursos inadecuados
- Calendarios irreales
- Objetivos no claros (Directores/Customer)
- Falta de compromiso del equipo
- Planeación inadecuada
- Problemas de Comunicaión
- Cambios de objetivos y recursos
- Conflictos entre departamentos



Skills Técnicos

- Generalidad
- Planeación
- Seguimiento
- Control

PM-Bok



Ciclo de vida de un Proyecto.

Areas de Conocimiento

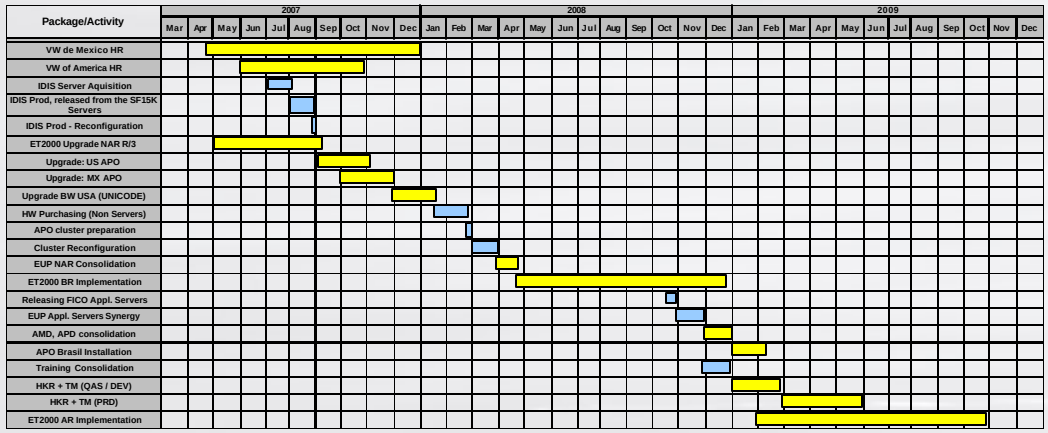
1. Gestión de Alcance
2. Gestión del Tiempo
3. Gestión del Costo
4. Gestión de la Calidad
5. Gestión de RH
6. Gestión de la Comunicación
7. Gestión del Riesgo
8. Gestión de Compras
9. Gestión de la Integración

Gestión del Alcance

- Que incluye y que no se incluye en el proyecto?
- Evitar ‘’gold-plating’’
- Project Charter
- Técnica Delphi
- Restricciones / Supuestos
- Scope management plan

Gestión del Tiempo

- Diagrama de Gantt
- Diagrama de redes
- Interacción con el equipo
- Estimación de tiempos (expertos, historia, pert, etc)
- Ruta crítica



Gestión del Costo

- Presupuesto basado en :
  - Tiempos
  - Riesgos
  - Inf. histórica
  - Calendario
- Herramientas :
  - Estimación Analoga
  - Botton-up
  - Paramétrica (por mt2)

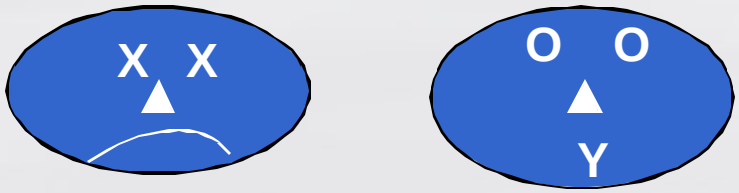
Gestión de Calidad

- El proyecto debe producir lo que se dijo que produciría y debe satisfacer necesidades reales.
- No es dar ‘’extras’’ al cliente
- ISO9000
- Kaizen
- CMMI
- 3 or Six Sigma
  - 1 sigma = 68.26%
  - 2 sigma = 95.46%
  - 3 sigma = 99.73%
  - 4 sigma = 99.99%

Gestion de Recursos Humanos

- Roles y responsabilidades
- ‘’Staffing’’
- Warroom
- Estilo de Liderazgo
- Manejo de conflictos (problem solving)
- Piramide de Maslow
- Teoría MacGregor o ‘’XY’’

equilibrio



Gestión de la Comunicación

- Plan de comunicación
- Que información y quien la debe recibir
- 90% del tiempo de un PMP
- Comunicación no verbal (55%)
- Escucha activa
- Retroalimentación (me estás oyendo inutil…)

Gestión del riesgo

- Quien controla a quien?? El proyecto o el PM
- Riesgos buenos y malos
- Probabilidad de que ocurran
- Impacto y Fechas
- Respuesta y Riesgos secundarios
- Tormenta de ideas, juntas seguimiento, delphi…etc
- Evitar, mitigar, aceptar, tranferir…
- Contingency plans Vs Workarouds

Gestión de Compras

- Contratos
- Hacer o comprar?
- Tipo de contrato
  - Tiempo y materiales
  - Precio fijo
- Orden de Compra (firma de una parte)

Gestión de la Integración

- Unir todas las piezas que forman el proyecto

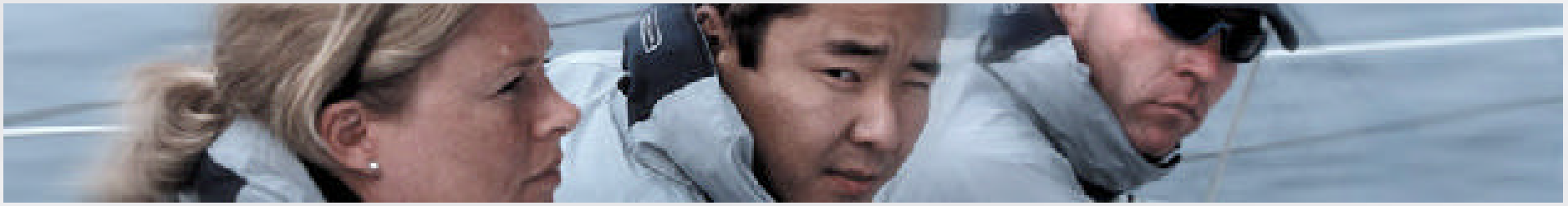
Futuro de los PMPs

- Puestos de Coordinación → PMPs

- T-Systems, AT&T, IBM, Bell South, Citibank,…etc

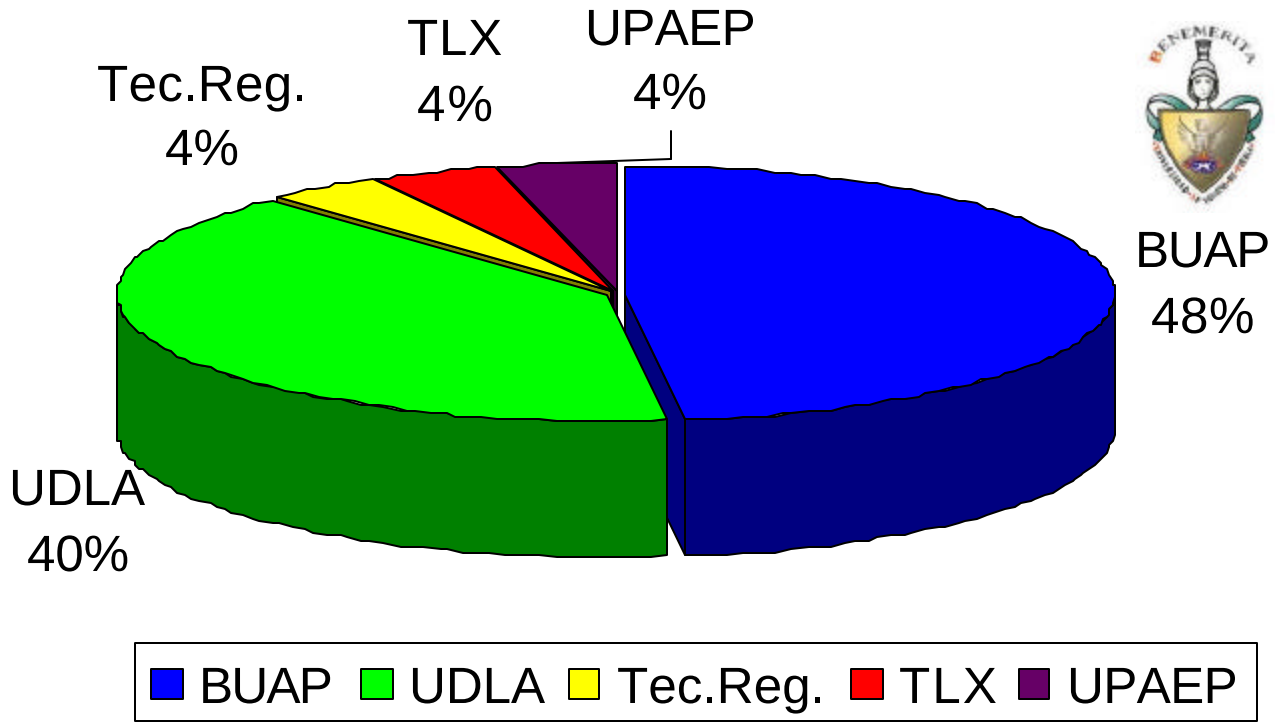
→ Solicitan que se certifiquen sus Líderes de Proyectos.

- Empresas globales exigen a proveedores que su LPs sean PMPs



En Puebla

- 30 PMPs / 22 en T-Systems



Recomendaciones

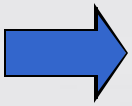
- **Autocapacitación**

- PMI (CAPM)
- CMMI
- ITIL
- Finanzas básicas
- Habilidades personales

- Inglés Fluido

Quieres ser PMP?

- Te gustaría tener responsabilidades con una limitada autoridad?
- Disfrutas trabajar con fechas límite imposibles, recursos limitados, con implacables patrocinadores ?
- Eres masoquista ?

Tu repuesta es Sí?  Eres candidato para PMP

Gracias por su atención !!!

José Manuel Rivera Hernandez, PMP
T-systems
ITO Projects
Tel.- 223-4605
jose.rivera@t-systems.com

Un Vistazo a la Minería de Datos

Christian A. Martínez
Instituto Tecnológico de Estudios Superiores de Monterrey Campus Puebla
pinkejo@acm.org

***Resumen*— El presente artículo muestra un análisis general de la minería de datos, haciendo una análisis desde sus inicios en la historia de la algoritmia, pasando por sus características básicas y llegando a las aplicaciones e importancia más actuales.**

***Palabras Clave*— Minería de datos, árboles de decisión, algoritmos, inteligencia artificial.**

I. Introducción

La minería de datos era un tema poco conocido tres décadas atrás, pero ahora ha tomado una importancia impresionante que está causando ruido dentro de las tecnologías de información, investigaciones de software y desarrollo de algoritmos, veamos porque.

II. ¿Qué es y cuáles son sus orígenes?

La minería de datos es una de las temáticas más importantes en nuestros días. Sin embargo, años atrás, pocas personas habían escuchado este término. La minería de datos es el resultado de una evolución con una larga historia, el término mismo se ha insertado desde los años 90 en el contexto de las tecnologías de información, algoritmia y desarrollo de software. Para los fines de este artículo presentemos una breve descripción de sus orígenes.

Las líneas de desarrollo en el ámbito de minería de datos tienen su origen en tres conceptos importantes. El mayor de ellos es la estadística. “Sin estadísticas, no existiría la minería de datos, pues son los fundamentos de la mayoría de las tecnologías que utilizan este concepto” [1]. La estadística clásica engloba conceptos como análisis de regresión, desviación estándar, varianza, análisis de clustering, intervalos de confianza, entre otros. Ciertamente, en las herramientas y técnicas utilizadas en minería de datos, el análisis de estadística clásica juega un rol sumamente importante.

La segunda línea de desarrollo de la minería de datos es la inteligencia artificial, mejor conocida como IA. Esta disciplina se encuentra basada en heurísticas, de forma opuesta a la estadística, pero debido a que su implementación necesitaba de computadoras con un poder de procesamiento alto, no fue práctica hasta los años 80’s, cuando las máquinas comenzaron a venderse más baratas con un procesamiento cada vez mayor.

La última familia que juega un papel en la historia de la minería de datos es el aprendizaje automático, que podemos describir como la unión de estadísticas e IA. Mientras la IA no era exitosamente comercial, sus técnicas fueron en gran importancia utilizadas para el aprendizaje automático. Su aplicación comenzó a jugar un papel importante en los 80’s y 90’s, tomando una ventaja significativa por su bajo costo a comparación de la IA. El aprendizaje automático puede considerarse parte de la evolución de la IA, porque conjunta heurísticas con análisis estadístico avanzado.

Con lo anterior podemos definir a la minería de datos como la unión de desarrollos históricos y recientes en estadística, IA y aprendizaje automático, pero concluyamos este punto con una definición más específica: “la minería de datos es un campo interdisciplinario que conjunta las técnicas de aprendizaje automático, reconocimiento de patrones, estadística, bases de datos y visualización, para dirigirla a la extracción e interpretación de bases de datos inmensas” [2].

III. ¿Para qué sirve?

Mostremos las tareas más importantes que usualmente la minería de datos debe completar.

A. Descripción

Muchas veces los investigadores y analistas buscan encontrar varios caminos para describir patrones y tendencias que se encuentran dentro de los datos. Los modelos de minería de datos deben ser lo más transparentes posibles. Esto es, los resultados deben describir patrones claros que son fáciles de intuir o interpretar.

Manuscrito presentado en Mayo 07, 2007, para la materia Bases de Datos Avanzadas (CB00826). Revisión por M.C. Carlos Proal Aguilar.

C.A. Martínez es Ingeniero en Tecnologías Computacionales con el plan ITC01 en curso 8vo. Semestre, Departamento de Tecnologías de Información del Instituto Tecnológico y de Estudios Superiores de Monterrey, Puebla, Pue., (e-mail:pinkejo@acm.org).

B. Estimación

Es similar a la clasificación a excepción de que está orientada a la funcionalidad numérica, en lugar de categórica. Los modelos se construyen utilizando registros completos que para nuevas observaciones, hacen una estimación basada en los valores de predicciones. Un ejemplo de estimación puede ser: "Estimar la calificación promedio de un estudiante graduado tomando como base la calificación promedio de estudiantes no graduados" [3].

C. Predicción

Es similar a la clasificación y estimación, con la diferencia de que en la predicción los resultados mienten a futuro. Cualquiera de los métodos usados para clasificación y estimación también puede utilizarse, bajo circunstancias apropiadas, en predicción. Ejemplo: "Predecir el incremento de porcentaje de muertes viales para el siguiente año si el límite de velocidad se incrementa" [3].

D. Clustering

Se refiere a la agrupación de registros, observaciones o casos en clases de objetos similares. Se diferencia de la clasificación en que no existe ninguna variable objetivo. La tarea de clustering no intenta clasificar, estimar o predecir el valor de una variable. En cambio, busca segmentar un juego de datos en segmentos relativamente homogéneos, donde la semejanza de registros dentro del grupo es maximizada y la semejanza de registros fuera del grupo es minimizada.

E. Asociación

Es el trabajo de búsqueda de atributos que "van juntos". La asociación procura descubrir reglas para cuantificar la relación entre dos o más atributos. Ejemplo: "Predicción de degradación en redes de telecomunicaciones" [3].

IV. ¿Cómo funciona?

Existe una gran variedad de algoritmos que a lo largo del desarrollo de la minería de datos se han implementado. A través de este conjunto de estrategias, la minería de datos puede solucionar problemas que se muestran en distintos ámbitos de negocios y la ingeniería de software. Mencionemos los más básicos:

A. Deducción de reglas rudimentarias

Conocida como "1R para 1-regla" [4], genera un árbol de decisión de un nivel como un conjunto de reglas que permiten tomar decisiones con respecto a un atributo específico.

B. Modelado estadístico

Esta técnica es parecida a la anterior, con la diferencia que utiliza todos los atributos para poder tomar decisiones.

C. Divide y vencerás

Utilizado para la construcción de árboles de decisión de manera recursiva. La única característica a decidir, es cómo determinar qué atributo se tomará como referencia para las decisiones, brindando un conjunto de ejemplos con diferentes clases.

D. Algoritmos covering

Es un método alterno al divide y vencerás, tomando cada clase en su turno y englobando todos los casos en ella, excluyendo al mismo tiempo las instancias que no se encuentran en la clase. De acuerdo a la descripción de este algoritmo, puedo inferir que funciona como algoritmo avaro en el que cada iteración toma la mejor decisión sin tomar en cuenta lo demás, caso contrario a la programación dinámica.

E. Clustering

Utilizado cuando no existe una clase que deba predecirse pero las instancias deben dividirse en grupos naturales.

V. ¿Quién lo utiliza?

Existen múltiples campos de aplicación, pero los negocios abarcan una parte importante de su funcionamiento para la resolución de una gran variedad de problemas entre los que se encuentran:

1) *Mejoras de procesos.*
2) *Comportamiento de los clientes potenciales.*
3) *Predicciones de ventas.*
4) *Prevención de estafas económicas.*
5) *Mercadotecnia y e-commerce.*

Como prueba de ello, hagamos referencia al taller KDD-2006 [6] en el que se tratan temáticas de minería de datos como componente de los procesos de negocio y la integración de tecnologías de minería de datos con otras tecnologías ya existentes en las corporaciones.

VI. ¿Dónde se implementa?

Existe una gran variedad de herramientas que el hombre ha desarrollado aplicando minería de datos: PolyAnalyst [7], que incorpora los retos más recientes en aprendizaje automático para el análisis de datos estructurados y no estructurados; Client Shepherd, para toma de decisiones inducidas por el cambio constante del ambiente empresarial, causando la migración de un producto o compañía a otros, con la implementación de patrones de migración; WEKA 3 [8], colección de algoritmos de aprendizaje automático para tareas de minería de datos, software desarrollado en java para aplicarse directamente a un conjunto de datos o llamarlo desde una aplicación propia desarrollada en el mismo lenguaje.

VII. Conclusión

Como hemos visto a lo largo de esta investigación, la minería de datos es una temática muy importante en cuanto a algoritmia y desarrollo de software se refiere. Muchos pensaron que jamás llegaría la época en la que existieran ordenadores poderosos que permitieran avanzar las investigaciones en el campo. Sin embargo,

como hemos visto, actualmente es un tema que cualquier persona relacionada con las tecnologías de información conoce. Es bien sabido que conforme pasa el tiempo, la tecnología se desarrolla cada vez más y logramos ver económicamente que cada vez una persona paga menos por más memoria, espacio o ancho de banda. Puedo aportar a este artículo que las empresas que se crean en la actualidad y no poseen tecnología avanzada, jamás van a lograr permanecer exitosamente en el mercado, pues con el desarrollo de software y aplicaciones que implementan inteligencia artificial, estadística y aprendizaje automático, la mano de obra humana es cada vez menos necesaria, pues los sistemas computacionales se tornan a sistemas expertos y las máquinas comienzan a realizar tareas de una forma más rápida e inteligente que el hombre.

No puedo decir que llegará el momento en que la fuerza humana pueda llegar a sustituirse por un robot o por la inteligencia de una máquina, pero lo que si puedo concluir es que los modelos de negocios, trabajo y desempeño laboral seguramente deberán adaptarse y cambiar el paradigma de manera que beneficien a las empresas y el hombre se acople a estos nuevos esquemas tecnológicos. ¿Pero hasta cuándo?

REFERENCIAS

[1] A Brief History Of Data Mining. Data mining software. <http://www.data-mining-software.com/data_mining_history.htm>

[2] Peter C., Pablo H., Rolf S., Jaap V., Alessandro Z. Discovering Data Mining: From Concept to Implementation. Upper Saddle River, NJ 1998, Prentice Hall.

[3] Daniel L.Discovering Knowledge in Data, an Introduction to DATA MINING. Hoboken, NJ 2005, Wiley-Interscience.

[4] Ian W., Eibe F. Data Mining, Practical Machine Learning Tools and Techniques. San Francisco, CA 2005, Elsevier.

[5] Shirish T., Srinivasan P., Tahsin K. TRIPS and TIDES: new algorithms for tree mining. Source Conference on Information and Knowledge Management archive 2006. Arlington, Virginia, USA 2006., Proceedings of the 15th ACM international conference on Information and knowledge management.

[6] Rayid G., Carlos S. Data mining for business applications: KDD-2006 workshop. New York, NY, USA 2006., Source ACM SIGKDD Explorations Newsletter archive.

[7] MEGAPUTER. <http://www.megaputer.com/>.

[8] WEKA The University of Waikato<http://www.cs.waikato.ac.nz/ml/weka/>.

Redes Neuronales Wavelet para Eliminar Ruido en Espectros Estelares.

Hugo Adrián García Elías, José Federico Ramírez Cruz
Instituto Tecnológico de Apizaco, Avenida Instituto Tecnológico S/N 90300
Apizaco, Tlaxcala, A. P. 19, México
hugoage@gmail.com, framirez@itapizaco.edu.mx

***Resumen*- La extracción de características y el análisis de espectros estelares es una tarea muy común en la comunidad astronómica, la cual en ocasiones se ve afectada por la presencia de ruido en los espectros estelares analizados, en este proyecto se propone un método para la eliminación de Ruido en Espectros estelares basado en Redes Neuronales Wavelet, en el cual se realizaron experimentos alterando el espectro de una estrella es decir agregando ruido al espectro y tomarlo como entrada para la Red Neuronal Wavelet donde se procesa y se compara la salida obtenida contra el espectro sin ruido, y los resultados obtenidos fueron satisfactorios.**

***Palabras Clave*- Espectros estelares, Redes Neuronales Wavelet, Ruido.**

I. INTRODUCCION

Las señales, durante su transmisión, siempre se encuentran bajo la influencia de otras señales no deseadas. Incluso, cualquier procesamiento que se realice a una señal tiende a introducir perturbaciones desagradables en ella misma. A estas perturbaciones que contaminan la señal transmitida o procesada se le llama ruido, y constituye una señal molesta que no guarda relación alguna con la útil.

Los espectros estelares contienen gran cantidad de información, la cual es importante para la comunidad astronómica, mediante el análisis de un espectro estelar se pueden conocer sus características. Existe la presencia de algunos factores como la temperatura atmosférica de la tierra, anomalías en el instrumento utilizado para adquirir el espectro, corrimientos al rojo, o al azul en los cuerpos estelares y otros factores que provocan ruido en el espectro estelar.

El espectro de una estrella se obtiene cuando descomponemos la luz que emite en los colores que la componen, haciéndola pasar por un elemento dispersor. Los espectros como sus huellas dactilares, comparándolos con los espectros conocidos podemos determinar su composición, el espectro de las estrellas es de origen térmico y, en la mayoría de ellas, está constituido por un fondo brillante, el continuo, cuya intensidad de radiación varía con la longitud de onda, que puede aproximarse inicialmente con la que seguiría un cuerpo negro de la misma temperatura efectiva que la estrella. Sobre el continuo se superponen líneas de absorción (oscuras) y, excepcionalmente, líneas de emisión (brillantes), como se muestra en la Figura I.1, que son emitidas por los elementos y compuestos químicos que constituyen la materia emisora, es decir, la atmósfera estelar.

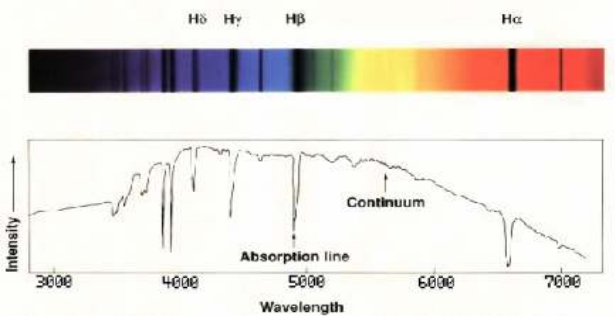


Figura I.1. Espectro Estelar.

En la Figura I.1 se muestra que un espectro estelar esta compuesto de valores de intensidad luminosa en diferentes longitudes de onda, los valores bajos de intensidad son llamados líneas de absorción y los

valores que se mantienen en una proporción constante de aparición son llamados espectro continuo.

En el presente trabajo se propone un método computacional que involucra técnicas de computación suave para detectar y eliminar el ruido presente en los espectros estelares, y así poder obtener mejores resultados al analizarlos, dichas técnicas son, las redes neuronales y la teoría de ondeletas o wavelets, aplicadas con gran éxito en el procesamiento de señales y la disminución del ruido presente en la señal procesada.

Las redes neuronales artificiales son modelos computacionales que tratan de emular de manera simplificada, el complejo funcionamiento del cerebro humano. Su capacidad de aprendizaje a través de ensayos repetidos, las ha hecho muy populares en una amplia variedad de aplicaciones en todas las ciencias.

La teoría de wavelets es una rama de las matemáticas cuyo estudio se centra en la construcción de un modelo para sistemas o procesos utilizando un tipo especial de señales conocidas como wavelets.

Las Redes Neuronales Wavelet son una nueva clase poderosa de redes neuronales que incorporan las más importantes ventajas del análisis multiresolusión introducidas por Mallat en 1989 [1]. Zhang y Benveniste en 1992 [2], encontraron una relación entre la Teoría de descomposición Wavelet y las Redes Neuronales.

Existen trabajos que utilizan técnicas computacionales para procesar espectros estelares, como en [3] donde proponen un algoritmo Hibrido para análisis espectral que combina estrategias evolutivas y algoritmos de optimización para ajustar líneas espectrales, en [4], se propone un algoritmo para eliminar ruido en conjuntos de datos para aprendizaje maquina aplicado a la eliminación de ruido en espectros estelares, es considerable la bibliografía sobre Redes Neuronales Wavelet las cuales son utilizadas para predecir y aproximar señales. En [5] se propone un método para el aprendizaje y aproximación de series de tiempo caóticas utilizando Redes Neuronales Wavelet. En [6] se propone un método para diagnosticar fallas en circuitos electrónicos utilizando Redes Neuronales Wavelet. En [7] se aplica un método con basado en Redes Neuronales Wavelet para eliminar ruido en imágenes, para visión por computadora. En [8] se propone un método para filtrado de datos usando el filtro de Kalman. En [10] proponen Redes Neuronales Wavelet con técnicas de aprendizaje hibrido.

II. DESARROLLO

En este proyecto se implementó una Red Neuronal Wavelet para eliminar el ruido presente en espectros estelares. Las Redes Neuronales Wavelet fueron propuestas por Zhang y Benveniste [2] en 1992 como una alternativa a las redes neuronales artificiales de tipo feed-forward utilizadas para aproximar funciones no lineales arbitrarias. Para esto se basaron en la teoría de la transformada wavelet.

Inicialmente se toma un espectro estelar sin ruido en seguida le agregamos ruido a dicho espectro y lo tomamos como entrada a la Red Neurona Wavelet, se procesa y la salida de la Red Neuronal Wavelet a continuación es comparada contra el espectro sin ruido.

A. Estructura de la Red Neuronal Wavelet

La arquitectura de la red neuronal Wavelet en este proyecto se diseño como estructura de tres capas, una capa de entrada, una capa oculta y una capa de salida, cada capa puede contener uno o mas nodos, en la Figura II.1 se muestra un diagrama esquemático de las Redes Neuronales Wavelet de tres capas.

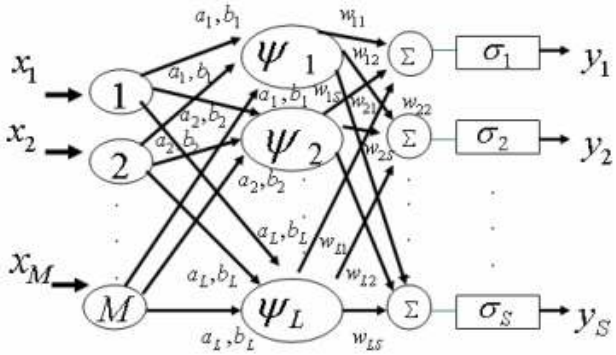


Figura II.1. Red Neuronal Wavelet

Como se ilustra en la Figura II.1, el vector que almacena el espectro con ruido se conecta con los

nodos de entrada de la red. Las funciones de activación de los nodos Wavelet en la capa oculta se derivan de una Wavelet Madre $\psi(x)$. La función wavelet Morlet se selecciono como Wavelet madre en esta red y se define en (1):

$$\psi(x) = \cos(1.75x)e^{-(1/2)x^2} \quad (1)$$

La función Wavelet Morlet se vuelve la función de activación con escala a_l y traslación b_l, Por consiguiente, la función de activación del l nodo wavelet $l = 1,2...,L$ se calcula con (2):

$$\psi_{a_l,b_l}(x) = a_l^{-1/2}\cos(1.75(\frac{x-b_l}{a_l}))e^{-1/2(\frac{x-b_l}{a_l})^2} \quad (2)$$

Entonces, la salida del l nodo wavelet con m variables de entrada $x_i, i = 1,2,...,M$, se calcula con (3):

$$\psi_l(x) = \sum_{i=1}^{M}\psi_{a_l,b_l}(x_i) \quad (3)$$

Cada salida de los nodos Wavelet en la capa oculta se multiplica por un valor de peso apropiado determinado por la capa oculta.

En la figura 2 los pesos w_{ls} que conectan el nodo Wavelet l con el nodo de salida s están indicados por el vector de pesos $w_l = [w_{l1},...w_{ls},...,w_{lS}]$ para $l = 1,2...,L$ y $s = 1,2...,S$ y S es el numero total de nodos de salida.

La función sigmoide es seleccionada como la función de activación σ de los nodos de salida en la capa de salida. Y el valor final calculado como valor del nodo de salida es calculado con (4):

$$y_s(x) = \sigma(\sum_{l=1}^{L} w_{ls}\psi_l(x)) \quad (4)$$

Notablemente, la salida $y_s(x)$ en (4) contiene, implícitamente, los parámetros de ajuste de la red: los pesos de conexión (w_{ls}) y los parámetros de escala (a_l) y traslación (b_l) en cada nodo Wavelet. Los parámetros de escala pueden ser calculados con (5):

$$a_l = 2^{-l} \quad (5)$$

Y los parámetros de traslación pueden ser calculados con (6):

$$b_l = x_i a \quad (6)$$

Los pesos w_{ls} se pueden actualizar con (7):

$$w_{ls}(k+1) = w_{ls}(k) + \Delta w_{ls}(k) + \delta_w[w_{ls}(k) - w_{ls}(k-1)] \quad (7)$$

$$\Delta w_{ls} = \xi\frac{\partial e}{\partial w_{ls}} \quad (8)$$

Donde ξ es la tasa de aprendizaje y δ_w es el factor de momento correspondiente.

El error en los nodos de la capa de salida puede ser calculado con (9):

$$e = y(s) - y^d(s) \quad (9)$$

Y

$$E = \frac{1}{2}e^2 \quad (10)$$

Donde $y^d(s)$ es la salida deseada, y $y(s)$ es la salida obtenida y E es el error cuadrático en la salida.

B. Método experimental para eliminar ruido en espectros estelares.

El método propuesto consiste en alterar el conjunto de datos correspondiente al espectro estelar agregando ruido y compararlo con el conjunto de datos que no contienen ruido.

En este proyecto el objetivo principal es filtrar los datos ruidosos y evaluar los datos filtrados. Se agrego el ruido artificial al azar a todo el espectro

estelar, por conveniencia se normalizo el espectro, para que los datos de las entradas y salidas deseadas tuvieran media cero y sus desviaciones estándar fueran iguales a 1. La manera de agregar ruido es generado a cada uno de los valores que componen el espectro estelar un valor de ruido aleatorio, y por consiguiente todos los datos son afectados con ruido. En la Figura II.2 se muestran tanto el espectro original (arriba) y el espectro afectado con el ruido (abajo).

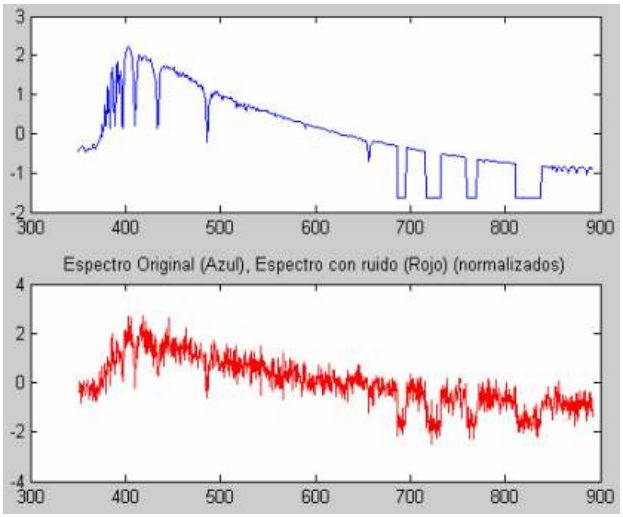


Figura II.2. Espectro Original (Arriba), Espectro afectado con ruido (Abajo)

Como se observa en la Figura II.2 existe una diferencia notable entre ambos casos, el espectro con ruido difiere considerablemente del espectro original.
El siguiente paso en el método propuesto es tomar como entradas a la Red Neuronal Wavelet el conjunto de datos correspondiente al espectro estelar con ruido y procesarlos en ella, en los experimentos realizados con la Red Neuronal Wavelet se obtuvieron resultados satisfactorios con el tipo de ruido agregado.

III. RESULTADOS

Los resultados mostraron la efectividad del empleo de las Redes Neuronales Wavelet en tareas de procesamiento de señales, específicamente en la cancelación de ruido. Más a detalle, fue posible constatar cómo la salida obtenida por la Red Neuronal Wavelet es prácticamente la misma que la Salida deseada es decir el espectro estelar sin ruido, con valores de error mínimos.
Los resultados obtenidos por la Red Neuronal Wavelet se muestran en la Figura III.1.

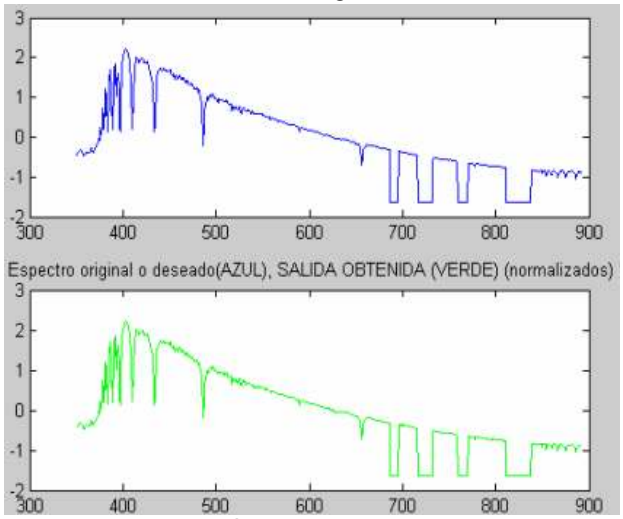


Figura III.1. Espectro Original o deseado (Arriba), Espectro Obtenido por la Red Neuronal Wavelet (Abajo)

En la figura III.1, se observa el espectro original (arriba) y el espectro obtenido por la Red Neuronal Wavelet como salida (abajo), se observa también que ambos espectros son en apariencia el mismo.
Se realizaron otros experimentos donde la entrada a la Red Neuronal Wavelet era un espectro diferente al de la estrella que se deseaba obtener como salida en considerando a el espectro de entrada como espectro con ruido, los resultados obtenidos en estos experimentos fueron satisfactorios, los valores de error fueron mínimos, y los espectros obtenidos fueron prácticamente los mismos que los espectros originales ó deseados, comprobando la capacidad de las Redes Neuronales Wavelet como aproximadores universales.
A manera de ejemplo, se muestra a continuación una tabla (Tabla III.1.) donde se aprecian algunos resultados obtenidos durante el trabajo (operación) con diferentes configuraciones de la Red Neuronal Wavelet (diferente numero de Nodos Wavelet en la Capa Oculta), y los valores del error total obtenidos en los diferentes experimentos

Tabla III.1 Tabla de Valores error y configuración de Nodos Wavelet con diferentes tipos de estrellas.

Estrella	Numero de Nodos Wavelet	Error
A8V	8	0.0154
A8V	15	0.0072
Jo_4000_BD+11_2998	6	0.0338
Jo_4000_BD+11_2998	12	0.0291
Jo_4000_G197-45	12	0.0889
Jo_4000_G197-45	15	0.0866
Jo_4000_BD+18_2890	8	0.0702
Jo_4000_BD+18_2890	15	0.0020
Jo_4000_BD+26_3578	6	0.0665
Jo_4000_BD+26_3578	10	0.0350
Jo_4000_BD+09_3223	4	0.0241
Jo_4000_BD+09_3223	6	0.0227

Como se puede observar en la Tabla 1 a mayor número de nodos Wavelet en la capa oculta disminuye el error de salida.

IV. CONCLUSIONES

En este artículo se presento un método de eliminación de ruido en espectros estelares Mediante Redes Neuronales Wavelet, donde se filtran los datos ruidosos y son comparados contra datos que no contienen ruido. El método fue probado con diferentes espectros estelares y los experimentos prueban que el ruido se elimina de los datos, obteniendo valores de error mínimos. Probando la capacidad de las Redes Neuronales Wavelet como aproximadores universales, es un método que no necesita tiempo elevado de procesamiento ya que las Redes Neuronales Wavelet, no son procedimientos iterativos que requieran cierto numero de iteraciones y no consumen demasiado tiempo de ejecución su aprendizaje consiste únicamente en la adición de neuronas wavelets para aumentar el grado de eliminación de ruido en el espectro.

RECONOCIMIENTOS

Agradezco al Instituto Tecnológico de Apizaco por las facilidades otorgadas para la realización de este proyecto, a la Dirección General de Educación Superior Tecnológica y a COSNET por la Beca Otorgada para el proyecto denominado: “Detección de Ruido En espectros Estelares Mediante Redes Neuronales y Ondeletas”. Clave: 042005065.

REFERENCIAS

[1] S. G. Mallat, "A theory for Multiresolution Signal Decomposition: The Wavelet Representation", IEEE Transactions on Pattern Analysis and Machine Intelligence. Vol II. No 7. July 1989

[2] Q. Zhang, and A. Benveniste, "Wavelet Networks", IEEE Transactions on Neural Networks. Vol 3. No 6. July 1992.

[3] Ramirez. J. Federico and Fuentes Olac. “A Hybrid algorithm for spectral analysis” experimental astronomy, 2003. Kluwer academic publishers. Printed in the Netherlands.

[4] Escalante, H. Jair. And Fuentes Olac (2004), “Noise Elimination with a Re-Sampling Algorithm” Workshop on Machine Learning for Scientific Data Analysis, pp. 307-316, Copyright Iberamia 2004.

[5] V. Alarcón-Aquino, E. S. García-Treviño, R. Rosas-Romero, J.F. Ramírez-Cruz, (2005) "Learning and Approximation of Chaotic Time Series Usign Wavelet Networks". Proceedings of the Sixth Mexican International Conference on Computer Science (ENC’05), México 2005

[6] Luo Zhi Yong and Shi Zhong Ke “Wavelet Neural Network Method For Fault Diagnosis Of Push-Pull Circuits**”.** Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, China 18-21 August 2005.

[7] Jian Nian Cai and Yang Cheng Jie. “ Applying a Wavelet Neural Network to Impulse Noise Removal”. Proceedings of The 2005 IEEE International Conference on Neural Networks and Brain ICNN&B'05 Hardware andApplications.

[8] Lin Cheng Jian. “Wavelet Neural Networks with a Hybrid Learning Approach”. Proceedings of the Journal Of Information Science And Engineering 22, 1367-1387 (2006).

[9] Kim, Kyoung Joo. Park, Jin Bae and Choi, Yoon Ho. “The Adaptive Learning Rates of Extended Kalman Filter Based Training Algorithm for Wavelet Neural Networks”. Proceedings of the Fifth Mexican International Conference on Artificial Intelligence 2006 (MICAI 06).

[10] E. S. García Treviño, V. Alarcón Aquino. “Chaotic Time Series Approximation Using Iterative Wavelet-Networks” Proceedings of the 16th IEEE International Conference on Electronics, Communications and Computers (CONIELECOMP 2006).

[11] Dian-chun Zheng , Chun-xi Zhang, Guo-qing Yang , Xue-yong Sun. “An Experiment Study of Partial Discharge Pattern Recognition Method Based on Wavelet Neural Networks”. Proceedings of the Conference Record of the 2006 IEEE International Symposium on Electrical Insulation.

[12] Wu, Shaoxiong. and Wu, Biying. “Wavelet Neural Network - based Control Chart Patterns Recognition” Proceedings of the 6th World Congress on Intelligent Control and Automation, June 21 - 23, 2006, Dalian, China.

[13] Xu, Jian-Xin and Tan, Ying “Nonlinear Adaptive Wavelet Control Using Constructive Wavelet Networks” Proceedings of IEEE Transactions On Neural Networks, Vol. 18, No. 1, January 2007.

Métodos de Reducción de Dimensionalidad y Ensamble de Clasificadores para la Clasificación Morfológica de Galaxias

Oscar Flores Conde [1], Hugo Adrián García Elías [1] y Tomás Morales Acoltzi [2]
[1] División de Estudios de Prograd o e Investigación, Instituto Tecnológico de Apizaco,
Av. Instituto Tecnológico de Apizaco S/N, 90300 Apizaco, México
[2] Centro de Ciencias de la Atmósfera, Universidad Nacional Autónoma de México,
Circuito Exterior S/N 04510, Ciudad Universitaria, Del. Coyoacán, México D.F.
oscar202@itapizaco.edu.mx, hugoage@gmail.com, acoltzi@atmosfera.unam.mx

Resumen: Uno de los problemas principales de la comunidad astronómica es la clasificación de objetos estelares. Cuando el número de características es grande, las técnicas de procesamiento se vuelven lentas y en ocasiones intratables, por tal motivo, existe la necesidad de utilizar técnicas que reduzcan la dimensión de los datos. En este trabajo se emplea Análisis de Componentes Principales, Análisis de Componentes Independientes y Análisis de Componentes Curvilíneos para tal motivo. Para el proceso de clasificación, se emplean ensambles de clasificadores que son más eficientes que sus componentes individuales en combinación de datos reducidos, logrando mejores clasificaciones que con una sola fuente de información. Además, se introduce una forma sistemática, automática y objetiva para obtener un conjunto de datos invariante a la escala, posición y orientación.

Palabras Clave: Clasificación de galaxias, PCA, ICA, CCA, ensamble de clasificadores

I. INTRODUCCIÓN

Uno de los problemas principales de la comunidad astronómica es la clasificación de objetos estelares, esta se hace de manera manual tomando del objeto información visual y de acuerdo al esquema de clasificación se realiza una inspección para encontrar el parecido a las características generales de alguna de las clases de galaxias. Se han realizado diversas investigaciones en torno al tema, debido a que no hay un sistema que pueda dar a ciencia cierta una clasificación de estos objetos estelares por su composición y posición en el universo, aunado a esto, los telescopios aún no cuentan con los alcances visuales suficientes para obtener más información que pueda describir de una manera más certera las características de los objetos. Los métodos de clasificación utilizados frecuentemente se realizan con distintas técnicas comparando los resultados de unos con otros. Cuando el número de características es grande, las técnicas de procesamiento se vuelven lentas y en ocasiones intratables, por tal motivo, existe la necesidad de utilizar técnicas que reduzcan la dimensión de los datos. Una de las técnicas de reducción de dimensionalidad más utilizadas es el uso del Análisis de Componentes Principales para obtener representaciones más compactas de la información.

El método propuesto se basa en la aplicación de ensamble de clasificadores utilizando las distintas representaciones dadas por las técnicas de reducción de dimensionalidad como lo es el Análisis de Componentes Principales (PCA), el Análisis de Componentes Independientes (ICA) y el Análisis de Componentes Curvilíneos (CCA).

Esta metodología funciona en dos aspectos; primero, la reducción de datos permite trabajar con

representaciones más compactas y así reducir la carga computacional que se requiere al procesar grandes cantidades de información, ya que al trabajar con información común o redundante en todo el conjunto de datos se esta desperdiciando tiempo de cómputo; segundo, al realizar un ensamble de clasificadores, se trabaja con métodos que mejoran la salida de clasificación de los algoritmos de forma individual. Al combinar estas técnicas, se obtienen tiempos de computo más cortos que si se procesa el conjunto de datos original sin reducción alguna. Storrie-Lombardi [1] et al. Propusieron una red neuronal "Feedforward" para clasificar las galaxias en 5 clases: E, S0, Sa+Sb, Sc+Sd, e irregulares, la configuración de la red neuronal fué de 13 neuronas en la capa de entrada, 13 en la capa oculta y 5 neuronas en la capa de salida, utilizando 5217 galaxias, las cuales fueron agrupadas aleatoriamente en dos grupos: uno de entrenamiento y uno de prueba; el conjunto de entrenamiento contenía 1700 imágenes y el conjunto de prueba 3517 imágenes.

Los resultados obtenidos por ellos fue de un 64% de exactitud en la clasificación. Owens [2] utilizó árboles de decisión oblicua para la clasificación. Repitió el experimento realizado por Storrie-Lomabrdi [1] et al., usando los mismos datos y características obteniendo un porcentaje entre el 63% y 64% de exactitud. Bazell y Aha [3] usaron ensambles de clasificadores para clasificar 800 galaxias. Usaron el clasificador Naive Bayes [4], una red neuronal y un algoritmo de inducción por árboles de decisión con poda. Consideraron de 2 a 6 clases, y 14 características para realizar la clasificación. Considerando 3 clases, reportaron que el ensamble de J48 produjo el mejor resultado con un 78.55% de exactitud en el caso de 5 clases. Odewahn [5], presenta un enfoque de clasificación de galaxias basada en reconstrucción de Fourier de imágenes de galaxias usando redes neuronales para entrenar los clasificadores que reconocían barras morfológicas de un 80% a un 90% y que identificaba los tipos de Hubble. Godeyra [6] y Lolling [6] usaron dos tipos automáticos de clasificadores de galaxias, el primero utilizó características de la forma geométrica como base de la clasificación, y el segundo uso los pixeles de la imagen directamente y redes neuronales para hacer la clasificación. La imagen directa basada en el clasificador neuronal aprendió un 97% de 171 patrones de entrenamiento presentados. Cuando a la red se le presentó un conjunto de entrenamiento de 37 patrones independientes, fue capaz de clasificar el 57% de los casos. Jorge de la Calleja y Olac Fuentes [9], proponen para la clasificación de galaxias la utilización de 3 algoritmos de aprendizaje máquina, así como imágenes que son independientes a la escala y orientación, y la aplicación de análisis de componentes principales (PCA), generando así una representación más compacta y manejable, para, finalmente, clasificar las imágenes por medio de los de algoritmos de aprendizaje máquina; además de realizar experimentos con otros algoritmos de aprendizaje como: Clasificador Naive Bayes [4], el Algoritmo de Inducción de la regla C4.5 [4] y el predictor Random Forest(RF) [10], realizan un ensamble de los clasificadores anteriores. En trabajos previos a éste, utilizaron regresión "locally-weighted" y redes neuronales para optimizar la clasificación.

Clasificación de Galaxias según Edwin Hubble

La forma más sencilla de clasificar las galaxias es por la observación de la forma que tienen. A principios de los años 20, Edwin Hubble y sus colaboradores habían acumulado un número considerable de fotografías de buena calidad de las nebulosas extragalácticas. A pesar de la variedad de formas se notaba cierta secuencia en la morfología de los objetos. Es entonces cuando Hubble propuso su ya famoso esquema de clasificación, dentro del cual caen la mayoría de las galaxias conocidas. Hubble aclaró que su clasificación no era más que un esquema empírico y que no implicaba una sucesión evolutiva; pero ante tan sugestiva progresión de las características morfológicas era tentador adscribirle un sentido evolutivo. Algunos propusieron que las galaxias se originaban como galaxias elípticas y evolucionaban a galaxias irregulares. El por qué existen diferentes tipos de galaxias ha sido un problema central de la astronomía. Algunos astrónomos proponen que el medio ambiente puede afectar la historia evolutiva de una galaxia. Otros atribuyen la evolución a choques o "fusiones" entre galaxias o bien a mecanismos un tanto cataclísmicos, posteriormente se han propuesto clasificaciones más finas que la de Hubble, como por ejemplo, la realizada por Vaucouleurs, las cuales, no son necesarias si la clasificación es solamente descriptiva

y no tiene una base teórica. El esquema de clasificación de Hubble comprende tres tipos principales de galaxias: espirales, elípticas e irregulares.

II. DESARROLLO

Estandarización de Imágenes de Galaxias

Debido a que las imágenes contienen ruido, tal como, objetos distantes (estrellas, nubes de gas, etc.), condiciones físicas de los instrumentos de captura (telescopios), condiciones de luz por objetos cercanos que intervinieron al momento de realizar las capturas, se toman solo los objetos de interés, aunado a esto, los objetos no se encuentran en el centro de la imagen, por lo que el banco de datos tiene que hacerse invariante a la posición, a la orientación y a la escala.

Este proceso se realiza de una forma automática, a través del siguiente método:

1. Se busca un umbral óptimo; para ello se recurre al método del umbral de Otsu [11], esto se hace para encontrar todas las regiones de la imagen.

2. Con la imagen umbralizada, se detectan todas las regiones que tienen valores de 255 (blanco) y se etiquetan, también se determina la región que ocupa cada objeto.

3. Una vez etiquetadas todas las regiones, se toma la que ocupa mayor área, que es el objetos de interés, así como la orientación que tiene ese objeto y el área que el objeto ocupa.

4. Se rota toda la imagen de acuerdo a la orientación del objeto de mayor área.

5. Se toma el área ocupada por el objeto de interés y se escala a 128x128 píxeles, para así estandarizar todas las imágenes.

Clasificación sin reducción de dimensión

Esta clasificación se realiza sin reducción de dimensionalidad para obtener porcentajes de clasificación y en base a ello, comprobar la eficiencia de los resultados obtenidos con los datos reducidos. Los experimentos se realizan con validación cruzada y ensamble de clasificadores con validación cruzada.

Cabe mencionar se utiliza el algoritmo de clasificación con 10 estados iniciales aleatorios, por lo que los ensambles constan de 10 clasificadores, y una vez que se obtienen las clases, se realiza validación cruzada.

III. RESULTADOS

A. Clasificación y Validación Cruzada.

La validación cruzada es un método de estimación predictiva de error, la cual separa el conjunto de datos en k grupos de igual tamaño (típicamente 10 grupos). k modelos predictivos son construidos, cada uno probado sobre un distinto grupo después de haber sido entrenado sobre los restantes grupos; este proceso puede ser repetido varias veces para incrementar la confiabilidad de la estimación. Los resultados de haber aplicado validación cruzada se muestran en la tabla III.1.

Tabla III.1: Resultados obtenidos con validación cruzada

Grupos	ADTree	J48	Naive Bayes	Random Forest
5	0.6522%	60.8696%	65.2174%	75% .
7	72.8261%	77.1739%	66.3043%	79.3478%.
10	76.087%	66.3043%	65.2174%	76.087% .

La mayoría de algoritmos dan resultados entre el 60% y 79 %, por lo que éstos deben mejorar con una reducción de dimensión ya que sólo se tomará la información más importante, eliminando así, información que no contribuye de manera significativa.

B. Clasificación con Ensamble de Clasificadores.

Para ver la eficiencia de los ensambles de clasificadores, se utilizan los clasificadores antes empleados con el método de “bagging”. Los resultados obtenidos son los mostrados en la tabla III.2.

Tabla III.2: Resultados obtenidos utilizando un Ensamble de Clasificadores.

Grupos	ADTree	J48	Naive Bayes	Random Forest	
5	72.8261%	69.5652%	69.5652%	76.087%	.
7	77.1734%	77.1739%	65.2174%	78.2609%	.
10	73.913%	70.6522%	63.0435%	76.087%	.

Los resultados de aplicar a los algoritmos de clasificación el método de "bagging" es que se obtienen mejores resultados de clasificación sólo en algunos casos, por lo que al comparar estos resultados con la salida de clasificación de la tabla III.1, se observa un incremento en la eficiencia de los mismos en los casos señalados.

C. Clasificación con datos obtenidos PCA.

Una vez obtenido el archivo de pruebas, se procede a realizar el proceso de reducción por PCA a los datos y clasificarlos, obteniendo los resultados mostrados en la tabla III.3.

Tabla III.3: Resultados obtenidos utilizando validación cruzada basada en PCA.

Grupos	ADTree	J48	Naive Bayes	Random Forest	
5	51.2195%	58.5366%	85.3659%	60.9756%	.
7	46.3415%	60.9756%	87.8049%	63.4146%	.
10	51.2195%	53.6585%	87.8049%	56.0976%	.

Con respecto a los resultados mostrados en la tabla III.1, los obtenidos con PCA son inferiores en un 20% aproximadamente, a excepción del algoritmo Naive Bayes que mejora los resultados en un 21% aproximadamente, por lo que este método de reducción no mejora significativamente, en los demás casos, la clasificación, sin embargo, se espera que los resultados de la tabla III.3 se mejoren con ensamble de clasificadores y el método de "bagging".

D. Clasificación con datos obtenidos de PCA y Ensamble de Clasificadores.

El conjunto de datos reducidos por medio del análisis de componentes principales utilizado en el experimento anterior, es utilizado con los algoritmos de clasificación, haciendo uso de ensamble de clasificadores con el método de "bagging", además de utilizar validación cruzada, esperando que los resultados mostrados en la tabla III.3 se mejoren, obteniendo así un mejor porcentaje de clasificación. los resultados obtenidos son mostrados en la tabla III.4.

Tabla III.4: Resultados obtenidos utilizando validación cruzada basada en PCA y Ensamble de Clasificadores.

Grupos	ADTree	J48	Naive Bayes	Random Forest	
5	63.4146%	58.5366%	80.4878%	65.8537%	.
7	56.0976%	53.6585%	82.9268%	65.8537%	.
10	58.5366%	60.9756%	85.3659%	63.4146%	.

De acuerdo a los resultados obtenidos, se observa que la aplicación de ensamble produjo una mejora en algunos de los resultados de clasificación con respecto los mostrados en la tabla III.3; también se puede observar que hubo un decremento en los resultados obtenidos por el algoritmo Naive Bayes, pero al comparar los resultados obtenidos por este algoritmo con los mostrados en la tabla III.2, estos mejoraron, así, con respecto a los demás resultados de la tabla III.2, no se nota una mejora en la clasificación.

E. Clasificación con datos obtenidos de ICA y Validación Cruzada.

La reducción de datos se realiza por medio de Análisis de Componentes Independientes, obteniendo los resultados que se muestran en la tabla III.5.

Tabla III.5: Resultados obtenidos utilizando validación cruzada basada en ICA.

Grupos	ADTree	J48	Naive Bayes	Random Forest	
5	46.5116%	45.3488%	46.5116%	52.3256%	.
7	47.6744%	45.3488%	40.6977%	45.3488%	.
10	50%	45.3488%	46.5116%	50%	.

Se puede observar que todos los resultados son bajos, en comparación con los que se muestran en la tabla III.3, por lo que esto da una pauta para no utilizar este método para la reducción de dimensionalidad de imágenes, o tal vez, se necesite otro procesamiento previo al realizado para mejorar la clasificación.

Para el caso de reconstrucción de imágenes utilizando este método, como se observó, conserva mucho más información que PCA.

F. Clasificación con datos obtenidos de ICA y Ensamble de Clasificadores.

Al igual que en los experimentos anteriores, se toma el conjunto de datos procesado para la prueba anterior, esperando mejorar los resultados anteriores, sólo para demostrar que el método de ensamble funciona, ya que como muestran los resultados de la tabla III.5 son inferiores a los de la tabla 3. Los resultados obtenidos se muestran en la tabla III.6.

Tabla III.6: Resultados obtenidos utilizando validación cruzada basada en ICA y Ensamble de clasificadores.

Grupos	ADTree	J48	Naive Bayes	Random Forest	
5	41.8605%	40.6977%	46.5116%	47.6744%	.
7	46.5116%	44.186%	44.186%	43.0233%	.
10	40.6977%	47.6744%	45.3488%	51.1628%	.

Por lo que se puede observar, los resultados de aplicar ensamble de clasificadores a datos reducidos por medio de ICA, son de un 1% a un 5 %, aproximadamente, menores a los mostrados en la tabla III.5, tal vez sea por la naturaleza del método, que no se mejoraron los resultados por medio de ensambles de clasificadores.

G. Clasificación con datos obtenidos de CCA y Validación Cruzada.

La reducción se realiza por medio de Análisis de Componentes Curvilíneos, como el método realiza un mapeo conservando los datos de una dimensión a otra, se eligen sólo 250 características de las imágenes de cada grupo, por lo que el conjunto de datos es de 96x250. Los resultados obtenidos por este método son los mostrados en la tabla III.7.

Tabla III.7: Resultados obtenidos utilizando validación cruzada basada en CCA.

Grupos	ADTree	J48	Naive Bayes	Random Forest	
5	94.5652%	85.8696%	98.913%	97.8261%	.
7	89.1304%	88.0435%	98.913%	98.913%	.
10	92.3913%	86.9565%	98.913%	96.7391%	.

Se puede observar que todos los resultados mejoraron de manera considerable con este método con respecto a todos los resultados anteriores (clasificación previa, con PCA e ICA), ya que como se mencionó anteriormente, al realizar una reducción de características, se encontró un patrón que distinguía los dos grupos de imágenes. Los resultados obtenidos son superiores a los obtenidos con PCA e ICA así como los de la clasificación sin reducción de dimensionalidad.

H. Clasificación con datos obtenidos de CCA y Ensamble de Clasificadores.

En el experimento anterior, se observó una gran mejora en los resultados de clasificación. En este experimento se aplica, al conjunto reducido por CCA a 250 características, clasificación por medio de ensambles y validación cruzada, obteniendo los resultados mostrados en la tabla III.8.

Tabla III.8: Resultados obtenidos utilizando validación cruzada basada en CCA y Ensamble de Clasificadores.

Grupos	ADTree	J48	Naive Bayes	Random Forest	
5	94.5652%	93.4783%	98.913%	98.913%	.
7	96.7391%	94.5652%	98.913%	98.913%	.
10	96.7391%	94.5652%	98.913%	98.913%	.

Los resultados obtenidos mejoraron aún más que en el experimento anterior con la utilización de ensambles de clasificadores y “bagging”, por lo que esta es la técnica más idónea a utilizar para la reducción de la dimensionalidad, ya que al realizar un mapeo de una dimensión a otra, se puede realizar mejor clasificación con “pocos datos” que conservan toda la información.

I. Resumen de general de resultados

Al agrupar los resultados obtenidos en cada uno de los experimentos por grupos de validación cruzada, se puede observar que la reducción de datos por medio de el método CCA arroja resultados favorables al realizar clasificación, incrementando ésta por medio de ensambles. Cada una de las tablas muestra los resultados obtenidos con clasificación individual y con ensamble de clasificadores, resaltando los mejores resultados. La tabla 9 muestra resultados obtenidos con 5 grupos de validación cruzada, la tabla 10 con 7 grupos y finalmente, la tabla 11 con 10 grupos de validación cruzada. En cada grupo de evaluación, se muestra un gran desempeño del método de reducción de dimensión CCA.

IV. CONCLUSIONES

Se concluye que las técnicas de reducción de dimensionalidad se pueden aplicar a cualquier tipo de datos incluyendo imágenes (como el caso de PCA y CCA), lo que se traduce en una representación más compacta de la información, que nos permite eliminar componentes que son muy parecidos o componentes que no contribuyen a nada en las imágenes, además con la eliminación de la tendencia media, se obtienen mejores resultados, ya que se elimina información redundante y se trabaja con la más significativa de cada imagen.

Se observa, que cada técnica trabaja de forma distinta, algunas conservando más información como el caso del Análisis de Componentes Curvílineos. Al realizar una comparación con los trabajos realizados anteriormente, se mejoró la clasificación en un 10% aproximadamente, obteniendo así un 98% de reconocimiento con la aplicación de técnicas no lineales, ya que se conserva más información que es útil y no como lo hacen los métodos lineales, como PCA o ICA, que bien pueden servir en problemas lineales y no así en problemas, como por ejemplo, tratamiento de señales.

Tabla III.9: Tabla comparativa de resultados obtenidos con 5 grupos de validación cruzada

	ADTree	J48	Naive Bayes	Random Forest
Sin Reducción	70.6522%	60.8696%	65.2174%	75%
Sin Reducción y ensamble	75.8261%	69.5652%	69.5652%	76.087%
PCA	51.2195%	58.5366%	85.3659%	60.9756%
PCA Y ensamble	63.4146%	58.5366%	80.4878%	65.8537%
ICA	46.5116%	45.3488%	46.5116%	52.3256%
ICA Y ensamble	41.8605%	40.6977%	46.5116%	47.6744%
CCA	94.5652%	85.8696%	98.913%	97.8261%
CCA Y ensamble	94.5652%	93.4783%	98.913%	98.913%

Tabla III.10: Tabla comparativa de resultados obtenidos con 7 grupos de validación cruzada.

	ADTree	J48	Naive Bayes	Random Forest
Sin Reducción	78.8261%	77.1739%	66.3043%	79.3478%
Sin Reducción y ensamble	77.1734%	77.1739%	65.2174%	78.2609%
PCA	46.3415%	60.9756%	87.8049%	63.4146%
PCA Y ensamble	56.0976%	53.6585%	82.9268%	65.8537%
ICA	47.6744%	45.3488%	40.6977%	45.3488%
ICA Y ensamble	46.5116%	44.186%	44.186%	43.0233%
CCA	89.1304%	88.0435%	98.913%	98.913%
CCA Y ensamble	96.7391%	94.5652%	98.913%	98.913%

Tabla III.11: Tabla comparativa de resultados obtenidos con 10 grupos de validación cruzada

	ADTree	J48	Naive Bayes	Random Forest
Sin Reducción	76.087%	66.3043%	65.2174%	76.087%
Sin Reducción y ensamble	73.913%	70.6522%	63.0435%	76.087%
PCA	51.2195%	53.6585%	87.8049%	56.0976%
PCA Y ensamble	58.5366%	60.9756%	85.3659%	63.4146%
ICA	50%	45.3488%	46.5116%	50%
ICA Y ensamble	40.6977%	47.6744%	45.3488%	51.1628%
CCA	91.3913%	86.9565%	98.913%	96.7391%
CCA Y ensamble	96.7391%	94.5652%	98.913%	98.913%

Como trabajos futuros a esta investigación, se buscará una representación de la misma información aplicando Análisis de Componentes Principales Probabilísticas con Datos Perdidos (PPCA-MV), y una mejora al Análisis de Componentes Independientes para que éste pueda trabajar con tratamiento de señales, ya que como se observa, esta técnica, aunque lineal, tiende a conservar más información, debido a la no gaussianidad que maneja.

REFERENCIAS

[1] Sodré L. Storrie-Lombardi L.J. Storrie M.C., Lahav O. "Morphological classication of galaxies by artificial neural networks". Monthly Notices of the Royal Astronomical Society, (8):259, 1992.

[2] Ratnatunga K.U. Owens E.A., Griffiths R.E. Ratnatunga k.u. “Using oblique decision trees for the morphological classication of galaxies!. Monthly Notices of the Royal Astronomical Society, (281):153, 1996.

[3] D.W. Aha D. Bazell. “Ensembles of classifiers for morphological galaxy classification”. Astrophisical Journal, (548):219–223, 2001.

[4] Thomas Mitchel. “Machine Learning”, McGraw Hill, 1997.

[5] S.C. Odewahn. “Astrophisical Journal”, pages 539,568, 2002.

[6] Lolling S.M. Godeyra S.N. “Morphological classication of galaxies using computer vision and anns”. ASS, (279):337, 2002.

[7] Olac Fuentes Jorge de la Calleja. “Machine learning and image analysis for morphological galaxy classification.”, Mon. Not. R. Atron. Soc., (349):89–93, October 2004.

[8] D.S. Madgwick. “Correlating galaxies morphologies andspectra on the 2df galaxy redshift survey”. Monthly Notices of the Royal Astronomical Society, (338):197–207, 2003.

[9] Olac Fuentes Jorge de la Calleja. “Automated classification of galaxy images”. In Proceedings of the Eight International Conference on Knowledge-Based Intelligent Information and Engineering Systems, Wellington, New Zealand, September 2004.

[10] L. Breiman. Random forest. Machine Learning, 45(1):5–32, 2001.

[11] N. Otsu. “A threshold selection method from gray-level histograms”. IEEE Transactions on Systems, Man., and Cybernetics, SMC-9(1):62–66, January 1979.

[12] O. F. Conde, J. F. Ramirez, T. Morales “Clasificación Morfológica de Galaxias utilizando Métodos de Reducción de Dimensionalidad y Ensamble de Clasificadores”, Proceedings of the Fifth Mexican International Conference on Artificial Intelligence 2006 (MICAI 06).

La Importancia de las Herramientas de V&V

Christian A. Martínez
Instituto Tecnológico y de Estudios Superiores de Monterrey Campus Puebla
pinkejo@acm.org

***Resumen*—El presente artículo explica brevemente algunas técnicas de Verificación y Validación que se utilizan en la fase de V&V del ciclo de vida de desarrollo del software. Propiamente con referencia al artículo, muestro la diferencia entre inspecciones simples e inspecciones técnicas formales, así como la metodología de peer review para proyectos de extreme programming.**

***Palabras Clave*—Verificación y Validación (V&V), Technical Reviews, Inspecciones Técnicas Formales, Peer Review.**

I. Introducción

Actualmente existen todavía empresas desarrolladoras de software que no toman con importancia la fase de Verificación y Validación (V&V). Seguramente son empresas que no se encuentran calificadas en algún nivel de certificación de CMM. Los clientes que buscan aplicaciones de software para sus negocios o empresas piensan que el costo de V&V es muy alto, pero la realidad y los múltiples casos de fracaso en proyectos de software hacen ver que el cliente termina pagando más del doble si omite esta fase de desarrollo en su producto. Technical Reviews, Inspecciones Técnicas Formales y Peer Review son algunas herramientas que aseguran la calidad en el proceso de desarrollo de software y las describiré brevemente citando algunas de sus ventajas y su importancia en la época tecnológica actual.

II. Technical Reviews (Inspecciones Simples)

Las inspecciones sirven para evaluar un producto de software a través de un equipo de personal calificado para determinar su confiabilidad con respecto a sus propósitos de uso e identificar discrepancias en relación con estándares [1]. Con esto se puede llevar la administración de evidencias para confirmar:

Manuscrito presentado en Frebrero 19, 2007, para la materia Verificación y Validación de Software (TC3008). Revisión por M.C. Alma Ríos Flores.

C.A. Martínez es Ingeniero en Tecnologías Computacionales con el plan ITC01 en curso 8vo. Semestre, Departamento de Tecnologías de Información del Instituto Tecnológico y de Estudios Superiores de Monterrey, Puebla, Pue., (e-mail:pinkejo@acm.org).

a) Si el producto de software es acorde con sus especificaciones.
b) Si el producto de software se ajusta a regulaciones, estándares, guías, planes y procedimientos aplicables al proyecto.

c) Si los cambios del software se han implementado satisfactoriamente y afectan solamente aquellos módulos del sistema identificadas en la especificación de cambios.

Asimismo, pueden surgir en este tipo de inspecciones recomendaciones para examinar o explorar diferentes alternativas en el diseño o especificación que se esté inspeccionando que requieran importancia.

Algunos de los productos que pueden evaluarse pueden ser: Software Requirement Specification, Software Design Description, Vision and Scope Document [3], Software User Documentation, entre otros.

Para las “Technical Reviews” deben definirse roles de: tomador de decisiones, líder de revisión, escriba y personal técnico de staff, que en mi opinión pienso son los roles mínimos necesarios para este tipo de inspección. Cabe mencionar que estas revisiones no son formales pero tienen gran importancia en la actualidad porque permite a los autores y diseñadores tener un retroalimentación con recomendaciones para la mejora de su producto, sin embargo, considero necesario que después de una o más technical reviews, deben realizarse inspecciones técnicas formales que aseguren la calidad del producto de software que se está desarrollando, pero eso lo veremos más adelante en el presente artículo.

La realización de una inspección requiere siempre de cinco aspectos de relevancia para llevarse acabo: conjunto de objetivos de la inspección, el producto de software que se examinará, plan de administración del proyecto de software, las anomalías actuales del software y la documentación de los procedimientos de revisión. Si alguna de estas características falta, hay que tomar en cuenta que puede haber problemas con respecto a la administración global del proyecto, es mejor siempre cumplir con ellas. No obstante, existen documentos extra que pueden servir para conformar una inspección, pueden ser como ejemplo: diagramas, reportes de revisión relevantes o estándares que se hayan utilizado.

Después de concluir con éxito una inspección, existen varios criterios de salida entre los que se encuentran: la revisión del proyecto, la revisión del software, lista de anomalías del software resueltas e inconclusas, y otros.

III. Inspecciones Técnicas Formales

A diferencia de las inspecciones rápidas, las inspecciones técnicas formales tienen una importancia mucho mayor en cuanto a verificación y validación se refiere. Este tipo de inspecciones permiten a los desarrolladores de software tener una revisión con mucho más detalle y por consiguiente, un aseguramiento de calidad que aumenta la plusvalía de su producto.

Hedberg e Iisakka las definen como métodos bien conocidos para detectar defectos en artefactos producidos en cualquier fase del desarrollo de software [2], *"es una evaluación sistemática de un producto de software por un equipo de personas calificado que examinan la confiabilidad del producto de software para la intención a la que se quiere utilizar e identifica discrepancias en especificaciones y estándares".* Siguiendo la opinión de Hedberg e Iisakka en su artículo de Calidad del Software, aseveran que la definición tiene dos ideas clave a su punto de vista: la inspección formal se lleva acabo por un equipo, lo que muestra que el autor no puede hacer una inspección formal por si mismo y que se realiza para un producto, no para un draft o prueba del producto. A estas palabras puedo inferir que cuando se solicita una revisión técnica formal es porque los autores han terminado ya su producto y el propósito es revisar si se necesitan reparaciones o modificaciones. Mientras el autor escribe su producto, como Vision and Scope Document [3], no hay chequeo, i.e. los verificadores no participan en la preparación.

A diferencia de una inspección sencilla, las inspecciones técnicas formales brindan una retroalimentación con mayores fundamentos y profundidad para los autores que la solicitan. Con este tipo de inspección puede mostrarse evidencia para verificar que el software satisface sus especificaciones, atributos de calidad, estándares, planes y procedimientos. Aunado a esto, permite también saber si existen desviaciones de estándares y utiliza los datos de ingeniería de software recabados para mejorar el proceso de inspección y su documentación.

Con respecto a las entradas, requiere más documentos que una inspección sencilla, como lo son: checklist de lo que se evaluará, especificaciones del hardware ó lista de errores ortográficos (typo list), y al ser formal no puede llevarse acabo si falta alguno de los miembros del equipo de inspección, si falta algún documento o si alguna de las personas relacionadas no ha revisado a detalle lo que se va a evaluar.

Pienso que las revisiones técnicas formales deberían tomarse en cuenta por todas las empresas desarrolladoras de software pues aquellas que no llevan una fase de verificación y validación a detalle, terminan gastando más en la corrección de errores que aquellas que la implementan. Es bien sabido que esta fase es de las más caras del ciclo de vida, pero no lo es tanto como el pago que debe hacerse si existe su omisión.

TABLA 1

Benefits \ Reference	Barnard & Price	Briand et al.	Chatzigeorgiou & Antoniadis	Gilb & Graham	Grady & van Slack	Porter et al.	Wiegers
Knowledge sharing and education		x		x			x
Increased project awareness and tracking	x	x	x	x			x
Process improvement	x	x	x	x			x
Finding more defects				x		x	x
Finding defects earlier and faster				x	x	x	x
Reduced development costs	x	x		x	x		x

Beneficios de las Peer Reviews

IV. Peer Reviews Aplicadas al Peer Programming

A. ¿Qué son y para qué sirven?

Desde el punto de vista científico, *"peer review es la evaluación científica en la búsqueda o propósitos para la competencia y originalidad por expertos calificados que buscan crear productos de la misma forma (peers)"* [4].

El peer programming es un método de desarrollo de software clasificado en los métodos ágiles, entre los que figura
también el extreme programming. Estos tipos de desarrollo implican poco tiempo en la elaboración de un producto y por consiguiente podemos deducir que su modelación y diseño deben ser rápidos y precisos para tener un producto final de calidad. Las revisiones técnicas diseñadas para métodos ágiles, por lo regular deben llevarse acabo por dos personas. Sin embargo, los métodos ágiles no son similares en este aspecto. Algunos métodos las incluyen, mientras que otros no. A su vez, las principales actividades de control de calidad en procesos ágiles se evalúan a través de pruebas de código y retroalimentación del cliente. Típicamente estas metodologías muestran que las revisiones del proceso de desarrollo y productos pueden reemplazarse por inspecciones informales y con esto hay que señalar que existen pocos métodos ágiles que las envuelven.

Aunque he explicado que existen varias metodologías, enfoquémonos a las limitaciones de esta investigación. Peer review en peer programming es un método de revisión paradójico. La idea es que dos desarrolladores trabajen juntos escribiendo el mismo código. Naturalmente, este doble trabajo cuesta. Los defensores dicen que este trabajo se compensa parcialmente desde el punto de vista que doble programador tiene un desarrollo más rápido con una densidad de defectos de código menores.

En general, el aseguramiento de la calidad en métodos ágiles como el peer programming recae en las pruebas de código en parejas y la interacción del cliente. Usualmente, deben existir este tipo de pruebas peer, pero son informales.

Pocas compañías de software consideran que las peer reviews tienen importancia en la calidad de sus productos. Sin embargo, han ajustado el método a sus recursos limitados. Sin importar cuánto pueden aportar en la cadena de valor, puedo decir que la técnica brinda una detección de defectos eficiente.

B. Beneficios y Desventajas

Las revisiones son unas de las pocas técnicas de aseguramiento de calidad en el desarrollo de software. Veamos en la tabla I [5] algunos de los beneficios encontrados en esta técnica y revisemos las desventajas en la tabla II [5]. Como podemos ver existen puntos de vista muy diferentes para esta técnica de verificación, pero yo creo que todo depende del producto de software que se debe desarrollar y el fin para el que se utilizará.

V. CONCLUSIÓN

Los métodos de prueba de software deben ser siempre conocidos y aplicados en las empresas de desarrollo de software que quieren asegurar una calidad alta en sus productos. Con Technical Reviews para revisiones rápidas en el producto, Inspecciones Técnicas Formales en la verificación de documentos de diseño y especificaciones del software ó con el uso de Peer Reviews, podrán mostrar siempre una evidencia tangible de que los productos que brindan han llevado un proceso correcto en su elaboración.

Aunque los clientes de ayer y hoy piensan que la aplicación de este tipo de herramientas eleva demasiado el costo de lo que compran, ya sea una aplicación estándar o un producto hecho a la medida, existen casos reales que muestran totalmente lo contrario.

En nuestro país ya existen empresas certificadas por CMM que para calificar con un nivel de madurez en desarrollo de software debieron haber mostrado técnicas de verificación en el proceso, involucrando algunas de las que se mostraron en esta investigación.

Yo creo que lo más importante, independientemente del método seleccionado, es que los desarrolladores y autores se complementen en trabajo en equipo empatizando en una selección de técnica correcta que sea acorde con el producto final. Inspecciones Técnicas Formales mínimo para la especificación del SRS en proyectos no muy grandes o su aplicación en todo el diseño para el desarrollo de productos mayores con el apoyo de Technical Reviews entre los documentos finales, pueden llevar al desarrollo de una aplicación al éxito. O bien, el uso de éstas últimas combinadas con las Peer Reviews en casos extremos de desarrollos que impliquen poco tiempo y buena calidad.

TABLA 2

Obstacle \ Reference	Chroust & Lexen	Ciolkowski et al.	Glass	Johnson	Laitenberger et al.	O'Neill	Shepard & Kelly
Lack of time	x	x	x	x		x	x
Lack of human resources	x				x		
Cost		x		x	x		x
Laboriousness			x	x			
Complexity or inadequate training	x	x		x			x
Resistance to change	x						
Inefficiency				x			x

DESVENTAJAS DE LAS PEER REVIEWS

Es necesario que nosotros como Ingenieros de Software intentemos mostrar esta importancia con nuestros clientes, pues sabemos que la naturaleza intangible de nuestro producto final, hace más difícil convencer que lo que hacemos implica mucho trabajo, muchas personas y mucha calidad.

Ayudémonos con las evidencias que dejan estas metodologías de prueba y otras más para convencer que nuestro trabajo debe ser bien remunerado y que sin duda, la falta de la aplicación de la tecnología computacional en la actualidad no permitirá tener una buena competencia en cualquier sector de mercado de hoy en día.

REFERENCIAS

[1] IEEE, IEEE Standard for Software Reviews IEEE Std 1028-1997. New York, NY 1997., Proceedings of the IEEE 1998.

[2] Hedberg, H., Iisakka, J., Technical Reviews in Agile Development: Case Mobile-DTM. Beijing, China Oct. 2006 Page(s): 347 – 353., Six International Conference.

[3] Wiegers, K.E. Vision and Scope Template. 1999.

[4] Brown T, Peer Review and The Acceptance of New Scientific Ideas. London May. 2004 Page 7.

[5] Harjumaa, L.; Tervonen, I.; Huttunen, A., Peer reviews in real life - motivators and demotivators. Oulu Univ., Finland, 19-20 Sept. 2005 Page(s): 29 – 36. Fifth International Conference.

Conociendo TQM, SCM & SQA

Christian A. Martínez
Instituto Tecnológico de Estudios Superiores de Monterrey Campus Puebla
pinkejo@acm.org

***Resumen*—El presente artículo muestra una explicación breve y clara de los conceptos TQM, SCM y SQA, además de información relevante de su uso, aplicación e importancia en la Ingeniería de Software.**

***Palabras Clave*—Total Quality Management (TQM), Software Configuration Management (SCM), Software Quality Assurance (SQA).**

I. Introducción

ESTA investigación presenta algunas definiciones hechas por diferentes autores e investigadores acerca de Total Quality Management (TQM), Software Configuration Management (SCM) y Software Quality Assurance (SQA), que tienen una importante relevancia en los departamentos áreas relacionados con la Verificación y Validación de Software.

Se muestran también algunos conceptos relevantes de las definiciones presentadas e información de algunas de sus aplicaciones, uso, técnicas, metodologías y pruebas encaminadas a los Proyectos de Desarrollo de Software en la actualidad.

El artículo se divide en tres partes básicas: II. TQM, III. SCM y IV. SQA, que se describen a continuación.

II. Total Quality Management (TQM)

TQM es una estrategia de dirección que se enfoca a la integración de la conciencia de calidad en todos los procesos de la organización. TQM ha sido extensamente utilizado en muchas áreas como la fabricación, educación, gobierno, industrias de servicio así como en programas de ciencia.

La Calidad Total proporciona un refugio bajo el que cada persona de la organización puede esforzarse y en conjunto lograr la satisfacción del cliente. TQM requiere que las organizaciones mantengan estándares de calidad en todos los aspectos del negocio. Esto requiere el aseguramiento de que las cosas se hagan bien desde la primera vez y los defectos y pérdidas de tiempo sean eliminados de las operaciones.

Kaizen [1], un personaje gurú de la calidad, lo define como: “enfoque a la mejora de proceso continua para hacer procesos visibles, repetibles y medibles”. Otros como Grunenwald [2], en su publicación sobre el costo de calidad como una base para la implementación del Total Quality Management, muestra el TQM como “una búsqueda de oportunidades, o cosas que arreglar”.

Total Quality Management se encuentra entre los medios de mejora más prominentes del siglo XX. Los investigadores han notado que muchas firmas han obtenido grandes ventajas operacionales y financieras con el uso de TQM, mientras otra gran cantidad han fallado miserablemente al ponerlo en práctica. Según el artículo de Ahire y Ravichandran [3], Evans acentúa la necesidad de desarrollar y probar los marcos que explican las interacciones entre varios factores de TQM para obtener los resultados operacionales de sus esfuerzos. De esta manera han llegado a definir el TQM como un esfuerzo organizacional para difundir la innovación en conjunto con las organizaciones.

Muchas veces el fracaso en la práctica del TQM no quiere decir que sea inefectivo, sino todo lo contrario. Y como muestran Clemson y Lowe [4] en su investigación, este puede ser una sugerencia para concluir que la práctica aislada del TQM es realmente lo que lo conlleva a su inefectividad. El problema no es el método ni su aplicación, sino el cambio de paradigma que debe enfrentar la gente que lo llevará a la práctica; si las actitudes y comportamientos de los ejecutivos no cambian, entonces la aplicación del TQM no funcionará.

La mayoría de los mejores consultores del TQM están convencidos con la necesidad de cambios culturales y estructurados como parte de una implementación del TQM exitosa. Muchos de ellos incluso tienen una muy buena creatividad en el desarrollo de técnicas para lidiar con este tipo de factores. Sin embargo, gran parte de este trabajo consiste de la reinvención de métodos existentes.

En general TQM necesita la habilidad del trabajo en conjunto hacia la parte más extrema de la estructura vertical y horizontal de las organizaciones. El éxito en su aplicación puede ser consecuencia muchas ocasiones de la aplicación de un gran número de métodos de cambio que complementan el TQM, pero no discutiremos esto debido a que esta temática no concierne a la presente investigación.

Manuscrito presentado en Enero 11, 2007, para la materia Verificación y Validación de Software (TC3008). Revisión por M.C. Alma Ríos Flores.

C.A. Martínez es Ingeniero en Tecnologías Computacionales con el plan ITC01 en curso 8vo. Semestre, Departamento de Tecnologías de Información del Instituto Tecnológico y de Estudios Superiores de Monterrey, Puebla, Pue., (e-mail:pinkejo@acm.org).

III. Software Configuration Management (SCM)

SCM para Roger Pressman [5] es un "conjunto de actividades designadas al control de cambio por medio de la identificación de productos que también cambiarán, estableciendo la relación entre ellos, definiendo los mecanismos para la dirección de diferentes versiones de estos productos, controlando los cambios impuestos y con una serie de revisiones y reportes de los cambios realizados". Con esto podemos decir que SCM es una metodología de control y dirección de proyectos de desarrollo de software.

El SCM abarca una gran cantidad de tareas, pero según el artículo y la investigación de McDonough [6] presenta una lista de las tareas de mayor importancia:

1) Preparación del plan SCM,
2) Dirección de los esfuerzos de SCM,
3) Identificación de configuración de SCM,
4) Control de configuración de SCM,
5) Contabilidad de estado de configuración de SCM,
6) Revisión de configuración de cuentas de SCM.

Todas ellas deben de llevar una dirección con una disciplina estricta, con lo que podemos decir que con la aplicación de todos los elementos del SCM básicamente se promueve un clima de control disciplinado.

Es muy importante mencionar que las tareas de mayor importancia mencionadas son subrayadas y mostradas en un estándar de la IEEE [7].

Para finalizar esta parte, quiero asentir que durante el ciclo de vida del desarrollo de software se produce un gran número de productos, como documentos, fragmentos de código y datos. Estos productos de trabajo pueden ser modificados y brindárseles un mantenimiento; como nos dicen Seawlho y Suwannasart [8] en su publicación sobre el modelo de SCM para las organizaciones CMM. Por esto, y gracias a la tecnología cambiante en la que las empresas siempre deben encontrarse a la vanguardia de lo más novedoso, las organizaciones de desarrollo de software necesitan prácticas para controlar y dirigir sistemáticamente los cambios que llevan consigo los proyectos de desarrollo. Todas estas prácticas dan como resultado lo que llamamos Software Configuration Management.

IV. Software Quality Assurance (SQA)

SQA es una actividad para probar la evidencia que se necesita para establecer confianza a todos los relacionados, de que las actividades que están ligadas a la calidad se están llevando acabo eficientemente. Son todas aquellas acciones planificadas o sistemáticas para proveer la confianza correcta de que un producto o servicio satisfará todos los requerimientos de calidad. La garantía de calidad se encuentra estrechamente relacionada con la dirección de calidad que demuestra la confianza externa basada en hechos hacia los clientes y todos los stakeholders que están ligados con las expectativas, necesidades y exigencias del producto. Este SQA asegura la existencia y efectividad de los procesos para que puedan mostrar por adelantado que los niveles esperados de calidad serán alcanzados [9].

Es mostrado en el artículo de Honda, Minomura y Komiyama [10] que existe una metodología-meta para el SQA llamada SQAP que se ha desarrollado y puesto en práctica para que las actividades de aseguramiento de calidad de software puedan ser efectiva y sistemáticamente ejecutadas en los proyectos de software. Esta metodología sigue cuatro lineamientos principales: fondo, conceptos básicos, lineamiento e implementación y educación; que no profundizaremos en esta investigación.

A pesar de lo anterior, la realidad es que la aplicación del SQA aún es ignorada o inefectiva para muchos profesionales en el ámbito de la calidad o simplemente no tienen la más remota idea de cómo implementar este programa de manera efectiva según relata Lowe [11]; quien expresa como meta principal de el SQA: construir calidad en el producto – mantener la calidad en el producto.

Llevar a la práctica el SQA trae consigo beneficios de importancia como son: especificación de problemas detectados en el diseño del proceso, reducción de explicaciones innecesarias durante los periodos de prueba críticos y funcionalidad del programa completamente probada, entre otros. Sin embargo, una de las grandes desventajas de falta de aplicación de un SQA es la independencia de la organización SQA del desarrollo de software.

V. Conclusión

Hoy en día muchos proyectos son realizados sin una correcta verificación, sin realización de pruebas y esto afecta directamente a los productos, servicios, clientes o usuarios que se encuentran relacionados con ellos. Con la aplicación y aprendizaje de la implantación en proyectos de los conceptos que he presentado, puede lograrse un buen equilibrio que satisfaga las políticas y requerimientos de calidad y de esta manera existan cada vez más empresas y clientes beneficiarios directos a su uso. Considero que en México faltan muchas medidas de calidad por implementar, pues en realidad la mayoría de los servicios brindados la llevan por los suelos.

Debemos seguir la tarea de aquellos que se preocupan por todos estos puntos e impactar la cultura de nuestro país con estos cambios. Un problema fundamental de los mexicanos es el miedo al cambio de paradigma, pero si queremos destacar como nación y como país, este puede ser un punto de relevancia. ¿Será posible llegar a ver un futuro país que pueda manejar la calidad de esta manera?

Referencias

[1] Total Quality Management Definition, http://en.wikipedia.org/wiki/Total_Quality_Management.

[2] William J. Grunenwald, Cost of Quality as a Baseline for Total Quality Management (TQM) Implementation. Aerospace and Electronics Conference, 1989. NAECON 1989., Proceedings of the IEEE 1989 National.
[3] Sanjay L. Ahire and T. Ravichandran, An innovation diffusion model of TQM implementation. Engineering Management, IEEE Transactions.
[4] Barry Clemson and Ernest Lowe, Total Quality Management and Comprehensive Change. Engineering Management Conference, 1992. 'Managing in a Global Environment'., 1992 IEEE International.
[5] Software Configuration Management, http://en.wikipedia.org/wiki/Software_configuration_management.
[6] James A. McDonough, A Structured Menu Of Software Configuration Management, Aerospace and Electronics Conference. 1993. NAECON 1993., Proceedings of the IEEE 1993 National.
[7] IEEE ANSI standard. 1987. IEEE Guide to Software Configuration Management. IEEE/ANSI Standard 1042- 1987.
[8] Pornthep Seawlho and Taratip Suwannasart, A SCM Workflow Model for CMM Organizations. Software Engineering Conference, 2003. Tenth Asia-Pacific.
[9] Quality Assurance, http://en.wikipedia.org/wiki/Software_Quality_Assurance.
[10] Katsumi Honda, Keisuke Minomura, Toshihiro Komiyama, Meta-Sqap: Meta-Methodology For Software Quality Assurance. Computer Software and Applications Conference, 1989. COMPSAC 89.
[11] John E. Lowe, SQA-A Customer Service Approach. Aerospace and Electronics Conference, 1991. NAECON 1991., Proceedings of the IEEE 1991 National.

GA-Gammon: A Backgammon Player Program Based on Evolutionary Algorithms

Oscar Irineo-Fuentes
Nareli Cruz-Cortés
Francisco Rodríguez-Henríquez
CINVESTAV-IPN
Electrical Engineering Department, Computer Science Section
Mexico
{oirineo,nareli}@computacion.cs.cinvestav.mx
francisco@cs.cinvestav.mx

Daniel Ortiz-Arroyo
and Henrik Legind Larsen
Computer Science and Engineering Department
Aalborg University Esbjerg
Denmark
{do,legind}@cs.aaue.dk

Abstract

In this paper we describe a genetic algorithm approach able to confection strong backgammon automata players. We first prepared an initial vector of weights representing a set of heuristic strategies suggested by expert human players. Then, employing a genetic algorithm approach we were able to fine tune such initial vector of weights by repeatedly testing it against Pubeval, a strong benchmark player program. The vector of weights was therefore used as an evaluation function for performing a genetic heuristic selection of the best board positions during a game. Best GA-Gammon *individuals so obtained were tested in separated 5000-game tournaments against* Pubeval *itself, and* Fuzzeval*, a fuzzy controller-based player. Our experimental results indicate that the best individuals generated by* GA-Gammon *show similar performance than* Pubeval*. Furthermore,* GA-Gammon *consistently outperforms* Fuzzeval.

1 Introduction and Related Work

The study of algorithms and heuristics that could enable computers to play board games at an expert human level has received considerable attention since 1950, when Claude E. Shannon designed a computer program to play chess [10]. Unlike chess, where a combination of pruned brute force searching approaches along with opening/closing data books has been applied successfully, backgammon requires the application of radically different strategies. Backgammon is a board game that combines luck and strategy. The use of dice in backgammon avoids applying brute force-based approaches that search for the optimal moves. Moreover, different strategies must be employed in the two phases of the game i.e.

the *contact phase* where player's checkers are intermixed and the *race phase* where there is no contact anymore.

During the last decade, researchers have proposed numerous approaches to create strong player programs in the domain of backgammon. In 1995 G. Tesauro created *TD-Gammon* [11] a backgammon program that has played at the master level with humans. This program achieved a remarkable success by learning playing strategies during self playing. *TD-Gammon* employs the temporal differences method to train an Artificial Neural Network (ANN) that is used in an evaluation function. The temporal differences training strategy basically adjusts the ANN's weights according to the results obtained during a sequence of games. *TD-Gammon* consists of two ANNs that were trained specifically for the two phases of the game. Unfortunately, being a proprietary technology, *TD-Gammon* can not be used to evaluate other approaches. However, there exists a publicly available evaluation function called *Pubeval*, which was also created by G. Tesauro. The weights included in *Pubeval*'s evaluation function, were obtained using ANNs. With *Pubeval* it is possible to create a strong backgammon player program that plays at intermediate level. *Pubeval* has become the *de facto* standard benchmark in backgammon.

Pollack et al. [6] published in 1997 a backgammon player program called *HC-Gammon*, which uses a Hill-Climbing technique to train a feed-forward neural network used to create an evaluation function. *HC-Gammon* starts with an initial champion program with all weights set to zero and proceeds by playing the current champion network against a slightly mutated challenger. When the challenger wins a game, the weights in the evaluation function are changed. Using this technique Pollack et al. concluded that Tesauro's *TD-Gammon* success was mainly due to the co-evolutionary structure of the learning task and the characteristics of the backgammon game itself, and in a minor degree to the sophisticated learning techniques employed. However, G. Tesauro refuted these observations in a later paper [12].

Sanner et al.'s [9] proposal was to develop an algorithm that emulates closely the human cognition process in the domain of backgammon. They argued that humans can not explore thousands of possible moves as computer programs do. Hence, more efficient methods must be used for learning. Based on the ACT-R theory of cognition, their program *ACT-R-Gammon* analyzes general features of backgammon that may be encountered in a winning or loosing game. Bayesian learning is employed to infer the likelihood that each of the features resulting from a move would be present in a winning game. *ACT-R-Gammon* achieved a winning rate of about 46% against *Pubeval* after playing $1,000$ games.

Azaria and Sipper [1] proposed *GP-Gammon*, a backgammon player that is created using Genetic Programming. *GP-Gammon* applies Genetic Programming to the evolution of strategies for playing backgammon. After rolling the dice, the program generates all possible next-move boards. Each individual LISP program generated receives the board configuration and returns a real number that represents the score given to that board. Then, the highest scoring board is selected for playing. *GP-Gammon* was reported as obtaining a winning rate of 58% against *Pubeval* after playing $2,000,000$ games.

Recently, a fuzzy controller-based backgammon program called *Fuzzeval*, was proposed in [2]. *Fuzzeval* grades the perceived strength of all possible valid board positions it can play, using a rule base obtained from an amateur human player. *Fuzzeval* adjusts automatically the membership functions associated with the linguistic variables employed in the rule base, by aligning them with the average values that were used in the past winning games. *Fuzzeval* achieved a winning rate of 42% against *Pubeval* after playing 100 games.

Another interesting approach is that of Qi and Sun [7]. Their work proposes to use a hybrid approach were a genetic algorithm is applied to a team of agents whose learning capabilities are based on neural networks. GA-based multi-agent reinforcement learning bidding approach called *GMARLB*. Reinforcement learning performed by the multi agent system is applied in the backgammon game domain. The general idea of this approach is that individual agents within a team should be built using two decision modules: the Q module and CQ module. A single controlling agent in the team is responsible for taking the appropriate actions at any time during a game. Using the Q module, the controlling agent selects the actions to be performed, whereas the CQ module determines whether the agent should continue working as the controller or relinquish its control to other agents. Once an agent relinquishes its control, a new agent is selected by bidding algorithms. Both, the Q and the CQ modules learning capabilities are based on neural networks. In [7]. it is reported that this approach achieved a winning rate of 56% against *Pubeval* after playing $400,000$ games. Nevertheless, an independent test recently carried out in [1] showed that the high performance reported in [7] was apparently due to measurements taken in too short tournaments (50 games). According to [1], experimental results show that the winning rate of *GMARLB* reduces to just 51.2% when confronted against *Pubeval* on 1000-game tournaments.

In this paper we propose the usage of a pure genetic algorithm strategy as opposed to the hybrid genetic algorithm/neural network approach essayed in [7]. Our algorithm produces nearly the same winning rates as that of [7] with a structure much simpler and a smaller number of training games. The genetic algorithm employed by our player, *GA-Gammon*, optimize an initial vector of weights that is used as an evaluation criteria for selecting the best possible valid move in a game. The weights are produced by the combination of diverse heuristic strategies proposed by expert human players. That initial vector is used as a seed for generating a total of twelve slightly modified vectors (individuals), which are then tested against Pubeval in 1000-game tournaments. A fraction of the best fitted individuals are selected for further processing in subsequent generations. As a result, individuals are methodically refined generation after generation. Those individuals showing winning performances above 48% are separated from the rest of the population. They are re-tested in 5000-game tournaments against Pubeval. This last step is intended for confirming the winning performance found during the evolutionary process as it has been found that this figure shows a wide range of variability from tournament to tournament. After launching an extensive search of best fitted individuals, our strategy was able to find individuals showing a performance of up to 50.0% when confronted against *Pubeval* on 5000-game tournaments.

Individuals with winning performances of 50% start appearing after an average of 20 generations using a population size of 40 individuals. Recall that each individual undergoes a 1000-game tournament against Pubeval. Therefore it is fair to say that our algorithm needs an average of $40 \times 20 \times 1000 = 800,000$ games for finding the strong players reported in Section 3.

The rest of this paper is organized as follows. Section 2 describes GA-Gammon in detail. The comparative performance results of GA-Gammon while playing against Pubeval and Fuzzeval are presented in Section 3. Finally, in Section 4 we describe future work and present some conclusions.

2 GA-Gammon an Intelligent Backgammon Player

In this work we use a Genetic Algorithm (GA) to evolve a set of weights associated to the heuristic strategies employed by human experts while playing backgammon. The vector of weights contains sixteen elements. The set of strategies employed was designed following the recommendations listed in [3, 8] by a group of expert human players. The general idea of GA-Gammon's approach is to promote those board states that are evaluated as beneficial for improving the performance of our player. The vector weights are evolved by a simple *Genetic Algorithm (GA)* with the goal of maximizing the number of victories achieved by GA-Gammon. The fitness function employed by the GA is obtained by setting the GA-generated individuals to play against *Pubeval*.

2.1 Description of the Genetic Algorithm

This section describes the main features of the GA employed in GA-Gammon.

Genetic Algorithms (GA) were proposed by J. Holland in the mid 70's [4, 5]. GAs are inspired by the Neo-Darwinian principles of adaptation and survival of the fittest individuals. Although originally proposed for improving/optimizing machine learning techniques, GAs have been more applied in the domain of optimization. GAs are population-based techniques whose main characteristic is the evolution of several potential solutions (regarded as *individuals*) at the same time. Algorithm 2.1 shows the basic skeleton of a GA [1].

From Algorithm 2.1 it can be seen that a crucial factor for achieving effectiveness when using genetic algorithms is to accurately map the variables to be optimized to *individuals*, a process known as *problem representation*. It is also important to come out with an evaluation function that allows us to establish which individuals are better fitted. Furthermore the single two main mechanisms that a genetic algorithm has for finding good solutions are the *crossover operator* and the *mutation operator*. The crossover operator defines how the parents' characteristics are transmitted to the children population. The mutation operator randomly modifies a small fraction of the children population with the purpose of introducing better individuals to the evolutionary process.

Algorithm 1 Basic Skeleton of a Genetic Algorithm

Require: The population size *PopulationSize*, number of *generations* N.
Ensure: Finds the "best" individuals.

1: Create an initial population of individuals of size *PopulationSize*.
2: **for** $i = 0$ to N **do**
3: Compute the *fitness* value to each individual in the population.
4: Based on their fitness value, select the individuals to be reproduced (*parents*).
5: Apply the *crossover operator* to the parents population to create the children.
6: Apply the *mutation operator* to the children population. Children are the new population.
end for
7: **Return**(Best survival individuals)

[1] It is noted that Algorithm 2.1 corresponds to the original version of a GA. Quite a few new operators have been proposed in the literature aiming to improve the search and/or optimization capabilities of the GAs.

In the rest of this Section we explain how the general framework of Algorithm 2.1 was applied to the problem in hand. We explain in detail the specific problem representation, fitness function, crossover and mutation operators utilized by our algorithm.

2.1.1 Representation

An individual in the population is composed of sixteen elements, i. e. a chromosome is composed of sixteen genes. Each gene represents a weight w.

Let us call each individual in the population as W, with $W = w_j$, and $j \in [1..16]$. Then an individual or chromosome is composed of sixteen genes or weights w_j.

The GA's population is composed of a set of individuals.

The weights take integer values from 1 to 100, except w_4, which is defined in the range [0..36] and w_9 in range [3..15]. In the beginning the vectors are created randomly, using values defined within the range chosen for each weight.

The individuals are represented using binary numbers.

2.1.2 The Fitness Function

Each individual i, where $i \in [1..PopulationSize]$, in the population plays $1,000$ games against *GA-Gammon*. The percentage of victories obtained is assigned as the *fitness* value for the individual i.

A game against *GA-Gammon* is played by an individual using its weight vector. After the dice are rolled, all possible valid moves that an individual can make are calculated. Each chromosome evaluates each board state assigning a score S to it. The score is calculated according to the rules presented in Tables 1 and 2. The board receiving the highest score is selected for playing.

Table 1 shows how the weights w_j are used to calculate the score S for a board state if the game is in the contact phase. The score computation in the race phase is shown in Table 2.

The entire processing steps performed by an individual while playing against Pubeval is illustrated in Figure 1.

The initial population is created following the indicated representation. Then, the GA is executed in the conventional way: Assigning the fitness value to each individual in the population (percentage of victories when playing 1000 games against pubeval). Based on the fitness value, the *selection operator* is applied in order to obtain the individuals to be reproduced, i.e. the parents. Parents are recombined by applying the *crossover operator* to obtain the children. The *mutation operator* is applied to the children. The children will be the new generation. These steps are repeated until a stop criterion is met. The complete GA's process is illustrated in Figure 2.

In our case, the GA is stopped if the best fitness value does not change through 5 generations. On average the algorithm executes 20 generations.

It was determined experimentally that better results are obtained when the elitism [2] is applied to the three best individuals, i. e. the best three individuals in the population are allowed to survive.

[2] Elitism is a mechanism that allows the best individual to survive in the next generation.

Table 1: Board score computation S for the contact phase.

Let T_k	be an integer variable, with $k \in [1..10]$ then
	T_1 = The number of pieces' blocks that are consecutive is multiplied by w_1. T_2 = The number of positions with two or more pieces multiplied by w_2 T_3 = The total number of captured pieces from the opponent multiplied by w_3. If the probability that opponent's pieces may enter the board (normalized between 0 and 36) is less than w_4 then $T_4 = w_5$, otherwise $T_4 = 0$. T_5 = The number of positions with 2 or more pieces in the home board multiplied by w_6. T_6 = The number of pieces left behind multiplied by $-w_7$. T_7 = The number of blots in the home board multiplied by $-w_8$. If the number of pieces in one position is bigger than w_9 then $T_8 = -w_{10}$. If the number of blots is bigger than 3, then $T_9 = -w_{11}$. $T_{10} = -w_{12}$ multiplied by the probability that a blot is captured.
	The value for the board score S in the contact phase is obtained as $S = \Sigma T_k$

Table 2: Board score computation for the race phase.

Let S	and T_k be integer variables, with $k \in [1..4]$ then
	T_1 = The number of pieces in the own outer board multiplied by $-w_{13}$. T_2 = The number of pieces in the opponent's outer board multiplied by $-w_{14}$. T_3 = The number of pieces in the opponent's home board multiplied by $-w_{15}$. If there is a piece outside of the home board and it is possible to move it to position 6 in the home board, then $T_4 = -w_{16}$.
	The value for the board score S in the race phase is obtained as $S = \Sigma T_k$

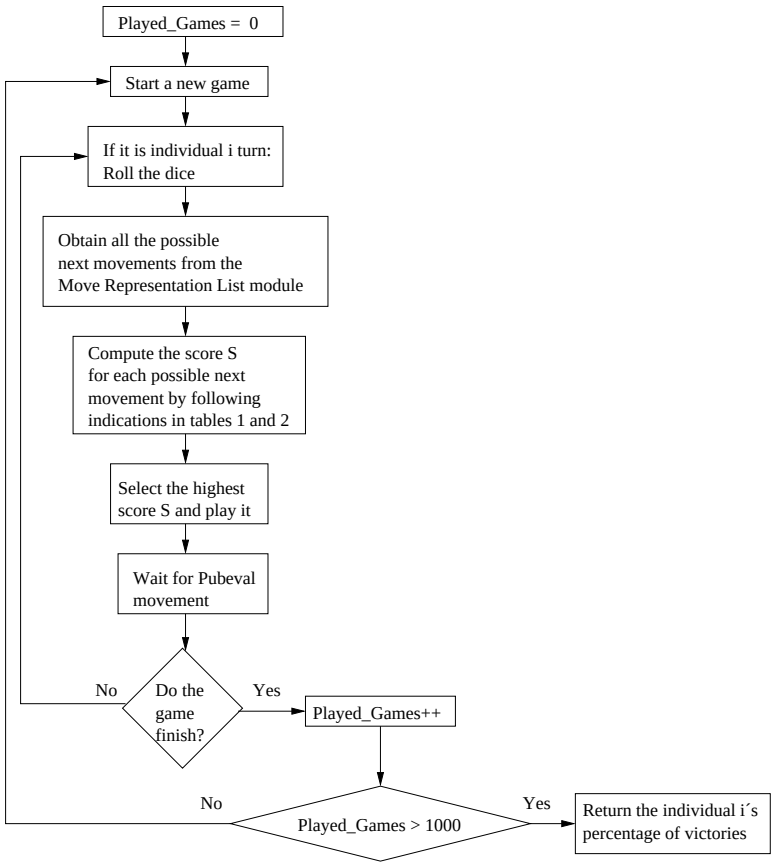


Figure 1: Processing steps performed by an individual i from the GA's population while playing against *Pubeval*.

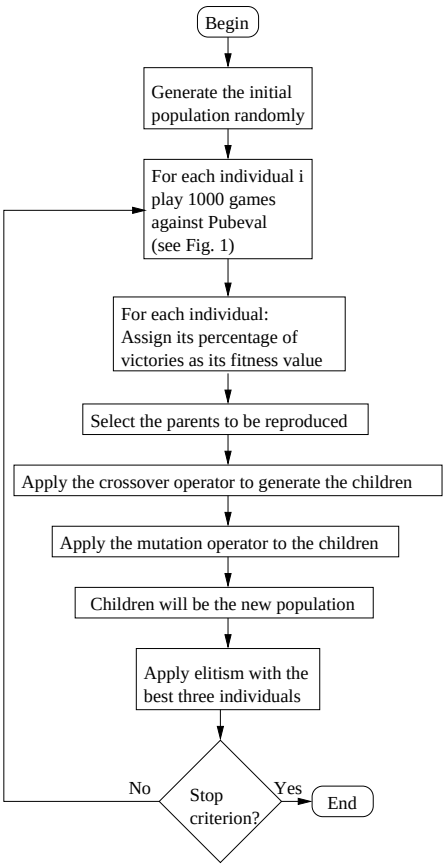


Figure 2: Genetic Algorithm General Structure.

3 Experimental Results

To validate the performance achieved by GA-Gammon we conducted a set of experiments, whose results are summarized in this Section. All our results were obtained by applying the following parameter values in the GA:

- Population size: 40 individuals
- Representation: Binary.
- Type of Selection: Stochastic Remainder with Replacement using Sigma scaling.
- Crossover rate: 0.9
- Mutation rate: 0.14

In order to determine the number of games that an individual should play against *Pubeval* we conducted a set of experiments. Thus, we observed that after 1000 games the variation in the winning rate is equal to 3.6% on average, after 2000 games the variation is equal to 1.2% and 0.2% after 3,000 games. Based on this information, we decided that a good compromise between winning rate and processing time would be to play 1000 games.

After we obtained the best individual from the GA process, GA-Gammon was set to play against *Pubeval* and *Fuzzeval*. The experiment consisted of playing against these players 5 sets of 1,000 games each.

Table 3: Performance comparison of GA-Gammon while playing against *Pubeval*.

	Type of Victories				
	Normal	Gammon	Backgammon	**Total**	**Percentage**
GA-Gammon	382	119	7	508	**50.59%**
Pubeval	361	127	4	492	49.41%

Table 4: Performance of GA-Gammon playing against *Fuzzeval*.

	Type of Victories				
	Normal	Gammon	Backgammon	**Total**	**Percentage**
GA-Gammon	485	78	13	576	**59.54%**
Fuzzeval	387	36	1	424	40.46

The best winning rate obtained by GA-Gammon by playing against *Pubeval* was 50.59%. The types of victories that were obtained during the tournament are shown in Table 3.

When GA-Gammon was set to play against *Fuzzeval*, the maximal winning rate obtained was 59.54%. The type of victories obtained for the best results are shown in Table 4.

In Table 5 is shown the comparison of the proposed GA-Gammon and other Backgammon players. GA-Gammon obtained very competitive results with a very simple schema.

4 Conclusions and Future Work

In this paper we have described *GA-Gammon*, a new approach to create strong backgammon player programs based on the application of evolutionary algorithms. *GA-Gammon*, employs some of the heuristic strategies that expert human players have used successfully. *GA-Gammon* employs a set of weight vectors that is considered the GA's population. Each individual in the population is set to play against *Pubeval* to determine its fitness value. The GA finds the best weight vector that maximizes the winning rate of our player.

GA-Gammon employs the information obtained from two sources of knowledge: 1) a set of heuristic playing strategies suggested by expert human players, and 2) a board score that is dependent on the percentage of victories obtained while playing against *Pubeval*.

Our experiments show that the selection of the different heuristic strategies plays an important role in *GA-Gammon*'s performance.

Table 5: Comparing GA-Gammon against other Backgammon Players

Player	%Wins vs *Pubeval*
Gp-Gammon[1]	56.8
GMARLB-Gammon [7]	51.2
GA-Gammon	**50.59**
ACT-R-Gammon [9]	45.94
Fuzzeval [2]	42.0
HC-Gammon [6]	40.00

GA-Gammon was evaluated by setting it to playing against *Pubeval* and *Fuzzeval*. Our experimental results indicate that *GA-Gammon* plays competitively with these players using a simple genetic algorithm. *GA-Gammon* obtained a winning rate of 50.0% against *Pubeval*, while clearly outperforming *Fuzzeval* with a winning rate of 59.5%.

It was shown that the proposed GA-Gammon player obtained very competitive results when compared against other players which are representatives of the state-of-the-art with a simple algorithm by training only 800,000 games in average.

In the future we will experiment with binary representation using Gray codes and different GA's parameters. Furthermore, we are planning to compute the GA-Gammon's fitness function by playing against a more powerful strategy such as TD-Gammon, instead of Pubeval.

References

[1] Y. Azaria and M. Sipper. GP-Gammon: Using Genetic Programming to Evolve Backgammon Players. In *EuroGP 2005*, volume 3447 of *Lecture Notes in Computer Science*, pages 132–142. Springer Verlag, 2005.

[2] M. Heinze, D. Ortiz-Arroyo, H. L. Larsen, and F. Rodríguez-Henríquez. Fuzzeval: A Fuzzy Controller-Based Approach in Adaptative Learning for Backgammon Game. In *Mexican International Conference on Artificial Intelligence (MICAI)*, volume 3789 of *LNAI*, pages 224–233. Springer-Verlag Berlin Heidelberg, 2005.

[3] E. Heyken and M. B. Fischer. *The Backgammon Handbook.* Crowood Press (UK), 1990.

[4] J. H. Holland. *Adaptation in Natural and Artificial Systems.* University of Michigan Press, Ann Arbor, 1975.

[5] J. H. Holland. *Progress in Theoretical Biology in R. Rosen and F. M. Snell editors*, volume 4. Academic Press, 1976.

[6] J. B. Pollack, A. D. Blair, and M. Land. Coevolution of a backgammon player. In *Artificial Life V: Proceedings of the Fifth International Workshop on the Synthesis and Simulation of Living Systems*, pages 92–98. MIT Press, 1997.

[7] D. Qi and R. Sun. Integrating reinforcement learning, bidding and genetic algorithms. In *International Conference on Intelligent Agent Technology (IAT-2003)*, pages 53–59. IEEE Computer Society Press, Los Alamitos, CA, 2003.

[8] B. Robertie. *Backgammon For Winners, 3rd Edition.* Cardoza, 2002.

[9] S. Sanner, J. R. Anderson, C. Lebiere, and M. Lovett. Achieving efficient and cognitively plausible learning in backgammon. In *17th International Conference on Machine Learning (ICML-2000)*, pages 823–830. Morgan Kaufmann, 2000.

[10] C. E. Shannon. Programming a computer for playing chess. *Philosophical Magazine*, 41(314), 1950.

[11] G. Tesauro. Temporal difference learning and td-gammon. *Communications of the ACM*, 38(3):58–68, 1995.

[12] G. Tesauro. Comments on co-evolution in the successful learning of backgammon strategy. *Machine Learning*, 32:241–243, 1998.

SIBOS

Universo 07

www.sibos.com.mx

3er. Congreso

Tecnologías de Información y Comunicación

Expandiendo tus ideas

Realizado en la semana del 28 de mayo al 1ro. de Junio del 2007

FCC - BUAP

Memorias del Congreso

Administración y Seguridad de Sistemas Linux

Dr. Santiago Domínguez Domínguez
sdguez@cs.cinvestav.mx

CINVESTAV
Departamento de Computación
México, D.F.

Congreso de Tecnologías de Información y Comunicación,
SIBOS 2007

Esquema

1. Motivación
   - ¿Por qué es necesaria la seguridad en Linux?
2. Administración
   - Filosofía de la Administración de Sistemas
3. Seguridad
   - Física y Local
4. Servicios y Mecanismos de Seguridad
5. Amenazas a la Seguridad y Preparación para la Seguridad
6. Conclusiones

¿Qué es la seguridad Computacional?

Podemos entender como seguridad un estado de cualquier sistema (de cómputo o no) que nos indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo.

Seguridad en Cómputo

Un conjunto de recursos destinados a lograr que los activos de una organización sean confidenciales, íntegros, consistentes y disponibles a sus usuarios, autenticados por mecanismos de control de acceso y sujetos a auditoría.

¿Por qué es necesaria la seguridad en Linux?

- *Ante todo Linux es un sistema multiusuario real*
- *Lo habitual es que cada máquina linux esté conectada a una red y además esté prestando servicios de red*
- *La seguridad es un requisito básico, ya que la red global es insegura por definición*
- *Con el acceso masivo y barato a Internet se han reducido notablemente los costos de un atacante para asaltar un sistema en red, a la vez que ha aumentado paralelamente el número de potenciales atacantes*

¿Qué queremos proteger?

- *¿Qué queremos proteger?*
- *¿Qué valor tiene lo que queremos proteger?*
- *¿Qué costo tiene la seguridad?*
- *¿De quién nos queremos proteger?*
- *¿Cuáles son los puntos débiles de nuestro sistema?*

¿Qué queremos proteger?

- *¿Qué queremos proteger?*
- *¿Qué valor tiene lo que queremos proteger?*
- *¿Qué costo tiene la seguridad?*
- *¿De quién nos queremos proteger?*
- *¿Cuáles son los puntos débiles de nuestro sistema?*

¿Qué queremos proteger?

- *¿Qué queremos proteger?*
- *¿Qué valor tiene lo que queremos proteger?*
- *¿Qué costo tiene la seguridad?*
- *¿De quién nos queremos proteger?*
- *¿Cuáles son los puntos débiles de nuestro sistema?*

¿Qué queremos proteger?

- *¿Qué queremos proteger?*
- *¿Qué valor tiene lo que queremos proteger?*
- *¿Qué costo tiene la seguridad?*
- *¿De quién nos queremos proteger?*
- *¿Cuáles son los puntos débiles de nuestro sistema?*

¿Qué queremos proteger?

- *¿Qué queremos proteger?*
- *¿Qué valor tiene lo que queremos proteger?*
- *¿Qué costo tiene la seguridad?*
- *¿De quién nos queremos proteger?*
- *¿Cuáles son los puntos débiles de nuestro sistema?*

Filosofía de la Administración de Sistemas

Temas que conforman la filosofía de la administración

Aún cuando los detalles específicos en la administración de sistemas pueden variar entre las plataformas, hay temas subyacentes que no.

- Automatizar todo
- Documentar todo
- Comunicar tanto como sea posible
- Conocer sus recursos
- Conocer a sus usuarios
- Conocer el negocio
- La seguridad no puede ser una ocurrencia posterior
- Planifique
- Espere lo inesperado

Supervivión de Recursos

- Monitorizar el rendimiento del sistema
- Monitorizar la capacidad del sistema
- ¿Qué monitorizar?
  - Monitorizar el poder del CPU
  - Monitorizar el ancho de banda
  - Monitorizar la memoria
  - Monitorizar el almacenamiento
- Herramientas de monitoreo
  - free, top, vmstat
  - sysstat (iostat, mpstat, sadc, sar)
  - oprofile, nice
  - df, du

- Ancho de banda
  - Buses: IDE/ATA, SATA y SCSI
  - datapaths: CPU a caché en chip, procesador gráfico a memoria de video
- Poder de procesamiento
  - Hechos sobre el poder de procesamiento
  - Consumidores de poder de procesamiento
  - Mejorando la escasez de CPU
- Problemas potenciales
  - Recursos compartidos
  - Recurso dedicado con un número fijo de dispositivos conectados a él
  - Mejorando la escasez de CPU
- Soluciones potenciales
  - Distribuir la carga
  - Disminuir la carga
  - Aumentar la capacidad

Memoria física y virtual

- El espectro de almacenamiento
  - Registros del CPU
  - Memoria caché
  - Memoria principal (RAM)
  - Discos duros
- La memoria virtual
  - Fallos de página (los datos no están en RAM)
  - El conjunto de direcciones del trabajo (memoria física)
  - Intercambio (swapping)
- Implicaciones de rendimiento de la memoria virtual
  - Escenario del peor caso
  - Escenario del mejor caso

Administración del almacenamiento

- Características de los dispositivos de almacenamiento
- Preparar el almacenamiento para ser utilizado
  - Particiones/cuotas
  - Sistemas de archivos
  - Estructura del directorio
  - Activando el acceso al almacenamiento
- Tecnologías avanzadas de almacenamiento
  - Almacenamiento accesible a través de la red (NFS)
  - RAIDs
  - Administración de volumenes lógicos (LVM)
- Actividades diarias
  - Monitorizar el espacio libre: df, /etc/mtab, /proc/mounts
  - Problemas de cuotas de usuarios
  - Problemas relacionados a archivos
  - Añadir/Eliminar almacenamiento

Servicios de red

- Impresión
  - Tipos de impresoras
  - Ubicación: locales, en red
- Correo seguro
  - SPAM (SpamAssassin)
  - Remailers
  - Virus (Amavis)
- Web seguro
  - SSL (Secure Socket Layer)
  - S-HTTP (Secure HyperText Transfer Protocol)
  - Certificados

Administración de cuentas de usuarios y acceso a recursos

- Administración de cuentas de usuarios
  - El nombre del usuario
  - grupos y permisos
  - Contraseñas
  - Información de control de acceso
- Administración de recursos de usuarios
  - ¿Quién puede acceder a los datos compartidos?
  - ¿Dónde los usuarios acceden a los datos compartidos?
  - ¿Qué barreras se colocan para prevenir el abuso de los recursos?

Planificación para desastres

- Tipos de desastres
  - Fallas del hardware
  - Fallas del software
  - Fallas ambientales
  - Errores humanos
- Respaldos
  - Datos diferentes
  - Software de respaldo
  - Tipos de respaldo
  - Media de respaldo
  - Almacenamiento de las copias de seguridad
  - Problemas de restauración
- Recuperación de desastres
  - Creación de un plan de recuperación de desastres
  - Sitios de respaldo: frío, templado y caliente
  - Disponibilidad del hardware y software

Tecnologías de respaldo

- tar: the tar archiving utility
  - tar -czf /mnt/backup/home-backup.tar /home
- cpio: copy files to and from archives
  -
  - find /home/ — cpio -o > /mnt/backup/home-backup.cpio
- dump: ext2/3 filesystem backup
- restore: restore files or file systems from backups made with dump
- AMANDA (The Advanced Maryland Automatic Network Disk Archiver)

La seguridad física

Las primeras medidas de seguridad que necesita tener en cuenta son las de seguridad física de sus sistemas. Hay que tomar en consideración quiénes tienen acceso físico a las máquinas y si realmente deberían acceder.

Niveles exigibles de seguridad física para un sistema operativo

- *Un arranque seguro*
- *Posibilidad de bloquear las terminales*
- *Por supuesto, las capacidades de un sistema multiusuario real*

La seguridad física

Las primeras medidas de seguridad que necesita tener en cuenta son las de seguridad física de sus sistemas. Hay que tomar en consideración quiénes tienen acceso físico a las máquinas y si realmente deberían acceder.

Niveles exigibles de seguridad física para un sistema operativo

- *Un arranque seguro*
- *Posibilidad de bloquear las terminales*
- *Por supuesto, las capacidades de un sistema multiusuario real*

La seguridad local

El mayor porcentaje de violaciones de un sistema son realizadas por usuarios locales

Medidas de seguridad adicionales

- *control de acceso a los usuarios*
- *del sistema de archivos*
- *del núcleo*
- *de red*
- *del root*

La seguridad local

El mayor porcentaje de violaciones de un sistema son realizadas por usuarios locales

Medidas de seguridad adicionales

- *control de acceso a los usuarios*
- *del sistema de archivos*
- *del núcleo*
- *de red*
- *del root*

Control de acceso

- *La necesidad de restringir el acceso a ciertas áreas*
  - *cuentas de usuario, grupos*
  - *seguridad de las claves*
- *Impedir la ejecución de aplicaciones*
  - *desde sus Webs*
  - *el bit SUID/SGID*
  - *en el directorio temp*
- *Impedir el listado de directorios*

Control de acceso

- *La necesidad de restringir el acceso a ciertas áreas*
  - *cuentas de usuario, grupos*
  - *seguridad de las claves*
- *Impedir la ejecución de aplicaciones*
  - *desde sus Webs*
  - *el bit SUID/SGID*
  - *en el directorio temp*
- *Impedir el listado de directorios*

Control de acceso

- *La necesidad de restringir el acceso a ciertas áreas*
  - *cuentas de usuario, grupos*
  - *seguridad de las claves*
- *Impedir la ejecución de aplicaciones*
  - *desde sus Webs*
  - *el bit SUID/SGID*
  - *en el directorio temp*
- *Impedir el listado de directorios*

Gestión de claves

La generación, distribución, almacenamiento, tiempo de vida, destrucción y aplicación de las claves de acuerdo con una política de seguridad.

- *Generación de claves*
- *Distribución de claves*
- *Almacenamiento de claves*
- *Tiempo de vida de claves*
- *Destrucción de claves*

Seguridad del sistema de archivos

- *Una norma básica de seguridad radica en la asignación a cada usuario sólo de los permisos necesarios para poder cubrir las necesidades de su trabajo sin poner en riesgo el trabajo de los demás.*
- *¿Como se puede poner en riesgo el correcto funcionamiento del sistema?*
- *¿Cómo podemos mantener un almacenamiento seguro?*

Seguridad del sistema de archivos

- *Una norma básica de seguridad radica en la asignación a cada usuario sólo de los permisos necesarios para poder cubrir las necesidades de su trabajo sin poner en riesgo el trabajo de los demás.*
- *¿Como se puede poner en riesgo el correcto funcionamiento del sistema?*
- *¿Cómo podemos mantener un almacenamiento seguro?*

Seguridad del sistema de archivos

- *Una norma básica de seguridad radica en la asignación a cada usuario sólo de los permisos necesarios para poder cubrir las necesidades de su trabajo sin poner en riesgo el trabajo de los demás.*
- *¿Como se puede poner en riesgo el correcto funcionamiento del sistema?*
- *¿Cómo podemos mantener un almacenamiento seguro?*

El árbol de directorios

- *El sistema de almacenamiento de información en sistemas Unix se organiza en un único árbol de directorios.*
- *Un primer criterio para mantener un sistema seguro sería hacer una correcta distribución del espacio de almacenamiento.*
- *No hay unas normas generales aplicables; el uso al que vaya destinado el sistema y la experiencia son las bases de la decisión adecuada.*
  - *Si el sistema va a dar servicio a múltiples usuarios: /home*
  - *Si el equipo va a ser un servidor de correo, impresión, etc: /var, /var/spool*
  - *Algunos directorios son necesarios en la partición raíz: /dev, /etc, /bin, /sbin, /lib, /usr, /boot*
  - *El directorio /usr/local contiene los programas compilados e instalados por el administrador.*

El árbol de directorios

- *El sistema de almacenamiento de información en sistemas Unix se organiza en un único árbol de directorios.*
- *Un primer criterio para mantener un sistema seguro sería hacer una correcta distribución del espacio de almacenamiento.*
- *No hay unas normas generales aplicables; el uso al que vaya destinado el sistema y la experiencia son las bases de la decisión adecuada.*
  - *Si el sistema va a dar servicio a múltiples usuarios: /home*
  - *Si el equipo va a ser un servidor de correo, impresión, etc: /var, /var/spool*
  - *Algunos directorios son necesarios en la partición raíz: /dev, /etc, /bin, /sbin, /lib, /usr, /boot*
  - *El directorio /usr/local contiene los programas compilados e instalados por el administrador.*

El árbol de directorios

- *El sistema de almacenamiento de información en sistemas Unix se organiza en un único árbol de directorios.*
- *Un primer criterio para mantener un sistema seguro sería hacer una correcta distribución del espacio de almacenamiento.*
- *No hay unas normas generales aplicables; el uso al que vaya destinado el sistema y la experiencia son las bases de la decisión adecuada.*
  - *Si el sistema va a dar servicio a múltiples usuarios: /home*
  - *Si el equipo va a ser un servidor de correo, impresión, etc: /var, /var/spool*
  - *Algunos directorios son necesarios en la partición raíz: /dev, /etc, /bin, /sbin, /lib, /usr, /boot*
  - *El directorio /usr/local contiene los programas compilados e instalados por el administrador.*

Permisos

Linux, como sistema multiusuario, asigna un propietario y un grupo a cada archivo (y directorio) y unos permisos al propietario, al grupo y al resto de los usuarios.

- *Propiedad (usuario y grupo) y permisos (rwx)*
- *Sticky bit: drwxrwxrwt 19 root root 8192 Jun 24 14:40 tmp*
- *Atributo SUID: (para archivos)*
  -rw-r–r– 1 root root 1265 Jun 22 17:35 /etc/passwd
  r-s–x–x 1 root root 10704 Apr 14 23:21 /usr/bin/passwd
- *Atributo SGID: (para archivos)*
- *Atributo SGID: (para directorios)*
- *SUID Shell Scripts*

Permisos

Linux, como sistema multiusuario, asigna un propietario y un grupo a cada archivo (y directorio) y unos permisos al propietario, al grupo y al resto de los usuarios.

- *Propiedad (usuario y grupo) y permisos (rwx)*
- *Sticky bit: drwxrwxrwt 19 root root 8192 Jun 24 14:40 tmp*
- *Atributo SUID: (para archivos)*
  -rw-r–r– 1 root root 1265 Jun 22 17:35 /etc/passwd
  r-s–x–x 1 root root 10704 Apr 14 23:21 /usr/bin/passwd
- *Atributo SGID: (para archivos)*
- *Atributo SGID: (para directorios)*
- *SUID Shell Scripts*

Seguridad del sistema de archivos

- *Enlaces: duros y simbólicos*
- *Tripwire: Verifica la integridad de la información almacenada en los archivos para detectar ataques locales (y también de red) en su sistema.*
- *Limitar el espacio: Un ataque posible a cualquier sistema es intentar consumir todo el espacio del disco duro.*
  - *Una primera protección contra este ataque es separar el árbol de directorios en diversos discos y particiones.*
  - *Otra protección es controlar el espacio de almacenamiento por usuario o grupo.*

Normas prácticas

- *nosuid, nodev, noexec (/etc/fstab)*
- *Sistemas de archivos en red: NFS*
- *umask (022, 033 y 077 en /etc/profile)*
- *Limitar recursos (/etc/pam.d/limits.conf)*
- *wtmp, utmp (last)*
- *Sticky bit*
- *SUID,SGID:find / -type f /(-perm -04000 -o -perm -02000 /)*
- *Permisos de escritura global (find / -perm -2 -print)*
- *Archivos extraños: Los archivos sin propietario pueden ser un indicio de que un intruso ha accedido a su sistema (nouser)*
- *Archivos peligrosos: La localización de archivos .rhosts*

Normas prácticas

- *nosuid, nodev, noexec (/etc/fstab)*
- *Sistemas de archivos en red: NFS*
- *umask (022, 033 y 077 en /etc/profile)*
- *Limitar recursos (/etc/pam.d/limits.conf)*
- *wtmp, utmp (last)*
- *Sticky bit*
- *SUID,SGID:find / -type f /(-perm -04000 -o -perm -02000 /)*
- *Permisos de escritura global (find / -perm -2 -print)*
- *Archivos extraños: Los archivos sin propietario pueden ser un indicio de que un intruso ha accedido a su sistema (nouser)*
- *Archivos peligrosos: La localización de archivos .rhosts*

Normas prácticas

- *nosuid, nodev, noexec (/etc/fstab)*
- *Sistemas de archivos en red: NFS*
- *umask (022, 033 y 077 en /etc/profile)*
- *Limitar recursos (/etc/pam.d/limits.conf)*
- *wtmp, utmp (last)*
- *Sticky bit*
- *SUID,SGID:find / -type f /(-perm -04000 -o -perm -02000 /)*
- *Permisos de escritura global (find / -perm -2 -print)*
- *Archivos extraños: Los archivos sin propietario pueden ser un indicio de que un intruso ha accedido a su sistema (nouser)*
- *Archivos peligrosos: La localización de archivos .rhosts*

Normas prácticas

- *nosuid, nodev, noexec (/etc/fstab)*
- *Sistemas de archivos en red: NFS*
- *umask (022, 033 y 077 en /etc/profile)*
- *Limitar recursos (/etc/pam.d/limits.conf)*
- *wtmp, utmp (last)*
- *Sticky bit*
- *SUID,SGID:find / -type f /(-perm -04000 -o -perm -02000 /)*
- *Permisos de escritura global (find / -perm -2 -print)*
- *Archivos extraños: Los archivos sin propietario pueden ser un indicio de que un intruso ha accedido a su sistema (nouser)*
- *Archivos peligrosos: La localización de archivos .rhosts*

Normas prácticas

- *nosuid, nodev, noexec (/etc/fstab)*
- *Sistemas de archivos en red: NFS*
- *umask (022, 033 y 077 en /etc/profile)*
- *Limitar recursos (/etc/pam.d/limits.conf)*
- *wtmp, utmp (last)*
- *Sticky bit*
- *SUID,SGID:find / -type f /(-perm -04000 -o -perm -02000 /)*
- *Permisos de escritura global (find / -perm -2 -print)*
- *Archivos extraños: Los archivos sin propietario pueden ser un indicio de que un intruso ha accedido a su sistema (nouser)*
- *Archivos peligrosos: La localización de archivos .rhosts*

Normas prácticas

- *nosuid, nodev, noexec (/etc/fstab)*
- *Sistemas de archivos en red: NFS*
- *umask (022, 033 y 077 en /etc/profile)*
- *Limitar recursos (/etc/pam.d/limits.conf)*
- *wtmp, utmp (last)*
- *Sticky bit*
- *SUID,SGID:find / -type f /(-perm -04000 -o -perm -02000 /)*
- *Permisos de escritura global (find / -perm -2 -print)*
- *Archivos extraños: Los archivos sin propietario pueden ser un indicio de que un intruso ha accedido a su sistema (nouser)*
- *Archivos peligrosos: La localización de archivos .rhosts*

Normas prácticas

- *nosuid, nodev, noexec (/etc/fstab)*
- *Sistemas de archivos en red: NFS*
- *umask (022, 033 y 077 en /etc/profile)*
- *Limitar recursos (/etc/pam.d/limits.conf)*
- *wtmp, utmp (last)*
- *Sticky bit*
- *SUID,SGID:find / -type f /(-perm -04000 -o -perm -02000 /)*
- *Permisos de escritura global (find / -perm -2 -print)*
- *Archivos extraños: Los archivos sin propietario pueden ser un indicio de que un intruso ha accedido a su sistema (nouser)*
- *Archivos peligrosos: La localización de archivos .rhosts*

Normas prácticas

- *nosuid, nodev, noexec (/etc/fstab)*
- *Sistemas de archivos en red: NFS*
- *umask (022, 033 y 077 en /etc/profile)*
- *Limitar recursos (/etc/pam.d/limits.conf)*
- *wtmp, utmp (last)*
- *Sticky bit*
- *SUID,SGID:find / -type f /(-perm -04000 -o -perm -02000 /)*
- *Permisos de escritura global (find / -perm -2 -print)*
- *Archivos extraños: Los archivos sin propietario pueden ser un indicio de que un intruso ha accedido a su sistema (nouser)*
- *Archivos peligrosos: La localización de archivos .rhosts*

Normas prácticas

- *nosuid, nodev, noexec (/etc/fstab)*
- *Sistemas de archivos en red: NFS*
- *umask (022, 033 y 077 en /etc/profile)*
- *Limitar recursos (/etc/pam.d/limits.conf)*
- *wtmp, utmp (last)*
- *Sticky bit*
- *SUID,SGID:find / -type f /(-perm -04000 -o -perm -02000 /)*
- *Permisos de escritura global (find / -perm -2 -print)*
- *Archivos extraños: Los archivos sin propietario pueden ser un indicio de que un intruso ha accedido a su sistema (nouser)*
- *Archivos peligrosos: La localización de archivos .rhosts*

Normas prácticas

- *nosuid, nodev, noexec (/etc/fstab)*
- *Sistemas de archivos en red: NFS*
- *umask (022, 033 y 077 en /etc/profile)*
- *Limitar recursos (/etc/pam.d/limits.conf)*
- *wtmp, utmp (last)*
- *Sticky bit*
- *SUID,SGID:find / -type f /(-perm -04000 -o -perm -02000 /)*
- *Permisos de escritura global (find / -perm -2 -print)*
- *Archivos extraños: Los archivos sin propietario pueden ser un indicio de que un intruso ha accedido a su sistema (nouser)*
- *Archivos peligrosos: La localización de archivos .rhosts*

Seguridad del núcleo

Linux tiene la gran ventaja de tener disponible el código fuente del núcleo. Esto nos permite la posibilidad de crear núcleos a medida de nuestras necesidades.
Para compilar el núcleo primero tendremos que configurar las opciones que nos interesen.

- *Los fuentes del núcleo se guardan habitualmente en el directorio /usr/src/linux*
- *Ejecutar make menuconfig (o make xconfig si estamos en modo gráfico)*

Seguridad del núcleo: Opciones de compilación

- *IP: Drop source routed frames (CONFIG_IP_NOSR)*
- *IP: Firewalling (CONFIG_IP_FIREWALL)*
- *IP: forwarding/gatewaying (CONFIG_IP_FORWARD)*
- *IP: firewall packet logging (CONFIG_IP_FIREWALL_VERBOSE)*
- *IP: always defragment (CONFIG_IP_ALWAYS_DEFRAG)*
- *IP: syn cookies (CONFIG_SYN_COOKIES)*

Seguridad de red

La seguridad de las conexiones en red merecen en la actualidad una atención especial, incluso por medios de comunicación no especializados, por el impacto que representan los fallos ante la opinión pública.

- *inetd*
- *TCP Wrapper*
- *Incidencias*
- *Comunicaciones seguras*

Inetd

El demonio inetd escucha todos los intentos de conexión y atiende las solicitudes que se realicen a su máquina.

- *Las solicitudes de conexión van dirigidas a un puerto (número de servicio).*
- *Los servicios de red que presta están descritos en /etc/inetd.conf o /etc/xinetd.d*
- *Los números de puertos están en /etc/services*
- *hosts_options*

TCP Wrappers

Un servicio que verifica el origen de las conexiones con su base de datos

- /usr/sbin/tcpd
- /etc/hosts.allow (equipos autorizados)
- /etc/hosts.deny (equipos a los que se les deniega la conexión)
- /var/log/secure (registros de conexión)

Un consejo que es conveniente seguir: No tenga abiertos los servicios que no necesita; esto supone asumir un riesgo a cambio de nada. Tampoco limite la funcionalidad del sistema, si tiene que usar un servicio, hágalo sabiendo lo que hace.

Niveles de seguridad

Hasta aquí tenemos tres niveles de seguridad

- prestar un servicio,
- autorizar una conexión, y
- validar un usuario

Registro y conocimiento de incidencias

A parte de todo esto, puede conocer las incidencias que ocurren durante el funcionamiento del sistema. Por un lado conviene familiarizarse con los procesos que se ejecutan habitualmente en una máquina.

- */var/log/messages*
- */var/log/secure*
- *dmesg*

Comunicaciones seguras

Para mantener las comunicaciones seguras con el fin de garantizar la privacidad e integridad de la información.

- *SSH (Secure Shell), stelnet*
- *Cryptographic IP Encapsulation (CIPE)*
- *SSL*
  - *Cifrado de datos*
  - *Autenticación de servidores*
  - *Integridad de mensajes*
  - *Opcionalmente, autenticación de cliente*

Seguridad del root

A menudo, el mayor enemigo del sistema es el propio administrador del sistema, sí, tiene todos los privilegios y cualquier acción puede ser irreversible y hacerle perder posteriormente mucho más tiempo que el que hubiera perdido por realizar las tareas de forma segura.

Hábitos seguros

- *Usar la cuenta de root sólo para realizar tareas concretas y breves*
- *Acceder a los privilegios de root sólo cuando sean necesarios*
- *Limite las acciones que realice como root al mínimo imprescindible*

Servicios de Seguridad

Servicios de seguridad

- *Confidencialidad*
- *Autenticación*
- *Integridad*
- *No repudio*
- *Control de acceso*
- *Disponibilidad*
- *Auditoría*

Mecanismos de Seguridad

- *Intercambio de autenticación*
- *Cifrado*
- *Integridad de datos*
- *Firma digital*
- *Control de acceso*
- *Tráfico relleno*
- *Control de encaminamiento*
- *Unicidad*

Amenazas a la Seguridad

Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo).

Las cuatro categorías generales de amenazas o ataques son

- *Interrupción*
- *Intercepción*
- *Modificación*
- *Fabricación*

Ataques Pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida.

- *Obtención del origen y destinatario*
- *Control del volumen de tráfico*
- *Control de las horas habituales*

Ataques Activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos

- *Suplantación de identidad*
- *Reactuación*
- *Modificación de mensajes*
- *Degradación fraudulenta del servicio*

Preparación para la Seguridad

La seguridad es un proceso continuo, que requiere tener previsto hasta lo imprevisible. Tener unos buenos hábitos y tomar unas pequeñas precauciones nos ayudarán mucho.

- *Determinar los servicios activos*
- *Proteger los archivos importantes*
- *Software actualizado*
- *Prevenir pérdidas de información*

¿Qué hacer en caso de RUPTURA?

No es una situación agradable, y aunque siempre sería preferible que no hubiera sucedido, conviene tener en mente una serie de normas que nos permitan una actuación rápida y certera que disminuya las consecuencias del incidente.

- *Detección de un ataque activo*
  - *Ataque local*
  - *Ataque en red*
  - *¿Somos el destino del ataque o somos un punto intermedio?*
- *El ataque ha concluido*
  - *Tapar el agujero*
  - *Evaluación de los efectos del ataque*
  - *Avisar*

Políticas de seguridad

Política de seguridad se suele definir como el *conjunto de requisitos* definidos por los responsables directos o indirectos de un sistema que indica en términos generales *qué está y qué no está permitido* en el área de seguridad durante la operación general del sistema.

- Una política de seguridad puede ser:
  - *Prohibitiva* si todo lo que no está expresamente permitido está denegado.
  - *Permisiva* si todo lo que no está expresamente prohibido está permitido.
- Cualquier política ha de contemplar seis elementos claves en la seguridad de un sistema
  - *Disponibilidad, Utilidad, Integridad, Autenticidad, Confidencialidad y Posesión*

Firewalls

Los firewalls son dispositivos que evitan las entradas de extraños en una red, filtrando o rechazando las peticiones de conexión de hosts.

Tareas de los Firewalls

- *Filtrado y análisis de paquetes*
- *Bloqueo de protocolo y contenido*
- *Autenticación y encriptación de usuario, conexión y sesión*

- *¿Quién puede entrar?*
- *¿Qué puede entrar?*
- *¿Dónde pueden entrar?*
- *¿Cómo pueden entrar?*

Conclusiones

La seguridad en cómputo es un conjunto de planes y estrategias enfocadas a reducir los riesgos de un sistema de cómputo o de una organización.

- *Proteger a unos usuarios frente a otros y protegerse a sí mismo*
- *Garantizar el buen funcionamiento de los servicios del sistema*
- *Porporcionar un adecuado manejo de los recursos hacia los usuarios*
- *Resguardar y proteger los activos del sistema: confidenciales, íntegros, consistentes y disponibles a sus usuarios, autenticados por mecanismos de control de acceso y sujetos a auditoría.*

Paso a paso

Un pequeño guión sobre qué pasos hay que seguir para mantener nuestro sistema libre de intrusos, así como nuestros datos y servicios a salvo.

- *Limitar el acceso al equipo y desactivar las opciones de la BIOS*
  - *Poner contraseñas: BIOS, LILO o GRUP*
  - *Deshabulitar el arranque desde CD, USB u otro dispositivo externo.*
- *Particionamiento*
  - *Separar los datos de usuario de los del sistema*
  - *Poner nosuid, noexec, nodev mount options en /etc/fstab en las particiones ext2/3, así como en /tmp*

- *Cuestiones de seguridad local*
  - *Configuración del kernel*
  - *Parches del kernel: actualizaciones, SELinux*
  - *Configurar y activar los logs*
  - *Comprobar la integridad de los archivos*
- *Limitar el acceso a la red*
  - *Configurar ssh, desintalar telnetd*
  - *Deshabilitar o desactivar inetd*
  - *Desactivar todos los servicios de red innecesarios*
  - *Configurar el firewall y los tcpwrappers*
  - *Restringir uso del servidor ftpd*
  - *Establecer túneles ssh para el correo IMAP o POP*
  - *Asegurar BIND, Sendmail, y demás demonios (usando chroot)*
  - *Instalar snort o alguna herramienta similar de logs*

- *Buenas contraseñas y acceso seguro*
  - *Habilitar el enmascaramiento y el MD5*
  - *Instalar y usar PAM para poner mayores restricciones en el acceso*
  - *Establecer los límites en /etc/security/limits.conf (si no usamos PAM)*
  - *Actualizar /etc/login.defs si estamos usando MD5 o PAM*
  - *Desactivar el acceso como root desde la red; usar su o sudo*
- *Políticas de seguridad*
  - *Las políticas deben ser conocidas por los usuarios*
  - *Prohibir el uso de sistemas que no encripten las contraseñas*
  - *Usar quotas en disco*
- *Informar de fallos en la seguridad*
  - *Suscribirse a cuentas de correo de informes de seguridad*
  - *Mantener el sistema actualizado (usar cron)*

Gracias...