

Sumario

<i>Editorial</i>	3
<i>Arquitectura del Software</i>	4
<i>Distribuciones de Linux</i>	8
<i>Sistemas de Detección de Intrusos</i>	12
<i>Noticias y Eventos</i>	16
<i>Oferta y Demanda Tecnológica</i>	17
<i>Ayudas y Subvenciones</i>	18

EDITA:

ITI – Instituto Tecnológico de Informática

Universidad Politécnica de Valencia
CPI - Edif. 8G Acceso B
Camino de Vera s/n
46022 Valencia

Tel.: 96 387 70 69
Fax: 96 387 72 39
<http://www.iti.upv.es>
e-mail: actualidadtic@iti.upv.es

DISEÑA:

domino publicidad
<http://www.dominopublicidad.com>

IMPRIME:

GRUPO QUATREMEDIA
<http://www.quatremedia.com>
Tel.: 902 903 987

Depósito Legal: V-3279-2003**ISSN:** 1696 - 5876

Actualidad



Boletín Trimestral del Instituto Tecnológico de Informática, dedicado a las Tecnologías de la Información y las Comunicaciones.

Número > 6
Febrero 2005**Plan de Formación ITI 2005****FEBRERO**

Ingeniería del Software Orientada a Objetos y UML.- 24 h. Del 28/02 al 11/03. Lunes, Miércoles y Viernes de 16:00 a 20:00. Fin de matrícula: 25/02/05. Precio: 240 euros.

MARZO

Venta Orientada al Negocio.- 14 h Del 14/03 al 22/03. Lunes y Martes de 16:00 a 19:30. Fin de matrícula: 10/03/05. Precio: 168 euros.

ABRIL

Introducción al uso de redes inalámbricas.- 24h. Del 06/04 al 21/04. Miércoles y Jueves de 16:00 a 20:00. Fin de matrícula: 04/04/05. Precio: 240 euros.

Programación Orientada a Objetos: Java.- 32 h. Del 11/04 al 26/04. Lunes, Martes y Viernes de 16:00 a 20:00. Fin de matrícula: 08/04/05. Precio: 300 euros.

Acceso a Bases de Datos con Java.- 28 h. Del 27/04 al 05/05. Todos los días de 16:00 a 20:00. Fin de matrícula: 24/04/05. Precio: 250 euros.

MAYO

Programación WEB con Java: Servlets y JSPs.- 24 h. Del 09/05 al 16/05. Lunes a Viernes de 16:00 a 20:00. Fin de matrícula: 04/05/05. Precio: 240 euros.

Comunicaciones con Java.- 24 h. Del 17/05 al 02/06. Martes y Jueves de 16:00 a 20:00. Fin de matrícula: 13/05/05. Precio: 240 euros.

Introducción al Testeo.- 8 h. Del 18/05 al 20/05. Miércoles y Viernes de 16:00 a 20:00. Fin de matrícula: 13/05/05. Precio: 80 euros.

Planificación y estimación del testeo.- 12 h. Del 23/05 al 27/05. Lunes, Miércoles y Viernes de 16:00 a 20:00. Fin de matrícula: 19/05/05. Precio: 120 euros.

Desarrollo de aplicaciones para dispositivos móviles con J2ME.- 30 h. Del 30/05 al 10/06. Lunes, Miércoles y Viernes de 16:00 a 21:00. Fin de matrícula: 25/05/05. Precio: 350 euros.

Más información: Daniel Sáez
formacion@iti.upv.es

Editorial

En esta edición de ActualidadTIC le presentamos una nueva serie de contribuciones técnicas sobre algunos de nuestros temas de trabajo, junto con información actual sobre formación, noticias y convocatorias.

Una vez más, nos complace hacerle llegar esta nueva edición de ActualidadTIC, la revista trimestral del Instituto Tecnológico de Informática (ITI).

El ITI es un centro de I+D+i abierto, cuya vocación es la de contribuir a la mejora de la competitividad de las empresas del sector informático. Con este fin, el Instituto trabaja conjuntamente con empresas tecnológicas, desarrollando e implantando mejoras en sus procesos, productos y servicios.

Nuestros diferentes grupos de investigación cuentan con un alto grado de preparación y experiencia, y sus áreas de trabajo abarcan temas tan diversos como el reconocimiento de voz, la visión artificial, los sistemas distribuidos, el testeo y calidad del software, los sistemas adaptativos complejos, las tecnologías de la programación y las aplicaciones científicas.

Este número de ActualidadTIC ofrece una nueva serie de artículos técnicos que describen algunos de los temas de trabajo del ITI.

El primero de los artículos hace hincapié en la importancia de la arquitectura del software, un aspecto fundamental para todo proyecto de cierta envergadura. El artículo destaca las ventajas derivadas de prestar una adecuada atención a este aspecto a lo largo de todas las fases de un proyecto de software.

La segunda contribución versa sobre las distribuciones de GNU/Linux. El artículo pretende servir como introducción para un público general, deseoso de conocer las características de diversas distribuciones y la utilidad de las mismas para su uso cotidiano.

Por último, el tercer artículo técnico profundiza en un aspecto concreto de la Seguridad Informática: la detección de intrusos. En materia de seguridad es fundamental, además de la prevención, contar con métodos para determinar cuándo ha tenido lugar una intrusión, a ser posible en tiempo real. La última contribución técnica de este número describe la forma de funcionamiento de los sistemas de detección de intrusos, y presenta algunas de las herramientas disponibles.

Esperamos que estos artículos, así como la información de actualidad que incluye el boletín sean de su interés y utilidad.

El Instituto tiene una clara vocación de socio tecnológico. Una empresa puede aprovechar el *know-how* y experiencia del ITI para involucrarse en nuevos proyectos o simplemente añadir funcionalidades competitivas a sus productos y servicios. El ITI estudia las necesidades de cada proyecto concreto y colabora en la definición, desarrollo y búsqueda de posibles fuentes de financiación.

En este año que acabamos de comenzar queremos incidir más, si cabe, en intensificar la relación con nuestras empresas asociadas. En este sentido es importante para nosotros el recibir sus inquietudes y necesidades para poder ayudarles y ofrecer el mejor servicio.

Enrique Selma

**Director Comercial del Instituto
Tecnológico de Informática**

Arquitectura del Software: arte y oficio

La arquitectura de un software puede entenderse como aquella estructura del programa que cohesiona las funcionalidades más críticas y relevantes (necesarias para el sistema), y que sirve de soporte al resto de funcionalidades finales (necesarias para el usuario). Su especificación es ampliamente aceptada como el problema central de diseño de un sistema de software complejo. Uno de los principios de las metodologías modernas de desarrollo de software es priorizar la definición, el diseño, la implementación y la evaluación de la arquitectura del software. La esencia de este principio es dedicar los mínimos esfuerzos a implementar un prototipo estable de arquitectura que garantice la viabilidad del proyecto en las fechas más tempranas posibles. Este artículo reflexiona sobre la importancia de priorizar la arquitectura tanto para el producto de software como para el proceso de desarrollo, y sobre los beneficios potenciales que esta práctica puede reportar.

Introducción

Casi todos hemos observado alguna vez la construcción de un edificio. Comienza por los cimientos, luego las columnas y vigas, las distintas plantas, hasta tener un esqueleto de soporte. Después se construyen paredes, suelos, puertas y ventanas, instalaciones eléctricas y de fontanería, bancadas, etc. Basta un mínimo de sentido común para ni siquiera imaginar la posibilidad de levantar una pared antes que las columnas. En resumen, primero se crea la estructura o esqueleto del edificio, y luego se ensamblan las distintas partes. La primera sirve de soporte a las segundas, que aportan la mayoría de las funcionalidades básicas del inmueble. ¿Qué pasaría si se cometen errores en una u otra? Si se olvida construir una columna y se detecta al finalizar el edificio, probablemente este no obtenga nunca la cédula de habitabilidad. Sin embargo, si lo que se olvida es instalar una bañera o un armario empotrado se pierde solo una funcionalidad del inmueble (para el usuario final), pero indudablemente será habitable y dicho fallo será probablemente subsanable con un esfuerzo relativamente pequeño.

Esta forma de proceder es una estrategia general de solución de problemas en multitud de disciplinas sociales y técnicas. Una de ellas es la creación de software. A diferencia de la construcción de un edificio "común", el software no se rige por leyes físicas ni por procedimientos conocidos, sino que es inherentemente específico y experimental. Como indica su nombre, la característica principal del software es ser *soft*, es decir, flexible, elástico y, en general, muy específico para la solución de una tarea concreta, sobre sistemas de hardware concretos, por personal con actitudes, aptitudes, formación y experiencia concretas. Todo esto hace del diseño de un software particular una tarea generalmente única, creativa, con las incertidumbres y riesgos que ello conlleva.

Uno de los principios de las metodologías modernas de desarrollo de software es priorizar la definición, el diseño, la implementación y la evaluación de la arquitectura del software, que es como se conoce al esqueleto o estructura del sistema. Desde el punto de vista de qué debe hacer el software, la arquitectura se define a partir de un conjunto de requisitos críticos funcionales, de rendimiento, o de calidad. Considerando cómo el software debe dar solución a tales objetivos, la arquitectura constituye el problema central de diseño, es decir, el conjunto de estructuras, clases y atributos principales del software y sus interfaces de comunicación. Desde otro punto de vista más tangible, la arquitectura se materializa en el conjunto de componentes de código fuente y ejecutables que implementan

Priorizar la arquitectura aporta beneficios al proceso de construcción del software.

dicho esqueleto, lo que posibilita demostrar y evaluar en qué medida el diseño da solución a aquellos requisitos críticos.

Dado que no existe una teoría establecida sobre cómo proceder, el diseño, implementación y evaluación de la arquitectura de un software complejo puede realizarse a través de un proceso iterativo de prototipado, demostración y corrección. Este proceso permite atender y resolver en los inicios del proyecto los riesgos asociados a los requisitos más críticos y a las decisiones de diseño más difíciles, que son aquellos que más pueden comprometer el éxito del proyecto. Así, el equipo de desarrollo debe diseñar, construir y estabilizar primero la arquitectura del software antes de diseñar e implementar el conjunto de componentes elementales que se integran en la arquitectura y que aportan las funcionalidades finales de usuarios.

La esencia del principio de priorizar la arquitectura es dedicar los mínimos esfuerzos a garantizar la corrección de las partes más importantes, costosas e indefinidas del sistema, y cuyo prototipo permita una demostración tangible de la viabilidad del proyecto.

Descripción de la arquitectura del Software

El software tradicional, como único proceso ejecutándose en un único ordenador, no supone arquitecturas complejas ni grandes riesgos. Sin embargo, los sistemas actuales aprovechan componentes comerciales, código abierto, sistemas distribuidos, nuevos y diversos lenguajes de programación, entornos de alojamiento (hosting) y de ejecución remota, y otras dependencias externas, que convierten a la arquitectura de un sistema en su producto técnico más crítico.

Alcanzar una arquitectura estable que dé garantías sobre la viabilidad del proyecto, se considera el punto de transición entre lo que se suele denominar la fase de ingeniería

Arquitectura del Software: arte y oficio

(definición del producto y su solución) y la fase de producción (construcción, integración, evaluación y entrega del producto). En la primera se toman las decisiones más importantes mientras que en la segunda se realizan los mayores gastos y esfuerzos.

La clave del éxito y a su vez la dificultad del principio de priorizar la arquitectura consiste en definir qué es y qué no es la arquitectura. Si incluimos demasiados detalles perdemos la propiedad de configuración mínima necesaria (o más simple posible), que nos permite demostrar, con el mínimo esfuerzo y en fechas tempranas, la corrección de la solución diseñada. Si, por el contrario, definimos una configuración más simple de lo necesario, estaremos probablemente ignorando requisitos, riesgos, o interacciones críticas, lo cual impide dar garantías sobre el éxito del proyecto antes de realizar los mayores esfuerzos y gastos de la fase de producción.

Desde un punto de vista de gestión del proceso de desarrollo, podemos identificar dos dimensiones para manejar la arquitectura:

- descripción de arquitectura: subconjunto del modelo de diseño del software. Incluye elementos significativos de la arquitectura y excluye el diseño de las componentes básicas. Resuelve decisiones sobre qué desarrollar, qué reutilizar y qué comprar. Contiene notación ad hoc (textos y gráficos) necesaria para comprender los modelos. Debe incluir también los criterios de evaluación de la arquitectura.
- versión estable de arquitectura: subconjunto suficiente de componentes ejecutables que permiten demostrar lo antes posible que el método de solución (diseño, tecnología, tiempo y costes estimados) puede resolver satisfactoriamente la definición del producto (objetivos, alcance, rendimiento, beneficios, calidad).

Desde una perspectiva técnica, como se ha comentado antes, la arquitectura engloba requisitos críticos, decisiones de diseño, componentes de código fuente, y componentes ejecutables, información que debe ser modelada e incluida en el documento de descripción de arquitectura. Este contexto de información puede ser representado a través de las siguientes vistas y diagramas UML:

- vista de casos de uso: describe los casos de uso críticos de la arquitectura; puede ser modelado estáticamente a través del diagrama de casos de uso;
- vista de diseño: describe los componentes del modelo de diseño significativos para la arquitectura, es decir, aquellos que aportan la estructura y funcionalidad básica del sistema; puede ser modelado estáticamente mediante diagramas de clases y objetos;
- vista de proceso: describe interacciones en tiempo de ejecución de los componentes de la arquitectura en un entorno distribuido, incluyendo distribución lógica de procesos, hilos de control, comunicación entre procesos; puede ser modelado estáticamente a través del diagrama de distribución (*deployment diagram*);
- vista de componente: describe los componentes del conjunto de implementación (código fuente) significativos

para la arquitectura desde la perspectiva de los programadores; puede incluir componentes de prueba, comerciales, de simulación, que luego pueden o no ser considerados en la vista de entrega; puede ser modelado estáticamente a través del diagrama de componente.

- vista de entrega: describe los componentes ejecutables de la arquitectura, incluyendo la correspondencia entre procesos lógicos y recursos físicos del entorno de explotación; puede ser modelado estáticamente a través del diagrama de distribución.

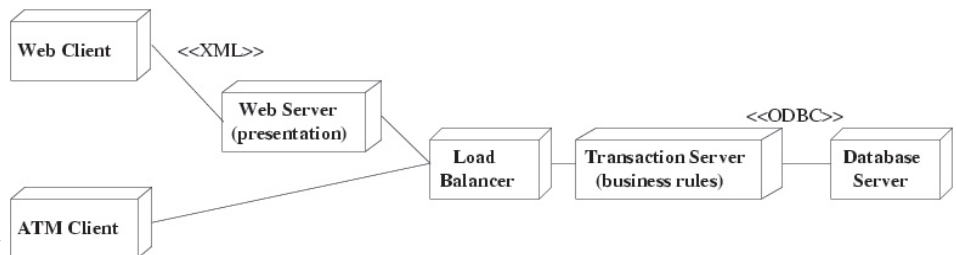


Figura 1: Ejemplo de diagrama de distribución (UML) de una arquitectura cliente-servidor. Muestra la relación entre los componentes críticos de mayor alcance ignorando detalles de bajo nivel del diseño. Fuente: Kazman et al., CMU/SEI-2004-TR-011, July 2004.

Las vistas de casos de uso y diseño son generalmente necesarias en cualquier sistema, mientras que las tres restantes dependen de la complejidad de su arquitectura. Todas las vistas pueden ser modeladas dinámicamente mediante los diagramas UML de comportamiento, es decir, los diagramas de secuencia, colaboración y actividad. Como se ha comentado antes, estas decisiones y diagramas deben incluirse, argumentarse y relacionarse en el documento de descripción de la arquitectura. A modo de referencia sobre qué aspectos considerar en la descripción de la arquitectura, la organización IEEE define el estándar IEEE Std 1471-2000 para tales efectos (ver http://standards.ieee.org/reading/ieee/std_public/description/se/1471-2000_desc.html).

Beneficios potenciales del principio de priorizar la arquitectura

La estrategia de priorizar la arquitectura aporta significativos beneficios en materia de corrección al proceso de construcción del software, entre ellos:

- evaluación de la solución (diseño + implementación) mediante demostraciones tangibles de sus capacidades desde fases muy tempranas de desarrollo;
- atención temprana a riesgos relacionados con la arquitectura que, generalmente, coinciden con aquellos que pueden conducir a mayores daños;
- propicia la construcción incremental del software (integración temprana) y las correspondientes actividades de verificación;
- propicia el desarrollo orientado a demostraciones periódicas de productos funcionales;
- interfaces correctas permiten una cooperación eficiente entre diseñadores e implementadores.

Arquitectura del Software: arte y oficio

En las siguientes secciones explicaremos con más detalle estos beneficios.

1. Evaluación basada en demostración

La razón principal que justifica priorizar la arquitectura es demostrar lo más pronto posible que la solución (el diseño) es correcta para resolver el objetivo (los requisitos). Como ya se comentó, la arquitectura es punto de transición entre la fase de ingeniería, donde se toman las decisiones más importantes, y la fase de producción, donde se aquellas decisiones se traducen en los mayores gastos del proyecto. En la primera intervienen usualmente un máximo de 2 ó 3 personas, quienes idean la solución y toman las decisiones críticas. En la segunda fase, un equipo de desarrolladores de tamaño variable en función de la complejidad del proyecto, colabora en la implementación de la solución durante un período de tiempo mayor.

La arquitectura es la materialización temprana, grosera y de mínimo coste de las decisiones más importantes. El prototipo ejecutable de arquitectura debe permitir demostrar que la solución ya es madura, es decir, que tales decisiones son efectivas para resolver los principales casos de uso del software que se va a construir antes de realizar los gastos ingentes asociados a la fase de producción, en la cual un equipo de desarrolladores implementará e integrará la mayor parte del código durante un período de tiempo casi siempre superior al de la fase de ingeniería. La arquitectura debe dar garantías de que la solución diseñada es realizable dentro de las restricciones de tiempo, personal, y presupuestos, o sea, que el proyecto es viable.

2. Atención a riesgos relacionados con la arquitectura

Otro principio esencial de los métodos actuales de desarrollo de software es la gestión de riesgos relacionados con el proceso de desarrollo o con el producto de software. Este principio significa identificar al inicio del proyecto las dudas e incertidumbres que existen sobre qué hacer o cómo hacerlo, y definir planes para investigarlas y resolverlas.

Si la arquitectura constituye los cimientos del software a construir, los riesgos relacionados con esta son lógicamente los más críticos del proyecto, es decir, aquellos que pueden producir los mayores errores o daños. Centrarse rápidamente en el diseño, implementación y estabilización de un prototipo de arquitectura implica tener que gestionar necesariamente dichos riesgos y resolverlos. Así estaremos eliminando las mayores causas potenciales de errores graves.

3. Integración temprana

Un tercer beneficio de priorizar la arquitectura es que propicia una estrategia incremental de construcción del

software como forma de aplicación del principio “divide y vencerás”.

Una arquitectura estable puede concebirse como una estructura de soporte del software, en la que se puedan ir integrando gradualmente las implementaciones de las diferentes funcionalidades finales. Cada nueva funcionalidad implementada e integrada es probada como unidad y como parte del todo en el que se inserta. Es decir, un nuevo requisito recién implementado puede ser inmediatamente validado desde la perspectiva del usuario en el contexto de la aplicación en el que se usará finalmente.

La integración temprana permite dosificar los esfuerzos de realización de tests de integración. Al integrar gradualmente cada funcionalidad en un prototipo de arquitectura previamente verificado y validado, la comprobación de la nueva funcionalidad dentro del prototipo se simplifica notablemente por reducirse las fuentes probables de error. Se deberá comprobar también que se mantiene la corrección de todo el prototipo en su interdependencia con la nueva funcionalidad.

4. Demostraciones periódicas a clientes y usuarios

Este procedimiento incremental de construcción garantiza que en cada instante del proceso de construcción del software exista un prototipo funcional validado, aunque parcialmente terminado. Así, cada prototipo parcial permitiría realizar demostraciones periódicas a clientes/usuarios finales con el propósito de detectar, tan pronto como aparezcan, desviaciones entre lo que estos esperan y el software implementado. Además, puede planificarse la construcción de forma que se priorice la integración de aquellas funcionalidades más útiles a clientes/usuarios, para crear versiones parciales usables por ellos. Esta forma de hacer facilita por tanto la visibilidad del progreso, es decir, el seguimiento y revisión de planes a través de la evaluación precisa de los estados parciales del producto. Existen otras dos ventajas adicionales de esta práctica. Por un lado, refuerza la moral del equipo de desarrollo al presenciar avances tangibles y frecuentes. Por otro lado, mejora sensiblemente la satisfacción y compromiso de clientes/usuarios al apreciar el desarrollo gradual de su producto, al sentirse partícipes del mismo, y al contar desde fechas tempranas con versiones usables, aunque incompletas.

5. Cooperación eficiente a partir de interfaces de módulos

La interfaz de un módulo de software se refiere a la forma en la que dicho módulo interactúa con el resto del sistema: cómo se identifica, cómo se activa, qué datos necesita, y qué resultados devuelve. La especificación correcta de las interfaces de los módulos de la arquitectura propicia la cooperación y el paralelismo en la implementación de estas partes. El responsable de cada parte observará el resto de las partes como cajas negras disponibles con las que sabrá cómo interactuar. En general dichas partes

Arquitectura del Software: arte y oficio

podrán desarrollarse en paralelo e integrarse posteriormente.

Conclusiones

Uno de los principios de las metodologías modernas de desarrollo de software es priorizar la definición, el diseño, la implementación y la evaluación de la arquitectura del software, que es como se conoce al esqueleto de soporte del sistema. La arquitectura implementa los requisitos más críticos a través de las estructuras de programa de mayor alcance en el sistema. Por ello la arquitectura encierra los mayores riesgos del desarrollo. La clave del éxito y, a su vez, la dificultad del principio de priorizar la arquitectura consiste en definir qué es y qué no es la arquitectura. Sus componentes deben ser los suficientes para garantizar la viabilidad del proyecto y, a su vez, los mínimos que permitan dar tales garantías con el mínimo gasto de tiempo, esfuerzo y recursos en general. Alcanzar una arquitectura estable reporta significativos beneficios al proceso de construcción del software, entre ellos la construcción incremental del software, la evaluación frecuente mediante demostraciones periódicas, la resolución de los riesgos más peligrosos en etapas tempranas, el aumento de la satisfacción y compromiso de clientes y usuarios,

Algunas referencias recomendables para ampliar información sobre la arquitectura del software:

<http://www.sei.cmu.edu/architecture/definitions.html>
<http://www.sei.cmu.edu/publications/documents/04-reports/04tr011.html>
<http://www-306.ibm.com/software/rational/uml/>
http://en.wikipedia.org/wiki/Software_architecture
<http://www.bredemeyer.com/whatis.htm>
<http://www.softwarearchitectureportal.org/WICSA/>

el mantener alta la moral del equipo de desarrollo, y una cooperación más efectiva entre sus miembros. A efectos prácticos, todo proceso de desarrollo de software, y en particular las metodologías de diseño y construcción, deben definirse a partir del reconocimiento de este protagonismo de la arquitectura dentro del producto de software y dentro del propio proceso.

Autor: Ramón Mollineda
 Más información:
otri@iti.upv.es

INSCRIPCIÓN ABIERTA

II JORNADAS DE TESTEO DE SOFTWARE

Una oportunidad para conocer las nuevas técnicas, modelos y metodologías que sirven para mejorar la calidad de nuestro software.

<http://www.iti.upv.es/JTS2005>
jts2005@iti.upv.es

21 y 22 de Abril de 2005
 Salón de Actos
 Centro de Desarrollo
 de Turismo
 Pº de la Alameda, 37
 Valencia

10% DESCUENTO PARA
 INSCRIPCIONES ANTES DEL 4
 DE MARZO

Colaboran:

COMPCWARE 

inQA.labs
 Software Testing 

Borland®

 UNIVERSIDAD
 POLITÉCNICA
 DE VALENCIA

Las II Jornadas sobre Testeo de Software, organizadas por el Instituto Tecnológico de Informática, contarán con la participación de expertos internacionales en el área de software testing así como con profesionales interesados en debatir y compartir experiencias sobre los cambios que se están produciendo en la calidad del software.

Objetivo:

Los beneficios que aporta un buen sistema de testeo de software incluyen el cumplimiento de plazos, la disminución de errores en el desarrollo e implantación, la reducción de costes y la mejora en la satisfacción del cliente.

La jornada pretende explicar la importancia y los fundamentos del testeo de software y describir los procesos básicos que cada compañía moderna de software debe implementar para garantizar cierto nivel de calidad en sus productos de software. Finalmente, la jornada se dirige a la presentación y explicación de técnicas, modelos y metodologías que se pueden utilizar para llevar a cabo un proceso básico de testeo.

Seminario complementario:

Con el fin de facilitar el aprovechamiento de las jornadas a todos los asistentes, se impartirá en forma independiente un seminario previo que tendrá por finalidad introducir los conceptos básicos del testeo. El seminario tendrá lugar el día 20 de abril de 16:00 a 20:00, en las instalaciones del ITI (Ciudad Politécnica de la Innovación, Edif. 8G, UPV - Camino de Vera S/N, Valencia).

Distribuciones de Linux

El sistema operativo GNU/Linux viene siendo una alternativa viable para todo tipo de usuarios. No solo por su coste, que puede llegar a ser nulo, sino también por ser una solución informática profesional de calidad, que puede ser utilizada tanto por empresas como por desarrolladores, o bien por usuarios sin experiencia.

La posibilidad de montar un sistema operativo a medida ha hecho que cualquier entidad que aporte una solución a un problema específico sea capaz de crear su propia distribución del sistema operativo. Hoy día ya se cuenta por centenas el número de distribuciones, lo que puede hacer que un usuario sin experiencia se encuentre indeciso a la hora de elegir la distribución que mejor se adapte a sus necesidades.

Este artículo define qué es una distribución, compara algunas distribuciones de GNU/Linux existentes y aporta algunos datos acerca de cómo elegir una distribución adecuada.

Introducción

Hoy más que nunca no solo se habla de, sino que también se utiliza GNU/Linux. Su utilización es cada vez mayor, tanto en empresas como para uso doméstico, impulsado por informáticos deseosos de obtener más provecho y control de sus ordenadores.

El creciente interés por este sistema operativo viene no solo por lo atractivo del precio, ya que no cuesta nada, sino también por sus cualidades para realizar tareas cotidianas, su fiabilidad y durabilidad, así como por un mejor funcionamiento en el caso de servidores y máquinas de altas prestaciones.

Siendo ya ampliamente utilizado como servidor en empresas por su robustez y fiabilidad, así como para la manipulación de imágenes en edición de películas y prensa escrita, GNU/Linux gana más funcionalidad a medida que se le exige. Para un usuario normal que necesita de un ordenador fácil de manejar y sin problemas, GNU/Linux ofrece soluciones que no siempre son del conocimiento general, ya que este sistema se mitifica como un sistema de alto nivel y propio para profesionales informáticos.

La posibilidad de montar un sistema operativo a medida de sus necesidades utilizando un *kernel* o núcleo del sistema específico o bien un núcleo general con aplicaciones específicas ha hecho que el número de distribuciones de GNU/Linux crezca día a día. En la actualidad se cuentan ya por centenas, lo que a la vista de un usuario común hace muy difícil saber qué tipos de distribuciones existen y cuál es la más conveniente.

**GNU/
Linux ofrece
soluciones para
profesionales de
la informática y
para el usuario
común.**

Una distribución GNU/Linux es un sistema operativo que reúne todo el software necesario para poner un ordenador a punto de uso. Está formado por un núcleo del sistema, que son programas que controlan cada uno de los dispositivos/componentes del ordenador, y un conjunto de aplicaciones diseñadas para los usuarios, como por ejemplo Netscape, Corel Draw o StarOffice.

En la actualidad existe una gran cantidad de distribuciones, en su mayoría creadas para satisfacer las necesidades concretas de colectivos determinados. Las distintas distribuciones GNU/Linux existentes hacen hincapié en temas tales como la facilidad de uso, la seguridad, las artes gráficas, etc.

Distribuciones Linux

Como ya hemos mencionado anteriormente, existe una infinidad de distribuciones, con lo cual resulta ser una tarea difícil para un usuario sin experiencia o incluso para una empresa sin personal cualificado elegir la distribución de GNU/Linux que mejor se adapte a sus necesidades.

Algunas más punteras como Suse, Red Hat, Conectiva, se atreven a sacar distribuciones preconfiguradas para que realicen distintos tipos de tareas, tales como servidor de correo, servidor web, almacén de datos, cortafuegos, etc. y que poseen una cantidad importante de aplicaciones.

Estas últimas están pensadas para usuarios de ordenador con necesidades básicas y de uso cotidiano como pueden ser editar textos, navegar por internet, ver películas o televisión, oír la radio o música... En fin, para uso personal o doméstico.

Distribuciones profesionales

Una distribución profesional viene a ser una distribución con más parámetros de configuración, cuyo usuario sabe



Distribuciones de Linux

exactamente lo que quiere y cómo hacerlo, lo que produce un sistema operativo estable y más eficiente.

En general son distribuciones utilizadas por programadores experimentados, dirigidas a desarrolladores de aplicaciones y profesionales informáticos con experiencia. Es el caso de las distribuciones Slackware, Gentoo o Debian, tres distribuciones en las cuales el profesional configura el sistema a su medida optimizando sus programas para que sea un sistema más estable, eficiente, rápido y seguro. No todo es tan fácil, sin embargo. Para conseguir esta precisión es necesario ser un informático experto o haber leído mucha documentación.

Distribuciones “a la carta”

Otra categoría está formada por las distribuciones de carácter específico, es decir, creadas con objetivos concretos y con propósitos determinados. Es el caso de Lliurex, Guadalinux o Linex, distribuciones creadas por las comunidades autonómicas de Valencia, Andalucía y Extremadura, respectivamente, que tienen por finalidad la promoción del desarrollo de software libre y la utilización de esa tecnología para la educación y formación en la cultura del software libre.

Existen otras aún más específicas, como es el caso de la distribución LRP (Linux Router Project), un GNU/Linux proyectado para una función específica de encaminador (*router*) de red.

El Instituto Tecnológico de Informática ha adquirido considerable experiencia en este campo a lo largo de los años dedicados a los sistemas GNU/Linux y otros sistemas de la gama UNIX. En la actualidad el Instituto trabaja en un proyecto destinado a la construcción de distribuciones de GNU/Linux dirigidas a empresas. El proyecto pretende crear distribuciones a medida para las empresas y tiene por finalidad el desarrollo de herramientas que faciliten la configuración y utilización de aplicaciones en GNU/Linux. Otro objetivo a destacar es el de crear distribuciones según las especificaciones del cliente, aprovechando todo el potencial del equipamiento de que este disponga. Esa iniciativa solo es posible gracias a que GNU/Linux es un sistema altamente flexible y configurable.

Distribuciones intuitivas

Las distribuciones de fácil manejo como Mandrake, Free-
windows o Lycoris son una nueva tendencia en este tipo de sistemas. Desarrolladas en un principio para el usuario sin experiencia y con gran facilidad de uso, vienen destacándose como la opción para aquel usuario que quiere un ordenador fiable sin necesidad de conocimientos informáticos para usarlo. El gran atractivo de ese tipo de distribución es la facilidad de configuración y usabilidad del sistema. Buscando crear aplicaciones intuitivas, son ya conocidas por una mayoría de usuarios de informática en general. Instalando cualquiera de estas distribuciones el usuario es capaz de configurar y mantener su ordenador, simplemente pulsando botones en la pantalla.

Viene a ser una mezcla entre la estabilidad proporcionada por su estructura fiable y consolidada, junto a programas intuitivos y fáciles de utilizar.

Distribuciones autoarrancables

Son distribuciones de ámbito general, utilizadas por usuarios curiosos por conocer lo que es un sistema operativo GNU/Linux, y muy bien aprovechadas por usuarios informáticos para corrección de errores en discos duros, configuración de ordenadores o bien para recuperar datos de una máquina teóricamente “muerta”.

Este tipo de distribuciones son autoarrancables, o sea, son distribuciones preinstaladas en un CD normal, que no necesitan copiar ningún programa en el disco duro del ordenador. El usuario debe solamente arrancar el ordenador con el CD puesto y su sistema estará listo para usarse. Distribuciones como Knoppix, Kurumin o Gentoo son ejemplos de este tipo de distribución.

Propiedades

Para que un usuario pueda tener parámetros con que comparar, haremos una pequeña comparativa entre algunas características de las distribuciones más populares del mercado.

Sistemas abiertos

En general el mantenimiento del software está a cargo de los desarrolladores del producto, que en el caso de sistemas abiertos pueden ser un equipo de desarrollo de un instituto científico o un grupo de programadores expertos.

La comunidad científica unida por internet colabora de forma significativa y bastante presente en la comunidad GNU/Linux con correcciones y pruebas de estas aplicaciones, facilitando así las correcciones y una mejor calidad.

Sin embargo muchas distribuciones poseen un equipo de desarrollo propio, responsable del mantenimiento de estos productos. Es el caso de Suse, Red Hat, Conectiva, Debian etc.

Transparencia

Uno de los actuales objetivos de las empresas o grupos de desarrolladores de GNU/Linux es conseguir la transparencia del sistema para el usuario. El objetivo es que los usuarios no tengan que preocuparse de qué tipo de máquina está ejecutando, sino simplemente utilizar sus aplicaciones con la finalidad de desarrollar su trabajo. Esa filosofía es una realidad en otros sistemas para funciones específicas, como es el caso del sistema MacOS utilizado por ejemplo para diseños en arquitectura de grandes empresas.

Flexibilidad

Poder cambiar la funcionalidad de una máquina sin tener que realizar todo el trabajo de instalación y configuración es una propiedad que el gerente debe tener en cuenta.

Distribuciones de Linux

Los sistemas operativos GNU/Linux poseen esta propiedad por naturaleza, por trabajar con módulos cargables según la necesidad del cliente.

Confiabilidad

Utilizar una distribución que ofrezca la seguridad de un funcionamiento correcto es también un punto importante a la hora de elegir entre sistemas operativos.

Las innumerables colaboraciones de usuarios expertos en correcciones y tests hacen que conseguir una fiabilidad aceptable resulte más fácil. En ocasiones es incluso posible contactar directamente con los desarrolladores del producto para informar de un determinado problema.

Rendimiento

Para que sea factible un cambio de sistema, por venta-

joso que sea el nuevo producto, las prestaciones en este nuevo sistema deben superar con creces al anterior.

Las distribuciones GNU/Linux están demostrando ser un producto maduro a la hora de realizar trabajos con costes computacionales de medio a alto como por ejemplo editar imágenes, utilizar simuladores de cargas para aviones o coches, cálculos estadísticos, etc., creando la posibilidad de que empresas pequeñas puedan adquirir la tecnología necesaria para competir con empresas de gran envergadura.

Comparativa de Distribuciones

La Tabla 1 ofrece un listado de algunas de las distribuciones más conocidas, para facilitar al lector la identificación de la distribución más cercana a su entorno. Las distribuciones se encuentran clasificadas por su facilidad de uso, instalación, manual disponible, páginas del desarrollador y aplicaciones disponibles.

Distribución	Versión	Facilidad de uso e instalación	Aplicaciones distribuidas	Manuales de instalación disponibles	Página del desarrollador	Lista de mirror
Mandrake	10.1	Principiante	Alto contenido de aplicaciones instaladas por defecto	Inglés, francés, español, alemán, italiano, chino	www.mandrake.soft	---
Red Hat	Red Hat Enterprise	Principiante	Alto contenido de aplicaciones instaladas por defecto	Inglés	www.redhat.com	---
Conectiva	10	Principiante	Alto contenido de aplicaciones instaladas por defecto	Inglés, español, portugués	www.conectiva.com	www.br.debian.org/distrib/ftplist
Fedora	Core 3	Principiante	Alto contenido de aplicaciones instaladas por defecto	Inglés, español	fedora.redhat.com	fedora.redhat.com/download/mirrors.html
Suse	SUSE LINUX Professional, SUSE LINUX Enterprise Server 9, SUSE LINUX Retail Solution	Principiante	Alto contenido de aplicaciones instaladas por defecto	Alemán, inglés, español	www.suse.com	No disponible
Debian	3	Medio	Pobre contenido de aplicaciones instaladas por defecto	Inglés, español, portugués, catalán, italiano	www.debian.org	www.br.debian.org/distrib/ftplist
Slackware	10	Alta	Pobre contenido de aplicaciones instaladas por defecto, todas deben ser compiladas	Inglés	www.slackware.com	alphageek.dyndns.org/linux/slackware-mirrors.shtml

Tabla 1: Características de algunas de las distribuciones más conocidas.

Distribuciones de Linux

Ventajas y Desventajas

Cada sistema operativo, sea GNU/Linux u otro, posee características que lo hacen específico para un sector del mercado. Describiremos aquí algunas ventajas y desventajas de las distribuciones GNU/Linux en relación con el mercado y la ofimática.

Ventajas

- Adaptación del sistema: Cada usuario puede cambiar el sistema de acuerdo con sus necesidades.
- Independencia del proveedor: Muchas son las empresas o universidades que ofrecen distribuciones de GNU/Linux.
- Costes: Muchas distribuciones son gratuitas. Es posible bajarlas de internet o copiarlas libremente.
- Documentación: Cada distribución posee un conjunto de manuales que viene con el CD de instalación. Además de eso, hay otros dos grupos importante en la documentación de aplicaciones Linux, que son *The Linux Documentation Project* y *Free Software Foundation*.
- Mantenimiento: Por tratarse de un sistema con muchos desarrolladores de todo el mundo, los programas son masivamente probados y consecuentemente su reparación es más rápida.
- Impulso de la economía local: Cualquier empresa puede ofrecer servicios o aplicaciones utilizando tecnología GNU/Linux. Esa posibilidad fomenta la creación de software para las empresas de la región como es el caso de las distribuciones autonómicas, como Lliurex (C. Valenciana), Guadalinux (Andalucía), Linex (Extremadura), Molinux (Castilla la Mancha), Max (Madrid) y Augustux (Aragón), .

Desventajas

- Necesidad de un cambio de mentalidad: Con el uso masivo de aplicaciones ya consolidadas en el mercado, el cambio a nuevas aplicaciones tiende a ser más difícil, por razones comunes como el coste en formación de personal cualificado o el bajo rendimiento en los primeros meses de utilización de nuevas herramientas, entre otras.
- Uso poco extendido en ofimática: El temor al cambio hace que esa tecnología tarde más tiempo en llegar al mercado dificultando la adopción de las herramientas por parte de los usuarios.
- Aplicaciones poco intuitivas: Muchas de las aplicaciones distribuidas en las distribuciones no poseen una interfaz intuitiva y amigable, lo cual dificulta su utilización.
- Al no existir una empresa fuente en el mercado detrás de GNU/Linux, este sistema no inspira la suficiente confianza a algunas empresas para moverlas a trabajar en ese sentido, ya que el futuro parece incierto para aquellos que no conocen ese trabajo.

Enlaces de interés

A continuación listamos algunos enlaces de interés, re-

lacionados con el tema de las distribuciones de GNU/Linux:

- Documentación:

The Linux Document Project: www.tldp.org
Free Software Foundation: www.fsf.com

- Distribuciones adicionales:

Turbolinux: www.turbolinux.com
Yellowdog: www.yellowdoglinux.com
Unitedlinux: www.unitedlinux.com
Lliurex: www.lliurex.net
Guadalinux: www.guadalinux.org
Linex: www.linex.org
Knoppix: www.knopper.net/knoppix/index-en.html
Gentoo: www.gentoo.org
Kurumin: www.guiadohardware.net/kurumin
Ycoris: www.lycoris.com
Freedows: www.freedows.com.br
DemoLinux: www.demolinux.org
Vector: www.vectorlinux.com

- Otros:

El siguiente sitio web reúne numerosas distribuciones de GNU/Linux disponibles para su descarga. Son distribuciones preparadas para ser grabadas en un CD. Tras terminar su descarga y grabación, ha de iniciarse el proceso de instalación.

Distribuciones diversas: www.linuxiso.org

Conclusiones

La posibilidad de montar un sistema operativo a medida, ha hecho que cualquier entidad con recursos humanos disponibles y dispuesta a involucrarse en este campo, pueda aportar una solución a un problema específico de su empresa, creando una nueva distribución o bien remodelando alguna ya existente.

A medida que los formatos de intercambio de datos se vayan estandarizando y sean absorbidos por el mercado, las distribuciones GNU/Linux irán ganando más espacio en el campo de la ofimática, por ser más rápidas y fáciles de usar.

Autor: Félix García
 Más información: sidi@iti.upv.es

Sistemas de Detección de Intrusos

Los sistemas de detección de intrusiones, bien sea dispuestos como software que se ejecuta en servidores y estaciones de trabajo, bien instalados en la infraestructura de red, monitorizan la actividad de los sistemas en busca de violaciones de la política de seguridad, tales como ataques de denegación de servicio, sustracción o modificación de información delicada, etc. Este artículo hace una introducción los IDS y los clasifica por tipos.

Introducción

Las organizaciones dependen cada vez más de sistemas informáticos para su funcionamiento diario. La existencia de atacantes, tanto internos como externos, que pretenden acceder ilegítimamente a sistemas informáticos, sea para sustraer información confidencial, o para modificar o eliminar información, sea con un interés concreto o por simple entretenimiento, hace que la seguridad sea algo que ha de evolucionar a la par que la tecnología se desarrolla.

Los cortafuegos son una herramienta indispensable para hacer ejecutar las políticas de empresa, pero el hecho de que suelen realizar un análisis muy superficial de la información que circula por la red (generalmente, se quedan a nivel de red), hace que muchos ataques sean simplemente invisibles para ellos.

En los 80 comenzaron los primeros desarrollos de programas que monitorizaban el uso de sistemas y redes. En los últimos años se ha producido un avance muy grande en esta área, y la mayoría de las empresas dedicadas a la seguridad ofrecen productos para la detección de intrusiones.

Los sistemas de detección de intrusiones (IDS) están constantemente vigilando, e incorporan mecanismos de análisis de tráfico y de análisis de sucesos en sistemas operativos y aplicaciones que les permiten detectar intrusiones en tiempo real.

Un IDS puede ser un dispositivo *hardware* autocontenido con una o varias interfaces, que se conecta a una o varias redes; o bien una aplicación que se ejecuta en una o varias máquinas y analiza el tráfico de red que sus interfaces ven y/o los eventos generados por el sistema operativo y las aplicaciones locales.

Para hablar sobre detección de intrusiones hay que definir qué entendemos por intrusión. Las intrusiones se definen en relación a una política de seguridad: una intrusión es una violación de la política de seguridad establecida. A menos que se conozca qué está permitido en un sistema y qué no, no tiene sentido hablar de detección intrusiones.

De manera más concisa se puede definir una intrusión como un conjunto de acciones deliberadas dirigidas a comprometer la integridad (manipular información), confidencialidad (acceder ilegítimamente a información) o disponibilidad de un recurso (perjudicar o imposibilitar el funcionamiento de un sistema).

Clasificación de los IDS

Los IDS se pueden clasificar desde varios puntos de vista. A continuación describimos las diversas clasificaciones posibles.

El paradigma de detección de anomalías puede detectar incluso ataques desconocidos.

Tipos de detección

En primer lugar los clasificaremos según la manera en que detectan las intrusiones.

Categorizamos las intrusiones en dos tipos principales, cuya distinción es importante porque nos conducirán a sistemas de detección esencialmente muy diferentes.

- Los **usos indebidos** son ataques bien definidos contra debilidades conocidas de los sistemas. Se los puede detectar buscando la ocurrencia de determinadas acciones concretas.

- Las **anomalías** se basan en la observación de desviaciones de los patrones de uso normales en el sistema. Se las detecta construyendo previamente un perfil del sistema a monitorizar y posteriormente estudiando las desviaciones que se produzcan con respecto a este perfil.

Las intrusiones por uso indebido siguen patrones bien definidos, por lo que se pueden detectar realizando búsqueda de patrones en el tráfico de red y en los ficheros de registro.

Las intrusiones por anomalía se detectan observando desviaciones significativas del comportamiento habitual. Para ello se mide una serie de parámetros (carga de CPU, número de conexiones de red en una unidad de tiempo, número de procesos, entre otros). Considerando que una intrusión involucrará un uso anormal del sistema, se pueden detectar las violaciones de seguridad a partir de patrones anormales de uso.

Los detectores de anomalías conocen, bien porque han sido programados por un experto, bien porque han pasado por una fase previa de **aprendizaje**, la actividad que resulta "normal" en el seno de un sistema. Mediante métodos estadísticos se intentará posteriormente comparar la información recibida en cada instante con el modelo de actividad válida, y aquello que se aparte excesivamente será etiquetado como intrusión. Esta comparación se puede realizar por técnicas estadísticas, por sistemas expertos basados en reglas, con redes neuronales, o con algún otro tipo de reconocimiento de patrones que pueda emitir con una certeza razonable si una determinada secuencia de eventos en un sistema forma parte del funcionamiento ordinario del mismo.

Sistemas de Detección de Intrusos

Es difícil detectar intrusiones por anomalías. No hay patrones fijos que se puedan monitorizar, por lo que se usan aproximaciones “borrosas” que suelen producir altas tasas de error. La correlación de los datos recibidos por los sensores es en la actualidad un área de investigación sujeta a estudio. Se persigue minimizar el número de falsos positivos (falsas alarmas) y de falsos negativos (ataques reales que pasan inadvertidos al sistema).

El paradigma de detección de anomalías parece bastante potente, pues en principio es capaz de detectar todo tipo de ataques, incluso ataques desconocidos hasta la fecha de su ocurrencia. En el caso de sistemas basados en reglas, exigen de un experto que pueda introducir correctamente dicho conjunto, que ha de ser periódicamente actualizado conforme las prácticas varíen. En el caso de sistemas basados en aprendizaje puede ocurrir que un atacante varíe muy lentamente su comportamiento para hacer casar una actividad maliciosa dentro de lo aceptable por el nuevo modelo aprendido. Los sistemas informáticos son por naturaleza muy cambiantes y los detectores

La
detección de
“signaturas”
conocidas llega a
alcanzar tasas
despreciables de
falsos positivos.

de anomalías pueden producir una tasa de falsos positivos inaceptable.

En la práctica se han extendido más los detectores de usos indebidos, que se basan en una base de datos de ataques conocidos, con una serie de reglas o “signaturas” que caracterizan los ataques y que permiten aseverar con prácticamente total certeza que se está intentando perpetrar un ataque. Estos sistemas solo pueden detectar fallos conocidos, para los que se haya introducido la signatura correspondiente en la lista. Dado que cada día aparecen nuevas vulnerabilidades, es importante que estos sistemas dispongan de mecanismos para actualizar frecuentemente la base de signaturas.

Fuentes de información

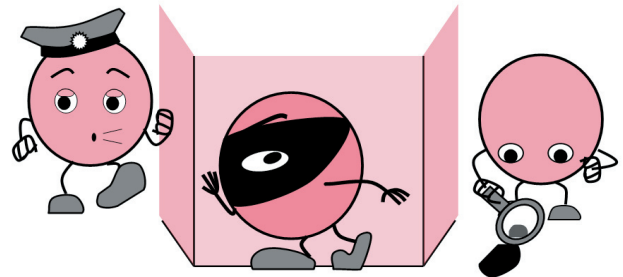
Dependiendo de las fuentes de información que se utilicen, los sensores usados por los IDS se clasifican en dos tipos: de red y de máquina. Cada tipo tiene unas capacidades diferentes en cuanto a los eventos detectables, por lo que en la práctica los IDS suelen nutrirse de sensores de ambos tipos. En la terminología tradicional de IDS, se habla de NIDS (Sistemas de Detección de Intrusos de Red) y de HIDS (Sistemas de detección de intrusos de máquina). En los sistemas híbridos o distribuidos, que abarcan más de un solo nodo, se habla de **sensores**: un solo sistema de detección de intrusiones puede alimentarse de más de un sensor. Como la mayoría de los sistemas de IDS comerciales son aparatos independientes dotados

de sensores de red que se conectan sin tener que instalar nada en ninguna otra máquina, se ha abusado bastante del término NIDS.

1. NIDS

Sistemas de detección de intrusos por red. Estos sistemas disponen de una o varias interfaces de red conectadas a determinados puntos estratégicos de la red. Monitorizan el tráfico que pasa por dichos puntos en busca de tráfico malicioso. Aunque estos sistemas en principio son dispositivos absolutamente pasivos, con frecuencia se colocan los NIDS en cortafuegos y enrutadores, de manera que el propio sistema puede forzar el cierre de conexiones y modificar reglas de filtrado de una manera más directa. Mediante uno solo de estos sistemas se puede monitorizar el tráfico tanto interno como externo de una red para muchas máquinas.

Los NIDS no suelen controlar toda la red sino determinados puntos estratégicos. La mayoría de las redes hoy en día son conmutadas, así que colocar los sensores de red suele implicar utilizar conmutadores especiales con un puerto “monitor” que reproduce todo el tráfico recibido en cualquiera de los puertos.



Los IDS, correctamente utilizados, ayudan a mejorar la seguridad de nuestras redes, pero no debemos descuidar los cortafuegos ni dejar de actualizar el software de las máquinas.

Este tipo de sistemas son bastante rápidos de instalar y mantener, y no dependen del sistema operativo instalado en las máquinas cubiertas. Suelen ser invisibles para los atacantes, por lo que los registros de sucesos que almacenan son poco vulnerables a la eliminación o alteración maliciosa, y suponen un recurso valioso para el almacenamiento de pruebas.

Diferentes ubicaciones de los NIDS nos proporcionarán diferentes perspectivas de la seguridad de la red. Colocados fuera del cortafuegos permiten evaluar los ataques que se intentan producir aunque no alcancen a los servidores internos, mientras que si se colocan en el interior del cortafuegos nos permiten evaluar si este está bien configurado.

2. HIDS

Sistemas de detección de intrusos de máquina. Así como los NIDS se instalan en determinados puntos de la infra-

Sistemas de Detección de Intrusos

estructura de red, los HIDS se instalan en las máquinas que componen la red: tanto servidores como estaciones de trabajo. Un sensor, instalado directamente como un módulo sobre una máquina, dispone de información de mayor nivel semántico que los NIDS: llamadas al sistema, eventos complejos dentro de aplicaciones de alto nivel, etc. Un sistema basado únicamente en red tendría que ser mucho más complejo para “entender” la gran diversidad de protocolos que existen, y los que se implementan por encima de éstos. Por otra parte, la tendencia actual al uso de conexiones encriptadas, de indiscutible interés para mejorar la seguridad de los sistemas, hace que un sistema que solo escuche la red disponga de muy poca información para distinguir el tráfico malicioso del aceptable. El tráfico en una conexión SSH o SSL es absolutamente inaccesible a un NIDS, aunque en el caso de SSL se han desarrollado cortafuegos que interceptan las conexiones, realizando una especie de ataque “hombre en el medio” que le permite analizar el contenido de conexiones que de otra manera sería inaccesible.

Los HIDS tienen acceso a los archivos de registro de lo que realmente sucedió, por lo que pueden conocer de manera fiable si un ataque fue exitoso o no, información generalmente no disponible para los NIDS.

Un sensor de máquina dispone de información específica del sistema y las aplicaciones, como inicios/cierres de sesión, acceso a ficheros, llamadas al sistema (pueden utilizarlas para saber el disco libre, la ocupación de la red, etc), y otros eventos, incluyendo aquellos que se originan localmente sin generar tráfico de red.

Tienen sobre los NIDS la ventaja de que permiten acceder a la información que por la red transita encriptada y que por lo tanto es opaca a ellos (p. ej., peticiones HTTPS inválidas).

Modo de análisis	Detectores de usos indebidos	
	Detectores de anomalías	
Tipo de sensores	De red	
	De máquina	Sistema operativo
		De aplicación
		Hardware
Tiempo de ejecución	Periódicos	
	De tiempo real	
Tipo de respuesta	Activos	
	Pasivos	
Arquitectura	Centralizados	
	Distribuidos	

Tabla 1: Posibles clasificaciones de los Sistemas de Detección de Intrusos.

Periódicos o de tiempo real

Así como los NIDS suelen dar respuesta en tiempo real, los primeros HIDS se ejecutaban periódicamente para

buscar indicios de intrusión. Después se fue reduciendo el intervalo entre la ocurrencia del evento y su análisis, hasta el punto que es posible gestionar los eventos en el instante de su registro. Los sistemas de red implementados como parte de la pila de red de las máquinas protegidas ofrecen las mismas prestaciones de respuesta inmediata (con posibilidad de cancelación de conexiones) que los NIDS.

Activos o pasivos

Los primeros IDS eran pasivos, se limitaban a informar de los intentos de intrusión al administrador. De poco sirve detectar un ataque para que horas después el administrador reciba un mensaje que informe de que se vio la intrusión pero no se intentó hacer nada por abortarla. Los IDS activos son capaces de tomar acciones correctivas orientadas a detener ataques en el mismo instante en que se producen.

Centralizados o distribuidos

Cuando la red de una organización adquiere una envergadura determinada, ya no es factible analizar todo el tráfico en un solo punto sin producir una degradación del rendimiento. En tal caso se instalan sistemas distribuidos, que disponen de varios sensores repartidos por diversas máquinas y puntos de la red, que se comunican con un nodo central donde se reciben todas las informaciones relevantes y donde se cruzan los datos para disponer de una visión más amplia del sistema como conjunto y detectar con mayor fiabilidad eventuales ataques. Esto permite producir además una única respuesta a intrusiones visibles desde varios puntos de la red.

Evasión de IDS

Es posible que el sistema no sea capaz de detectar una determinada instancia de ataque conocido al ser incapaz de encontrar la coincidencia con el patrón de búsqueda, si el atacante se las arregla para introducir pequeñas variaciones en su interacción con la máquina precisamente con el objetivo de evadir el IDS. Por ejemplo, algunas estrategias de evasión explotan leves diferencias en la manera en que la pila TCP reensambla fragmentos, o la manera en que se procesan paquetes inválidos, etcétera. La mayoría de los productos IDS de hoy en día incluyen protecciones contra las técnicas de evasión de IDS.

Sistemas de decepción

Son un tipo especial de sistema de detección de intrusiones orientados a atraer la atención de potenciales intrusos para que no ataquen a los sistemas reales y para obtener información acerca de sus métodos. Son los llamados *honeypots* (tarros de miel): máquinas simuladas, verosímiles y relativamente poco ocultas. Dado que ningún usuario legítimo debería querer jamás intentar conectarse

Sistemas de Detección de Intrusos

a un *honeypot*, toda conexión al mismo puede informarse inmediatamente y etiquetarse como un intento de intrusión. Los *honeypots* están configurados para registrar los eventos extensamente. La irrupción de un intruso en estas máquinas permite a los administradores obtener información sobre su *modus operandi*, e incluso recabar pruebas o indicios que pudieran inculpar al delincuente en un juicio.

Análisis forense

Los IDS ofrecen un interesante servicio para el análisis forense después de la consumación de ataques. Es posible que un IDS no haya sido capaz de detener la acción de un atacante, pero sí puede haber guardado un registro de los mensajes que transitaron por la red a tal efecto. Aunque cualquier atacante que tenga cierto nivel hará todo lo posible por borrar sus huellas, falsificar direcciones, explotar máquinas de terceros para enmascararse, etcétera, toda información que se almacene puede ayudar a seguir la pista del atacante, a mejorar los sistemas de detección y reacción automatizada a dichos ataques, e incluso como indicios ante instancias judiciales.

Algunas herramientas disponibles

Snort

Snort, uno de los sistemas más utilizados actualmente, es un sistema de código abierto de detección de intrusiones de red, capaz de llevar a cabo análisis de tráfico en tiempo real y registro de paquetes en redes IP. Puede efectuar análisis de protocolos, búsqueda de cadenas o patrones en el contenido y puede utilizarse para detectar una gran variedad de ataques y sondeos, tal como desbordamientos de búfer, escaneos invisibles, ataques CGI, sondeos SMB, intentos de determinación del sistema operativo, y otros.

Snort utiliza un flexible lenguaje de reglas para describir el tráfico que debería recoger o pasar, así como un motor de detección que hace uso de una arquitectura de plugins modular. Entre su base de reglas incluye miles de comprobaciones en busca de ataques de denegaciones de servicio. Ofrece la posibilidad de alertar en tiempo real, al incorporar mecanismos para registrar a syslog, a fichero, a sockets Unix, o mediante Samba, enviar mensajes emergentes a clientes Windows.

Además de ser un sistema completo de detección de intrusiones de red, sirve como analizador de paquetes al estilo de *tcpdump*, y como herramienta para registrar el tráfico. Se puede compilar en una veintena de plataformas distintas, tanto sistemas Unix como Win32.

Prelude

Snort es el IDS de red libre más potente, pero en su arquitectura no contempla la posibilidad de usar sensores de máquina, lo cual motivó la aparición del proyecto, tam-

bién libre, Prelude, que utiliza una arquitectura distribuida, con canales autenticados y encriptados, y sensores para diversos sistemas operativos. Prelude no pretende reinventar la rueda en IDSs de red, y de hecho es capaz de nutrirse de Snort, e incluso incluye él mismo un motor que utiliza los ficheros de reglas de su predecesor.

Intrudec

El ITI está desarrollando un prototipo de sistema de detección de intrusiones, Intrudec. Se trata de una arquitectura distribuida, con tolerancia a fallos, altamente modular, con soporte para sensores tanto de red como de máquina, que se comunican de manera segura para permitir la correlación de los diversos eventos ocurridos en distintos puntos de la red y en los distintos sistemas monitorizados. Para la correlación se utilizan diversos algoritmos, cuyo desarrollo y ajuste constituyen la labor de investigación principal del grupo de Sistemas Fiables en el área de la detección de intrusiones. Intrudec complementa al proyecto Tigerweb, que este grupo ha estado desarrollando y manteniendo en los últimos dos años. Tigerweb es un sistema de detección remota de vulnerabilidades accesible vía web que proporciona informes bien organizados y en castellano, orientados a ser entendidos por personal no experto en el área de la seguridad de los sistemas informáticos (Actualidad TIC, vol 2, págs. 4-7).

Futuro y conclusiones

Los IDS son una herramienta más que podemos utilizar para mejorar la seguridad de nuestros sistemas. Los IDS no reemplazan a los cortafuegos, ni nos evitan la tarea de mantener las máquinas actualizadas y correctamente configuradas.

Los propios IDS, en especial si se basan en búsqueda de patrones, han de mantenerse puntualmente actualizados. Las alertas generadas han de ser cuidadosamente analizadas para tomar las medidas pertinentes lo antes posible -de ahí la importancia de que los sistemas tengan una tasa baja de falsos positivos.

Existen actualmente fuertes críticas a los IDS estándar, por el hecho de que en principio un IDS detecta intrusiones pero no toma medidas correctivas. Esto ha llevado a algunos expertos a afirmar que los IDS no resultan eficaces, sobre todo considerando los costes de implantación y mantenimiento, y que su futuro puede ser virar hacia los IPS (Sistemas de Prevención de Intrusiones), productos combinados con cortafuegos que sí son capaces de adoptar medidas correctivas inmediatas (cortar conexiones, cambiar reglas de filtrado...).

Autor: Raúl Salinas

Más información: seguridad@iti.upv.es

Noticias y Eventos

Jornada para fomento de la participación en el VI Programa Marco

Los pasados días 27 y 28 de enero el ITI reunió a expertos internacionales en TI y pymes de la Comunidad Valenciana, en unas jornadas/taller con el objeto de fomentar la participación en proyectos del VI Programa Marco de la Unión Europea. Las jornadas contaron con la participación de la Dra. Tanja Vos (experta en Sociedad de la Información para PYMERA y directora del grupo SQuaC del ITI) y con la colaboración de PYMERA, RedIT, GAIA, CDTI y las ETIs PATENT y DETECT-IT.

Durante el encuentro se informó a las pymes sobre los diversos instrumentos y oportunidades de participación que existen en el VI Programa Marco, el principal instrumento de financiación de la I+D+i de las Pymes en el mundo, y las ventajas que ello implica.

La participación en estas iniciativas europeas supone la posibilidad de desarrollar investigación subvencionada al 50%, pudiéndola compaginar con otras subvenciones públicas nacionales o autonómicas, además de mejorar el posicionamiento tecnológico de la empresa frente a la competencia, así como la apertura a nuevos mercados y nuevas vías de cooperación.

Proyecto Europeo DeDiSys



El ITI participa como socio en el proyecto DeDiSys (Dependable Distributed Systems), iniciado el pasado mes

de octubre y financiado por el VI Programa Marco de la Unión Europea. El consorcio está formado por ocho socios, entre instituciones académicas y empresariales.

El proyecto DeDiSys pretende optimizar la fiabilidad en sistemas de software distribuidos basados en componentes. Los sistemas de software distribuidos son un factor dominante para el crecimiento económico sostenible de la UE, sirviendo como base para aplicaciones innovadoras. Los elementos claves para conseguir sistemas escalables y mantenibles son la fiabilidad y la disponibilidad, ya que de otro modo la complejidad de los sistemas distribuidos los haría incontrolables.

DeDiSys comprende una arquitectura, reglas para la integración de tecnología, servicios abiertos, métricas y métodos de evaluación bien definidos, así como el desarrollo de los prototipos necesarios. El objetivo es la integración entre infraestructuras existentes y componentes comerciales. Además, DeDiSys propone un método innovador para tratar los fallos de nodos y enlaces.

DeDiSys utiliza la replicación para conseguir tolerancia a fallos y persistencia de forma transparente, pero a diferencia de otras aproximaciones, se centra en el compromiso entre disponibilidad y consistencia mediante la hibridación de técnicas de replicación síncronas y asíncronas. Este compromiso puede ser medido y configurado específicamente para permitir el nivel óptimo de disponibilidad específico para cada aplicación.

Se espera que los resultados de este proyecto de investigación sean utilizables en aplicaciones para control de tráfico aéreo, así como para mejorar la fiabilidad y se-

guridad de aplicaciones en entornos móviles y sistemas distribuidos de control de acceso. En estas áreas están trabajando parte de las instituciones empresariales participantes en el proyecto.

Los administradores, desarrolladores, gerentes, etc. interesados en los sistemas distribuidos pueden formar parte del Grupo de Interés del proyecto.

Más información: <http://www.dedisys.org>

Participación en FOROSEC

El pasado 26 de enero ITI participó como experto en el área de seguridad informática en la Jornada FOROSEC. FOROSEC (Foro para la Seguridad de los Sistemas de Información) es una red temática en seguridad informática formada por cinco centros tecnológicos especializados en TIC y Seguridad de los Sistemas de Información, con el objetivo de proveer a las organizaciones de una red experta en seguridad enfocada a acercar las nuevas tecnologías para la seguridad, mejorar sus servicios de negocio electrónico e incrementar su competitividad y su capacidad tecnológica.

El Prof. Pablo Galdámez, responsable del Grupo de Seguridad y Sistemas Fiables del ITI, expuso la situación actual de los sistemas de seguridad y las nuevas tendencias. Entre otras cuestiones, su presentación destacó la conveniencia de implantar las medidas informáticas adecuadas para controlar los riesgos de seguridad, y repasó las amenazas que últimamente están creciendo de forma importante, que aprovechan vulnerabilidades de los programas instalados para realizar acciones en los equipos infectados sin que el usuario lo sepa.

Feria CeBIT

Entre los próximos días 10-16 de marzo, la ciudad alemana de Hannover acogerá la edición de CeBIT2005. Los responsables de la primera feria europea de las TIC han percibido la necesidad de "adaptar el evento a la nueva realidad de un sector que ya no crece a las cuotas que lo hacía en la segunda mitad de los años 90". De acuerdo con Reinhold Umminger, director de CeBIT, "el túnel de las TIC ha quedado atrás", aunque hay que esforzarse para no dejar el desarrollo del sector en manos de Asia y Norteamérica.

Desde su punto de vista, "Europa tiene un gran potencial porque somos 500 millones de ciudadanos caminando hacia la sociedad de la Ciencia", y anticipó, citando a Eito, que este año el sector cerrará con unos ingresos en Europa de 611.000 millones de euros, lo que supone un crecimiento del 3,1 por ciento con respecto al año previo. Vertebrada en esta ocasión en tres grandes áreas — telefonía móvil, software de empresa y electrónica de consumo — la nueva edición contará con la participación de 6.200 expositores, 32 de los cuales son españoles.

Más información sobre el evento en: <http://www.cebit.de>

Más información:

otri@iti.upv.es

Oferta y Demanda Tecnológica

Las siguientes Demandas y Ofertas Tecnológicas proceden de empresas innovadoras, Institutos Tecnológicos y Universidades de toda Europa y son promocionadas por la Red de Centros de Enlace para la Innovación (Red IRC).

Interesados, contactar con Carolina Quintá: otri@iti.upv.es



OFERTA DE TECNOLOGÍA

Ref. 25010503 - Servidor y terminales en red para grupos de trabajo. Una empresa alemana ha desarrollado una nueva plataforma. Se basa en un servidor con un máximo de 10 terminales conectadas, lo que permite reducir el número de licencias de software a adquirir. Los terminales pueden acceder a los programas y a los datos del servidor a través de una conexión RJ45. La plataforma está indicada para pequeños negocios y para entornos de formación. La empresa está interesada en alcanzar acuerdos de cooperación y comercialización con asistencia técnica.

Ref. 25010504 - Red M2M inalámbrica para el acceso remoto a través de Internet. Una empresa francesa ha desarrollado una tecnología para conectar varios aparatos de forma inalámbrica y para acceder a ellos de forma remota desde Internet. La tecnología permite gestionar desde Internet varios equipos remotos localizados en la misma zona. Varios nodos de radio conectan los aparatos a la red inalámbrica local y un gateway almacena, procesa y transmite los datos a Internet sin necesidad de utilizar un PC. La empresa está interesada en alcanzar acuerdos comerciales con asistencia técnica.

Ref. 24010503 - Software para la gestión integral de empresas. Una empresa gallega ha desarrollado un software para controlar y gestionar los procesos de negocio de cualquier tipo de empresa, desde el aspecto comercial hasta los aspectos financieros. Todos los módulos de la aplicación se interconectan perfectamente con el objetivo de conseguir un manejo sencillo. Las aplicaciones están basadas en un sistema cliente-servidor e integran diferentes bases de datos (Oracle, SQL Server, SQL Base, etc.) y funcionan en Windows 98, NT, etc. La empresa está interesada en alcanzar acuerdos de comercialización con asistencia técnica.

Ref. 24010514 - Cristales fotónicos para eliminar la luz de difracción. Un grupo de investigación de una universidad catalana ha desarrollado un método para eliminar la difracción de la luz utilizando cristales fotónicos. Este método mejora significativamente el rendimiento de diversos aparatos ópticos y permite reducir su tamaño en un orden de magnitud. Las aplicaciones incluyen microscopía, micro y nanolitografía y comunicaciones ópticas. El grupo de investigación busca socios industriales o centros de investigación para el desarrollo de aplicaciones con este método.

Ref. 21010502 - Software para el desarrollo y gestión de documentación de productos peligrosos. Una empresa belga ha desarrollado un software para el desarrollo y gestión de documentación internacional de

productos peligrosos. Este software cumple con los requisitos de seguridad en cuanto a la gestión de documentación y especialmente la relacionada con productos peligrosos. Permite generar diferentes tipos de informes en 30 idiomas y dispone de una base de datos con todas las sustancias peligrosas para diferentes sectores. El software está indicado para la industria química, farmacéutica, plásticos, cosmética e industrias que utilizan componentes peligrosos. La empresa está interesada en alcanzar acuerdos de licencia.

Ref. 21010507 - Sistema de reservas de cursos y de gestión logística para instituciones educativas. Una empresa finlandesa ha desarrollado un software para realizar la reserva en tiempo real de clases, cursos, profesores y otros recursos dentro de instituciones educativas. El sistema se estructura en tres niveles (funciones básicas de reserva con calendarios, funcionalidades adicionales como búsqueda de vacantes y sistema de reserva de conferencias con horarios), es flexible y de manejo sencillo y rápido. Incluye interfaces adaptadas a las necesidades del usuario así como funciones automáticas de alerta (SMS, e-mail). El software ha sido utilizado con éxito en el mercado local y ahora la empresa busca socios europeos para alcanzar acuerdos de licencia, "joint venture" o comercialización.

Ref. 19010506 - Pantalla con conexión de fibra óptica y sin suministro eléctrico. Un instituto alemán de I+D ha desarrollado una pantalla con conexión de fibra óptica para aplicaciones en las que no se necesita suministro eléctrico. Además de su flexibilidad, este aparato es inmune a las interferencias electromagnéticas, una característica de gran importancia para necesidades de entretenimiento en entornos industriales públicos y privados. Cada punto de la pantalla se puede iluminar con cualquier color posible. La luz se transmite a través de las fibras ópticas a una distancia hasta de 25 m. El instituto busca fabricantes y usuarios para alcanzar acuerdos de cooperación, licencia y comercialización con asistencia técnica.

Ref. 17010502 - Sistema para la emisión de Guías Electrónicas de Programas (EPG) en televisión interactiva digital. Una PYME alemana ha desarrollado un software basado en el estándar DVB para emisiones de televisión digital europea. Este software permite presentar en pantalla una guía de programas para la televisión digital. La información del programa proporcionada por los proveedores de contenidos es transformada en información que puede ser decodificada por las principales plataformas receptoras. Se trata de un software flexible y funciona independientemente de la plataforma utilizada. La empresa busca operadores de sistemas de emisión de televisión, editores y productores de receptores digitales para alcanzar diferentes acuerdos de colaboración.

DEMANDA DE TECNOLOGÍA

Ref. 25010511 - Hardware y software para aplicación GIS. Una empresa italiana ha desarrollado un servicio GPS para ayuntamientos y aplicaciones de geomarketing. Se trata de una aplicación GIS integrada para monitorizar el flujo del tráfico en las ciudades y hacer un seguimiento de los accidentes de vehículos y de la contaminación. La empresa busca socios para desarrollar el módulo del flujo del tráfico, producir el sistema de monitorización en carreteras y de información a los conductores y desarrollar el software para el sistema de navegación. También busca entidades de capital riesgo.

Ref. 24010501 - Software para básculas de cocina. Un inventor británico ha desarrollado una serie de básculas de cocina con lectura electrónica que actúa como un libro de cocina. El inventor busca una empresa que desarrolle un software para que se comuniquen entre sí el sistema de pesaje, un lector de tarjetas y la pantalla LCD. Sobre la pantalla se presentará un menú desplegable similar a los de los teléfonos móviles. La empresa debe tener experiencia en componentes electrónicos y visualización en pantallas LCD. El inventor está interesado en alcanzar acuerdos de "joint venture" o licencia.

Ref. 17010513 - Software para el mantenimiento de sistemas de gestión de la calidad. Una empresa chipriota especializada en sistemas de gestión de la calidad (ISO 9001:2000, HACCP e ISO 14000) busca un software para el mantenimiento de estos sistemas de gestión. El software debe reducir el papeleo necesario para la gestión de los sistemas. El producto buscado debe estar disponible en el mercado y debe controlar y administrar las auditorías internas y externas, las acciones correctoras y de prevención, los suministradores, las reclamaciones del consumidor, la calibración y mantenimiento de equipos, la formación y la revisión y retirada de documentos. La empresa desea alcanzar acuerdos de licencia y comercialización con asistencia técnica.

Ref. 14010514 - Monitorización tridimensional de heridas en tejidos blandos durante el proceso de regeneración. Una empresa británica fabricante de equipos médicos busca tecnología de monitorización tridimensional para medir la forma y el tamaño de heridas en tejidos blandos durante el proceso de regeneración, ante todo úlceras de presión y úlceras de pierna. La tecnología buscada no debe entrar en contacto con el tejido, debe ser segura y compatible con un uso portátil alimentado con baterías. La empresa, líder en la prevención, cicatrización y gestión de úlceras de presión, está interesada en alcanzar acuerdos de colaboración técnica o licencia.

Ayudas y Subvenciones

otri@iti.upv.es

Ámbito Nacional

INICIATIVA DE FORMACIÓN CONTINUA EN LAS EMPRESAS

Organismo: INEM - FONDO SOCIAL EUROPEO

Beneficiarios: Todas las empresas que tengan centro de trabajo en el territorio del Estado Español, con independencia de su tamaño y ubicación, que desarrollen formación para sus trabajadores y coticen por la contingencia de formación profesional.

Modalidad de participación:

• **Acciones de formación continua.**

Acciones relacionadas específicamente con el objeto social o actividad de la empresa y aquellas de carácter general, dirigidas a proporcionar competencias profesionales transferibles a otras empresas o ámbitos laborales, cuya ejecución se planifica, organiza y gestiona por las empresas para sus trabajadores, tanto con sus propios medios como recurriendo a contrataciones externas.

• **Permisos individuales de formación.**

Permiso que la empresa podrá conceder a un trabajador para recibir, en horario de trabajo, una formación dirigida a la mejora de su capacitación personal y profesional. Esta formación deberá estar reconocida por una titulación oficial.

Modalidades de las Ayudas: Las empresas que cotizan por la contingencia de formación profesional dispondrán de un crédito anual para la formación continua. Las empresas que concedan permisos individuales de formación dispondrán de un crédito adicional de hasta un 5% respecto de su crédito anual para la formación continua.

Plazo: Acciones formativas a partir del 02/03/2004. Las acciones formativas iniciadas a partir del 01/01/2004 y con anterioridad a la fecha de entrada en vigor de la Orden, podrán ser bonificadas sin que les sea de aplicación el requisito de comunicación a la Fundación Estatal.

PROGRAMA DE INCORPORACIÓN DE DOCTORES Y TECNÓLOGOS A EMPRESAS: TORRES QUEVEDO

Organismo Gestor: MCYT-FONDO SOCIAL EUROPEO

Beneficiarios: Empresas, Centros Tecnológicos y Asociaciones Empresariales con un centro de trabajo en terreno nacional al que se incorporarán los investigado-

res contratados, y que deseen realizar un proyecto de investigación industrial, de desarrollo tecnológico o un estudio de viabilidad técnica previo.

Actuaciones apoyables: Contratación de Doctores o Tecnólogos (retribución bruta más cuota empresarial de la Seguridad Social correspondiente).

Requisitos de ayuda: En el caso de los Centros Tecnológicos y Asociaciones empresariales, el puesto de trabajo ofertado deberá responder a las demandas de las empresas del sector en el que se enmarque el Centro Tecnológico. En el caso de grandes empresas, las ayudas deberán aplicarse para llevar a cabo actividades de I+D+I adicionales respecto de las que venga realizando la empresa.

Plazo: Hasta el 30 de Julio de 2005.

FINANCIACIÓN DE PROYECTOS DE I+D+I EMPRESARIALES

Organismo Gestor: Centro para el Desarrollo Tecnológico Industrial (CDTI)

Beneficiarios: Sociedades Mercantiles con capacidad técnica para desarrollar un proyecto de I+D+i y capacidad financiera para cubrir con recursos propios un mínimo del 30% del presupuesto.

Actuaciones apoyables:

1. Proyectos de Desarrollo Tecnológico
2. Proyectos de Innovación
3. Proyectos de Investigación Industrial Concertada

Tipo de ayuda: Créditos a tipo de interés "cero", con largo plazo de amortización, que cubren hasta el 60% del presupuesto total. El Centro solo apoya proyectos viables, pero no exige garantías reales para la concesión de sus créditos. La financiación proviene básicamente de los recursos propios del Centro y del Fondo Europeo de Desarrollo Regional (FEDER). Estos créditos incluyen una cláusula de riesgo técnico según la cual, en caso de que el proyecto no alcance sus objetivos técnicos, la empresa queda exenta de reintegrar la totalidad del préstamo.

PROGRAMA ARTE/PYME II

Organismo Gestor: MCYT - FONDO SOCIAL EUROPEO

Objetivo: Integración de las PYME en la Sociedad de la Información, cofinanciando proyectos basados en el comercio electrónico que involucren la utilización de Servicios Avanzados de Telecomunicaciones (SAT) para satisfacer necesidades comunes de colectivos de PYME.

Beneficiarios:

1. Organizaciones públicas o privadas que, sin ánimo de lucro, tengan la finali-

dad de prestar servicios de apoyo a las PYME, mediante la realización de proyectos comunes de asistencia o la promoción de servicios.

2. *Agrupaciones de interés económico de empresas* que cumplan la finalidad del párrafo anterior.

El Programa va dirigido a las PYMES como destinatarios finales de los proyectos.

Actuaciones apoyables: Proyectos basados en el comercio electrónico cuyos objetivos puedan encuadrarse dentro de alguna de las siguientes líneas de actuación:

- a. Estudios de necesidades y viabilidad.
- b. Proyectos piloto.
- c. Implantación de Centros de SAT.
- d. Promoción del uso de SAT.

Tipo de ayuda: El importe de las subvenciones podrá superar el 60% del coste de la actividad a desarrollar por el beneficiario. Serán subvencionables las actividades cuyo gasto se haya comprometido con fecha posterior a la presentación de la solicitud y anterior a la fijada para la finalización del proyecto.

Plazo: Hasta el 30 de junio de 2006.

PROGRAMA OPERATIVO DE INICIATIVA EMPRESARIAL Y FORMACIÓN CONTINUA DEL FONDO SOCIAL EUROPEO

PROGRAMA DE FORMACIÓN EN TELECOMUNICACIONES (FORINTEL)

Organismo Gestor: MCYT - FONDO SOCIAL EUROPEO

Objetivo: Organización e impartición de acciones formativas presenciales, a distancia (teleformación) o mixtas sobre materias relacionadas con los Servicios Avanzados de Telecomunicaciones y las tecnologías que les proporcionan soporte.

Beneficiarios: Empresas y Organismos Intermedios.

Actuaciones apoyables:

1. Actuaciones de formación general.
2. Actuaciones de formación de usuarios de telecomunicaciones y nuevas tecnologías de la información.
3. Actuaciones dirigidas a la formación de profesionales que desempeñen puestos de trabajo relacionados con la telecomunicaciones y las tecnologías de la información.

Tipo de ayuda: Subvención del 70% del coste de la actuación, excepto si se trata de grandes empresas (50%). En las zonas del objetivo 1 el porcentaje de ayuda se incrementa un 10%.

Plazo: Hasta el 30 de junio del 2006.

Ámbito Internacional

PROGRAMAS EUREKA E IBEROEKA

Organismo: CDTI – MCYT (PROFIT)

Objetivo: Impulsar la competitividad de las empresas mediante el fomento de proyectos basados en tecnologías innovadoras.

Beneficiarios: *Empresas y Centros Tecnológicos* capaces de realizar proyectos de I+D de carácter aplicado en colaboración con otras empresas y/o Centros Tecnológicos de otros países de Eureka e Iberoeka.

Actuaciones apoyables: Realización de proyectos tecnológicos internacionales, orientados hacia el desarrollo de productos, procesos o servicios con claro interés comercial en el mercado internacional y basados en tecnologías innovadoras.

Tipo de ayuda: Cada país asume la financiación de sus empresas e institutos tecnológicos

- FASE DE DEFINICIÓN: Un 75% de subvención a través del Programa de Fomento de la Investigación Técnica (PROFIT) del Ministerio de Ciencia y Tecnología.

- FASE DE DESARROLLO: Un 60% con créditos CDTI sin intereses a pagar en un plazo máximo de 8 años. Hasta un 35% en subvenciones con fondos PROFIT compatibles con otras subvenciones autonómicas o regionales.

Plazo: Durante todo el ejercicio 2005.

VI PROGRAMA MARCO DE LA UNIÓN EUROPEA ESTRUCTURACIÓN DEL ESPACIO EUROPEO DE LA INVESTIGACIÓN

Programa específico de investigación, desarrollo tecnológico y demostración denominado Estructuración del Espacio Europeo de la Investigación (2002-2006)

Convocatorias de propuestas de acciones indirectas de IDT:

- DOUE C 34/05, 09/02/2005. Ciencia y Sociedad: Acontecimientos científicos europeos; Ciencia y sociedad más allá del VI PM. **FP6-2005-Science-and-Society-13** (Plazo: 24/05/2005).

- DOUE C 13/07, 19/01/2005. Encuentros científicos y cursos de formación Marie Curie. **FP6-2005-Mobility-4** (Plazo 05/18/2005).

- DOUE C 309/07, 15/12/2004. Plan: Desarrollo de la red de comunicaciones. **FP6-2004-Infrastructures-6** (Plazo 17/03/2005).

- DOUE C 309/06, 15/12/2004. Campo temático prioritario: Actividades horizontales de investigación con participación de las PYME : Proyectos de investigación cooperativa y Proyectos de investigación colectiva. **FP6-2004-SME-COOP y FP6-2004-SME-COLL** (Plazo 14/09/2005).

- DOUE C 309/05, 15/12/2004. Propuestas de becas de acogida para la transferencia de conocimientos Marie Curie. **FP6-2004-Mobility-3** (Plazo: 18/05/2005).

- DOUE C 309/04, 15/12/2004. Premios René Descartes 2005. **FP6-2004-Science-and-society-12** (Plazo 10/05/2005).

- DOUE C 268/08, 04/11/2004. Acceso transnacional, actividades de integración y medidas de acompañamiento. **FP6-2004-Infrastructures-5** (Nueva publicación de 2004/C 263/11) (Plazo 03/03/2005).

- DOUE C 263/11, 26/10/2004. Acceso transnacional, actividades de integración y medidas de acompañamiento. **FP6-2004-Infrastructures-5** (Plazo 03/03/2005).

- DOUE C 257/05, 19/10/2004. Refuerzo de la información económica y tecnológica. **FP6-2004-INNOV-5** (Plazo 10/02/2005).

- DOUE C 255/08, 15/10/2004. Convocatorias dentro del programa específico de investigación, desarrollo tecnológico y demostración (Plazo 16/02/2005).

SOCIEDAD DE LA INFORMACIÓN

Organismo: COMISIÓN DE LA UE

Objetivo: Conseguir una investigación más centrada e integrada a escala comunitaria y articular y fortalecer las bases del Espacio Europeo de Investigación. Fomentar la participación de las PYME.

Beneficiarios: *Empresas y Centros Tecnológicos* capaces de realizar proyectos de I+D+i en colaboración con otras empresas y/o Centros Tecnológicos de países miembros de la UE o países Asociados.

Actuaciones apoyables: Proyectos de carácter innovador.

Tipo de ayuda: Subvención a fondo perdido para empresas y Centros Tecnológicos. La participación de las PYME está abierta en las distintas prioridades temáticas y a través de los diferentes instrumentos. Espacios específicos de apoyo a las PYME, en forma de acciones de investigación cooperativa (Proyectos Craft) y colectiva (Proyectos Colectivos).

Plazos:

- **10/05/03 - 27/04/2006.** Manifestaciones de interés para la prestación de asistencia en el ámbito de diversas actividades propias de las Direcciones

que participan en el programa de TSI, a partir de los objetivos del programa de trabajo 2003-2004 (<http://www.cordis.lu/calls/>).

- **15/12/04-14/09/05. 4ª convocatoria.- FP6-2004-IST-1; 15/12/04-26/05/05. 5ª convocatoria.-FP6-2005-IST-2.**

- **16/11/04-22/03/05. FP6-2004-IST-4** - Propuestas de acciones indirectas de IDT dentro del programa específico de investigación, desarrollo tecnológico y demostración "Integración y fortalecimiento del Espacio Europeo de la Investigación" Prioridad temática: Tecnologías de la sociedad de la información (TSI). Referencia: FP6-2004-IST-4.

Ver página web del Programa:

<http://www.cordis.lu/fp6>

<http://www.sost.es>

E-TEN

Convocatoria:

DOUE C 283/06, 11/20/2004. Convocatoria de expertos independientes para el programa eTEN (2005-2006) (Plazo 31/12/2006)

Objetivo: La realización de proyectos de interés común en materia de interoperación y desarrollo de redes transeuropeas de telecomunicaciones.

Beneficiarios: Organizaciones individuales y consorcios que respondan a las condiciones definidas en las convocatorias.

Información General: Las propuestas deberán referirse a una de las siguientes líneas de acción: A1: Gobierno y administración electrónicas (eGovernment) (eAdministration), A2: Salud en línea (eHealth) (eHealthcare), A3: Inclusión electrónica (eInclusion), A4: Aprendizaje electrónico (eLearning), A5: Confianza y seguridad, A6: Acciones complementarias de apoyo y coordinación.

Procedimiento: Se invita a las organizaciones individuales o consorcios (si se trata de consorcios, una de las organizaciones deberá erigirse en contratista principal y agente responsable) a que presenten propuestas relativas a los proyectos.

La ayuda financiera comunitaria podrá revestir la forma de cofinanciación de la fase de estudio o, cuando se justifique una intervención complementaria por tratarse de una aplicación innovadora de interés público, bonificaciones de intereses sobre préstamos, contribuciones a las primas de garantías de créditos y subvenciones directas en casos debidamente justificados.

Referencias en Internet: http://europa.eu.int/information_society/programmes/eten/index_en.htm