

# Actualidad **TIC**

Revista del Instituto Tecnológico de Informática  
Número 1      Año 2003

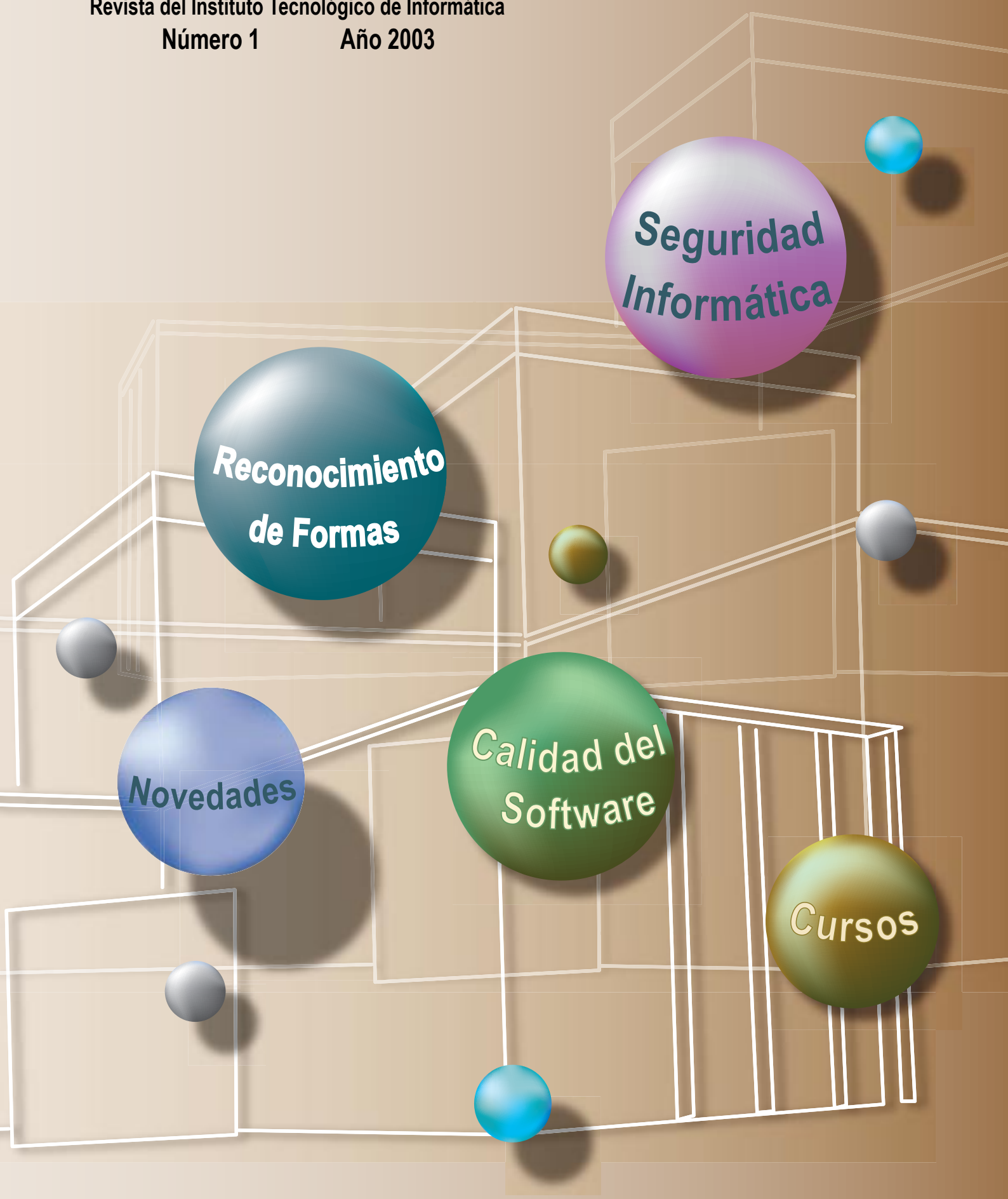
**Reconocimiento  
de Formas**

**Seguridad  
Informática**

**Novedades**

**Calidad del  
Software**

**Cursos**



**Sumario**

|   |    |
|---|----|
| Ferias de Interés   | 2  |
| Editorial   | 3  |
| Seguridad Informática   | 4  |
| Grupo de Reconocimiento de Formas y Tecnología del Lenguaje (PRHLT) | 8  |
| Calidad y Testeo del Software                                       | 12 |
| Noticias Breves   | 17 |
| Cursos  | 17 |
| Ayudas y Subvenciones   | 18 |

**EDITA:****ITI**

Instituto Tecnológico de Informática

Universidad Politécnica de Valencia  
Camino de Vera s/n  
46071 Valencia

Tel.: 96 387 70 69  
Fax: 96 387 72 39  
<http://www.iti.upv.es>  
e-mail: [iti@iti.upv.es](mailto:iti@iti.upv.es)

**DISEÑA:**

Instituto Tecnológico de Informática

**IMPRIME:**

Moliner-40  
(Gómez Coll, S.L. Servicios Editoriales)

**Depósito Legal:** V-3279-2003

**ISSN:** 1696 - 5876

**Actualidad TIC**

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

Número 1, Julio 2003

**Ferias de Interés**

**FOROTECH** – Forum sobre Nuevas Tecnologías

Del 24 al 27 de Septiembre de 2003 - Bilbao

<http://www.feriadebilbao.com/castellano/certamen03/cumbre/menu.htm>

**EXPOINTERNET**

Del 01 al 14 de octubre de 2003 – Barcelona

<http://www.aui.es/expointernet>

**SIMO TCI** – Feria internacional de Informática, Multimedia y Comunicaciones

Del 04 al 09 de noviembre de 2003 - Madrid

<http://www.simo.ifema.es/ferias/simo/default.html>

**ITO** – Salón Monográfico de Integración de Telefonía con Ordenadores

Del 09 al 11 de marzo de 2004 - Madrid

<http://www.siti.es/ito>

**IND.ao** - Salon international de l'informatique et des nouvelles technologies pour l'industrie

Del 22 al 26 de marzo de 2003 – Paris

<http://www.industrie-expo.com/index.htm>

**CEBIT HANNOVER**

Del 18 al 24 de marzo de 2004

<http://www.cebit.de>

**HANNOVER MESSE**

Del 19 al 24 de abril de 2004

<http://www.hannovermesse.de>

## Editorial

*Con este primer número comienza la andadura de Actualidad TIC, que aspira a convertirse en una valiosa herramienta de comunicación entre el Instituto y las Empresas Asociadas.*

Las Tecnologías de la Información y las Comunicaciones forman un sector dinámico donde los cambios frecuentes están a la orden del día, con la introducción de nuevos productos y tecnologías, y con la sensación aparente de imperiosa necesidad de aplicación de los mismos.

El Instituto Tecnológico de Informática nació con la vocación de ayudar en la incorporación de aquellas tecnologías más interesantes para la obtención de productos y servicios diferenciales, capaces de situar a las empresas de nuestro entorno en una buena posición competitiva. En este sentido, el Instituto ha venido utilizando como instrumento su actividad en I+D+I, en Formación y en Asesoría Tecnológica. Con la edición de la presente revista inauguramos un nuevo instrumento para la consecución de nuestros objetivos, mediante la divulgación de nuestras actividades y también de las de nuestros asociados. En este primer número presentamos contribuciones técnicas en tres de las áreas de trabajo del Instituto.

La Seguridad y la Fiabilidad de los sistemas de información constituyen una preocupación cada vez más importante de cualquier organización, al apoyarse habitualmente alguna de sus actividades críticas en sistemas informáticos. En muchos casos el soporte de tales actividades se lleva a cabo gracias al acceso a los sistemas a través de redes de comunicación, en especial Internet. Desde el Instituto creemos que los aspectos relacionados con la seguridad de los sistemas de información son extremadamente importantes, por lo que hemos lanzado un grupo de trabajo en esta línea. El primer artículo presente en este número da una visión general de la temática que pretendemos abordar desde el Instituto.

Por otra parte, el grupo de Reconocimiento de Formas ofrece una visión general de los temas en los cuales está trabajando el Instituto dentro de esta área, y que tienen un gran interés por sus aplicaciones potenciales en un amplio rango de sectores, tanto industriales como de servicios,

especialmente en lo que se refiere a la aplicación de la visión artificial y el reconocimiento de voz y la tecnología del lenguaje.

Otra de las áreas de interés del Instituto es la de Calidad del Software. De todos es conocida la dificultad existente a la hora de desarrollar soluciones de un modo satisfactorio (tanto para el cliente como para el desarrollador). En muchos casos se puede aumentar el grado de satisfacción de los agentes involucrados introduciendo mejoras en los procesos de desarrollo. Conscientes de este problema el Instituto ha lanzado líneas de actuación tendentes a mejorar este proceso de desarrollo. El artículo que presentamos en este número da algunas de las claves de esta actuación.

Las comunicaciones técnicas que presentamos son forzosamente cortas y poco numerosas, dado el tamaño inicial de la publicación con el que iniciamos esta andadura.

En el futuro esperamos contar con más y más descriptivas contribuciones, tanto por parte del personal del Instituto como por parte de nuestras Empresas Asociadas, con el fin de constituir esta revista en un vehículo valioso de relación y comunicación entre los asociados y el Instituto, para lo cual esperamos contar con vuestra colaboración.



José M. Bernabéu Aubán  
*Director Científico-Técnico del ITI*

## Seguridad Informática

Desde la consolidación de Internet como medio de interconexión global, los incidentes de seguridad relacionados con sistemas informáticos vienen incrementándose de manera alarmante. Este hecho, unido a la progresiva dependencia de la mayoría de organizaciones hacia sus sistemas de información, viene provocando una creciente necesidad de implantar mecanismos de protección que reduzcan al mínimo los riesgos asociados a los incidentes de seguridad. En este artículo, vamos a proporcionar una visión general de los aspectos más relevantes de la seguridad informática, observando esta disciplina desde un punto de vista estratégico y táctico. Para ello destacaremos la conveniencia de afrontar su análisis mediante una aproximación de gestión, concretamente con un enfoque de gestión del riesgo. Para completar esta visión introductoria a la seguridad informática, mencionaremos las amenazas y las contramedidas más frecuentes que deberían considerarse en toda organización.

### Introducción

La seguridad informática, de igual forma a como sucede con la seguridad aplicada a otros entornos, trata de minimizar los riesgos asociados al acceso y utilización de determinado sistema de forma no autorizada y en general malintencionada. Esta visión de la seguridad informática implica la necesidad de gestión, fundamentalmente gestión del riesgo. Para ello, se deben evaluar y cuantificar los bienes a proteger, y en función de estos análisis, implantar medidas preventivas y correctivas que eliminen los riesgos asociados o que los reduzcan hasta niveles manejables.

En general cualquier persona consideraría poco razonable contratar a un agente de seguridad en exclusiva para proteger su domicilio. Posiblemente sería una medida de seguridad excelente para evitar accesos no autorizados a nuestro domicilio, sin embargo, muy pocos lo considerarían, simplemente por motivos económicos. Tras evaluar el valor de los bienes a proteger, lo habitual sería considerar otras medidas más acordes con el valor de nuestros bienes. Podríamos pensar en una puerta blindada, un conserje compartido con otros vecinos o incluso un servicio de vigilancia privada basada en sensores, alarmas y acceso telefónico con una central de seguridad. Combinando estas medidas preventivas con otras correctivas como podría ser una póliza de seguro contra robo, alcanzaríamos un nivel de seguridad que podría considerarse adecuado. Muchas veces sin hacerlo de forma explícita, habríamos evaluado el valor de nuestros bienes, los riesgos, el coste de las medidas de seguridad disponibles en el mercado y el nivel de protección que ofrecen.

En seguridad informática, los principios mostrados con nuestro ejemplo de seguridad en el domicilio son igualmente aplicables. Las únicas diferencias aparecen por las particularidades técnicas asociadas a los sistemas informáticos. La valoración económica de los bienes a proteger puede ser muchas veces una tarea compleja, la casuística de los riesgos potenciales muy grande, y la complejidad y diversidad de las medidas de seguridad disponibles dificulta su selección. Sin embargo, el fondo sigue siendo el mismo, seguridad implica proteger alguna entidad frente a un conjunto de riesgos y en este caso riesgos relacionados con los sistemas informáticos.

En este artículo vamos a dar una visión general a los aspectos más relevantes de la seguridad informática, comenzando con una visión de la seguridad como parte integral de la gestión empresarial, continuaremos con la descripción de las amenazas más frecuentes que pueden comprometer los sistemas informáticos y con la descripción de las medidas más efectivas para contrarrestarlas. Por último, finalizaremos mencionando las actividades más significativas que venimos realizando en el Instituto Tecnológico de Informática en materia de seguridad.

### Objetivos de la Seguridad Informática

El objetivo de la seguridad informática es proteger los recursos informáticos valiosos de la organización, tales como la información, el hardware o el software. A través de la adopción de las medidas adecuadas, la seguridad informática ayuda a la organización cumplir sus objetivos, protegiendo sus recursos financieros, sus sistemas, su reputación, su situación legal, y otros bienes tanto tangibles como inmateriales. Desafortunadamente, en ocasiones se ve a la seguridad informática como algo que dificulta la consecución de los propios objetivos de la organización, imponiendo normas y procedimientos rígidos a los usuarios, a los sistemas y a los gestores. Sin embargo debe verse a la seguridad informática, no como un objetivo en sí mismo, sino como un medio de apoyo a la consecución de los objetivos de la organización.

En general el principal objetivo de las empresas, es obtener beneficios y el de las organizaciones públicas, ofrecer un servicio eficiente y de calidad a los usuarios. En las empresas privadas, la seguridad informática debería apoyar la consecución de beneficios. Para ello se deben proteger los sistemas para evitar las potenciales pérdidas que podrían ocasionar la degradación de su funcionalidad o el acceso a los sistemas por parte de personas no autorizadas. De igual forma, las organizaciones públicas deben proteger sus sistemas para garantizar la oferta de sus servicios de forma eficiente y correcta.

En cualquier caso, los gestores de las diferentes organizaciones deberían considerar los objetivos de la propia organización e incorporar la seguridad de los sistemas desde un punto de vista amplio, como un medio con el que gestionar los riesgos que pueden

comprometer la consecución de los propios objetivos, donde la cuantificación de los diferentes aspectos, muchas veces económica, debe ser central.

## Gestión del Riesgo

La protección de los sistemas y de la información no suele eliminar completamente la posibilidad de que estos bienes sufran daños. En consecuencia, los gestores deben implantar aquellas medidas de seguridad que lleven los riesgos hasta niveles aceptables, contando para ello con el coste de las medidas a implantar, con el valor de los bienes a proteger y con la cuantificación de las pérdidas que podrían derivarse de la aparición de determinado incidente de seguridad.

Los costes y beneficios de la seguridad deberían observarse cuidadosamente para asegurar que el coste de las medidas de seguridad no excedan los beneficios potenciales. La seguridad debe ser apropiada y proporcionada al valor de los sistemas, al grado de dependencia de la organización a sus servicios y a la probabilidad y dimensión de los daños potenciales. Los requerimientos de seguridad variarán por tanto, dependiendo de cada organización y de cada sistema en particular.

En cualquier caso, la seguridad informática exige habilidad para gestionar los riesgos de forma adecuada. Invirtiendo en medidas de seguridad, las organizaciones pueden reducir la frecuencia y la severidad de las pérdidas relacionadas con violaciones de la seguridad en sus sistemas. Por ejemplo, una empresa puede estimar que está sufriendo pérdidas debidas a la manipulación fraudulenta de sus sistemas informáticos de inventariado, de contabilidad o de facturación. En este caso puede que ciertas medidas que mejoren los controles de acceso, reduzcan las pérdidas de forma significativa.

Las organizaciones que implantan medidas adecuadas de seguridad, pueden obtener un conjunto de beneficios indirectos que también deberían considerarse. Por ejemplo, una organización que cuente con sistemas de seguridad avanzados, puede desviar la atención de potenciales intrusos hacia víctimas menos protegidas, puede reducir la frecuencia de aparición de virus, puede generar una mejor percepción de los empleados y otros colaboradores hacia la propia empresa, aumentando la productividad y generando empatía de los empleados hacia los objetivos organizativos.

Sin embargo, los beneficios que pueden obtenerse con medidas de seguridad presentan costes tanto directos como indirectos. Los costes directos suelen ser sencillos de evaluar, incluyendo la compra, instalación y administración de las medidas de seguridad. Por su parte pueden observarse costes indirectos, como decremento en el rendimiento de los sistemas, pueden aparecer necesidades formativas nuevas para la plantilla o incluso determinadas medidas, como un excesivo celo en los controles, pueden minar la moral de los empleados.

En muchos casos los costes asociados a las medidas de seguridad pueden exceder a los beneficios esperados por su implantación, en cuyo caso una correcta gestión llevaría a plantearse su adopción frente a la posibilidad de simplemente tolerar el problema.

## Amenazas

Los sistemas informáticos son vulnerables a multitud de amenazas que pueden ocasionar daños que resulten en pérdidas significativas. Los daños pueden variar desde simples errores en el

uso de aplicaciones de gestión que comprometan la integridad de los datos, hasta catástrofes que inutilicen la totalidad de los sistemas. Las pérdidas pueden aparecer por la actividad de intrusos externos a la organización, por accesos fraudulentos, por accesos no autorizados, por el uso erróneo de los sistemas por parte de empleados propios, o por la aparición de eventualidades en general destructivas.

Los efectos de las diversas amenazas pueden ser muy variados. Unos pueden comprometer la integridad de la información o de los sistemas, otros pueden degradar la disponibilidad de los servicios y otros pueden estar relacionados con la confidencialidad de la información. En cualquier caso una correcta gestión de los riesgos debe implicar un profundo conocimiento de las vulnerabilidades de los sistemas y de las amenazas que los pueden explotar. Las propias características de las organizaciones deben influir en las medidas de seguridad que resulten más adecuadas y más eficientes en términos de costes, para contrarrestar las amenazas o incluso para tolerarlas conociendo en todo caso sus implicaciones.

A continuación vamos a mostrar las amenazas más frecuentes que deberían ser tenidas en cuenta por toda organización como fuentes potenciales de pérdidas. Conviene destacar que la importancia de una u otra amenaza varía de forma significativa entre organizaciones distintas y que debería hacerse un estudio individualizado de sus repercusiones concretas y de la probabilidad de su aparición.

### 1. Errores y omisiones

Los errores de los empleados al utilizar los sistemas pueden comprometer la integridad de la información que maneja la organización. Ni siquiera las aplicaciones más sofisticadas están libres de este tipo de problemas, que pueden reducirse con refuerzos en controles de integridad de los datos y con un adiestramiento adecuado del personal.

Muchas veces, simples errores pueden comprometer no únicamente la integridad de los datos, sino incluso puede que causen la aparición de nuevas vulnerabilidades en los sistemas. Este tipo de amenazas es si cabe más relevante en las empresas que se dedican al sector de las nuevas tecnologías, desarrollando e implantando sistemas, muchas veces interconectados entre diversas organizaciones. Un simple error de programación, en la administración, o la carencia de la formación necesaria para evaluar las implicaciones de seguridad de determinada aproximación de desarrollo, puede causar vulnerabilidades que afecten no únicamente a las organizaciones usuarias de los sistemas, sino también a las propias empresas que los desarrollan que se podrían ver muy perjudicadas en su imagen corporativa.

### 2. Intrusiones

Bajo esta amenaza se incluyen tanto actividades claramente fraudulentas, como meras intrusiones efectuadas por determinados individuos con el único fin de probar sus "habilidades" o incluso actos de sabotaje, terrorismo informático o espionaje industrial. Las actividades fraudulentas, incluido el robo, puede que sean las más preocupantes para muchas organizaciones, sobre todo para aquellas que tengan bienes de elevado valor, gestionados mediante sistemas informáticos. Ejemplos de este tipo de organizaciones pueden ser las entidades financieras, los organismos públicos que generen acreditaciones oficiales o incluso empresas de distribución o comercio electrónico, donde los sistemas informáticos pueden ser

susceptibles de alteración malintencionada con objeto de obtener provecho económico.

Los autores de las intrusiones pueden ser tanto externos a la propia organización, como internos. Es reseñable destacar que muchos estudios sobre fraudes y robos mediante tecnologías de la información coinciden en señalar que la mayoría de las actividades fraudulentas son realizadas por personal vinculado a la propia organización. Pueden ser empleados con acceso a sistemas o información no controlada, antiguos empleados con conocimientos tanto de los sistemas como de las medidas de seguridad internas o personas vinculadas en cierta forma con la organización y que gozan de determinados privilegios que muchas veces se esconden bajo aparentes relaciones cordiales con la propia empresa.

En muchos casos las intrusiones generan importantes daños económicos, pero en todos los casos causan una importante sensación de desprotección en toda la organización, que se agrava si no es posible identificar a los autores de las intrusiones, las técnicas empleadas para cometerlas o los objetivos que persiguen.

La creciente importancia de las intrusiones maliciosas en los sistemas informáticos la podemos encontrar reflejada en el siguiente

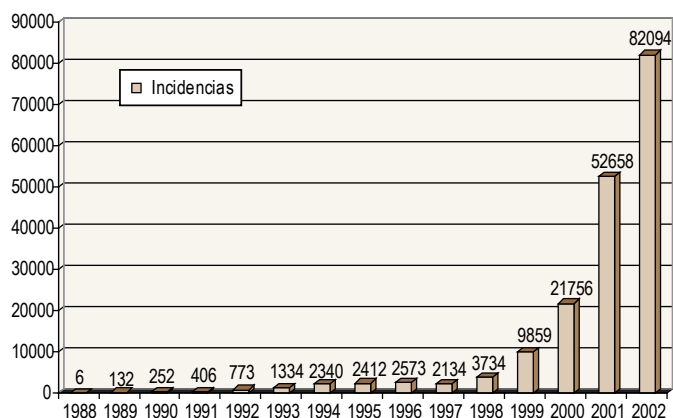


Figura 1: Evolución de las incidencias intervenidas por el CERT/CC (fuente: [www.cert.org](http://www.cert.org)).

gráfico, donde se puede observar el alarmante incremento de incidentes de seguridad ocurrido en los últimos años.

Concretamente el gráfico muestra el número de incidentes ocasionados por intrusiones, y comunicados al CERT, un organismo de reconocido prestigio internacional dedicado a la prevención y análisis de los incidentes de seguridad aparecidos en Internet. Conviene destacar que las cifras únicamente muestran los datos comunicados al CERT, y que vienen a representar a las intrusiones efectuadas por parte de individuos externos a las propias organizaciones. Los datos se refieren a todo el mundo, sin embargo también destacamos que las cifras provienen mayoritariamente de grandes empresas, asentadas fundamentalmente en los Estados Unidos, Europa y Japón. Sin embargo, pese a lo parcial de las cifras, no deja de resultar ilustrativa la curva de crecimiento y las magnitudes de los incidentes constatados.

### 3. Accidentes y desastres

Eventualidades tan cotidianas como la simple rotura de una cañería, la pérdida de fluido eléctrico o la rotura de equipos o mecanismos de comunicaciones pueden tener efectos claramente negativos sobre los sistemas de información. Debe incluso contemplarse la posibilidad de aparición de eventos más graves, como incendios, atentados terroristas, inundaciones causadas por la

propia naturaleza, tormentas eléctricas o actividades reivindicativas descontroladas de determinados colectivos.

### 4. Lógica maliciosa

Entre estas amenazas encontramos los virus, los gusanos, los caballos de Troya y las bombas lógicas. Aun existiendo diferencias técnicas entre ellas, el nexo común a todas estas amenazas consiste en que se trata de software creado en general para causar daño. Los costes asociados a su aparición pueden ser significativos y varían en función de la virulencia de sus acciones. Pueden suponer simplemente pérdidas debidas a la dedicación de personal y recursos a su eliminación o pérdidas mucho mayores si resultan afectados, corrompidos o destruidos sistemas críticos para la organización.

### 5. Amenazas a la privacidad de las personas

La acumulación de enormes cantidades de datos de carácter personal por entidades públicas y privadas, unida a la capacidad de los sistemas informáticos para combinar y procesar las informaciones vienen generando claras amenazas a la privacidad de los individuos. La constatación de estas amenazas por parte de la mayoría de países ha llevado a la elaboración de leyes y normas que limitan el tratamiento de los datos de carácter personal.

Estas amenazas no sólo afectan a los individuos, sino también a toda organización que manipule información sensible de personas. De no observarse la legislación vigente y en caso de no implantar las medidas adecuadas para su cumplimiento, se pueden derivar pérdidas, tanto económicas por las correspondientes multas, como de imagen corporativa.

### Medidas de Seguridad

Existe un gran abanico de medidas de seguridad que pueden reducir el riesgo de pérdidas debidas a la aparición de incidentes en los sistemas informáticos. Muchas veces al hablar de medidas de seguridad, solo se mencionan las meramente técnicas, como cortafuegos, antivirus o sistemas de copias de respaldo. Sin embargo, las medidas más efectivas suelen ser las medidas de gestión planteadas a medio y largo plazo desde un punto de vista estratégico y táctico.

A continuación mencionaremos brevemente las medidas y sistemas de seguridad más frecuentes agrupándolas bajo dos aspectos. Medidas de gestión y medidas técnicas. Las primeras deben ser implantadas por los gestores de las organizaciones como parte de los planes estratégicos y tácticos, mientras que las segundas se corresponden con herramientas y sistemas técnicos diseñados para evitar, controlar o recuperar los daños que pueden sufrir los sistemas por la aparición de determinadas amenazas de seguridad.

### 1. Medidas de gestión

Los gestores de toda organización deberían contemplar la seguridad informática como parte integral de las estrategias y tácticas corporativas. Una vez plasmada la importancia de los sistemas para la consecución de los propios objetivos y los riesgos que puede suponer para la empresa la pérdida de integridad de su información, la indisponibilidad de sus sistemas o la violación de la confidencialidad

de su información, pueden plantearse con mayor rigor el resto de medidas encaminadas a servir a los objetivos empresariales.

Emanando de la vertiente estratégica de la información y de los sistemas corporativos, suelen generarse dos herramientas de gestión no menos importantes: las políticas de seguridad y el plan de contingencia.

Las políticas de seguridad de una organización son las normas y procedimientos internos que deben seguir los integrantes de la organización para respetar los requerimientos de seguridad que deseen preservarse. Debe describirse la criticidad de los sistemas y de la información, los roles de cada puesto de trabajo y la mecánica de acceso a los sistemas, herramientas, documentación y cualquier otra componente del sistema de información. Resulta frecuente desglosar las políticas de seguridad en procedimientos detallados para cada componente del sistema de forma individualizada, así por ejemplo, pueden crearse documentos que describan las políticas de tratamiento de correos electrónicos, políticas de uso de Internet, de copias de respaldo, de tratamiento de virus y otra lógica maliciosa, políticas formativas en materia de seguridad para la plantilla, etc. Conviene destacar que las políticas de seguridad deben emanar de la estrategia corporativa y que se trata de documentos que deberían conocer todos los integrantes de la plantilla.

Por su parte, el plan de contingencia describe los procedimientos que deben seguirse ante la aparición de eventualidades significativas que puedan suponer graves consecuencias para la organización. Debe detallarse los pasos a seguir, por ejemplo en caso de destrucción total de los sistemas por inundación, fuego, etc. Muchas veces la simple elaboración del plan descubre defectos en los sistemas que pueden ser paliados con relativa facilidad. Por ejemplo puede descubrirse que no se mantienen copias de respaldo de información crucial para la empresa en lugares físicamente seguros, o al menos en lugares distantes a la ubicación de los sistemas susceptibles de daños.

## 2. Medidas técnicas

Existen innumerables herramientas y sistemas de seguridad orientadas a preservar la integridad, confidencialidad y disponibilidad de información y sistemas. La oferta en este sentido es muy numerosa y toda organización debería dedicar un esfuerzo significativo a su estudio y selección. En este breve artículo, más que describir con detalle todas las herramientas y medidas de seguridad aplicables y sus variaciones disponibles en el mercado, nos limitaremos a mencionar las técnicas más utilizadas, apuntando finalmente algunas de las más novedosas.

Entre las técnicas más consolidadas encontramos las copias de respaldo, los antivirus, los cortafuegos, los mecanismos de autenticación y la criptografía. Las copias de respaldo y en general cualquier forma de redundancia, se encaminan a garantizar la disponibilidad de los sistemas frente a cualquier eventualidad.

Los antivirus pretenden evitar la aparición de lógica maliciosa y en caso de infección tratan de eliminarla de los sistemas. Entre los antivirus conviene destacar aquellos que inspeccionan los correos electrónicos evitando la infección de sus destinatarios. Por su parte, los cortafuegos tratan de reducir el número de vías potenciales de acceso a los sistemas corporativos desde el exterior, estableciendo limitaciones al número de equipos y de servicios visibles. Otra de las técnicas imprescindibles en toda organización la forman los mecanismos de autenticación. Estos mecanismos pueden variar desde esquemas simples basados en los pares usuario contraseña, hasta complejos sistemas distribuidos basados en credenciales o

sistemas de autenticación biométricos basados en el reconocimiento mecanizado de características físicas de las personas. Por último, todo esquema de seguridad debe contemplar en una u otra medida el cifrado de información sensible. A veces puede ser suficiente el cifrado de las contraseñas, mientras que en otras resulta imprescindible el cifrado de las comunicaciones y de las bases de datos.

Como medidas más avanzadas, podemos mencionar la esteganografía, la detección de vulnerabilidades y la detección de intrusos. Las técnicas esteganográficas tratan de ocultar información. A diferencia de la criptografía, que trata de hacer indecifrabla la información, la esteganografía trata de evitar que siquiera se note su existencia. Por ejemplo las empresas dedicadas a producir documentos digitales, pueden estar interesadas en incluir determinada marca invisible de forma que sea demostrable su autoría y puedan perseguirse copias ilegales.

Las herramientas de detección de vulnerabilidades suelen verse como herramientas de auditoría, que pueden mostrar las vías que con mayor probabilidad utilizarían los intrusos para acceder a los sistemas. Por último, los sistemas de detección de intrusos tratan de descubrir, muchas veces en tiempo real, accesos no autorizados a los sistemas, tanto desde el exterior de la organización, como desde dentro de las propias instalaciones de la empresa.

## Seguridad en el Instituto Tecnológico de Informática

El área de Sistemas Fiables del Instituto Tecnológico de Informática, centra su trabajo en la investigación y desarrollo de entornos orientados a aumentar la fiabilidad y la disponibilidad, donde la seguridad informática se plantea como uno de los ejes fundamentales.

En esta área vienen realizándose proyectos de consultoría y auditoría de seguridad informática, cubriéndose los aspectos estratégicos, tácticos y técnicos de los sistemas informáticos. El objetivo de estos proyectos consiste en la elaboración de un procedimiento de consultoría utilizable por terceras empresas consultoras.

Además de la consultoría, se están desarrollando diversos proyectos de investigación y desarrollo, entre los que destacan IntruDec y TigerWeb. El primero consiste en un sistema de detección de intrusos basado en el reconocimiento de patrones de conducta sospechosos, observables al analizar el tráfico en la red y al analizar la actividad de los equipos informáticos. Por su parte, TigerWeb es una herramienta de detección de vulnerabilidades perimetrales. Con esta herramienta se puede obtener una visión aproximada de las vías más fácilmente explotables por potenciales intrusos para acceder a los sistemas desde el exterior de la organización.

Por último, el grupo de Sistemas Fiables también se encuentra inmerso en la investigación de las implicaciones de seguridad que tiene el empleo de sistemas inalámbricos y móviles, estudiando entre otros los mecanismos de autenticación, cifrado, encaminamiento y las arquitecturas software más convenientes donde se contemple la seguridad desde el punto de vista particular de este tipo de entornos.

Autor: Pablo Galdámez

Para más información sobre Seguridad Informática:  
seguridad@iti.upv.es

## Grupo de Reconocimiento de Formas y Tecnología del Lenguaje (PRHLT)

En este artículo se describen las actividades de investigación del grupo de Reconocimiento de Formas y Tecnología del Lenguaje (Pattern Recognition and Human Language Technology- PRHLT) del Instituto Tecnológico de Informática. Se presentan someramente las tecnologías que abarca el Reconocimiento de Formas y las principales aplicaciones de estas metodologías. Finalmente se pasa revista a una serie de aplicaciones recientemente desarrolladas por el grupo PRHLT en sus dos líneas principales de actuación: Procesado de Imágenes y Procesado del Lenguaje.

### Introducción

El grupo PRHLT desarrolla sus actividades de investigación y desarrollo en el ámbito del Reconocimiento de Formas (RF).

El RF es una disciplina bien establecida en las ciencias y en las ingenierías desde hace más de 20 años, con aplicaciones fuertemente implantadas en prácticamente todos los sectores productivos. La principal base metodológica del RF es la estadística. Desde este enfoque, entre las principales tecnologías que abarca el RF cabe mencionar los métodos de Extracción, Selección y Transformación de Características, técnicas de Clasificación, tanto Supervisada como No-Supervisada ("Clustering"), métodos de Interpretación, aproximaciones Basadas en Distancias, etc. En este marco, las principales actividades del grupo PRHLT se pueden agrupar en dos líneas:

- Procesado de Imágenes. Técnicas de análisis y reconocimiento de imágenes y visión por computador.

Aplicaciones: OCR, análisis de documentos, identificación de huellas dactilares, sistemas de ayuda a los discapacitados, detección automática de defectos en estampados textiles, identificación de rostros humanos, detección de cáncer prostático, etc.

- Procesado del Lenguaje, Reconocimiento Automático del Habla y Comprensión del Lenguaje. Traducción automática de texto y voz en dominios limitados. Traducción predictiva interactiva.

Aplicaciones: servicios de información telefónica, dispositivos controlados por la voz, etc., traducción de textos técnicos, traducción simultánea (voz) en servicios de hotel, etc. Sistemas de ayuda a la traducción de calidad de textos generales.

El PRHLT mantiene una colaboración estrecha con diversos grupos de investigación y empresas de España y otros países de la Unión Europea en las áreas mencionadas arriba. Asimismo, el PRHLT participa activamente en diversos proyectos y contratos de I+D en estas áreas.

En las siguientes secciones se presentarán brevemente algunas de las aplicaciones más interesantes recientemente desarrolladas por el PRHLT. Para mayor información se puede visitar <http://prhlt.iti.es>, y en particular, <http://prhlt.iti.es/demos/demos.htm> y <http://prhlt.iti.es/proyectosGrupo.htm>.

### Procesado de Imágenes

#### Reconocimiento Automático de Huellas Digitales

La identificación basada en huellas digitales es la más antigua y la más utilizada en muchas aplicaciones de identificación de individuos. El carácter individual de la huella digital puede ser representado por un patrón de valles y crestas así como por unos puntos característicos denominados "minucias", que son los finales y las bifurcaciones de las crestas.

Las técnicas de comparación de huellas digitales pueden ser clasificadas en dos categorías: basadas en minucias y basadas en correlaciones. Las basadas en minucias primero encuentran las minucias para posteriormente establecer sus posiciones relativas dentro de la huella. Las técnicas basadas en correlaciones requieren la localización precisa de un punto de referencia y están afectadas por translaciones y rotaciones de la imagen. La primera técnica es más robusta a las translaciones y rotaciones de la imagen de la huella pero suele ser muy difícil conseguir una buena detección de las minucias a partir de imágenes ruidosas. Para ello en nuestro sistema de Identificación de Huellas Dactilares se aplica una batería de técnicas de preproceso de imagen y se obtiene un conjunto aceptable de minucias. Una vez las minucias han sido detectadas se necesita una medida de similitud entre dos huellas basada en sus respectivos conjuntos de minucias. La invarianza a la translación, escalado y rotación se consigue aplicando todas estas transformaciones al conjunto de minucias asociado. El mejor emparejamiento de ambos conjuntos es seleccionado y la similitud de ambas huellas viene dada en términos de similitud de ambos conjuntos de minucias.

#### Reconocimiento de Rostros

Gracias al uso de las técnicas de preproceso más recientes y al empleo de un innovador esquema de representación de características locales, se han desarrollado diversas aplicaciones para la identificación de rostros humanos.

La tarea de reconocimiento de rostros se divide en tres etapas bien diferenciadas: preproceso de la imagen original, extracción de vectores de características y clasificación.

El primer objetivo del preproceso es la selección del conjunto de píxeles pertenecientes a las regiones de la cara con mayor información discriminativa. Esto se consigue mediante el cálculo de la varianza local en una pequeña ventana para cada uno de los píxeles y la selección de aquellos que superan un umbral global.

En la siguiente etapa se implementa una técnica novedosa de extracción de características. Una imagen se representa mediante un conjunto numeroso de vectores de características correspondientes a los píxeles seleccionados en la etapa de preproceso. Cada píxel seleccionado genera un vector de valores de gris a partir de la concatenación de las filas de una pequeña ventana centrada en el mismo. Los valores de gris pertenecen a la imagen que se obtiene al aplicar la operación de gradiente sobre la original. Evidentemente, todos los vectores extraídos de la misma imagen son etiquetados con el mismo identificador. Los vectores así obtenidos son sometidos a un proceso de reducción de dimensionalidad mediante la conocida técnica de Análisis de Componentes Principales (PCA), con lo que se consigue una representación más compacta de la información contenida en cada ventana procesada.

Finalmente, se utiliza un proceso de clasificación que podría ser incluido en la familia de técnicas conocida como "direct voting scheme". Para ello, todos los vectores de características extraídos de una imagen de "test" son clasificados mediante la regla de los k-Vecinos Más Próximos. La clase ganadora de cada vector clasificado incrementa la cuenta general de "votos" para esa clase, de manera que aquella clase que finalmente más votos acumula tras la votación de todos los vectores pertenecientes a la misma imagen de "test" es la proporcionada como resultado de la clasificación de la imagen actual.

### Reconocimiento Óptico de Formularios Impresos y Manuscritos

Nuestro sistema de reconocimiento de formularios impresos emplea algoritmos avanzados de OCR (reconocimiento óptico de caracteres) para la extracción de información alfanumérica de los campos de un formulario. En este caso, los algoritmos de OCR han sido entrenados únicamente con caracteres impresos, pero el reconocimiento de caracteres manuscritos también es posible.

Nuestros sistemas de OCR para caracteres manuscritos aislados extraen automáticamente estos caracteres (alfabéticos o numéricos) de los campos manuscritos de los formularios. El uso de modelos particularizados, aprendidos automáticamente a partir de muestras, permite que el sistema pueda trabajar con cualquier lengua y cualquier tipo de alfabeto. Además, se puede aplicar un postproceso lingüístico a los resultados del reconocimiento para aumentar la precisión cuando el texto a reconocer presenta restricciones léxicas o sintácticas conocidas.

### Reconocimiento de Texto Manuscrito

El "Reconocimiento de Texto Manuscrito Continuo" (RTMC) está demostrando ser una tarea de gran desafío en Reconocimiento de

Formas. Aunque el texto está básicamente compuesto de caracteres, las aproximaciones tradicionales de reconocimiento de caracteres aislados (OCR) generalmente fracasan en la tarea de RTMC. Sin lugar a dudas, esto ocurre a causa de la imposibilidad material de segmentar de manera fiable un texto continuo en sus caracteres individuales. Sin embargo, los seres humanos realizan estas tareas de segmentación y reconocimiento de una manera natural y sin aparente esfuerzo. La precisión se alcanza gracias a un "reconocimiento retardado" hasta tener suficiente información para satisfacer los niveles más altos de percepción y lograr así una comprensión de (parte de) lo escrito. Como "subproducto" se consigue reconocer las palabras constituyentes, los caracteres que las componen y la correspondiente segmentación implícita. Parece claro que esta inherente habilidad humana viene dada por una fuerte inter-cooperación entre diferentes niveles de conocimiento: morfológico, léxico, sintáctico y semántico.

Esta es la misma situación que aparece en el campo del Reconocimiento del Habla. En este campo, las técnicas existentes de mayor éxito están basadas en la inter-cooperación de las mencionadas fuentes de conocimiento para conseguir un reconocimiento global. Por esta razón, el sistema aquí presentado se basa en adaptar tecnologías propias del RH para su uso en RTMC.

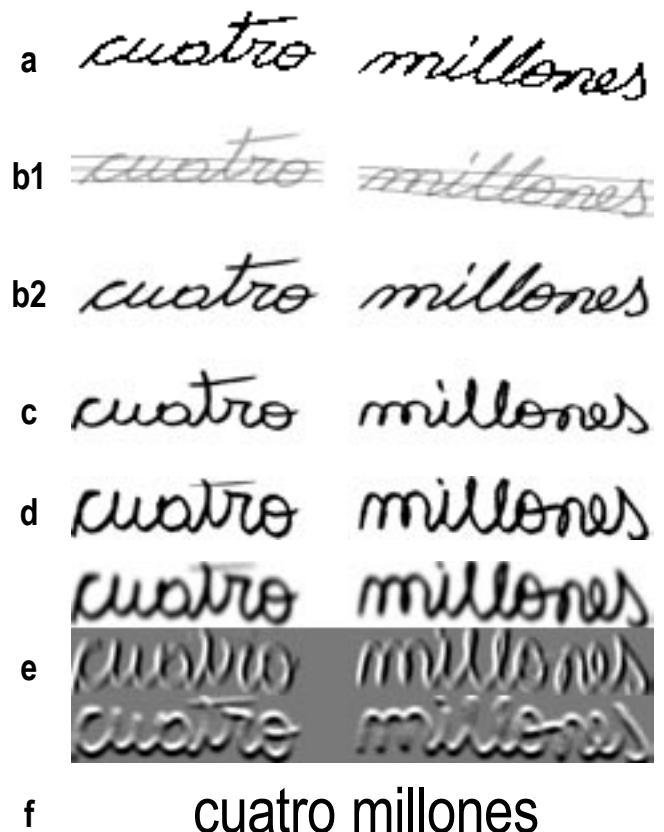


Figura 1: Proceso de reconocimiento de texto manuscrito.

La figura 1 describe el proceso de reconocimiento completo. Los paneles a-d) muestran las sucesivas etapas de preproceso llevadas a cabo con imagen original para la normalización de los atributos de estilo de la escritura. El panel e) es la representación final de la señal en forma de secuencia de vectores de niveles de gris y gradientes horizontales y verticales. Esta representación es directamente

procesada por el reconocedor global, el cual ofrece la hipótesis de reconocimiento (perfectamente correcta, en este caso) que se muestra en el panel f).

### Procesado del lenguaje

#### Comprensión del habla

En un planteamiento tradicional, la comprensión del habla se realiza en dos etapas: una fase de reconocimiento de la elocución pronunciada y una fase de comprensión propiamente dicha de la frase reconocida. El sistema desarrollado en el grupo PRHLT adopta una aproximación alternativa en la que se integran estas dos etapas.

una figura determinada está presente en el área de dibujo, o borrar determinadas figuras. La figura 2 muestra un panel con el estado de este prototipo cuando ha recibido la orden "Se añade un círculo grande y oscuro encima del triángulo mediano". A partir de la señal vocal resultante de la pronunciación de esta frase (panel central), el sistema obtiene directamente la fórmula lógica "La(x) & Da(x) & C(x) & M(z) & T(z) & A(x,z) & Ad(x)"; es decir, x es "Large", "Dark", "Circle" y "Medium"; z es "Medium" y "Triangle"; x esta(rá) "Above" z; x se debe añadir ("Add"). Como subproducto, también se obtiene la frase reconocida que, en este caso, coincide exactamente con la que se había pronunciado.

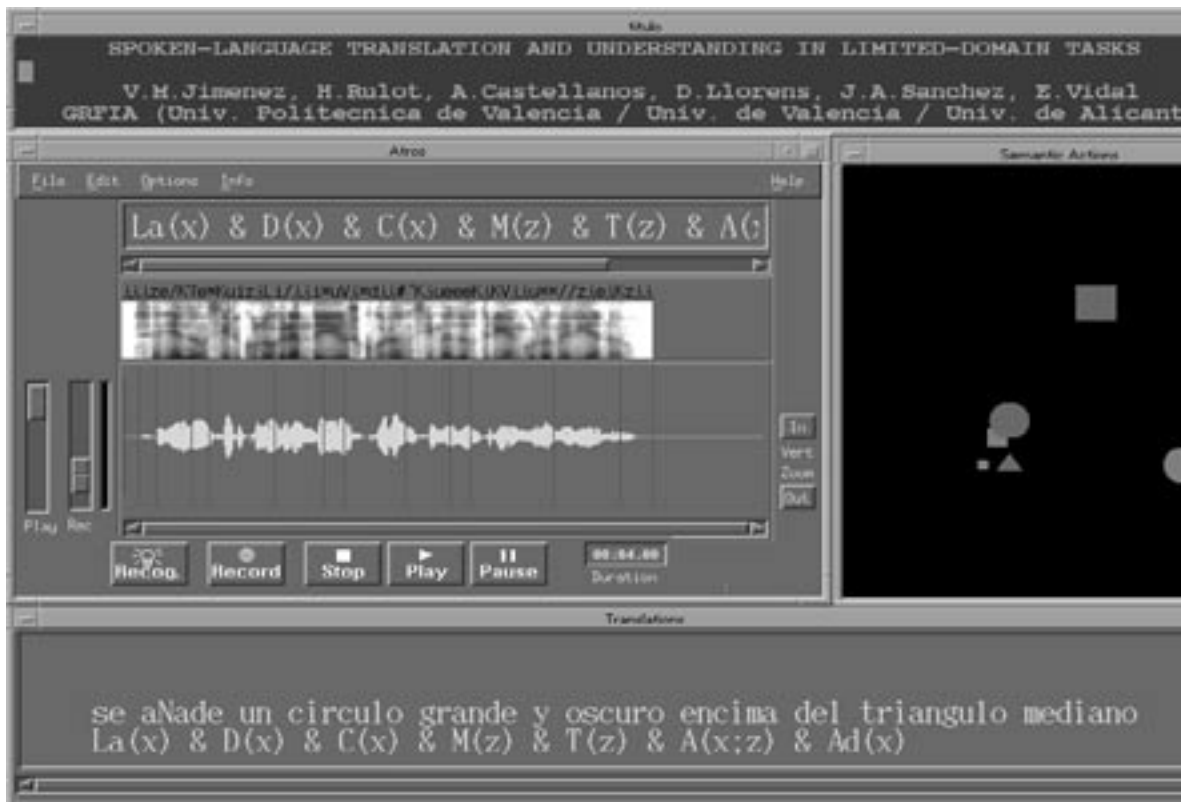


Figura 2: Panel del prototipo MLA.

Esto se hace mediante un transductor de estados finitos que actúa como modelo de lenguaje para el reconocimiento del habla y, simultáneamente, obtiene una forma lógica asociada a la frase pronunciada. Esta forma lógica refleja el significado de la frase. Los sistemas de estas características pueden llevar a cabo con éxito la comprensión del habla en tareas de dominio restringido. Siguiendo estas ideas hemos implementado un prototipo para una tarea denominada Miniature Language Acquisition (MLA). En esta tarea se permite al usuario dibujar círculos, triángulos o cuadrados en un área de dibujo mediante órdenes orales en lenguaje natural. El sistema permite especificar el tamaño y color de las figuras y su posición relativa a otras figuras. También se puede consultar si

### Centralita Automática Dirigida por Voz

La tarea básica de una operadora de centralita telefónica es responder a una llamada telefónica en la cual se demandan algunos servicios, como por ejemplo conectar con una extensión de teléfono local. El principal objetivo al implementar una centralita automática dirigida por voz es gestionar los servicios que una operadora humana puede ofrecer. El estado del arte de las técnicas de Reconocimiento Automático del Habla y Comprensión del Lenguaje permite implementar una centralita automática dirigida por voz. Cuando se trabaja en dominios limitados, un sistema simple puede complementar

de una manera eficiente el trabajo de una operadora humana. Nuestra centralita automática dirigida por la voz es un sistema de reconocimiento de voz continua. Esta característica permite al usuario hablar utilizando frases en lenguaje natural. Además, está basado en una plataforma hardware de bajo coste. El sistema ofrece dos servicios: conectar con el correspondiente número de teléfono de personas de la organización y proporcionar su número de teléfono. Si el usuario no da suficiente información, el sistema automáticamente le solicita datos más específicos. El escenario típico es el siguiente: alguien llama a la centralita automática; esta procesa la entrada oral, decodifica su significado y lleva a cabo la operación solicitada. La centralita telefónica tiene que devolver los resultados de la petición al usuario o recabar más información de este. Es posible que exista más de una persona en la organización con el nombre inicialmente indicado por el usuario. Entonces, el sistema pregunta al usuario por un nombre más específico. Finalmente, el sistema pasa la llamada a la persona solicitada.

### Traducción del habla

Hoy en día, los sistemas de reconocimiento automático del habla con mayor éxito se basan en redes de estados finitos estocásticas. La traducción del habla puede abordarse de una manera similar al reconocimiento del habla. Los transductores de estados finitos estocásticos, que son una particularización de las redes de estados finitos estocásticas, han demostrado ser muy adecuados como modelos de traducción. Los sistemas de traducción del habla más comunes en la actualidad se basan en una arquitectura serie, compuesta por un sistema de reconocimiento del habla y seguidamente por un sistema de traducción de texto, lingüístico o estadístico. El uso de redes de estados finitos estocásticas es realmente adecuado para arquitecturas totalmente integradas, donde los modelos acústicos se integran en el modelo de traducción de manera similar a como se hace en reconocimiento de habla. Esta es una de las características innovadoras de nuestro sistema. Uno de los objetivos principales del proyecto EuTrans fue el desarrollo de sistemas de traducción para tareas de dominio restringido con entrada oral.

### Traducción predictiva interactiva

La tecnología disponible en la actualidad solo permite abordar adecuadamente aplicaciones de traducción automática en dominios limitados. Cuando el dominio de aplicación se generaliza (o incluso se extiende a una lengua completa), la traducción completamente

automática y de calidad no parece posible de momento. Sin embargo sí es posible desarrollar sistemas útiles de traducción asistida. Entre los paradigmas bajo los que se pueden desarrollar sistemas de este tipo se encuentra la Traducción Predictiva Interactiva (TPI). Bajo esta denominación se engloban técnicas de traducción asistida en las que el sistema trata de predecir lo que un traductor humano escribiría. Para ello se usan dos fuentes de información: una frase o párrafo en el lenguaje origen que se desea traducir y algún fragmento de la traducción de esta frase a la lengua destino, que ha sido ya validada por el traductor humano. Con estas informaciones, el sistema predice (una parte de) el resto de la traducción, la cual es nuevamente validada y/o corregida por el traductor humano antes de que sea re-utilizada por el sistema para realizar nuevas y más precisas predicciones. En el ITI se está actualmente llevando a cabo un importante proyecto sobre TPI: el TransType2 (TT2). En TT2 se pretende desarrollar sistemas de traducción asistida que permitan hacer frente a la creciente demanda de traducciones de alta calidad. Se desarrollarán seis versiones diferentes del sistema para la traducción entre inglés y francés, castellano y alemán. La solución propuesta por TT2 se basa en la incorporación de un motor de Traducción Automática dentro de un entorno de TPI. De esta manera, el sistema combina las ventajas de dos paradigmas: por una parte la traducción asistida, en la cual el traductor humano asegura una salida de alta calidad. Por otra parte, la traducción automática, en la que la máquina proporciona la eficiencia necesaria para lograr un aumento de productividad. Para la implementación del motor de traducción empleado en TT2, se utilizan transductores estocásticos de estados finitos, que han demostrado su adecuación para traducción automática en aplicaciones de dominio limitado. Son interesantes por su simplicidad y por la posibilidad de inferir modelos automáticamente a partir de corpus de entrenamiento bilingües. Permiten una búsqueda muy eficiente sobre nuevos datos de test tanto en modo completamente automático como predictivo. Además, se pueden emplear técnicas híbridas de estados finitos y traducción estadística para producir transductores más precisos. En este caso el aprendizaje se basa en utilizar pares de entrenamiento alineados a nivel de palabra mediante técnicas estadísticas.

Autor: Enrique Vidal

Para más información sobre el Grupo de Reconocimiento de Formas y Tecnología del Lenguaje:  
grftl@iti.upv.es

## Calidad y Testeo del Software

Mientras en los grandes centros tecnológicos del mundo es una prioridad desde hace varios años, el concepto de calidad en el software es prácticamente desconocido por un número importante de empresas españolas. Aprender a hacer bien las cosas lleva tiempo, pero es una necesidad si se quiere desarrollar software correcto de forma eficiente. Un proceso de software dirigido por estándares de calidad, soportado por herramientas integradas de gestión automática, integrado con un buen proceso de testeo y realizado por personal capacitado garantiza la construcción de productos consistentes con los requisitos de clientes cumpliendo restricciones de tiempo y presupuesto. Este artículo presenta el concepto de calidad sobre un conjunto de procesos interrelacionados de ingeniería y gestión del software que cooperan dentro del ciclo de vida de un software para construir un producto de software de calidad. El ITI está actualmente involucrado en la definición de metodologías propias de evaluación de la calidad de procesos y productos de software, entre ellos, de métodos de testeo de software para certificar la calidad de los productos finales.

### Introducción

El desarrollo actual de software continúa siendo muy propenso a errores. Un gran número de proyectos termina con grandes retrasos, excediendo sustancialmente presupuestos y recursos planificados. Es frecuente encontrar a desarrolladores trabajando desorganizadamente bajo fuertes condiciones de estrés, dentro de un proceso de software con pobre o nula calidad.

Según un informe reciente del Instituto de Estudios Laborales titulado "Nuevas formas de organización del trabajo y productividad: la visión de la Comisión Europea" (Computerworld, num. 952, pág. 27, diciembre de 2002), España tiene una productividad de un 23% y un 8% inferior a la de los EEUU y la media de Europea, respectivamente. Entre otras causas, el informe destaca la no existencia de modelos de colaboración (en favor del modelo de confrontación), la ausencia de una cultura organizativa centrada en las personas, la falta de confianza en el capital humano, y la no orientación de los funcionamientos empresariales hacia la calidad.

Mientras empresas informáticas de Estados Unidos, Japón, India y parte de Europa llevan años consolidando la calidad en el software como el único camino para desarrollar software correcto en tiempos y presupuestos competitivos, el concepto de "calidad en el software" en España es aún prácticamente desconocido por un número importante de empresas. Es usual la institucionalización de malas prácticas y una carencia notable de profesionales con formación adecuada para cambiar esta situación. Estas son las conclusiones de otro estudio reciente (Computerworld, pág. 2, septiembre de 2001) cuyos resultados señalan que aproximadamente el 30% de las empresas de software españolas no siguen ningún procedimiento de calidad, un 60% basan sus desarrollos en el modelo ISO 9001, y sólo un 3% basa su funcionamiento en las metodologías del CMM. A este último modelo (CMM) se le reconoce con respecto al primero (ISO 9001) mayor rigor y especificidad en la definición de los procesos internos del desarrollo de software, así como el ser una metodología de mejora progresiva. Por otra parte, el Consejo Superior de Informática del Ministerio de Administraciones Públicas ha definido una metodología de planificación, desarrollo y mantenimiento de sistemas de información que se llama Métrica, actualmente en su versión 3, que está siendo implantado por múltiples organismos tanto públicos como privados.

El objetivo de este artículo es presentar el concepto de calidad en el software como parte del proceso de ciclo de vida del software, haciendo énfasis en una breve caracterización de este concepto en áreas y técnicas de ingeniería y gestión del software.

### Qué es calidad y gestión de la calidad

La Organización Internacional de Estándares (ISO, por sus siglas en inglés), que ejerce un rol importante en uniformar definiciones, ha publicado varios estándares relacionados con calidad en general y, en particular, con calidad en el software. Estándares como ISO 8402, 9000, 14598 definen calidad del software como la capacidad de un conjunto de características de un producto, sistema o proceso para satisfacer requisitos de clientes y otras partes interesadas.

El estándar de gestión de la calidad ISO 9000 es actualmente sinónimo de calidad y de buenas prácticas. La teoría detrás de este estándar es que una organización bien gestionada con un proceso de ingeniería bien definido es más probable que construya productos consistentes con los requisitos del cliente cumpliendo restricciones de tiempo y presupuesto, que organizaciones pobremente gestionadas sin un proceso definido. Dentro de la familia ISO 9000, la norma ISO 9000-3 es específica para desarrollo de software y su mantenimiento. La gestión de la calidad del software dentro de este contexto es definida como todas las acciones coordinadas para dirigir y controlar una organización con respecto a calidad del software.

### Gestión de la calidad: 4 pilares del desarrollo

La gestión de la calidad del software actúa sobre 4 pilares que componen el proceso de desarrollo de software:

- procesos de ciclo de vida
- técnicas (¿cómo?)
- organización (¿quién?)
- infraestructura (¿con qué?)

Este artículo se centrará únicamente en los dos primeros pilares, procesos y técnicas, que son los que tienen una vinculación más directa con la calidad del producto final. La organización se basa en las personas, en su formación o especialización, y en cómo se

organizan para desarrollar un proyecto. La infraestructura, por su parte, son las instalaciones, equipamiento, servidores, medios de comunicación, de los que se dispone para el desarrollo de software.

### Procesos del ciclo de vida

El ciclo de vida de un software es el período de tiempo que comienza con la concepción de la idea de un software y que termina con la vida útil del mismo. Durante este período de tiempo cooperan un conjunto de procesos interrelacionados, denominados procesos del ciclo de vida, con el objetivo de construir un producto de software de calidad. Los modelos y estándares internacionales como ISO 12207, IEEE 1074 y CMMI identifican procesos que componen el ciclo de vida de un software. Tomando como base estos estándares, a continuación se identifican las siguientes áreas de procesos:

- **Procesos primarios de ingeniería:** son las actividades primarias del ciclo de vida, aquellas incluidas en las disciplinas técnicas. Independientemente del modelo de ciclo de vida seleccionado (e.g. cascada, espiral, V, W), siempre será necesario el análisis de requisitos, diseño, implementación, validación y verificación, y mantenimiento.
- **Procesos de gestión de proyectos:** cubre las actividades de estimación, planificación del proyecto y asignación de recursos, medición del progreso, seguimiento y control del proyecto, gestión de riesgos y gestión de las relaciones con los clientes.
- **Procesos de aseguramiento de la calidad:** son actividades sistemáticas y planificadas, necesarias para dirigir y controlar los procesos del ciclo de vida con el objetivo de proporcionar suficiente confianza de que el proceso y los productos del desarrollo satisfacen aceptablemente estándares de calidad. Estas actividades ejercen, por tanto, una función de watchdog, controlando todos los procesos del ciclo de vida de software.

La siguiente tabla ilustra la organización de procesos en las diferentes áreas:

| ÁREAS DE PROCESOS |                           |                         |                        |
|-------------------|---------------------------|-------------------------|------------------------|
| PROCESOS          | Ingeniería                | Gestión                 | Calidad                |
|                   | análisis de requisitos    | estimación              | prevención             |
|                   | diseño                    | planificación           | detección y corrección |
|                   | implementación            | medición                | evaluación y mejora    |
|                   | validación y verificación | control y seguimiento   |                        |
|                   | mantenimiento             | gestión de riesgos      |                        |
|                   |                           | relaciones con clientes |                        |

En las secciones que siguen se hace una caracterización breve de cada proceso, haciendo énfasis en aquellos aspectos que definen la calidad del mismo, y que condicionan, en última instancia, la calidad global del ciclo de vida del software.

### Procesos primarios de ingeniería

#### 1. Gestión de Requisitos

La Gestión de Requisitos es el proceso de captura de requisitos, su especificación en un formato bien definido, el uso de prácticas de comunicación (prototipos, entrevistas) para refinar la comprensión de lo que quiere el cliente, la revisión periódica de la consistencia entre

requisitos y otros contenidos del desarrollo (diseño, código, manual de usuarios), y la gestión de cambios en los requisitos durante todo el proyecto.

Una gestión insuficiente de requisitos es una de las causas más frecuentes de que los proyectos se retrasen, sobrepasen sus presupuestos o tengan menos funcionalidad de la esperada. El éxito en la gestión de requisitos depende del conocimiento y la aplicación apropiada de diferentes fundamentos, por ejemplo, metodologías de análisis de requisitos, modelos de representación, prácticas de comunicación, metodología de gestión de cambios en los requisitos, técnicas de verificación y validación de la completitud y corrección de los requisitos y de su consistencia con otros productos del software.

Un gestión correcta y completa de requisitos debe permitir su uso como base para estimar, planificar, diseñar, implementar y verificar y validar el software.

#### 2. Diseño

El Diseño es el proceso de definición de la arquitectura del sistema, de las estructuras de datos y de los algoritmos a emplear, antes de realizar la construcción del software. Algunos fundamentos que garantizan diseños robustos son el conocimiento de estilos (estructurado, OO) y conceptos (modularidad, abstracción) básicos de diseño, algoritmos y estructuras de datos primarias, esquemas típicos de arquitecturas, herramientas de diseño, entre otros.

Los ciclos de vida modernos de software prestan especial atención al diseño de arquitectura, cuya solución suele ser una tarea prioritaria. Organizaciones preocupadas por la calidad de su proceso de software documentan soluciones genéricas de diseño en función del dominio de aplicación a resolver, e incluyen experiencias previas de la aplicación de estas soluciones.

#### 3. Implementación

Cuando se llega a la implementación dentro de un proceso correcto de software, la mayoría del trabajo creativo ya ha sido realizado. En este sentido, la implementación se considera una tarea de bajo nivel. Es decir, prácticas pobres de diseño pueden forzar la reescritura de gran parte del sistema, no siendo necesariamente así en el caso de usar prácticas pobres de codificación. Sin embargo, estas malas prácticas pueden provocar errores sutiles cuya detección y corrección puede costar días o semanas. Por lo tanto, una organización que haga de la calidad una prioridad no debe desconocer ciertos fundamentos de construcción del software, por ejemplo, prácticas correctas y uniformes de codificación, directrices para el uso de tipos de datos, reglas para empaquetar código en módulos, clases o ficheros, prácticas de testeo de unidad y de depuración, estrategias de integración, etc.

La estandarización de las prácticas de implementación de un software simplifican notablemente los esfuerzos de trabajo en grupo, en especial, aquellos orientados al mantenimiento del propio software o al reuso de código en futuros proyectos por personas diferentes.

#### 4. Mantenimiento

De acuerdo a IEEE 1219, el mantenimiento de software es el conjunto de actividades de modificación de un producto de software después de entregado, para corregir fallos, mejorar su rendimiento u otros atributos, o adaptar el producto a un entorno modificado.

Una vez comienzan a operar con el sistema, los usuarios pueden encontrar errores y aspectos que quieran mejorar, los mantenedores

realizan los cambios, después de lo cual los usuarios vuelven a usarlos y a proporcionar nueva información de mejora. Este ciclo de mantenimiento extiende la vida del producto de software. En muchos casos, el mantenimiento es el proceso más largo del ciclo de vida.

El mantenimiento de software es difícil de realizar y gestionar. Sin embargo, este proceso se simplifica notablemente si los procesos primarios previos de ingeniería han sido correctamente realizados y documentados.

### 5. Verificación y Validación

Como proceso de validación y de verificación (V&V) se entiende cualquier actividad orientada a determinar si los objetivos se han cumplido o no. Más específicamente:

- Verificación comprueba la consistencia del software con respecto a especificaciones y requisitos; es decir, responde a ¿se ha construido correctamente el software?
- Validación comprueba si lo que se ha especificado (e implementado) es lo que el usuario realmente desea; es decir, responde a ¿se ha construido el software correcto?

Las tareas de V&V no solo se aplican a productos de software, sino también a otros productos resultantes del proceso del desarrollo. Las primeras tareas de V&V al análisis y a la especificación de requisitos, por ejemplo, comprobando que el proyecto es viable, que las especificaciones documentadas son completas, correctas, precisas, legibles, evaluables, y que, en general, responden a las expectativas del cliente. La V&V del diseño debe garantizar que los requisitos no están incompletos o incorrectamente diseñados. En el caso de la implementación y codificación, la V&V de software es comúnmente conocida como testeo de software.

Existen muchas definiciones incorrectas del testeo de software que conducen a una inadecuada aplicación de este proceso, por ejemplo, “el testeo demuestra que no hay errores”, o “el testeo demuestra que un programa funciona correctamente”. Según Edsgar Dijkstra “el testeo puede demostrar la presencia de errores, no su ausencia”. Por lo tanto, se realiza test al software para detectar errores que, una vez corregidos, mejoran la calidad o fiabilidad del mismo. Existen distintos tipos de testeo en función de la unidad de software a la que se aplique y del objetivo que se persigue, por ejemplo, el testeo de unidad, de integración, de sistema y de aceptación.

Finalmente, las actividades de V&V son también necesarias durante la operación y el mantenimiento del software. Cuando se realiza un cambio en el software, se debe examinar el impacto del cambio sobre el sistema y considerar qué actividades de V&V es necesario repetir para garantizar, al menos, la misma calidad en el software antes del cambio.

### Procesos primarios de gestión

Los fundamentos de gestión consisten en estimar el tamaño del proyecto de software a desarrollar y los recursos (tiempo, personas, medios) necesarios para su construcción, definir y gestionar riesgos e incertidumbres asociados al desarrollo, planificar el proceso de desarrollo asignando recursos a las tareas en función de las estimaciones y riesgos analizados, y finalmente controlar y dar seguimiento al progreso del plan y al uso de los recursos planificados. En proyectos complejos con riesgos importantes, es frecuente realizar re-estimaciones y refinar planificaciones según se va avanzando en el proyecto y se van aclarando incertidumbres iniciales.

### 1. Estimación

El proceso de estimación puede definirse a partir de tres pasos básicos: primero, estimar el tamaño del proyecto a partir de un análisis preliminar de requisitos; luego estimar el esfuerzo total (en unidades de tiempo) que requiere el desarrollo de un proyecto de tal tamaño; por último, estimar el tiempo de desarrollo del proyecto en función del esfuerzo estimado y del personal con el que se cuente para su realización.

La diferencia entre un procedimiento de calidad y otro improvisado es que el primero define metodologías para hacer estimaciones objetivas y contrastadas dando lugar a estimaciones precisas, mientras que en el segundo las estimaciones son resultados de análisis subjetivos y no contrastados conduciendo a resultados vagos, casi siempre, muy optimistas.

### 2. Gestión de Riesgos

Usualmente, cuando realizamos el análisis de un proyecto, aparecen incertidumbres sobre su comprensión, sobre el método de solución, sobre las herramientas de solución, entre otras. De no atender prioritariamente estos aspectos inciertos, conocidos formalmente como riesgos, se convertirán en fuentes potenciales de errores en nuestro proceso.

Una de las líneas esenciales de la gestión moderna de software es la gestión dinámica de riesgos. Este proceso periódico consiste en identificar y analizar cada riesgo, estimar su probabilidad de ocurrencia y su posible impacto en el cronograma, y definir un plan de gestión del mismo, el cual es un grupo de acciones orientadas a prevenir el riesgo o a corregir sus consecuencias, en función del proceso que resulte menos costoso. Una gestión global incluye además el mantenimiento de listas actualizadas de riesgos ordenados por peligrosidad, de forma que nos sea posible centrarnos en aquellas incertidumbres potencialmente más destructivas.

Un procedimiento de calidad para el desarrollo de software debe incluir una metodología de gestión de riesgos, así como un registro de riesgos y errores frecuentes en la organización que ayuden a evitar omisiones importantes.

### 3. Planificación

La planificación consta de dos partes: la división del proyecto en tareas y la asignación de recursos a tareas, es decir, ordenar las tareas en el tiempo, asignándoles recursos humanos y materiales para su realización. El tiempo asignado a una tarea depende de múltiples factores: tamaño y complejidad de la tarea (productos de la estimación), grado de conocimiento o de incertidumbre que tenemos sobre ella (análisis de riesgos), y de la preparación y experiencia del personal que debe realizarla.

En proyectos con riesgos importantes, el tiempo de desarrollo no suele ser cerrado, sino en forma de rango dependiendo de los riesgos presentes. Su posible presentación a clientes debe acompañarse de un documento que relacione incertidumbres con el rango. Estos proyectos deben ser periódicamente re-estimados y su planificación refinada, tareas que deben ser también planificadas.

Es recomendable dentro de un procedimiento de calidad la existencia de una metodología con directrices para realizar planes de desarrollo, relacionada con las metodologías de elaboración de estimaciones y de gestión de riesgos.

#### 4. Control y Seguimiento

Las actividades de control y seguimiento consisten en verificar que el progreso del proyecto se ajusta al plan y a los estándares, es decir, que se están cumpliendo los plazos, costos, y los objetivos de calidad. En otras palabras, el control y seguimiento es un conjunto de actividades de validación y verificación del proceso de desarrollo. Idealmente, estas actividades deben aportar absoluta visibilidad del progreso del desarrollo.

Algunas de estas actividades son revisiones y auditorías técnicas, revisiones de hitos, reportes de estado, realizar mediciones (tiempo, presupuesto) y comparar con estimados, etc.

Las tareas de control y seguimiento deben ser también planificadas. Sin ellas no es posible gestionar un proyecto ni sus riesgos, y no hay forma de saber si los planes se están cumpliendo o no. Un control efectivo permite detectar anticipadamente problemas en el cronograma, cuando aún hay tiempo suficiente para actuar sobre él.

#### 5. Medición de Estadísticos

Una de las claves del progreso a largo plazo de una organización de software es la medición de datos para analizar la calidad del software y la productividad. Aparte de las típicas mediciones sobre costos y tiempos en proyectos, recolectar datos históricos sobre cuán largo es un programa (en líneas de código) o un análisis de requisitos (en número y complejidad de requisitos), nos creará bases objetivas para realizar futuras estimaciones en nuevos proyectos que suelen ser generalmente mejores que el instinto puro.

Procesos más sofisticados colectan mediciones sobre los cambios (errores, mejoras o nuevos requisitos) entre sucesivas versiones, por ejemplo, del documento de análisis de requisitos o de cualquier producto de software. Estas mediciones sobre el número y naturaleza de los cambios permiten conocer más objetivamente el nivel de estabilidad o madurez del producto objeto de medición, el grado de flexibilidad ante cambios, entre otras características.

El procedimiento de calidad de desarrollo de software de una organización, debe definir qué mediciones realizar, con qué objetivo y periodicidad, y cómo van a ser colectadas. Es usual disponer de un software que soporte la recolección automática o semiautomática de estas mediciones, y su uso de acuerdo a los fines para los que han sido definidas.

#### 6. Gestión de Relaciones con los Clientes

El conocimiento y aplicación de buenas prácticas en las relaciones con clientes producen beneficios directos para el desarrollo de un software. Buenas relaciones con los clientes disminuyen el tiempo real y percibido de desarrollo, pues eliminan fuentes importantes de errores y riesgos para el proyecto, y propician una cooperación más activa y comprometida por parte de clientes y usuarios. Estas prácticas se extienden por múltiples áreas de la ingeniería y la gestión, por ejemplo, definir y gestionar riesgos asociados con los clientes, emplear prácticas activas de comunicación para ayudar a clientes a comprender lo que quieren, involucrar a clientes y usuarios en actividades de control del progreso del proyecto, emplear modelos incrementales de ciclos de vida que proporcionen al cliente señales periódicas y tangibles de progreso, entre otras.

Como en los casos anteriores, la organización debe documentar la política de gestión de las relaciones con clientes.

#### Procesos de Aseguramiento de la Calidad del Software

El aseguramiento de la calidad del software (ACS) consiste en controlar que los productos y procesos del desarrollo de software cumplen estándares de completitud y calidad. Como se ha comentado, ACS cumple el rol de watchdog de los procesos del ciclo de vida del software.

Existen dos formas de obtener software de calidad. La primera es prevenir la falta de calidad, definiendo normas, estándares, métodos y técnicas apropiadas durante los procesos del ciclo de vida. La segunda es detectar y corregir la falta de calidad (e.g. errores en el código, en el diseño, en manuales de usuarios, o código complejo mal documentado) a través de la evaluación de procesos, mejoramiento de procesos, revisiones y, por supuesto, testeado de software.

Las actividades de aseguramiento de la calidad deben ser planificadas, con sus correspondientes asignaciones de recursos humanos y materiales. O sea, asegurar la calidad cuesta dinero. Sin embargo, la falta de calidad también tiene un precio. Joseph Juran, uno de los más notables teóricos de la economía de la calidad, propuso en 1951 el análisis de costos relacionados con la calidad en su libro *Quality Control Handbook*. Juran distingue 3 tipos de costos de aseguramiento de la calidad:

- Costos de prevención: costos de actividades específicamente diseñadas para prevenir una calidad pobre.
- Costos de detección: costos de actividades orientadas a encontrar problemas de calidad.
- Costos de fallos: costos derivados de una calidad pobre, por ejemplo, el costo de corregir errores y el costo de atender quejas de

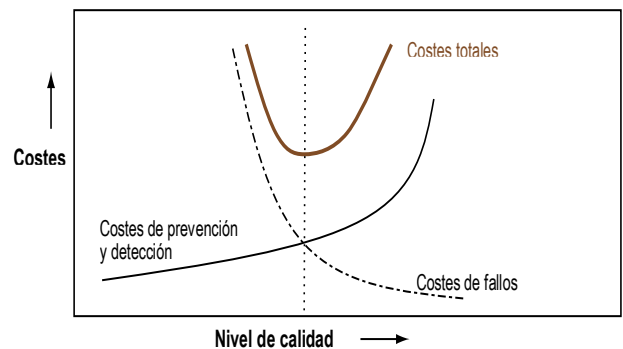


Figura 1: Relación entre costes (Juran).

usuarios, entre otros.

La relación entre estos costos es ilustrada por Juran en la Figura 1. Juran indica que “el costo de las actividades de aseguramiento de la calidad necesarias para alcanzar niveles de calidad altos crece geoméricamente según nos acercamos a la perfección”. Perseguir la perfección, por tanto, no es rentable porque un pequeño incremento en calidad requerirá una gran inversión. Las inversiones en aseguramiento de la calidad deben hacerse mientras el costo total de prevenir y detectar problemas sea menor que el costo de corregirlos.

#### 1. Prácticas de prevención

Los estándares son uno de los medios más efectivos para garantizar la calidad del software. Prácticamente para cada producto a elaborar (manual de usuario, interfaz, código, análisis de requisitos, etc.) o proceso a realizar (análisis de riesgos, diseño, planificación, etc.) deben existir estándares o normas organizacionales que definan

directrices sobre cómo hacerlo. Los estándares tienen dos beneficios principales: i) evitan improvisaciones, olvidos y errores al definir qué hacer y cómo hacerlo y ii) proponen una manera uniforme de hacer que facilitan comparaciones entre proyectos y colaboraciones entre equipos de trabajo diferentes.

Otro grupo de técnicas orientado a prevenir errores y omisiones es el de métodos formales, que hace referencia a una variedad de técnicas de modelación matemáticas aplicables al diseño de sistemas informáticos. Los métodos formales pueden ser usados para especificar y modelar el comportamiento de un sistema y para verificar matemáticamente que el diseño y la implementación del sistema satisfacen sus especificaciones. Estas técnicas pueden ser aplicadas prácticamente a todos los niveles del ciclo de vida del software, por ejemplo, un lenguaje de especificaciones formales para escribir requisitos (VDM, OCL), proceso de transformación de requisitos en código ejecutable que garantice que el código satisface las propiedades especificadas, probar las propiedades de las especificaciones a través de técnicas automáticas como verificación de modelos y prueba de teoremas, formalismos para derivar casos de pruebas a partir de las especificaciones de software, entre otras.

Los métodos formales no son una estrategia de "todo o nada". Aplicar métodos formales solo a las partes más críticas de un sistema es una estrategia útil y muy efectiva. La verificación formal completa debe aplicarse únicamente en sistemas críticos que requieran la máxima fiabilidad.

## 2. Prácticas de detección y corrección

La práctica más conocida de detección de errores es el testeo de software. Aparte de ser un proceso primario de ingeniería (Verificación y Validación) para asegurar que las especificaciones y necesidades del usuario final se satisfacen, el testeo de software también pertenece a las actividades de detección de la gestión de la calidad pues ellas pueden detectar fallos de calidad.

Las actividades de testeo pueden clasificarse en estáticas o dinámicas. Las técnicas de testeo estático detectan errores sin ejecutar el programa, por ejemplo, inspecciones o recorridos de código son técnicas que consisten en detectar errores a través de la lectura de código. El testeo dinámico, por su parte, implica la ejecución de programas.

A su vez, las técnicas dinámicas pueden subdividirse en dos estrategias generales: testeo de comportamiento (caja negra, basado en datos, entrada/salida, basado en requisitos), en la que el tester es completamente ajeno al código fuente del programa, y está únicamente interesado en casos en los que el programa no se comporta como se espera, y el testeo estructurado (caja blanca, basado en lógica, basado en código,) en la que el tester examina la estructura interna del programa con el objetivo de derivar casos de test.

La derivación de casos de test es, independiente de la estrategia de testeo utilizada, su parte más importante y difícil. Existen múltiples técnicas para este fin que varían desde la aplicación informal de heurísticas simples (testeo según la experiencia, testeo de ciclo de datos, testeo de combinación de datos) hasta la derivación formal utilizando modelos como grafos de flujo de datos o de control.

## 3. Evaluación y mejora de proceso

La mejora de procesos de software (SPI, de Software Process Improvement) se orienta a reducir costos y riesgos de los procesos,

acortar el tiempo del proceso de desarrollo, y a incrementar la calidad del producto. Existen múltiples métodos, y técnicas que pueden ser usadas para determinar la efectividad de un proceso y para definir las correspondientes acciones de mejora. Estos modelos se dividen en dos estrategias principales: enfoque top-down, por ejemplo, CMMI, SPICE y BOOTSTRAP, que se basan fundamentalmente en evaluación y en modelos, y enfoque bottom-up, por ejemplo, GQM, QIP y AMI, los cuales aplican fundamentalmente mediciones como guías básicas de mejora.

Los modelos de madurez de proceso de desarrollo de software, como los antes mencionados, no han tratado adecuadamente el proceso de testeo. ¿Qué es exactamente un proceso maduro de testeo? ¿Cómo se debe organizar y poner en marcha la mejora de un proceso de testeo? ¿Cómo se debe incorporar a la organización de una empresa? Para responder a estas preguntas existen modelos especializados para medir la madurez y mejorar el proceso de testeo, por ejemplo, TIM (Test Improvement Model), TOM (Test Organisation Maturity Model), TPI (Test Process Improvement Model) y TMM (Testing Maturity Model).

## Servicios de Calidad del Software

El ITI está involucrado en la definición de una metodología propia de evaluación de la calidad del proceso de software basada en el modelo CMM (Capability Maturity Model), y en el modelo de gestión descrito en el libro Software Project Management: A Unified Framework de Walker Royce. Como consecuencia de una evaluación satisfactoria, el ITI certificará con un sello propio un nivel de calidad en el proceso de software de una organización. Complementariamente se elaborará un informe con la caracterización del estado actual del proceso, sugerencias y recomendaciones de mejoras, y conclusiones finales. La metodología persigue juzgar la efectividad del proceso de software de una organización e identificar aquellas áreas susceptibles de ser mejoradas. La propia metodología pretende ser la herramienta que describa el camino a seguir para incrementar gradualmente la madurez del proceso de software.

El ITI también ha desarrollado servicios de testeo de software que ofrecen a las empresas la posibilidad de adquirir información sobre:

- La eficacia de su proceso de testeo. Estos servicios se dirigirán a la evaluación y el asesoramiento del proceso de testeo de software para poder definir pasos de mejora graduales y controlados. Estos servicios proporcionarán una vista independiente de donde está y a dónde va la empresa.
- La calidad de su propio software o software externo que desean comprar para el uso interno. Estos servicios estarán dirigidos al testeo y evaluación de productos finales de software.

Para la ejecución de todas estas actividades, el ITI cuenta con personal con certificado ISEB que utiliza métodos ampliamente aceptados y probados como TPI, TMM, TMAP, y estándares internacionales mencionados arriba, todo lo cual es una garantía de calidad. Sin embargo, ITI no trata estos métodos como dogmas sino administra, controla y adapta estos métodos por medio de investigación constante con orientación práctica.

Autores: Ramón Mollineda, Tanja Vos  
Para más información sobre Calidad y Testing:  
scq@iti.upv.es

## Noticias Breves

### Goldratt en Solucion.es TIC

El Dr. Eliyahu Goldratt, gran gurú del mundo de los negocios, estuvo presente como conferenciante en la 3ª edición de Solución.es TIC. Este pensador expuso sus teorías sobre el mundo de la gestión empresarial y las nuevas tecnologías, el viernes 9 de mayo en la sala de conferencias de Feria Valencia bajo el lema: "Después de la Meta". La jornada, patrocinada por el Instituto Tecnológico de Informática con el apoyo de la Generalitat Valenciana, despertó un gran interés entre los más de 600 asistentes al evento.



### Se certifican las 4 primeras empresas participantes en el proyecto de promoción de la calidad promovido por el ITI.

El primer semestre de 2003 finaliza con la certificación ISO 9001:2000 por AENOR de las empresas: CLASE 10, IVAL INFORMÁTICA, PULSO INFORMÁTICA Y TESI en el marco del proyecto "Implantación de un sistema de gestión de la calidad ISO 9000:2000 en las empresas del sector informático" apoyado por el Plan de Consolidación y Competitividad de la Pyme.

### Tiger Web: Un nuevo servicio de Seguridad Informática

El Instituto Tecnológico de Informática ha desarrollado la herramienta de análisis de vulnerabilidades Tiger Web. A petición de las empresas, la herramienta, a la que se accede vía web, realiza una extensa serie de pruebas sobre los ordenadores que dispongan de una dirección IP externa, buscando vulnerabilidades que podrían ser utilizadas por usuarios malintencionados para acceder, corromper, destruir o impedir el acceso a dichos sistemas.

## Cursos

Uno de los objetivos fundamentales del ITI consiste en organizar un buen servicio de formación que permita preparar a las empresas en el uso de las Tecnologías de la Información y que tenga localizados a los mejores profesores de las distintas materias, provenientes en su mayoría de las Universidades Valencianas. En virtud de ello, el Instituto realiza cursos estándar y a medida, los cuales se pueden celebrar en cualquier punto de la geografía española, dentro de la propia empresa o, si es más conveniente, en las instalaciones del ITI.

Los **cursos a medida** son acciones de formación que, partiendo de módulos disponibles, se pueden desarrollar adaptándolos a las condiciones particulares de cada empresa, con el objeto de mejorar la tecnología informática de la empresa.

Además, se realizan **cursos subvencionados** al 85% por el Fondo Social Europeo y el IMPIVA, para empresas industriales con sede social o establecimiento de producción industrial en la Comunidad Valenciana. Durante los meses de junio y julio, se han dictado tres cursos de formación continua:

uno sobre **Seguridad de Datos en la Empresa** y otros dos basados en **Lenguaje de Programación Java**. Estos son cursos subvencionados al 85% por el Fondo Social Europeo y el IMPIVA, para empresas industriales con sede social o establecimiento de producción industrial en la Comunidad Valenciana.

Para el mes de septiembre se espera la realización de un **curso sobre Administración de Sistemas Linux**, al cual se invita a participar a todos aquellos que tengan experiencia demostrable en este campo y que sean autónomos o trabajadores en activo. El curso tiene una duración estimada de 30 horas y tendrá lugar los días lunes, miércoles y viernes entre el 15 y el 29 de septiembre, de 16:00 a 20:00 hs.

Más información: [otri@iti.upv.es](mailto:otri@iti.upv.es)

## Ayudas y Subvenciones

### ÁMBITO AUTONÓMICO

#### PLAN DE FOMENTO DE LA I+D+I EN EMPRESAS DE BASE TECNOLÓGICA

##### PROGRAMA DE DESARROLLO E INNOVACIÓN TECNOLÓGICA

**Organismo Gestor:** IMPIVA

**Beneficiarios:** Pymes con sede social o establecimiento productivo en la Comunidad Valenciana.

**Actuaciones apoyables:** Proyectos empresariales de desarrollo tecnológico que supongan la obtención de productos, procesos o servicios innovadores o mejores tecnológicamente respecto a lo ya existente en la Comunidad Valenciana. Proyectos empresariales individuales(1) o en cooperación bajo contrato con centros de investigación (2).

**Tipo de ayuda:** Para proyectos en la modalidad 1, subvenciones a fondo perdido de hasta el 45% del coste elegible del proyecto. Para proyectos en la modalidad 2, subvención de hasta el 45% de la parte correspondiente a la empresa y de hasta el 70% del coste del centro de investigación.

**Plazo:** Durante todo el ejercicio 2003.

##### PROGRAMA DE CREACIÓN Y PROMOCIÓN DE EMPRESAS DE BASE TECNOLÓGICA

**Organismo Gestor:** IMPIVA

**Beneficiarios:** Pymes con sede social o establecimiento productivo en la Comunidad Valenciana que tengan la consideración de empresas de base tecnológica.

**Actuaciones apoyables:** Acciones vinculadas a la constitución o inicio de nueva actividad de empresas que explotan los resultados de proyectos de investigación.

**Tipo de ayuda:**

1. Subvención a fondo perdido de hasta un 50% del coste elegible (máximo de 60.000 Euros). Bonificación del tipo de interés de un préstamo avalado por una entidad autorizada por el Ministerio de Economía:

-Ayuda de hasta 5 puntos porcentuales del tipo de interés anual

-Operación máxima subvencionable: 300.000 Euros / Importe mínimo de la operación: 6000 Euros.

-Plazos del préstamo: 7 ó 5 años con 2 ó 1 de carencia respectivamente, o sin carencia.

2. Avales concedidos a través de la línea de avales concertada entre el IMPIVA y la Sociedad de Garantía Recíproca de la Comunidad Valenciana (SGR).

**Plazo:** Durante todo el ejercicio 2003.

#### PLAN DE MEJORA DE LA COMPETITIVIDAD Y DESARROLLO DEL TEJIDO INDUSTRIAL

##### PROGRAMA DE APOYO A NUEVAS EMPRESAS INDUSTRIALES DE CARÁCTER INNOVADOR O DIVERSIFICADOR

**Organismo Gestor:** IMPIVA

**Beneficiarios:** Pymes de nueva creación (posterior al 1 de enero de 2002) con sede social o establecimiento productivo en la Comunidad Valenciana que realicen una actividad de carácter innovador o diversificador.

**Actuaciones apoyables:** Acciones vinculadas a la constitución o inicio de nueva actividad empresarial: elaboración de un plan de negocios, legalización y constitución de la nueva empresa, trabajos de asesoramiento para la puesta en marcha del negocio, estudios de mercado.

**Tipo de ayuda:**

Subvención a fondo perdido de hasta un 50% de los gastos correspondientes a:

-Los costes de constitución y primer establecimiento que se relacionan como elegibles con un máximo de 3.000 Euros.

-Los servicios de asesoramiento necesarios para el desarrollo del proyecto y promoción del mismo hasta un máximo de 6.000 Euros.

**Plazo:** Durante todo el ejercicio 2003

##### PROGRAMA DE MODERNIZACIÓN TECNOLÓGICA

**Organismo Gestor:** IMPIVA

**Beneficiarios:** Pymes con sede social o establecimiento productivo en la Comunidad Valenciana

**Actuaciones apoyables:**

-Actuación 1: Préstamos avalados por una entidad autorizada, dirigidos a la financiación de activos fijos materiales, fijos inmateriales vinculados a la inversión.

-Actuación 2: Avales concedidos a través de la línea de avales concertada entre el IMPIVA y la Sociedad de Garantía Recíproca de la Comunidad Valenciana para inversores de mayor nivel tecnológico que requieran de unas garantías adicionales.

**Tendrán prioridad los proyectos con asesoramiento de Centros Tecnológicos.**

**Tipo de ayuda:**

-Para proyectos en la actuación 1: Ayuda de hasta 5 puntos sobre el tipo de interés.

-Para proyectos en la modalidad 2: Avales concedidos a través de la línea de avales concertada entre el IMPIVA y la Sociedad de Garantía Recíproca de la Comunidad Valenciana.

**Plazo:**

-Actuación 1: 25 de septiembre de 2003.

-Actuación 2: Durante todo el ejercicio 2003

#### PROGRAMA DE FORMACIÓN A MEDIDA PARA EMPRESAS

**Organismo Gestor:** IMPIVA

**Beneficiarios:** Pymes con sede social o establecimiento productivo en la Comunidad Valenciana.

**Actuaciones apoyables:** Cursos de formación presentados por pymes diseñados e impartidos por centros de la Red de Institutos Tecnológicos de la Comunidad Valenciana (REDIT). Tendrán una duración de entre 10 y 30 horas, y podrán prepararse para un grupo de entre 1 y 10 trabajadores. Podrán desarrollarse tanto en las instalaciones del Instituto Tecnológico como en las de la propia empresa solicitante. Todos los alumnos deben ser residentes en la Comunidad Valenciana y serán empresarios o trabajadores en activo.

**Tipo de ayuda:** El importe máximo de la ayuda por proyecto podrá llegar hasta el 45% de los costes elegibles, con un máximo de 90 Euros por hora de formación.

**Plazo:** Durante todo el ejercicio 2003.

### ÁMBITO NACIONAL

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

**Organismo Gestor:** MINISTERIO DE CIENCIA Y TECNOLOGÍA -FONDO SOCIAL EUROPEO

**Beneficiarios:** Empresas y Centros Tecnológicos que cuenten con un centro de trabajo en las zonas del objetivo 1 y 2, y que deseen llevar a cabo actividades de investigación o reforzar una línea de I+D+i existente, mediante la realización de un proyecto de investigación industrial o un estudio de viabilidad técnica previo.

**Actuaciones apoyables:** Contratación de Doctores o Tecnólogos para llevar a cabo tareas de investigación industrial o un estudio de viabilidad técnica previo.

**Tipo de ayuda:** En el caso de las zonas definidas como Objetivo 1 por la normativa europea (Andalucía, Asturias, Canarias, Castilla-La Mancha, Castilla-León, Comunidad Valenciana, Extremadura, Galicia y Región de Murcia), financia **hasta el 75 por ciento del coste de contratación, con un total de hasta**

**70.000 euros para la contratación de cada doctor y más de 50.000 euros para cada tecnólogo** durante un máximo de tres años. En el caso de las zonas definidas como Objetivo 2, las ayudas ascienden a 47.000 y 35.000 euros. Además, **existe una deducción fiscal adicional del 10 por ciento por la contratación de personal** dedicado a tareas de I+D. Asimismo, las **ayudas del Programa Torres Quevedo son compatibles con otras ayudas comunitarias, nacionales o regionales** (siempre que no procedan de Fondos Estructurales de la Unión Europea).

**Plazo:** Hasta el 30 de Junio de 2004 .

**PROGRAMA CRECE DE LA EOI (ESCUELA DE ORGANIZACIÓN INDUSTRIAL).**

**Organismo Gestor:** MINISTERIO DE CIENCIA Y TECNOLOGÍA -FONDO SOCIAL EUROPEO.

**Objetivo:** Desarrollo de un programa de formación y asesoramiento dirigido a emprendedores y PYMES con una atención especial a las Nuevas Tecnologías, durante el periodo 2001 – 2006.

**Beneficiarios:** El programa está dirigido a:  
 1. **CREACIÓN DE EMPRESAS:** Emprendedores que quieran crear empresas, tanto en sectores con notable componente tecnológico como en sectores "tradicionales" en los que se pondrá un énfasis especial en las Tecnologías de la Información y las Comunicaciones.  
 2. **CONSOLIDACIÓN DE EMPRESAS:** PYMES de reciente creación que necesiten un apoyo para su consolidación, especialmente en el campo del e-business y las nuevas tecnologías.

**Modo de Implantación del programa:** Se desarrollará en todas las Comunidades Autónomas y en colaboración con numerosos socios con implantación local, especialmente las Cajas de Ahorro a través de la C.E.C.A

**Plazo:** Hasta 2006.

**FINANCIACIÓN DE PROYECTOS DE I+D+I EMPRESARIALES EN EL MARCO DEL PLAN NACIONAL DE I+D+I**

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

**Beneficiarios:** Sociedades Mercantiles con capacidad técnica para desarrollar un proyecto de investigación, desarrollo o innovación tecnológica y capacidad financiera para cubrir con recursos propios un mínimo del 30% del presupuesto total del proyecto.

**Actuaciones apoyables:** Proyectos de Desarrollo Tecnológico; proyectos de Innovación Tecnológica; proyectos de Investigación Industrial Concertada.

**Tipo de ayuda:** Créditos a tipo de interés "cero" y con largo plazo de amortización que cubren hasta el 60% del presupuesto total del proyecto.

El Centro sólo apoya proyectos viables técnica y económicamente, pero no exige garantías reales a la empresa promotora para la concesión de sus créditos. La financiación que presta el CDTI proviene básicamente de los recursos propios del Centro y del Fondo Europeo de Desarrollo Regional (FEDER).

**PROGRAMA ARTE/PYME II**

**Organismo Gestor:** MINISTERIO DE CIENCIA Y TECNOLOGÍA -FONDO SOCIAL EUROPEO

**Beneficiarios:**  
 1. Las organizaciones públicas o privadas que, sin ánimo de lucro, tengan la finalidad de prestar servicios de apoyo a las PYME, mediante la realización de proyectos comunes de asistencia o la promoción de servicios que contribuyan a la mejora de la competitividad de la PYME.  
 2. Agrupaciones de interés económico de empresas que cumplan la finalidad del párrafo anterior.

El Programa ARTE/PYME II 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: estudios de necesidades y viabilidad, proyectos piloto, implantación de Centros de Servicios Avanzados de Teleco-municación o promoción del uso de Servicios Avanzados de Telecomunicación.

**Tipo de ayuda:** El importe de las subvenciones podrá, aisladamente o en concurrencia con otras subvenciones o ayudas, superar el 60% del coste de la actividad a desarrollar por el beneficiario. Solamente 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. Los bienes subvencionados deberán destinarse a los objetivos que justifican la concesión de la subvención durante un período mínimo de tres años.

**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:** MINISTERIO DE CIENCIA Y TECNOLOGÍA -FONDO SOCIAL EUROPEO

**Beneficiarios:** Empresas y Organismos Intermedios.

**Actuaciones apoyables:** Actuaciones de formación general: actuaciones de formación de usuarios de telecomunicaciones y nuevas tecnologías de la información; actuaciones dirigidas a la formación de profesionales que desempeñen puestos de trabajo relacionados

con la telecomunicaciones y las tecnologías de la información.

**Modalidades:**  
 -Proyecto o actuación individual: llevados a cabo por una entidad solicitante.  
 -Proyecto o actuación en cooperación: llevados a cabo por dos o más entidades.

**Tipo de ayuda:** Subvención del 70 % del coste de la actuación, cualquiera sea el tipo de beneficiario, excepto si se trata de grandes empresas, en cuyo caso la subvención sería del 50 %. En las zonas del objetivo 1 (Comunidad Valenciana) el porcentaje de ayuda se incrementa un 10%.

**Plazo:** Hasta el 30 de junio de 2006.

**ÁMBITO INTERNACIONAL**

**PROGRAMAS EUREKA E IBEROEKA**

**Organismo Gestor:** CDTI – MINISTERIO DE CIENCIA Y TECNOLOGÍA (PROFIT)

**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 Iberoeika.

**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.

**Plazo:** Durante todo el ejercicio 2003.

**VI PROGRAMA MARCO DE LA UNIÓN EUROPEA**

**Organismo Gestor:** COMISIÓN DE LA UNIÓN EUROPEA

**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 pequeñas y medianas empresas (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:** Realización de proyectos de carácter innovador.

**Para más información :**  
[otri@iti.upv.es](mailto:otri@iti.upv.es)



UNIVERSITAT  
POLITÈCNICA  
DE VALÈNCIA



 GENERALITAT VALENCIANA  
CONSELLERIA D'INDÚSTRIA, COMERC I ENERGIA

**IMPIVA**