ISSN: 1870-7157

TECNOCULTURA

Investigación · Ciencia · Tecnología · Cultura

Publicación cuatrimestral del Tecnológico de Estudios Superiores de Ecatepec. Año 9, No 22, mayo-agosto del 2010

Críptografía de curva elíptica

Sistema de asistencia tecnológica

Extracción de patrones de huellas digitales: algoritmos MAIO vs Empate

Los sistemas distribuidos y el reto de compartir recursos en las organizaciones

La calidad en los procesos de software

El Tecnoilógico de Estudios superiores de Ecatepec cuenta con un sistema de gestión de calidad certificado bajo la Norma ISO 9001:2000 en sus procesos de inscripción, reinscripción y titulaci{on, con reconocimiento ante EMA, UKAS y ANAB

editorial

Estimado lector:

El ámbito tecnológico, se ha convertido desde hace varias décadas, en una actividad inseparable del progreso de la sociedad, muestra de ellos son los cinco interesantes temas que abordamos en este número de la Revista Tecnocultura.

En primer lugar, abortamos el tema de la Criptografía de Curva Elíptica, que permite construir sistemas de encriptación de información. En el artículo se describe qué son, cómo se utilizan, sus ventajas y la comparación con otros sistemas utilizados para el mismo fin.

Posteriormente, un tema de actualidad y de impacto directo en la sociedad, los Sistemas de Asistencia Tecnológica; nos habla de cómo se puede mejorar el desarrollo de las personas con algún tipo de discapacidad, a través de la aplicación de recursos tecnológicos con el objeto de aumentar, mantener o incrementar sus habilidades, mejorando su calidad de vida.

Sabía usted, querido lector que cada persona en el mundo tiene su propia forma de huellas digitales y que éstas son diferentes a las de cualquiera otra persona que jamás haya existido. Éste interesante tema, es abordado en el artículo Extracción de Patrones de Huellas Digitales, analizado desde el punto de vista de los modelos matemáticos. En éste se proporciona un estudio comparativo de los algoritmos Maio y Empate, los cuales son ampliamente utilizados en este ámbito.

Siguiendo con temas informáticos, el artículo Los Sistemas Distribuidos y el Reto de Compartir Recursos en las Organizaciones, nos habla de las principales características y beneficios de estos sistemas, cuya intención es convertir un grupo de máquinas aisladas en un sistema coherente cuyo objetivo principal es la distribución de información. Actualmente los sistemas informáticos juegan un papel importante en las empresas, se podría decir que son el sistema nervioso de la organización, permitiendo que la información llegue a todas las áreas, fomentando la actuación conjunta y coordinada, sin importar las distancias físicas que las separen.

Finalmente, la globalización y las crisis económicas, han obligado a las empresas mexicanas a producir más y mejor. Por ello, son cada vez más las empresas que implementan algún modelo de calidad, que les permita optimizar su producción y obtener la satisfacción del cliente. Actualmente como la tecnología está involucrada en todos los ámbitos, existen programas que ayuda en ésta tarea, proporcionando una guía para mejorar los procesos en las empresas y administran el desarrollo, adquisición y mantenimiento de los productos o servicios. Sobre este interesante tema pueden conocer en el artículo La Calidad en los Procesos de Software.

Esperamos que la presente publicación, sea del interés de todos nuestros lectores.

Directorio

Compromiso
Gobierno que cumple

Responsable de la publicación
Beatriz Barrera Castañeda

Corrección de estilo
Rafael Ortiz Hernández

Diseño:
Mara Brisa López Vargas

SECRETARÍA DE EDUCACIÓN
SUBSECRETARÍA DE EDUCACIÓN MEDIA SUPERIOR Y SUPERIOR
TECNOLÓGICO DE ESTUDIOS SUPERIORES DE ECATEPEC

Contenido

Tecnocultura, revista de divulgación del conocimiento científico, tecnológico y humanístico del Tecnológico de Estudios Superiores de Ecatepec. Año 6, No.22, mayo-agosto *de 2010. Número de autorización del Comité Editorial de la Administración Pública Estatal CE:*
Edita y distribuye la Unidad de Relaciones Públicas y Difusión, domicilio: Av. Tecnológico (antes Valle del mayo) s/n, Col. Valle de Anáhuac, C.P. 55210, Ecatepec, Estado de México. Teléfono 50 00 23 14. Correo electrónico: difusion@tese.edu.mx. Imprenta:

Número de Reserva de Derechos al Uso Exclusivo del Título ante el Instituto Nacional del Derecho de Autor de la Secretaría de Educación Pública: 04-2006-090109555900-102, ISSN: 1870-7157. Certificados de Título y de Contenido en trámite. Se imprimen 1000 ejemplares.

Criptografía de curva elíptica

A. Hernández Estrada[1]
A. Gonzales-Quevedo[1]
I. Cardiel-Alcocer Guillermo[2]
J. E. Rámirez-Navarrete[2]
E. Corona-Organiche[2]

Resumen

La mayor parte de los sistemas de encriptación de clave pública basan su seguridad en la solución de algún problema matemático, ya que las posibilidades de encontrar la respuesta son sumamente bajas, debido a la gran cantidad de números generados. Las curvas elípticas son de nueva generación, usadas en criptografía para formar claves o firmas digitales, especialmente en criptografía asimétrica. Una de sus mayores ventajas es la velocidad que ofrece, debido a que requiere longitudes de clave mucho menor a las de criptosistemas como RSA o Diffie Hallman.

En este documento, estudiaremos inicialmente la formación de una curva elíptica y cómo se están utilizando para construir sistemas de encriptación de clave pública, además de una comparación con otros sistemas criptográficos utilizados en la actualidad.

Palabras clave: Curva elíptica, Criptografía de curva elíptica, Clave pública.

Introducción

Todos los sistemas de encriptación conocidos en la actualidad, basan su seguridad en la resolución de algún problema matemático que por su gran magnitud, es casi imposible de resolver en la práctica en un tiempo menor al esperado.

Como una opción, en 1985 Neil Koblitz y Victor Miller propusieron el Elliptic Curve Criptosystem (ECC) o Criptosistema de Curva Elíptica, basado en los métodos de Diffie-Helman y DSA de clave pública (Belingueres, 2005, 29).

El ECC puede ser usado tanto para encriptar como para firmar digitalmente, y hasta hoy no se ha conocido algún ataque que recorte el tiempo exponencialmente calculado

Acerca de los autores...

[1] Tecnológico de estudios Supriores de Ecatepec (TESE)
[2] División de Ingeniería en Sistemas Computacionales del TESE

para romper el ECC, lo que facilita su uso al crear claves más pequeñas sin necesidad de grandes recursos computacionales.

Las curvas elípticas

En criptografía, se habla de curva elíptica en referencia a una ecuación

$$y^2=x^3+Ax+B \quad (1)$$

que cumple:

$$4A^3+27B^2 \neq 0 \quad (2)$$

Al asignar diferentes valores a A y B, obtenemos un conjunto de curvas que, al ser dibujadas, ofrecen una forma similar. Son ejemplos de curvas elípticas $y^2=x^3-x$ a la izquierda de la Figura 1 y $y^2=x^3-x+1$ a la derecha de la misma.

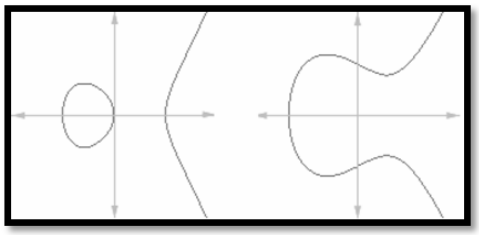


Figura 1
Familia de Curvas Elípticas

Las curvas elípticas tienen ciertas características que las hacen especiales en el mundo de la criptografía. Una de éstas consiste en la posibilidad de generar un punto en una curva, partiendo de dos puntos dados (o incluso de uno). Este concepto es fácil de entender partiendo de la Figura 2, como sigue.

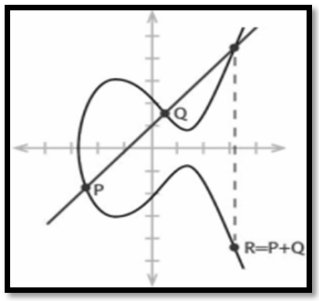


Figura 2
Suma de P y Q.

Usamos como puntos de partida P y Q, dos puntos conocidos. Trazaremos una línea entre P y Q. Si la línea corta la curva en un tercer punto, lo reflejaremos a través del eje, dando lugar a un nuevo punto R. Esta operación se representa como:

$$R = P + Q \quad (3)$$

En caso de que la línea que pasa por P y Q no corte a la curva en ningún otro punto, diremos que corta la curva en un punto O en el infinito y representaremos esta operación como:

$$P + Q = O \quad (4)$$

Partiendo de la suma, no es difícil encontrar un mecanismo que nos permita realizar multiplicaciones de tipo kP, siendo k un escalar. Por ejemplo, imaginemos que que-

remos realizar la operación 13P, es decir, multiplicar 13 por un punto P. Bastaría con realizar la siguiente secuencia de doblado de puntos:

$$P,\ 2P = P + P,\ 4P = 2P + 2P,\ 8P = 4P + 4P,\ 13P = 8P + 4P + P \quad (5)$$

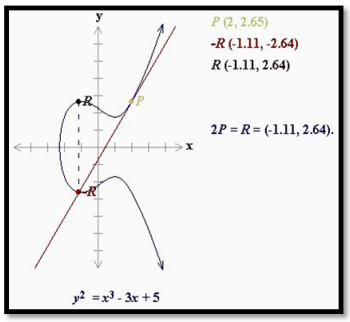


Figura 3
Suma del mismo punto P

Este simple mecanismo para generar nuevos puntos, dota a una curva elíptica (Figura 3) de la posibilidad de realizar operaciones aritméticas sobre ella, que es la base de los criptosistemas mencionados.

En criptografía, las curvas elípticas se usan sobre campos finitos ($\mathbb{F}q$) con q muy grande. Un ejemplo de campo finito podría ser $\mathbb{F}5=\{0,1,2,3,4\}$. De manera que el número 7 representado en el campo finito correspondería a

$$7 \bmod 5 = 2 \quad (6)$$

Cuando se usan campos finitos, el número de puntos que hay en una curva también es finito. Este número se llama orden de la curva y se representa como $\#\mathbb{E}$. Debemos diferenciarlo del orden de un punto, que se refiere al valor k más pequeño (diferente de 0) que multiplicado por P da O.

El problema del logaritmo discreto (DPL)

La criptografía de clave pública basa su fuerza en la dificultad de resolver ciertos problemas matemáticos. Uno de los más usados es el logaritmo discreto (Discrete Logarithm Problem DLP). Este problema se basa en la dificultad que representa resolver una ecuación de tipo

$$x = ay \bmod n \quad (7)$$

donde x, a y n son conocidas y e es la variable que se busca. De hecho, para valores de n e y suficientemente grandes, es computacionalmente imposible resolver el problema, al menos con los algoritmos y ordenadores actuales.
Otros criptosistemas han sido propuestos, cuya seguridad se basa en el DLP, entre ellos están:

- Los esquemas de acuerdo de claves, derivados del Diffie-Hellman, como ElGamal, la familia de protocolos MTI y el protocolo STS (Station-to-Station).

- El esquema de firma digital ElGamal y sus variantes, como DSA (Digital Signature Algorithm), el esquema de firma de Schnorr, y el esquema ElGamal con recuperación de mensaje de Nyberg-Rueppel.

El algoritmo más rápido conocido para resolver este problema, es el Index Calculus, que permite resolverlo en tiempo subexponencial.

El problema del logaritmo discreto en curvas elípticas (ECDLP)

Existe un problema similar al del logaritmo discreto que puede usarse con curvas elípticas. Anteriormente, hemos visto cómo realizar una operación tipo Q = kP de una forma sencilla. Sin embargo, obtener k y P partiendo sólo de Q, es computacionalmente difícil. De hecho, el algoritmo más rápido que permite encontrar una solución es el Rho de Pollard, pero éste es de tiempo exponencial, mucho más lento que en el caso del ataque a DLP mediante el Index Calculus.

Este hecho es muy importante, pues la dificultad de resolver ECDLP frente a DLP permite que los criptosistemas que se basan en el primero, usen claves mucho más cortas. Así, los sistemas que usan ECDLP requieren mucha menos memoria y capacidad de proceso.

Una clave RSA de 4,096 bits, ofrece la misma seguridad que la de un criptosistema de Curva Elíptica de 313 bits.

La similitud de las definiciones, hace que todos los criptosistemas basados en el DLP puedan ser adaptados utilizando curvas elípticas. De esta forma, existen variantes en los protocolos y esquemas anteriores convertidos a curvas elípticas, y entonces tenemos ECDSA, EC Diffie-Hellman, encriptación EC ElGamal, etcétera.

Algunas leves modificaciones técnicas son necesarias para adaptarlos al grupo de las curvas elípticas, pero los principios subyacentes son los mismos que para los otros sistemas basados en el DLP.

Comparación con otros criptosistemas

Seguridad: el nivel de seguridad está determinado por el valor de la información, el tiempo que debe ser protegida, el tamaño de los parámetros que serán usados, entre otros. Los sistemas basados en ECC brindan la misma protección que los ya tradicionales, como se puede observar en la Tabla 1, donde los niveles de seguridad se dan en bits según la longitud de la clave.

Nivel de Seguridad	Esquema Simétrico (tamaño de clave)	Esquema Basado en ECC (tamaño de n)	DSA/RSA (tamaño del módulo)
56	56	112	512
80	80	160	1024
112	112	224	2048
128	128	256	3072
192	192	384	7680
256	256	512	15360

Tabla 1
Tamaños de clave comparables (en bits)

Eficiencia: se deben considerar los siguientes factores:

- Sobrecarga en Cálculos: Cuánto tiempo de ejecución se requiere para transformar las claves privadas y públicas.

- Tamaño de Clave: Cantidad de bits requeridos para almacenar el par de claves y otros parámetros (Tabla 2 y 3).

	Parámetros del Sistema	Clave Pública	Clave Privada
RSA	n / a	1088	2048
DSA	2208	1024	160
ECC	481	161	160

Tabla 2
Tamaño de los parámetros del sistema y par de claves (en bits)

	Tamaño de Firma
RSA	1024
DSA	320
ECC	320

Tabla 3
Tamaño de firma (en bits)

- Ancho de banda: Cantidad de bits que deben ser comunicados para transferir un mensaje (Tabla 4).

	Tamaño del mensaje encriptado
RSA	1024
DSA	2048
ECC	321

Tabla 4
Tamaños de mensajes encriptados (en bits)

Por lo tanto todos estos ahorros provocan una sobre carga en cálculos más eficiente en una proporción considerablemente menor de tiempo mejorando el consumo y reduciendo el tamaño del código.

Intercambio de claves usando curva eliptica con Diffie-Hellman (ECDH)

El intercambio de claves de Diffie-Hellman es un protocolo que hace posible un intercambio secreto y seguro de claves entre dos partes que no han tenido un contacto previo. Se usa ampliamente en criptografía y se basa en el problema del logaritmo discreto (DLP). Por lo tanto, puede usarse el mismo algoritmo a través del problema ECDLP.

Al algoritmo puede resumirse en los siguientes pasos:

1. Alice y Bob eligen una curva elíptica E sobre un campo finito $\mathbb{F}q$, de manera que el ECDLP sea computacionalmente difícil. También eligen un punto P en dicha curva de modo que su orden sea un número primo grande.

2. Alice elige un entero grande a, calcula PA = aP y envía PA a Bob.

3. Bob elige un entero grande b, calcula PB = bP y envía PB a Alice.

4. Alice calcula aPB = abP

5. Bob calcula bPA = abP

Al finalizar el algoritmo, tanto Alice como Bob disponen de abP, pero un usuario que escuche el canal, sólo habrá podido obtener PA y PB, los cuales no le permiten calcular abP a menos que resuelva el ECDLP. Alice y Bob únicamente necesitarán extraer una clave a partir de abP y usarla para enviar datos cifrados. Para tal propósito, podrán usar cualquier algoritmo simétrico como DES, AES, etcétera.

Algoritmo de curva elíptica para firma digital (ECDSA)

El algoritmo de firma digital para curvas elípticas está basado en el estándar de firma digital DSA. Este algoritmo ofrece un esquema que permite firmar documentos y verificar las firmas. Los pasos a seguir para generar claves (firmar y verificar la firma), se muestran a continuación:

Alice genera un par de claves:

1. Alice elige una curva E con orden $\#\mathbb{E}$ = fr, de manera que r sea un primo grande.
2. Alice busca un punto en la curva de orden r.
3. Alice elige un número aleatorio d situado en el intervalo [2, r-2] y calcula Q = dP.
4. La clave pública corresponde a (E,P,r,Q) y la clave privada a d.

Alice firma un documento M. (h(M) corresponde al hash de M)

1. Alice elige un número aleatorio k en el intervalo [2, r-2].
2. Se calcula el punto (x, y) = kP
3. R=x mod r
4. s = k-1 (h(M) +Rd) mod r, si s es igual cero, empezamos de nuevo.
5. La firma de Alice es (R,s) y se transmite junto con el mensaje M.

Bob verifica la firma de Alice.

1. Bob obtiene la clave pública de Alice.
2. w = s-1 mod r
3. u1 = h(M) w mod r
4. u2 = Rw mod r
5. (x, y) = u1P + u2P
6. v = x mod r
7. Si v es igual a R, la firma es válida.

Conclusiones

Los sistemas basados en curva elíptica ofrecen un mejor rendimiento, hablando en términos computacionales, a pesar de que su implementación no ha llegado a un alto porcentaje como un método de encriptación aceptado, puesto que aún no posee el nivel de confianza que se gana a través de los años, sin embargo, tiene un futuro prometedor, ya que su implementación no requiere de grandes equipos de computo.

Referencias...

[1] Belingueres, Gabriel. Introducción a los Criptosistemas de Curva Elíptica, Chucabuco Buenos Aires, Argentina, 2005.

[2] Certicom, Certicom ECC tutorials, http://www.certicom.com/index.php

[3] De Win,E. and Prencel, B. Elliptic Curve public key Cryptosystems - an introduction,

[4] Hankerson, Darrel, Menezes, Alfred and Vanstone, Scott. Guide to Elliptic Curve Cryptography, 2003.

[5] NIST, Digital Signature Standar, FIPS PUB 186-2, http://csrg.ncsl.nist.gov/fips/, Enero 2000.

Sistema de asistencia tecnológica

Daniel Alcocer León*
Javier Norberto Gutiérrez Villegas*
Israel Isaac Gutiérrez Villegas*

Resumen

Según datos estadísticos, el índice de discapacidad en México ha aumentado considerablemente. El desarrollo de tecnologías de asistencia, busca que, a través de la automatización y reingeniería de los métodos para realizar pruebas de diagnóstico del estado clínico de pacientes con impedimentos, se pueda ayudar al especialista en el área y al paciente, con resultados óptimos y precisos, y a su vez que, mediante los parámetros que éste arroje, se pueda generar una herramienta de terapia funcional y especializada, según las circunstancias de cada persona.

El Sistema Neurológico de Asistencia Tecnológica realiza un test especializado, con base en normas de evaluación, para que a su vez genere el estado clínico previo, con el cual se procesa la información a fin de crear una herramienta de apoyo o rehabilitación personalizada y acorde a las necesidades del paciente.

Acerca de los autores...

*** Tecnológico de Estudios Superiores de Ecatepec.**

Introducción

Una persona con discapacidad "es aquella que presenta una limitación física o mental de manera permanente o por más de seis meses, que le impide desarrollar sus actividades en forma que se considera normal para un ser humano".

Existen diferentes tipos de discapacidad, las más conocidas son:

- Motriz, que se refiere a la pérdida o limitación de una persona para moverse, caminar, o mantener algunas posturas de todo el cuerpo o de una parte del mismo.
- Visual, que incluye la pérdida total de la vista, así como dificultad para ver con uno o ambos ojos.
- Mental, abarca las limitaciones para el aprendizaje de nuevas habilidades, alteración de la conciencia y capacidad de las personas para conducirse o comportarse en las actividades de la vida diaria, así como en su relación con otras personas.
- Auditiva, corresponde a la pérdida o limitación de la capacidad para escuchar.
- Del lenguaje, que engloba las limitaciones y problemas para hablar o transmitir un significado entendible.

Los motivos que producen discapacidad en las personas pueden ser variados, y se clasifican en cuatro grupos de causas principales: nacimiento, enfermedad, accidente y edad avanzada. Por tanto, es necesario ayudarse de diferentes tecnologías para poder atender todos los requerimientos que por derecho tienen las personas con discapacidad.

En la actualidad, la tecnología ya puede auxiliar a personas con impedimentos físicos o mentales para comunicarse, moverse y llevar a cabo sus funciones básicas. El uso de la asistencia tecnológica permite que la gente con diversas discapacidades aumente su funcionamiento, su movilidad y se desarrolle con éxito en el aspecto social y académico, de acuerdo con su capacidad.

Marco teórico

La neurología es la especialidad médica que trata los trastornos del sistema nervioso. Específicamente se ocupa de la prevención, diagnóstico, tratamiento y rehabilitación de todas las enfermedades que involucran al sistema nervioso central, el sistema nervioso periférico y el sistema nervioso autónomo, incluyendo sus envolturas (meninges), vasos sanguíneos y tejidos como los músculos.

Áreas cognoscitivas y procesos que se evalúan:

- Orientación.
- Atención y Concentración: Deficiencias en el nivel de conciencia o estado de activación.
- Atención selectiva
- Atención sostenida
- Control atencional
- Memoria

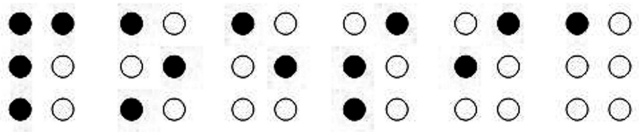
- Memoria sensorial
- Memoria a corto plazo
- Memoria a largo plazo
- Memoria de trabajo

El estudio de la Comunicación Humana puede subdividirse en tres áreas:

- Sintáctica: abarca los problemas relativos a la transmisión de información. Se refiere a los problemas de codificación, canales, capacidad, ruido, redundancia, etcétera.

- Semántica: el significado constituye la preocupación central de la semántica. Toda información compartida presupone una convención semántica.

- Pragmática: cuando la comunicación afecta a la conducta. Comunicación y conducta se usan como sinónimos, ya que toda conducta comunica. Comunicar no implica solo el lenguaje verbal. Así, desde la perspectiva de la pragmática, toda conducta y no solo el habla, es comunicación. Además, no solo interesa el efecto de una comunicación sobre el receptor, sino también el efecto que la reacción del receptor tiene sobre el emisor.



Asistencia Tecnológica es todo tipo de equipo o servicio que puede ser usado para aumentar, mantener o mejorar las capacidades funcionales de las personas con impedimento. Los equipos de Asistencia Tecnológica son objetos, sistemas o productos adquiridos comercialmente, adaptados o construidos a base de las características y necesidades particulares de cada persona con impedimento.

Algunos ejemplos de equipos de asistencia tecnológica son: bastones, andadores, sillas de ruedas, tableros de comunicación, audífonos, equipos adaptados para recreación y computadoras adaptadas, entre otros.

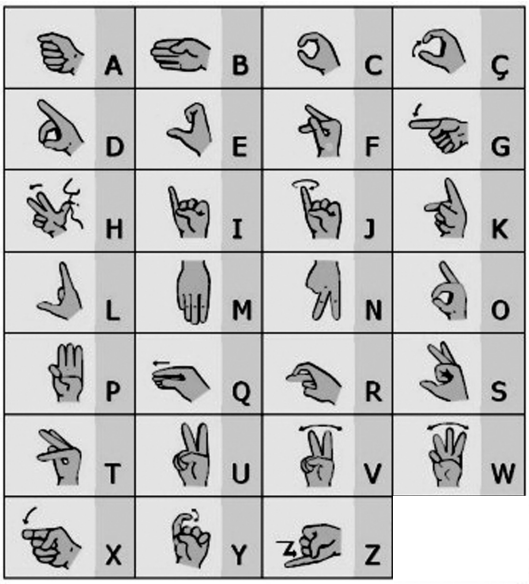
Los sistemas de comunicación no vocal son todos aquellos que permiten la expresión a través de símbolos, distintos a la palabra articulada directamente a través de herramientas. Dichos sistemas han sido llamados también sistemas alternativos de comunicación.

Resultados

Las medidas económicas adoptadas para las pruebas sobre el lenguaje y la audición por medio de las instituciones públicas y particulares se han visto rezagadas por los altos costos que estas implican y por el mantenimiento que requiere.

Es necesario crear una conciencia altruista y participar generosamente en la innovación tecnológica para mejorar enormemente la calidad de vida de las personas con impedimentos. Por ejemplo los aparatos de asistencia tecnológica ayudan a las personas a leer, escuchar, hablar, escribir, aprender, completar tareas, y a participar en la sociedad. Esta medida debe ser tomada en cuenta.

El desarrollo de recursos tecnológicos en las diferentes ramas del conocimiento humano, han tocado la puerta desde hace ya algún tiempo al campo de la rehabilitación identificándose a sí mismas como Ayudas Tecnológicas. Una de las áreas de mayor desarrollo en este enfoque se dio con la ingeniería biomédica con la que nace el término: tecnología de rehabilitación la cual se comprende como todos aquellos recursos materiales y tecnológicos que puedan contribuir con el proceso de habilitación y/o rehabilitación de la persona con discapacidad.



Los avances en el área de la ingeniería permitieron generar un conocimiento cada vez más especializado de las necesidades de esta población, buscando dar una mayor cantidad de recursos, surgiendo la antes ya mencionada asistencia tecnológica.

El término de Tecnología Asistiva es un término derivado del ingles: "Assistive Technology", La Asistencia Tecnológica es el sinónimo utilizado en Latinoamérica a pesar de que el anglicismo es el más conocido por la traducción al español de la mayoría de los textos existentes.

Este concepto consiste básicamente en la aplicación de diversos recursos tecnológicos para la persona con discapacidad, aunque a diferencia de su antecesor este concepto se genera en una visión más amplia de la persona y su interacción con los diversos ambientes en los que pueda encontrarse. Consiste en diversos servicios, instrumentos, programas, herramienta, maquinas o sistemas cuyo objetivo es el de aumentar mantener o mejorar las habilidades presentes en la persona, para compensar todas las limitaciones existentes acorde con su condición discapacitante ya sea esta de índole motriz, sensorial o cognitiva.

Un Equipo de Asistencia Tecnológica es cualquier objeto, equipo, sistema o producto adquirido comercialmente, adaptado o construido con el propósito de aumentar, mantener o mejorar las capacidades funcionales de las personas con impedimentos.

Tomando en cuenta todos los aspectos que intervienen dentro de la tecnología planteada, se pretende que el sistema neurológico de lenguaje y audición sea una herramienta útil que compita a la par con la mayoría de las invenciones pertenecientes a la asistencia tecnológica.

El sistema pretende crear un test especializado seguido por normas de evaluación, para que a su vez genere un estado clínico previo, con el cual, se procesa la información creando una herramienta de apoyo o rehabilitación personal y especifica dependiendo las necesidades del paciente.

En general, el desarrollo de tecnología de automatización y reingeniería de los métodos de realización de pruebas para diagnosticar el estado clínico de pacientes con impedimentos, servirá de ayuda para el especialista en el área de la comunicación humana y para el paciente, con resultados óptimos y precisos para que a su vez por medio de los parámetros que éste arroje, pueda generar una herramienta de terapia funcional y especializada según las circunstancias.

Esta asistencia debe ayudar a instituciones que brinden servicios a la comunidad de escasos recursos y a su vez debe ser una herramienta eficaz para el desarrollo de personas con impedimentos físicos, neuronales y con limitaciones económicas. Dicha aportación informática debe ayudar a desarrollar capacidades de las personas y especialmente niños que requieren un trabajo muy duro para poder combatir las dificultades que les han presentado.

Bibliografía...

[1] Bhatnagar, S.C. & Andy, O.J. Neurociencia para el estudio de las alteraciones de la comunicación. Editorial Masson, 1997.

[2] Gómez, P. & Gómez, M.E. Lenguaje y cerebro. Publicaciones de la Universidad de Valladolid, 1985.

[3] Gómez, P. & Gómez, M.E. Elementos de psiconeurobiología del lenguaje. Universidad Nacional de Educación a Distancia, 1988.

[4] Guyton, A.C. Anatomía y fisiología del sistema nervioso, Editorial Médica Panamericana, 1997.

[5] Kalat, J.W. Biological Psychology. 4th. ed. Brooks/Cole Publishing Company, Pacific Grove, 1992.

[6] Luria. Fundamentos de neurolingüística, Toray-Masson, 1980.

[7] Lenneberg, E.H. Fundamentos biológicos del lenguaje, Alianza Editorial, Alianza Universidad, 1985.

[8] Manning, L. Neurolingüística. Cuadernos de la U.N.E.D. Universidad de Educación a Distancia. 1991.

[9] Mora, F y Sanguinetti, A.M., Diccionario de Neurociencias, Alianza Editorial, 1994.

[10] Narbona, J. & Chevrie-Muller, C. El Lenguaje del niño: desarrollo normal, evaluación y trastornos, Editorial Masson, 1997.

[11] Ponz, F y Barber, A.M. Neurofisiología. Col. Ciencias de la Vida. Editorial Síntesis. 1989.

[12] Rodríguez, S. & Smith-Agreda, J.M. Anatomía de los órganos del lenguaje, la visión y audición, Editorial Médica Panamericana, 1999.

[13] http://cuentame.inegi.gob.mx/, discapacidad, 2008.

[14] http://www.terapiacupacional.com/, terapia ocupacional, 2008.

[15] http://asistenciatecnologica.blogspot.com/ asistencia tecnológica, 2006.

[16] www.escuelapnud.org/ponencias, 2009.

Extracción de patrones de huellas digitales: algoritmos MAIO vs Empate

Armando González Quevedo[1]
A. Estrada Hernández[1]
J. E. Ramírez Navarrete[2]
I. Cardiel[2]
E. Corona Organiche[2]

Resumen

La extracción de patrones de huellas digitales por medio de modelos matemáticos se ha desarrollado en las últimas décadas. Cada nuevo modelo que se plantea, proporciona un mayor conjunto de características de la huella digital que se analiza, logrando con ello una mejor identificación de la misma. El presente artículo proporciona un estudio comparativo de los algoritmos (modelos matemáticos) Maio y Empate, los cuales son ampliamente utilizados para la extracción de patrones de huellas digitales. El estudio permite concluir que el algoritmo MAIO proporciona una mejor extracción de características de una huella digital.

Palabras clave: Algoritmo Maio, huella digital, algoritmo Empate, minutas.

Introducción

Para la elaboración del Algoritmo de Maio, se ha tomado una base de datos de imágenes de cinco huellas dactilares, cuatro de las misma han sido creadas con el programa Sfinge, desarrollado por el grupo de biometría del Dr. Darío Maio [1]. Este programa nos permite

Acerca de los autores...

[1] Tecnológico de estudios Supriores de Ecatepec (TESE)
[2] División de Ingeniería en Sistemas Computacionales del TESE

crear huellas dactilares eligiendo las características de la misma, como puede ser el tipo de estructura, el número de crestas, el ruido, etcétera. La otra imagen es una de las huellas dactilares utilizada en el estudio del Dr. Darío Maio y Davide Maltoni, la cual ha sido sometida a un filtraje y realce de las crestas, eliminado el ruido y pequeños cortes que aparecían en la imagen original.

El algoritmo de Empate es el encargado de calcular la semejanza entre dos huellas, siendo el de empate por minutas el más conocido y ampliamente usado para reconocimiento de huellas digitales.

Desarrollo de algoritmo MAIO

Base de datos: A continuación se pueden encontrar diferentes tablas con las imágenes [2] de las huellas dactilares y sus principales características utilizadas para el desarrollo del software; cabe mencionar que el tipo de formato empleado para la imagen es de tipo .tif [3]

A los resultados obtenidos, se les ha realizado una inspección para poder observar errores en el seguimiento de la imagen. Normalmente los errores de seguimiento se solucionan en el post-procesado de la imagen, es decir, una vez realizada la extracción de minutas, se someten a un duro filtraje. En este caso, se han clasificado los errores encontrados en las imágenes para intentar solucionarlos durante la extracción de minutas y no en la etapa de post-procesado, mejorando así el seguimiento y logrando que el algoritmo tarde menos en su ejecución. De esta forma, ya que no perderá tiempo en seguir zonas erróneas y la etapa de post-procesado será más rápida.

Para una fácil compresión, se muestra el resultado del seguimiento realizado por el algoritmo en tablas. Cada una contiene el nombre de la imagen estudiada, la

Imagen 1

Características imagen Esfinge.

Imagen 2

Características imagen Esfinge.

Imagen 3

Características imagen Esfinge.

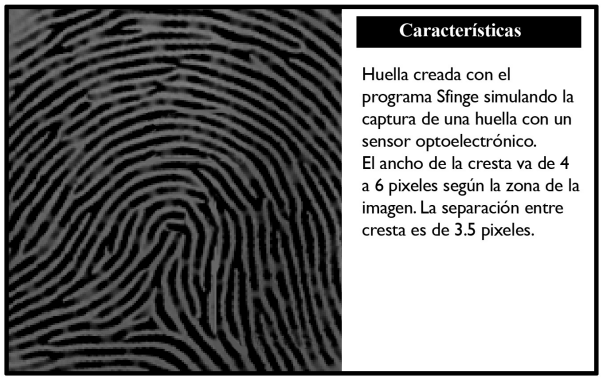


Imagen 4

Características imagen Esfinge.

NOMBRE DE LA IMAGEN	
IMAGEN RESULTANTE DE LA HUELLA DACTILAR UNA VEZ PROCESADA POR EL ALGORITMO	LA ZONA AMPLIADA DEL ERROR
	TIPO DE ERROR

Tabla 1

Ejemplo presentación resultados seguimiento

imagen resultante del algoritmo, y en la parte derecha los errores encontrados, así como una ampliación de la zona, tal y como se muestra en la tabla1.

El Algoritmo de Maio sólo realiza búsquedas de minutas (terminaciones y bifurcaciones) y no formas de las huellas dactilares como deltas, loopings, etcétera.

Algoritmo de Empate

Este algoritmo se basa en alineación de la huella de entrada con la plantilla de la base de datos, y se divide en dos pasos: Etapa de alineación y etapa de empate.

Etapa de alineación

El primer paso es tomar puntos de la cresta asociada a la minucia (durante la extracción de la minucia, la cresta donde reside también es almacenada y el origen de la misma coincide con la coordenada de la minucia). Los puntos se toman a una distancia igual al ancho entre crestas (distancia en píxeles entre una cresta y otra).

Empatando las crestas, se obtiene un umbral que de superar el valor de 0.8, da una primera estimación de semejanza. Definiendo Rd y RD es el conjunto de crestas asociadas con las minucias de entrada y de la plantilla, respectivamente. La ecuación (1) [4] de empate se describe como sigue:

$$S = \frac{\sum_{i=0}^{L} \mathbf{d_i D_i}}{\sqrt{\sum_{i=0}^{L} d_i^2 D_i^2}}$$

L denota el ancho entre crestas y $d \in \mathbb{R}^d$ y $D \in \mathbb{R}^D$. Cuando S ($0 \leq S \leq 1$) es mayor a 0.8, se continúa con el empate minucia a minucia, caso contrario, se pasa a la siguiente huella.

Si S es mayor a 0.8, se realiza la rotación de las minucias con respecto a una minucia de referencia $(x, y, \theta)^d$:

$$\begin{pmatrix} x_i^A \\ y_i^A \\ \theta_i^A \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta & 0 \\ \sin\theta & -\cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} * \begin{pmatrix} x_i - x^d \\ y_i - y^d \\ \theta_i - \theta^d \end{pmatrix}$$

Etapa de empate

La etapa de empate, ante todo, debe poseer cierto grado de flexibilidad, dado que es prácticamente imposible tener datos que empaten de manera perfecta. Para esto, se emplean ventanas de veinte por veinte pixeles, rango dentro del cual puede variar la ubicación de la minucia. De igual modo, se acepta un grado de tolerancia de un tercio de pi para el valor de la orientación. Para las minucias que se encuentren dentro de estos valores de tolerancia, son empatadas como minucias coincidentes, caso contrario se continúa con la siguiente minucia.

El porcentaje de empate es igual al número total de minucias coincidentes, para el número total de minucias en la plantilla de comparación.

$$\%\ \text{de Empate} = \frac{NME}{NTM} * 100$$

NME: Número de minucias empatadas
NTM: Número de minucias totales

Conclusiones

A través de este articulo, fue posible observar que el algoritmo de Maio debido a que realiza una creación de imágenes de una sola huella, almacenadas en una base de datos, creadas con el programa Sfinge, tomando características especificas en cada una de las imágenes, finalmente realiza búsqueda de terminaciones y bifurcaciones y no formas de huellas dactilares; en cambio, el algoritmo de Empate únicamente compara la imagen captada con la que está almacenada previamente en la base de datos.

Bibliografía...

[1] Darío Maio es Catedrático en la Universidad de Bolonia. Él es Presidente de la Cesena Campus y director del Laboratorio de Sistemas biométricos, Italia. Ha publicado más de 150 trabajos en numerosos campos, incluidos los sistemas de computación distribuida, el rendimiento del equipo de evaluación, diseño de base de datos, sistemas de información, redes neuronales, agentes autónomos y sistemas biométricos.

[2] Imágenes creadas por Marcos J. Lorda Piñol en trabajo de Titulación: Ingeniería Técnica Industrial con Especialidad en Electrónica Industrial, en la Escola Técnica Superior Enginyeria Universitat. Rovira I Virgili. He has published over 150 papers in numerous fields, including distributed computer systems, computer performance evaluation, database design, information systems, neural networks, autonomous agents and biometric systems.

[3] Formato TIF (formato de archivo de imágenes con etiquetas) es un formato de archivos de gráficos de mapa de bits, permite almacenar imágenes muy grandes (más de 4 GB comprimidos).

[4] Descrita por Diego Barragán – Pablo Vallejo en su trabajo llamado Reconocimiento de Huellas Digitales con Matlab

Davine Maltoni, Dario Maio, anil K.Jain and Salil Prabhakar. "Handbook of Fingerprint Recognition", Springer, 2003.

Dario Maio and Davine Maltoni, "Direct Gray-Scale Minutae Detection in Fingerprints", IEE transaction on pattern analysis an machine intelligence, january 1997.

Marino Tapiador Mateos y Juan A. Sigüenza Pizarro, Tecnologías Biométricas Aplicadas a la Seguridad. Editorial Alfaomega Ra-Ma.

Los sistemas distribuidos y el reto de compartir recursos en las organizaciones

Blanca Esther Martínez León*

Resumen

Los sistemas distribuidos son la herramienta tecnológica perfecta para compartir recursos, pero también conlleva retos, y es ahí donde la función de los ingenieros o informáticos es romper tales barreras para que se lleve a cabo una comunicación exacta. Múltiples empresas se han visto en la necesidad de integrarse a estas nuevas tecnologías, dado que la necesidad ha creado una fuerte demanda por la capacidad de acceso a bases de datos a través de la Internet. En este artículo se presenta una comparativa entre una multicomputadora y un sistema distribuido, barreras que siguen siendo tema de investigación para que puedan mejorar sus principales ventajas.

Palabras clave: Sistemas distribuidos, Multicomputadora.

Introducción

Hoy día, los sistemas informáticos juegan un papel cada vez más importante en las modernas organizaciones empresariales, hasta el punto de condicionar el éxito o fracaso en un entorno económico y social, tan dinámico como el que caracteriza el mundo actual.

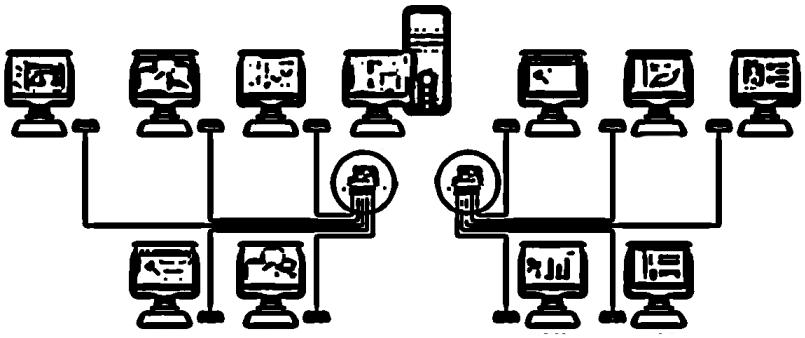
El sistema de información actual es como el sistema nervioso de un organismo, ya que éste se encarga de hacer llegar a tiempo los datos que necesitan los distintos elementos de la organización empresarial (departamentos, áreas funcionales, equipos de trabajo, delegaciones, etcétera), permitiendo de esta forma una actuación conjunta coordinada, ágil y orientada hacia los resultados.

Acerca del autor...

* Licenciada en Sistemas de Computación Administrativa, por la Universidad del Valle de México.

Tecnológico de Estudios Superiores de Ecatepec

La globalización ha llevando a las empresas a un proceso económico fundamental, que consiste en la progresiva integración de las distintas economías nacionales en una sola economía de mercado mundial; sin embargo, la globalización es un proceso autónomo y un orden espontáneo, que depende más bien del crecimiento económico, del avance tecnológico y la conectividad humana.



Los sistemas distribuidos

La competencia entre las empresas se ha hecho evidente, ya que por un lado, aumenta la cantidad y calidad de los productos o servicios, así como el poder político de las empresas sobre los países. Debido a ello, es necesario agilizar la comunicación entre diferentes empresas que se encuentran ubicadas en zonas geográficas apartadas, a fin de que compartan recursos, información, sistemas o bases de datos, sin importar las plataformas o la variedad de tecnologías, y son precisamente los sistemas distribuidos los que añaden un paradigma común, que ofrece una manera uniforme de ver y conocer todo el sistema.

La intención del sistema distribuido es convertir un grupo de maquinas débilmente conectadas en un sistema coherente, basado en un solo concepto. A veces el paradigma es sencillo, pero en otras es complejo. En todos los casos, la idea es siempre proporcionar algo que unifique el sistema.

Dichos sistemas son similares a las multicomputadoras, en cuanto a que cada nodo tiene su propia memoria privada, sin memoria física compartida en el sistema. No obstante, los sistemas distribuidos están acoplados con más debilidad aún que las multicomputadoras.
En principio de cuentas, los nodos de una multicomputadora por lo regular tienen un CPU, memoria RAM, una interfaz de red y tal vez un disco duro para paginar. En contraste, cada nodo de un sistema distribuido es una computadora completa, con un surtido integral de periféricos. Además, los nodos de una multicomputadora generalmente están en el mismo recinto para poder comunicarse a través de una red propia de alta velocidad, mientras que los nodos de un sistema distribuido se encuentran dispersos en todo el mundo.

Por último, todos los nodos de una multicomputadora ejecutan el mismo sistema operativo, comparten el mismo tipo de archivos y están sometidos a una administración común, mientras que con los nodos de un sistema distribuido, podrían ejecutarse distintos sistemas operativos, cada uno con su propio sistema de archivos y bajo diferentes administraciones.

Como ejemplo, una multicomputadora consiste en 512 nodos trabajando en un mismo recinto de una compañía o universidad, mientras que un sistema distribuido representativo, consiste en miles de maquinas que cooperan de manera informal a través de Internet.

Una vez descrita la diferencia entre una multicomputadora y un sistema distribuido, es posible apreciar la diferencia entre ambos y reconocer el alcance que puede tener un sistema distribuido que apoye y funcione como la espina dorsal de las grandes empresas, cuya inquietud principal es compartir su información.

Asimismo, esta diferencia lleva a distintos modelos de programación y a una amplia variedad de formas de pensar. Sin embargo, desde la perspectiva de las aplicaciones, los multiprocesadores y las multicomputadoras no son más que grandes anaqueles llenos de equipo en un cuarto destinado para ellos. Ambos se utilizan para resolver problemas computacionalmente intensivos, pero un sistema distribuido, que conecta computadoras por Internet, suele ocuparse mucho más de comunicación que de cómputo, y se emplea de diferentes maneras.

Justamente para que puedan resolver problemas, hay que tomarlos seriamente y lograr sobrepasar las siguientes barreras en los sistemas distribuidos que pudieran estar trabajando dentro de una empresa:

Heterogeneidad. La heterogeneidad se aplica en los siguientes elementos: redes, hardware de computadores, sistemas operativos, lenguajes de programación (ejemplo: el concepto de máquina virtual ofrece un modo de crear código ejecutable sobre cualquier hardware), e Implementaciones de diferentes desarrolladores, que deberán trabajar como una sola.

Extensibilidad. Es la característica que determina si el sistema puede expandirse de varias maneras. Un sistema puede ser abierto o cerrado con respecto a extensiones de hardware o de software. Los sistemas distribuidos abiertos pueden extenderse a nivel de hardware mediante la inclusión de computadoras a la red y a nivel de software por la introducción de nuevos servicios y la reimplementación de los antiguos. Otro beneficio de ellos, es su independencia respecto a proveedores concretos.

Seguridad. Consta de tres elementos; confidencialidad (solamente usuarios autorizados); disponibilidad (momento y tiempo que se necesite), e integridad (no se pueda alterar).

Escalabilidad. Que el hardware y software permitan el crecimiento de recursos y usuarios.

Tratamiento de fallos. La capacidad que tiene el sistema de seguir trabajando a pesar de que algún punto en la red caiga, los demás seguirán operando de manera independiente sin darse cuenta de la falla.

Concurrencia. Permitir que diversos usuarios tengan acceso al mismo recurso, casi simultáneamente y sin contratiempos.

Algunas ventajas de los sistemas distribuidos en las empresas

- Mayor comunicación. Permite enviar o recibir archivos a diferentes clientes.
- Incremento al compartir los recursos. Uso de dispositivos de almacenamiento masivo por diferentes usuarios.
- Trabajo en conjunto y compartido. Hace factible que distintos usuarios estén comunicados y compartiendo datos o información al mismo tiempo, sin importar la plataforma de su PC.
- Capacidad de crecimiento. Con el tiempo, es más fácil y económico agregar equipo para mejorar el rendimiento de este sistema distribuido.

El vínculo cliente/servidor es un proceso distribuido. Los usuarios, aplicaciones y recursos se hallan distribuidos en respuesta a las necesidades del negocio y quedan enlazados por una sola LAN o WAN o por una serie de subredes.

Cabe mencionar que el modelo o esquema cliente-servidor es un conjunto de clientes (computadoras personales dotadas de una interfaz) y servidores (equipo de computo con características

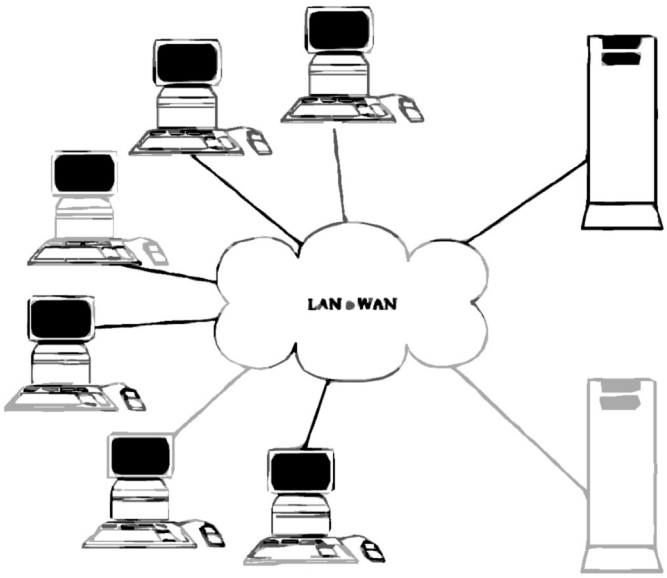


Figura 1:

El Sistema Distribuido y su esquema cliente–servidor

sobresalientes) que están conectadas entre sí a través de un medio, y además comparten recursos distintos, la red LAN o WAN podría ser Internet.

Conclusiones

Presentar las barreras que aún tienen los sistemas distribuidos, es una forma realista de mostrar la situación que habrán de afrontar las empresas que deseen utilizar esta tecnología. Pero, como hemos visto, si es administrada y configurada seriamente, las ventajas pueden ser excelentes.

Es preciso reconocer que todavía existen áreas en las bases de datos distribuidas, que se encuentran en investigación y desarrollo, las cuales son un reto tecnológico para los investigadores.

Las organizaciones que buscan competir y mantenerse en el mercado, adoptan este tipo de tecnologías que facilitan el trabajo de los usuarios, comparten recursos y procuran un trabajo en conjunto.

Bibliografía...

Andrew S. TanenBaum (2003). Sistemas Operativos Modernos, México, Pág. 549-580

Gómez Vieites, Álvaro y Suárez Rey, Carlos, (2007). Sistemas de Información, Herramientas prácticas para la Gestiona Empresarial, 2da. edición ampliada y actualizada, Pág. 2-19

Presuman, Roger S. (2002). Ingeniería de Software Quinta Edición. McGraw-Hill Interamericana, Madrid, Pág. 312-345.

Williams, Stalling (2000). Sistemas Operativos, 2da. edición, Prentice Hall, Pág. 460-480.

http://it.ciidit.uanl.mx/~elisa/presentations/computo_moderno.pdf

http://mixtli.utm.mx/~resdi/Ventajas_y_Retos_en_el_uso_de_las_bases_de_datos_distribuidas.pdf

La calidad en los procesos de software

Ana Ma. López Rangel*
Jesús Emmanuel Ramírez Navarrete**
C. Edgar Corona Organiche**

Resumen

Los cambios económicos y tecnológicos, están obligando a las empresas mexicanas a producir mejor, pues requieren enfrentarse a una competencia más agresiva, además de sortear las crisis económicas que sufren otros países y afectan al nuestro. Debido a esto, se recurre a la implementación de calidad como una oportunidad de mejorar los procesos, logrando con esto mayor competitividad, así como una reducción de costos y mantenimiento. Como consecuencia, las empresas han decidido aplicar algún modelo de calidad, como el Capability Maturity Model Integration (CMMI), que es el más reconocido a escala mundial para la implementación de calidad en los procesos.

El concepto de calidad que se busca en nuestro país, tiene que ver con los requisitos de los consumidores, dado que un producto o servicio sólo tiene calidad en la medida que satisface las expectativas del cliente. Además, es una filosofía que debe convertirse en la forma de vida de todos los integrantes de la organización y que, por esta razón, buscan también alcanzar el reconocimiento como empresas socialmente responsables (ESR) y como empresas ambientalmente responsables (EAR). Aunque la Responsabilidad Social Empresarial es inherente a la empresa, recientemente se ha convertido en una nueva forma de gestión y de hacer negocios, donde esta misma se ocupa de que sus operaciones sean sustentables en lo económico, lo social y lo ambiental, reconociendo los intereses de los distintos grupos con los que se relaciona y buscando la preservación del medio ambiente, así como la sustentabilidad de las generaciones futuras. (www.empresa.org.)

La globalización de la economía, el General Agreetment on Tariffs and Trade (Acuerdo General sobre Comercio y Aranceles, GATT, por sus siglas en inglés), el Tratado de Libre Comercio (TLC), la abrupta apertura de nuestro mercado, etcétera, dan cuenta de un proceso que ha puesto en crisis a las empresas mexicanas; muchas de éstas han cerrado sus puertas al no poder competir, otras más se han visto obligadas a buscar modelos que las ayuden a ser más competitivas y productivas, para no perder sus mercados nacionales y ganar otros en el extranjero. Dentro de ese grupo que busca nuevos modelos administrativos, hay algunas que

Acerca de los autores...
*** Alumna de la Maestría en Ingeniería en Sistemas Computacionales, TESE.**
**** Tutor adscrito a la Maestría en Ingeniería en Sistemas Computacionales, TESE.**

han optado por el control total de calidad, pero cabe preguntarse si la calidad es una respuesta a las necesidades de las empresas mexicanas.

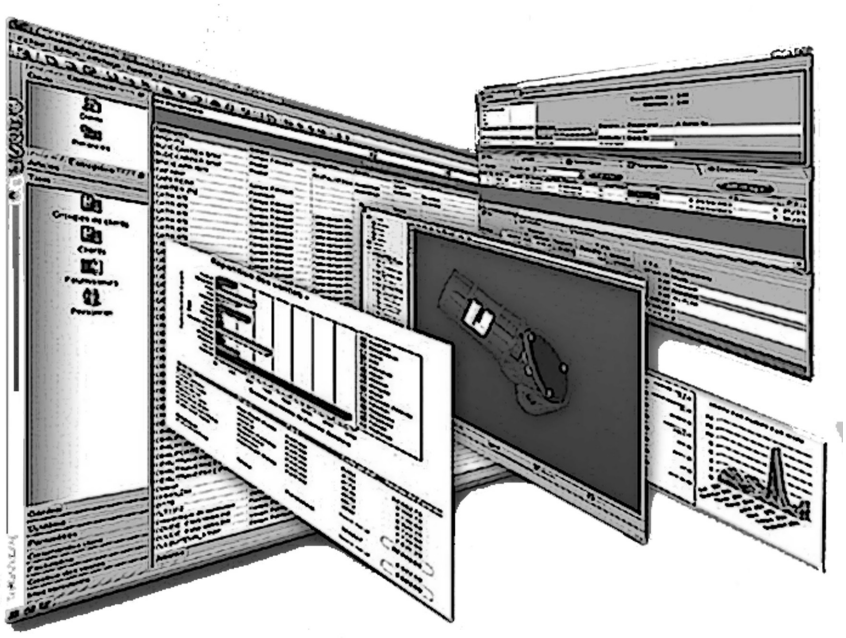
Francisco González Prado, Director General del Instituto Mexicano de Control de Calidad (IMECCA), expresó en un artículo publicado en el diario El Financiero, que las empresas mexicanas no podrán competir en los mercados internacionales si no mejoran en áreas como: calidad, productividad y distribución. Además el acceso de los productos y servicios mexicanos a los mercados mundiales sólo estará disponible para aquellas empresas que certifiquen la calidad; debido a que en los últimos años, la certificación en este rubro se ha convertido en la carta de presentación de las empresas para ingresar a nuevos mercados (González, 1994).

El reto u oportunidad a la que se enfrentan las empresas mexicanas, las obliga a ser más competitivas en calidad, costo y servicios, dejar atrás la forma tradicional de administración y adoptar una nueva, que les permita hacer frente a las presiones competitivas y mejorar la calidad de todo el negocio, no sólo en las áreas de producción.

La adopción de la filosofía de calidad total, requiere una transformación cultural, una nueva manera de administrar el negocio, donde el énfasis cambia de las utilidades a la satisfacción del cliente, donde en lugar de administrar resultados, se administran y mejoran continuamente los sistemas y procesos que los producen.

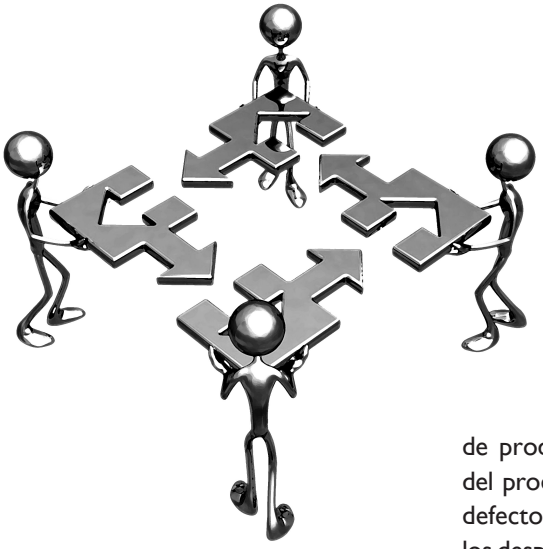
De ahí que se establecen algunas características sobre la calidad:

- La calidad no se controla, se produce proactivamente.
- La calidad está basada en la prevención y no en la detección de defectos.



- La calidad se fundamenta en el mejoramiento constante de los procesos. La mejoría depende de la medición y retroalimentación permanente.
- La calidad está orientada al consumidor o usuario, sus opiniones, necesidades y expectativas deben investigarse e integrarse al diseño de productos o servicios.
- La calidad está orientada a prioridades.
- La calidad depende de la capacidad de innovación y participación de los empleados en los procesos laborales. El diseño, aplicación y control del mejoramiento, se genera desde la base (los operarios).
- La calidad depende de hacer bien las cosas desde la primera vez. Esto exige que el estándar sea cero defectos y la medida de la calidad sea el costo del incumplimiento.

Con lo anterior, se obliga a las organizaciones a mejorar el proceso



de producción, cuidar el diseño exacto del producto final, reducir al mínimo los defectos, evitar los retrabajos, eliminar los desperdicios, uniformar los productos, lograr exactitud en el manejo de materiales, lo cual trae consigo la disminución de costos; asimismo, cuidar todos estos detalles en la producción, evitar las devoluciones, las quejas, los gastos para cubrir garantías, entre otros. Por ello, queda claro que la calidad y el incremento de la productividad van de la mano.

La calidad no es sólo una estrategia para incrementar la productividad; la calidad debe entenderse y ser transmitida como un valor que genera actitudes y comportamientos en el trabajo; es buscar conscientemente los máximos estándares deseables, es un estilo de vida, es una cultura, donde lo principal es el trabajo, el servicio y la completa entrega.

Este proceso de mejora continua, obliga a todos los integrantes de la organización a incrementar su educación; la capacitación, por tanto, es un eje importante de la calidad. Así pues, se debe crear una conciencia de calidad que además de productividad, incite a un uso racional de los recursos, al no desperdicio de ningún tipo, y que también cree responsabilidad social, conciencia ecológica y una real preocupación por cambiar nuestros hábitos de consumo; en fin, calidad es el uso de la naturaleza sin detrimento de ésta.

Las políticas de calidad se ejercen desde la cúspide de la pirámide ocupacional, por lo que es un gran reto para los directivos el atenderlas y mantenerlas, además de que dicha responsabilidad implica adquirir e implementar tecnología de punta y métodos innovadores que contribuyan a elevar la productividad (en el entendido de que productividad y calidad van de la mano) y así poder asegurar su posicionamiento en el mercado (Espinosa-Pérez).

No obstante, en muchos casos, las empresas no tienen claros los conceptos más elementales de calidad, no poseen estrategias, políticas ni objetivos en torno a ésta; carecen de planeación a largo plazo, y es común que no cuenten con manuales administrativos de calidad o programas de capacitación.

La calidad en procesos de software. ¿Por qué certificarse?

La calidad del software está determinada por la interacción de factores como las personas, la tecnología, la organización y los datos, los cuales son manejados por el proceso. En esa medida, los resultados obtenidos dependerán de la calidad del mismo y de la sinergia que se logre con todos los componentes involucrados.

El modelo CMMI (Capability Maturity Model Integration) es uno de los procesos más influyentes en lo que respecta a la mejora del proceso, y se ha ubicado como el mejor referente internacional de calidad exigido por las compañías que contratan software a nivel mundial. Este modelo proporciona una base para la evaluación de la madurez de las organizaciones de software y ofrece una guía para implementar una estrategia de mejora continua de procesos, que dan como resultado la mejora del producto.

El propósito de CMMI es proporcionar una guía para mejorar los procesos de la organización y la habilidad para administrar el desarrollo, adquisición y mantenimiento de productos o servicios (Oktaba et al.).

Este modelo de procesos tiene dos representaciones: continua y por etapas, siendo la diferencia entre éstas la evaluación por niveles de la capacidad de procesos o de la madurez de la organización, respectivamente. Las áreas de procesos (AP) en este modelo se agrupan en cuatro categorías: Gestión de Proyectos, Soporte, Gestión de Procesos, y de Ingeniería.

La representación del modelo CMMI, define cinco niveles de madurez, dentro de los cuales se puede encontrar una organización. Un nivel de madurez, representa un indicador evolutivo que puede ser alcanzado por el proceso de software. Dichos niveles pretenden lograr objetivos de calidad de acuerdo con la capacidad del proceso de software, los cuales una vez cumplidos, permitirán trascender al siguiente. Los cinco niveles de madurez en el CMMI, son:

- **NIVEL 1 –** Inicial. El proceso de software es impredecible, sin control y reactivo. El éxito de los proyectos depende del talento de las personas involucradas.
- **NIVEL 2 –** Gestionado. Existen procesos básicos de gestión en los proyectos (costo, calendario, funcionalidad). Los procesos existentes hacen que se puedan repetir éxitos en proyectos de similares características.
- **NIVEL 3 –** Definido. Existe un proceso de software documentado y estandarizado dentro de la organización. Todos los proyectos utilizan una versión a medida del proceso.
- **NIVEL 4 –** Gestionado Cuantitativamente. La organización recolecta métricas del proceso software y de los productos desarrollados. Tanto el proceso como los productos, se entienden y controlan cuantitativamente.
- **NIVEL 5 –** En Optimización. Existe una mejora continua del proceso software, basada en la realimentación cuantitativa del mismo y la puesta en práctica de ideas y tecnologías innovadoras (Oktaba et al,).

Los cambios económicos, junto con los tecnológicos, son quizá los que más van a afectar la manera de hacer las cosas en México. No sólo es la globalización de los mercados, que han obligado a nuestras empresas a producir mejor, al enfrentarse a una competencia más agresiva y decidida a ganar, sino que también se tiene que saber paliar las crisis económicas que sufren otros países y que afectan al nuestro. Debido a ello, cada vez son más las empresas que inician la implementación de algún modelo de calidad en sus procesos. Desafortunadamente, el reto más grande con el que se enfrentan, son los altos costos que implica pagar a consultores externos para que guíen a la empresa hacia esta implementación, además del desafío de cambiar el estilo de trabajo habitual de los empleados por una cultura de calidad, donde lo principal sea la completa satisfacción del cliente.

Aunque es un camino difícil de recorrer, es posible conseguirlo con el trabajo en equipo y esfuerzo de toda la organización. Y como ejemplo, existen ya 14 empresas mexicanas certificadas en CMM, entre ellas están IDS, Praxis, Neoris, Delphi, Aspel, Telepro, y 27 están certificadas en CMMI, entre las que están Sinersys, Innevo, CFE, IMSS y Mexware. Sin embargo, muchas empresas más deberán recorrer este camino para lograr sobrevivir al mundo globalizado en el que hoy se encuentran. (IX Congreso Internacional para MiPyMes).

Por lo tanto, en un mundo cada vez más interdependiente y en constante cambio, los mexicanos debemos aprender a producir y negociar en un ambiente hostil y a enfrentar los retos de la apertura económica, con una mentalidad ganadora, de excelencia, servicio y calidad.

Bibliografía...

"Manual de Contenidos de Forum Empresa". Más información en www.empresa.org.

González Prado, Francisco, El Financiero, 16 de mayo de 1994, pág. 28

Elvia Espinosa Infante, Rebeca Pérez Calderón, Estudios sobre Calidad Total, Departamento de Administración UAM. http://www.azc.uam.mx/publicaciones/gestion/num5/doc05.htm

Hanna Oktaba, Mario Piattini, Francisco J. Pino, María Julia Orozco, Claudia Alquicira. CompetiSoft. Mejora de Procesos Software para pequeñas y medianas empresas, Ed. AlfaOmega, , págs. 224-246.

IX Congreso Internacional para MiPyMes, Lic. Sergio Carrera Riva Palacio, Director General de Comercio Interior y Economía Digital, Subsecretaría de Industria y Comercio. http://www.compite.org.mx/eventosn/RELATORIAS/MEMORIAS/2a.%20Sesi%C3%B3n%20Simultanea/2a.%20Simultanea%20Don%20Alberto%203/SECRETARIA%20DE%20ECONOMIA/SECRETARIA%20DE%20ECONOMIA.ppt

Compromiso
Gobierno que cumple

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE ECATEPEC

Organismo Público Descentralizado del Estado de México

NUEVE CARRERAS

INGENIERÍAS:

- Electrónica y Telemática
- Mecatrónica
- Mecánica
- Industrial
- Sistemas Computacionales
- Química
- Bioquímica

- Cursos de Educación Continua
- Diplomados
- Centro de Idiomas (inglés y francés)

LICENCIATURAS:

- Informática
- Contaduría y Administración

POSGRADOS (Maestrías):

- Ingeniería Química
- Ingeniería Bioquímica
- Ingeniería en Sistemas Computacionales
- Ingeniería Mecatrónica

Informes:
Av. Tecnológico s/n. Esq. Av. Carlos Hank González (Av. Central), Col. Valle de Anáhuac, Ecatepec de Morelos, Estado de México, C.P. 55210
Teléfonos 50 00 23 42 y 50 00 23 43 **www.tese.edu.mx**

GOBIERNO DEL
ESTADO DE MÉXICO

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE ECATEPEC