

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA
FACULTAD DE INGENIERÍA



Maestría y Doctorado en Ciencias e Ingeniería

**“DISEÑO DE UN SISTEMA PARA EL ALMACENAMIENTO Y
RECUPERACIÓN DE EXPEDIENTES CURRICULARES
ELECTRÓNICOS UTILIZANDO TARJETAS INTELIGENTES”**

TESIS

QUE PARA OBTENER EL GRADO DE

Maestro en Ciencias

PRESENTA

Julio César Castillo Ramírez

DIRECTOR

M.C. Jorge Eduardo Ibarra Esquer

CODIRECTOR

M.C. Brenda Leticia Flores Ríos

Mexicali, Baja California, 8 de Junio de 2007

Investigación Exploratoria

- Planteamiento del problema
- Antecedentes
- Definición del objetivo general y objetivos específicos



Marco Teórico e Investigación Descriptiva

- Revisión bibliográfica
- Análisis de la información recopilada
- Documentación



Elaboración del Diseño

- Análisis de requerimientos
- Elaboración de propuesta de diseño
- Diseño de la arquitectura de bases de datos distribuida
- Diseño del mecanismo de autenticación
- Diseño del esquema de almacenamiento de información en la tarjeta inteligente
- Diseño de la estructura del expediente curricular electrónico

Fábrica de Diplomas



Factores:

- Personas que desean pertenecer a un status o campo laboral
- Solventar el pago total de los estudios
- Bajo desempeño académico para acreditar asignaturas
- Necesidad por comprobar en corto plazo un nivel de estudios
- Las TI han facilitado la falsificación y distribución

Fábrica de Diplomas



Afecta:

- Calidad de los procesos de formación académica
- Crecimiento económico, cultural y de valores de las organizaciones y de la sociedad

Antecedentes



- Mecanismos tradicionales de validación de comprobantes de estudios y experiencia laboral
 - Cédula profesional
- Modelos para estructurar información académica y de experiencia laboral (XMLRésumé)
- Tecnología de tarjetas inteligentes
 - Información de salud (Health Card)
 - Información académica

Objetivo general



Diseñar un sistema basado en tarjetas inteligentes que permita almacenar y recuperar de manera segura y eficiente, expedientes curriculares electrónicos para brindar una alternativa en la verificación de la validez de documentos probatorios de las personas que cuentan con estudios de nivel profesional.

Objetivos específicos



- Establecer los requerimientos para el diseño de un sistema que brinde una alternativa eficiente y segura, para la verificación de la validez de documentos probatorios.
- Proponer el uso de tarjetas inteligentes como mecanismo seguro de autenticación e identificación para tener acceso al sistema de almacenamiento y consulta de expedientes curriculares electrónicos.

Objetivos específicos



- Proponer y desarrollar un modelo para el almacenamiento y representación de expedientes curriculares electrónicos, con una estructura bien definida, que sea fácil de interpretar, y que sirva como estándar para su uso por las instituciones educativas y empresas del todo el país.
- Diseñar y presentar la arquitectura del sistema de almacenamiento y recuperación de expedientes curriculares electrónicos.

Investigación Exploratoria

- Planteamiento del problema
- Antecedentes
- Definición del objetivo general y objetivos específicos



Marco Teórico e Investigación Descriptiva

- Revisión bibliográfica
- Análisis de la información recopilada
- Documentación



Elaboración del Diseño

- Análisis de requerimientos
- Elaboración de propuesta de diseño
- Diseño de la arquitectura de bases de datos distribuida
- Diseño del mecanismo de autenticación
- Diseño del esquema de almacenamiento de información en la tarjeta inteligente
- Diseño de la estructura del expediente curricular electrónico

Revisión y análisis bibliográfico

- **Tecnología de tarjetas inteligentes**

- Historia y evolución
- Aplicaciones
- Tecnologías

- **Seguridad de la Información**

- Elementos
- Mecanismos
- Criptografía

Tarjeta Inteligente



Definición:

Es un dispositivo que tiene las características físicas similares a las de una tarjeta de crédito convencional y que además tiene un circuito integrado empujado, con memoria y capacidades de procesamiento de información, que le permite ejecutar aplicaciones para almacenamiento y transferencia de información en forma segura, confiable y eficiente.



Investigación Exploratoria

- Planteamiento del problema
- Antecedentes
- Definición del objetivo general y objetivos específicos



Marco Teórico e Investigación Descriptiva

- Revisión bibliográfica
- Análisis de la información recopilada
- Documentación



Elaboración del Diseño

- Análisis de requerimientos
- Elaboración de propuesta de diseño
- Diseño de la arquitectura de bases de datos distribuida
- Diseño del mecanismo de autenticación
- Diseño del esquema de almacenamiento de información en la tarjeta inteligente
- Diseño de la estructura del expediente curricular electrónico

Análisis de requerimientos



1) Almacenamiento

- Título de grado
- Idiomas
- Diplomados
- Publicaciones
- Seminarios
- Reconocimientos
- Certificados
- Experiencia laboral

Análisis de requerimientos



2) Mecanismo de acceso seguro y privacidad

- Acceso desde cualquier institución o empresa
- Consentimiento de la persona
- Identificación de la persona

Análisis de requerimientos



3) Representación de la información

- Estructura bien definida
- Puedan ser interpretados por las instituciones y empresas
- Especificar los elementos de cada documento probatorio

Análisis de requerimientos



4) Control del sistema

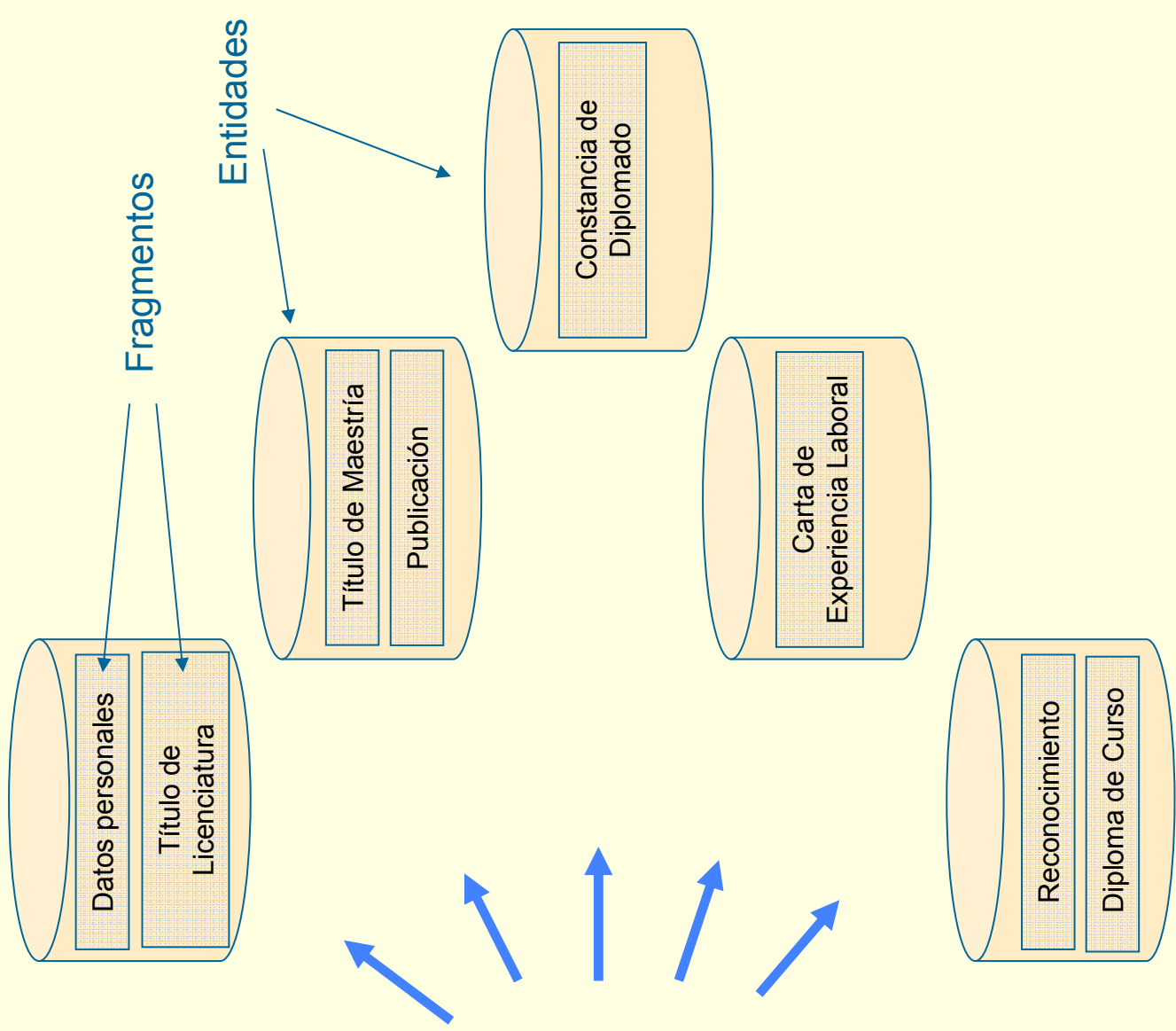
- Verificación, almacenamiento y administración de documentos
- Disponibilidad de la información en todo momento

Diseño del sistema - Distribución de la información

Análisis de modelos de almacenamiento

- Se requiere una base de datos muy extensa
- El sistema debe estar disponible en todo momento
- Un sólo punto de falla no es una solución viable
- Distribución de responsabilidades = Autonomía de los datos
- Fragmentar y distribuir los expedientes curriculares

Expediente Curricular



Arquitectura del sistema

- 1) Servidores de administración de bases de datos (DBMS)
- 2) Servidores de aplicaciones
- 3) Aplicaciones cliente

Arquitectura del sistema

1) Servidores de administración de bases de datos (DBMS)

- Almacenamiento de los expedientes curriculares
- Realización de búsquedas
- Extraer documentos del mismo servidor y de otros servidores
- Presentar el resultado de las consultas al servidor de aplicaciones
- Funciones de administración, respaldos, optimización

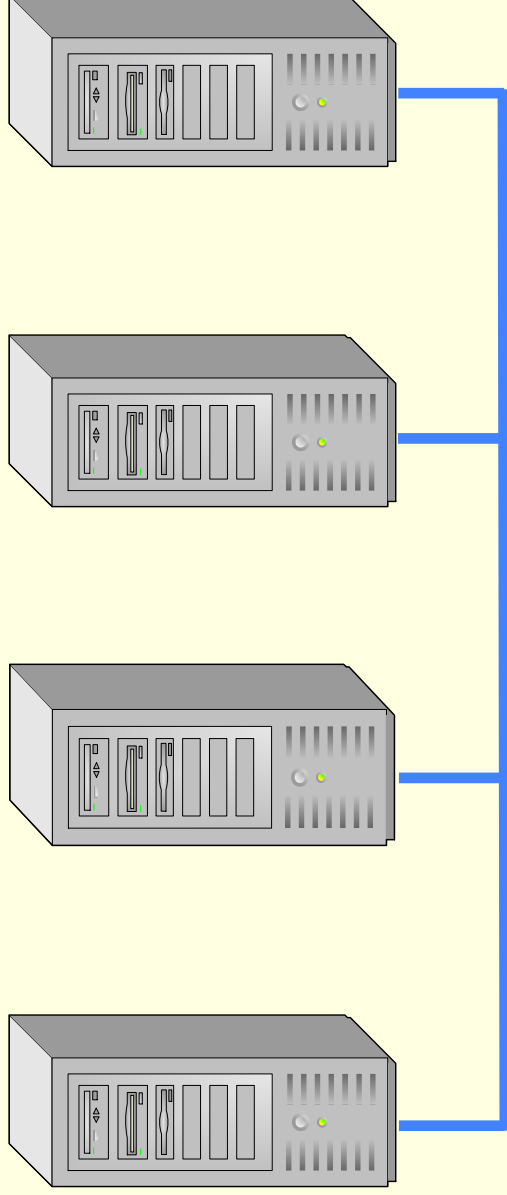
Arquitectura del sistema



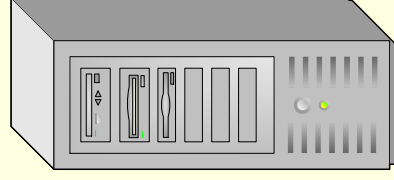
Berkeley DB High Availability (Oracle)

- Escalabilidad
- Flexibilidad
- Administración sencilla
- Acceso concurrente
- Alta disponibilidad
- Confiabilidad (propiedades ACID)

Réplicas



El maestro **distribuye** los cambios a todas las réplicas



Maestro

Las consultas de **lectura** se pueden dirigir al maestro o a cualquier réplica

Servidores de Bases de Datos

Las consultas de **actualización** se dirigen únicamente al servidor maestro

Arquitectura del sistema



2) Servidores de aplicaciones

- Capa intermedia entre clientes y DBMS
- Recibe solicitudes para visualizar los expedientes curriculares
- Monitorea la carga de tráfico de las réplicas
- Comunicación con servidores DBMS de otras entidades
- Interfaces de entrada de datos (Controlador)
- Interfaces de presentación de datos (Vistas)

Arquitectura del sistema



3) Aplicaciones cliente

- Comunicación con el servidor de aplicaciones
- Desplegar información sobre los expedientes curriculares
- Comunicación con la tarjeta inteligente (utilizando un middleware)

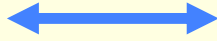
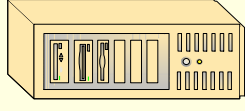
Arquitectura del sistema



Entidades de Certificación

- Validación, almacenamiento y administración de documentos probatorios.
- Contendrá:
 - Un servidor de aplicaciones
 - Uno o más servidores de bases de datos
- Una entidad de certificación por estado de la república
- Diseño escalable

Servidor de Aplicaciones



Clientes



Entidades de Certificación



Jalisco

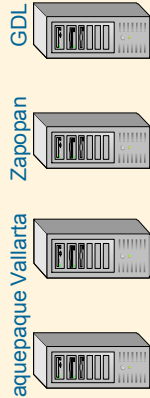
Sonora

Jalisco

Sonora

Baja California

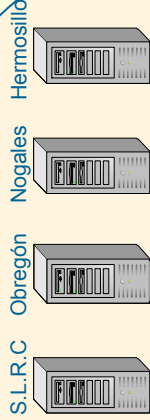
Réplicas



Maestro

Tonalá

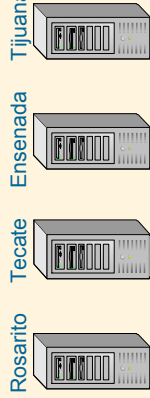
Réplicas



Maestro

Guaymas

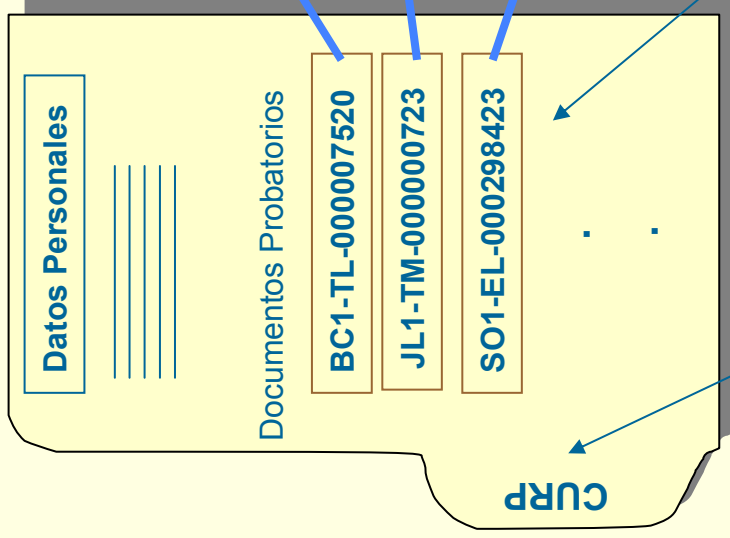
Réplicas



Maestro

Mexicali

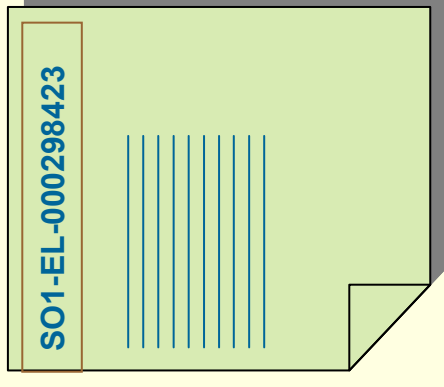
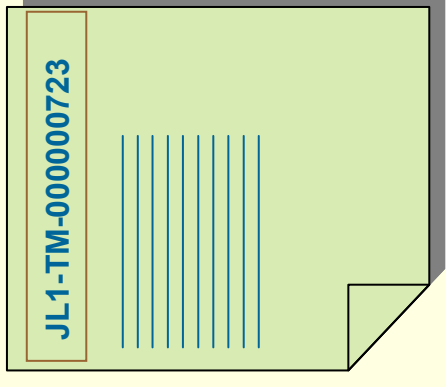
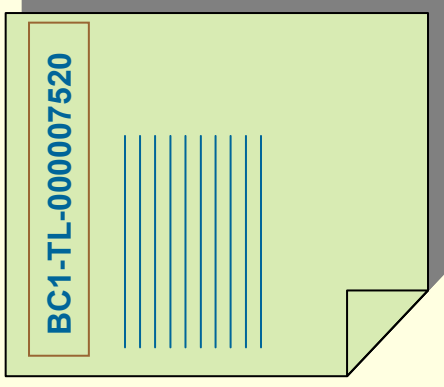
Expediente Curricular



Documentos probatorios

Identificadores de documentos probatorios

Identificador de Expediente Curricular (Clave CURP)



Seguridad en los enlaces

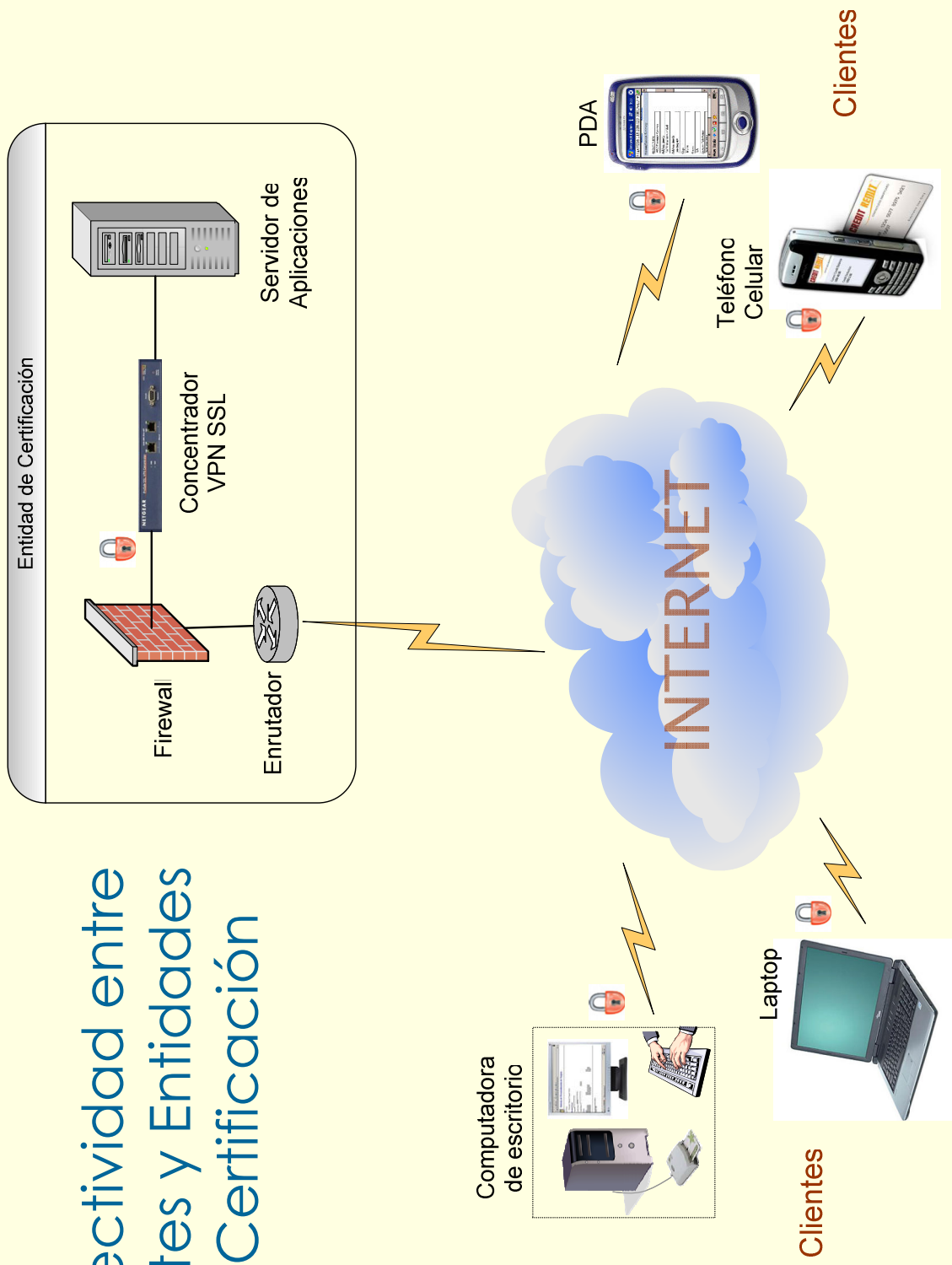


1. Conectividad entre clientes y entidades de certificación
2. Conectividad entre entidades de certificación

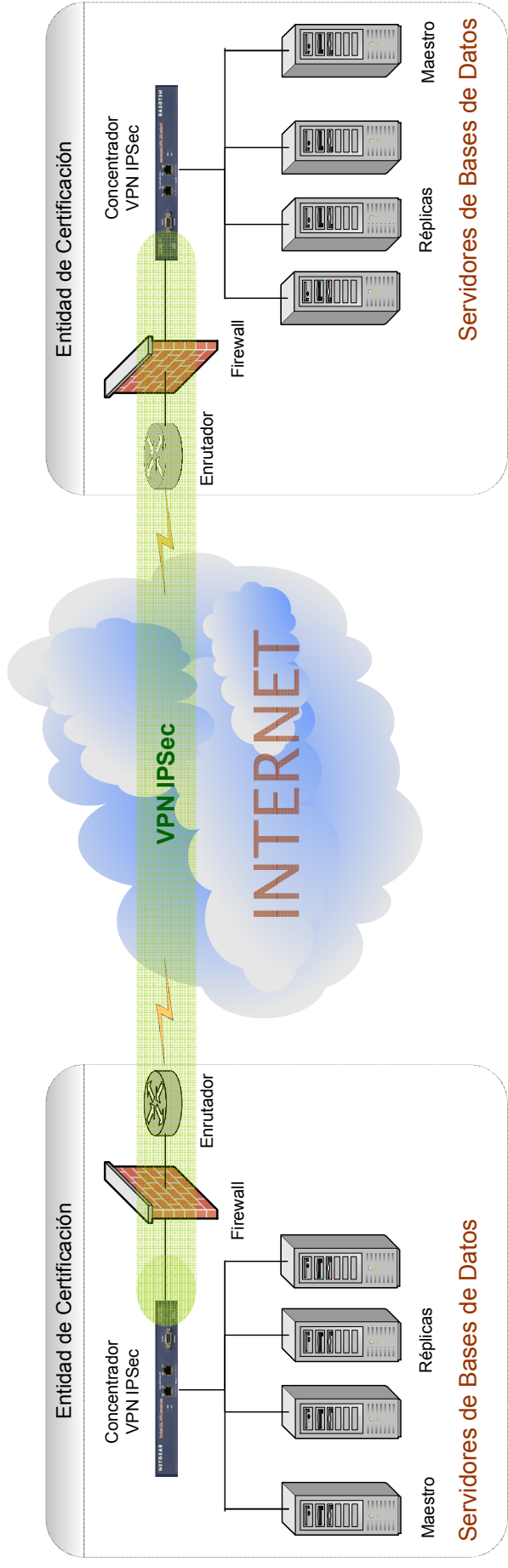
Uso de Redes Privadas Virtuales en Internet (VPN)

- VPN utilizando protocolo IPsec
- VPN utilizando protocolo SSL

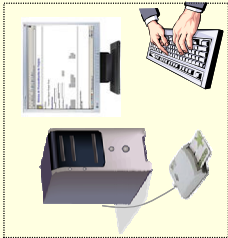
Conectividad entre clientes y Entidades de Certificación



Conectividad entre Entidades de Certificación



Computadora de escritorio



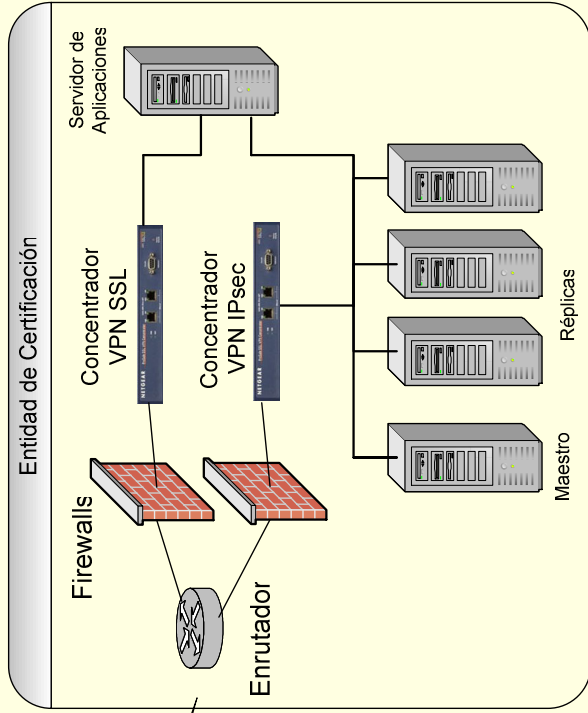
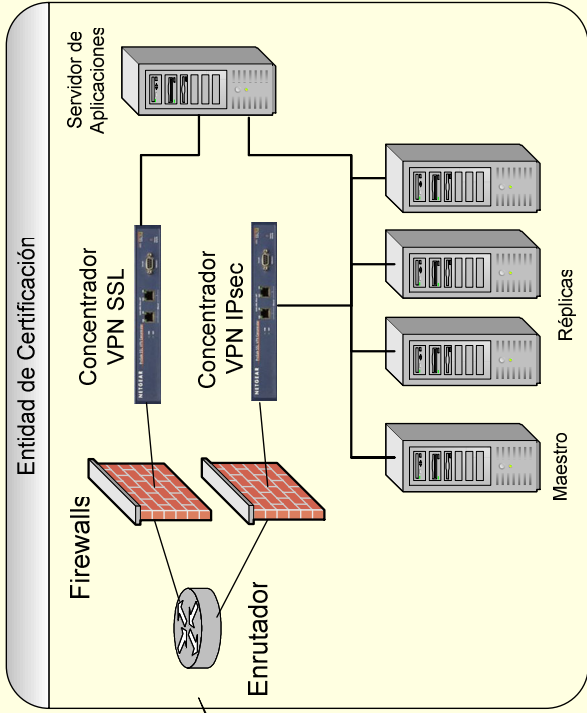
Laptop



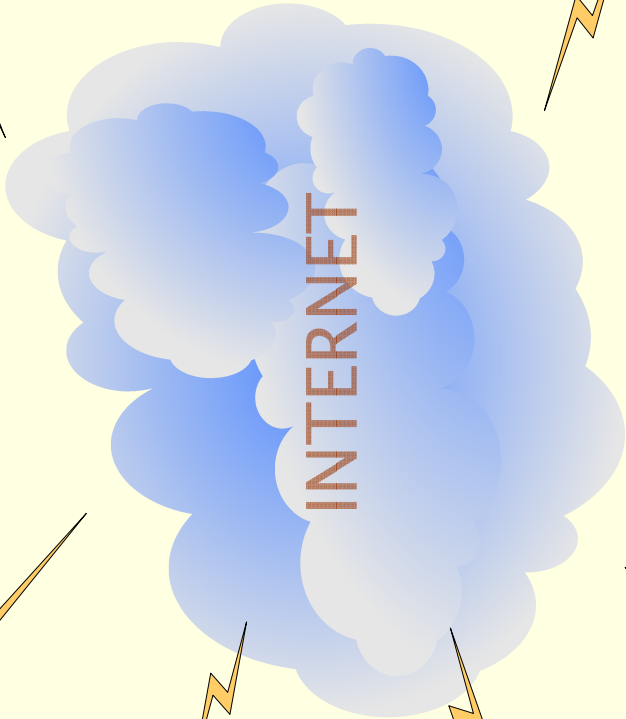
Teléfono celular



PDA



INTERNET



Proceso de autenticación

Tarjetas inteligentes como llave de acceso

- Análisis de kits de desarrollo
 - Capacidad de memoria
 - Compatibilidad con estándares
 - Información técnica
 - Mecanismos de seguridad
 - Costo

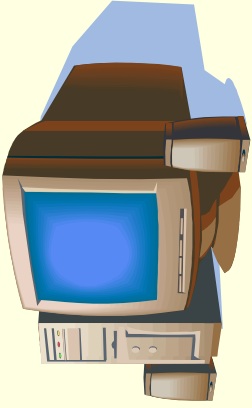
Proceso de autenticación

Tarjetas inteligentes como llave de acceso

- Se analizaron kits de 3 empresas
 - Axalto
 - Cardlogix
 - Advanced Card Systems (ACS)

- Se seleccionó el kit de la empresa ACS

Terminal



Comando / Respuesta

INICIA SESION

RNDc

AUTENTICA

3-DES (RNDt, #Kt)

3-DES (RNDt, #Ks)

Calcula 3-DES (RNDc, #Kt)

Genera número aleatorio RNDt

Calcula llave de sesión Ks

Verifica 3-DES (RNDt, #Ks)

Tarjeta ACOS2



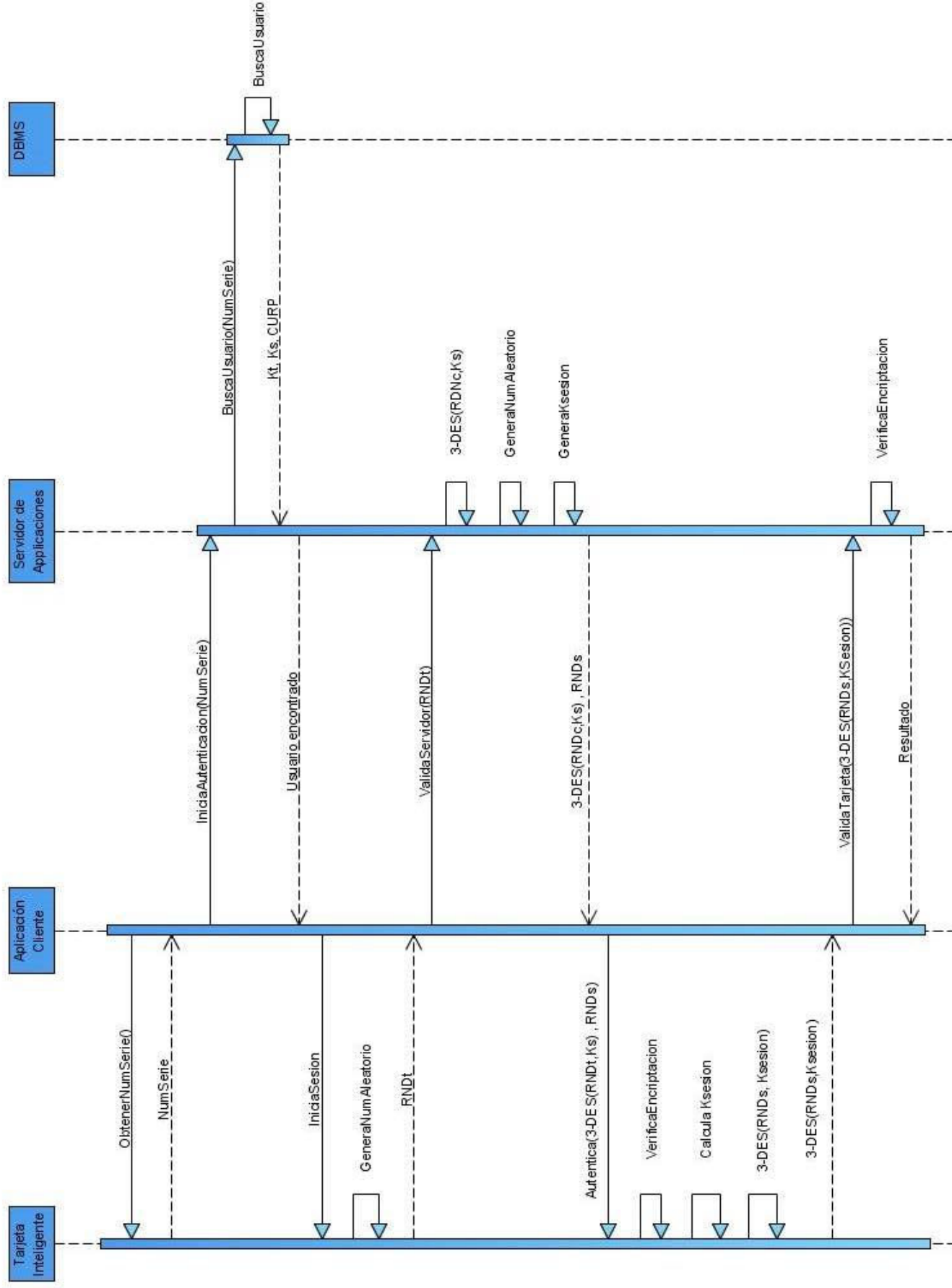
Genera número aleatorio RNDc

Verifica 3-DES (RNDt, #Ka)

Calcula llave de sesión Ks

Calcula 3-DES (RNDt, #Ks)

sd Diagrama de Secuencia - Proceso de Autenticación



Proceso de autenticación

No. de serie (8 bytes hex)	ID de usuario (Clave CURP)	Llave de Tarjeta (K_T) (16 bytes hex)
81 0F 17 A1 DC 0E A0 00	CARJ730814HBCSML09	90 45 67 45 34 67 56 89 FE 56 EF 67 90 23 56 DE
A1 0F 17 A1 DC 0E A0 00	RACO780914HBCSML04	45 86 34 56 23 A5 AC 67 60 12 A4 5E 10 64 10 B1
21 0F 17 A1 DC 0E A0 00	SICA711212HBCSML906	14 58 39 20 E9 F7 CA 45 48 29 30 49 58 F7 7E A5
C9 0E 17 A1 DC 0E A0 00	RORM801211MDFSBL09	FE EF 51 09 48 23 18 48 EE A7 84 99 AA E4 34 11
FF F9 BF F7 3E FF FF FF	TACA691114HBCSML01	01 11 34 86 38 FF A6 A9 09 00 47 39 48 AB
FF B5 E7 7F FC 9F FF BE	SOQL720624HBCSML03	11 11 46 69 47 00 FF 44 68 47 77 7F CD AA 65 88
FF BF FF F7 3E DF FF FF	FISL760712HBCSML08	46 57 68 AD AA BC 67 47 88 93 47 F5 7E 9A AD 77

Datos que se almacenan en la tarjeta inteligente

- Almacenamiento de información personal
- Aplicaciones “Offline”
- Estimación de espacio
- Esquema de almacenamiento (XML)

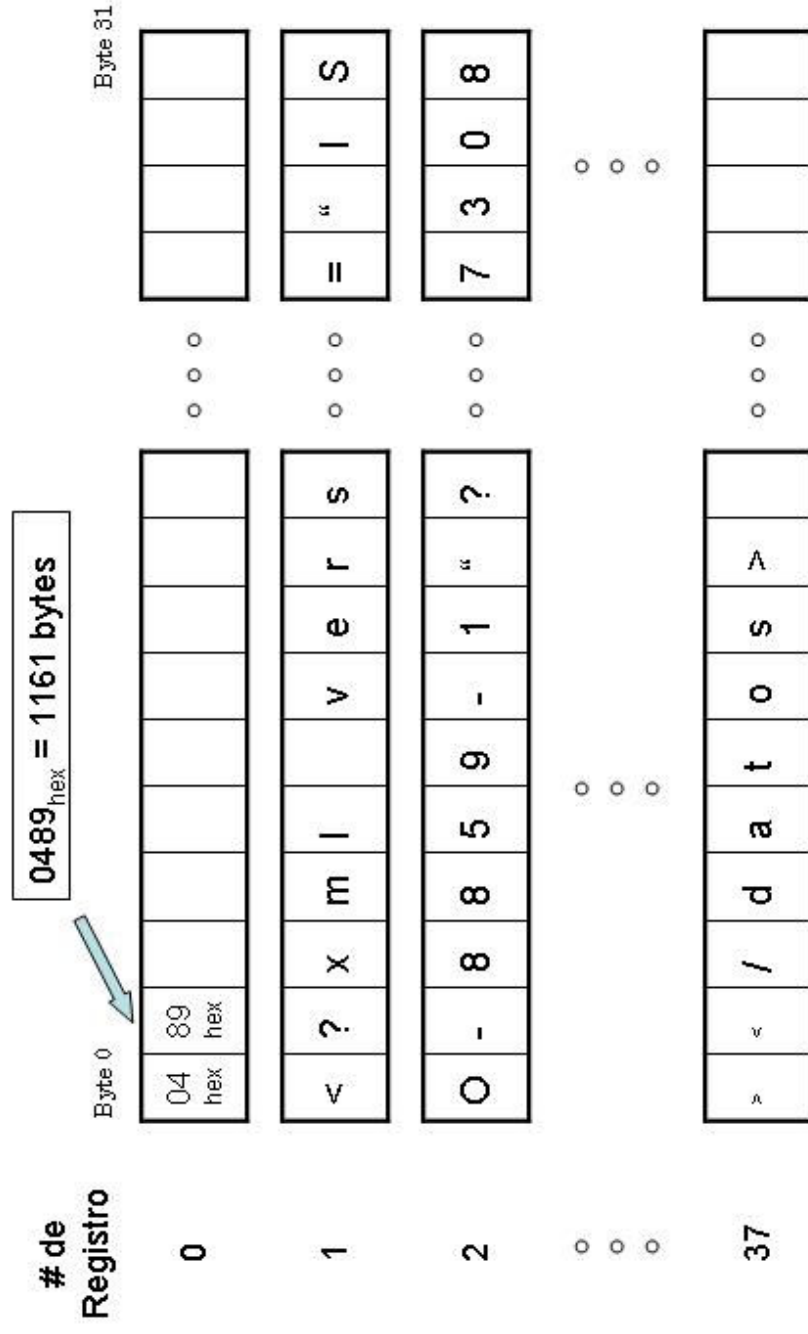
Estimación de espacio

Campo	Tipo	Tamaño (bytes)	Ejemplo
CURP	char	18	CARJ730814HBCSML09
Nombre completo	char	50	Julio César Castillo Ramírez
Fecha de nacimiento	date	8	14081973 (14 agosto de 1973)
Ciudad de nacimiento	char	20	Mexicali
Estado de nacimiento	char	20	Baja California
País de nacimiento	char	2	MX (México)
Sexo	char	1	M (Masculino)
Domicilio - País	char	2	MX (México)
Domicilio – Estado	char	20	Baja California
Domicilio - Ciudad	char	20	Mexicali
Domicilio - Colonia	char	20	Residencias
Domicilio - Calle	char	20	Olga
Domicilio- Número	char	6	84-C
Teléfono fijo	char	20	(686)566-42-98
Teléfono móvil	char	20	(686)135-9211
Tipo de Sangre	char	3	O+
Total =			250 bytes

Documento XML

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!-- DTD - Datos personales - ACOS2 -->
<!-- V.1.0 - 12mayo2006 -->
<!ELEMENT datos (curp,usuario,contacto*,actualizacion)>
<!ELEMENT usuario (nombre,paterno,materno?,nacimientto,sexo,domicilio,tel*,sangre?,grado*)>
<!ELEMENT nacimiento (fecha,ciudad,estado,pais)>
<!ELEMENT domicilio (ciudad,estado,pais,colonia,calle,num)>
<!ELEMENT tel (tipo,numtel,ext*)>
<!ELEMENT contacto (nombre,paterno,materno?,domicilio,tel*)>
<!ELEMENT curp (#PCDATA)>
<!ELEMENT nombre (#PCDATA)>
<!ELEMENT paterno (#PCDATA)>
<!ELEMENT materno (#PCDATA)>
<!ELEMENT sangre (#PCDATA)>
<!ELEMENT grado (#PCDATA)>
<!ELEMENT fecha (#PCDATA)>
<!ELEMENT ciudad (#PCDATA)>
<!ELEMENT estado (#PCDATA)>
<!ELEMENT pais (#PCDATA)>
<!ELEMENT colonia (#PCDATA)>
<!ELEMENT calle (#PCDATA)>
<!ELEMENT num (#PCDATA)>
<!ELEMENT sexo (#PCDATA)>
<!ELEMENT tipo (#PCDATA)>
<!ELEMENT numtel (#PCDATA)>
<!ELEMENT ext (#PCDATA)>
<!ELEMENT actualizacion (#PCDATA)>
```

Mecanismo de almacenamiento



Expediente curricular electrónico

Basado en XMLRésumé

- Objetivo
- Historial
- Grados académicos
- Habilidades
- Publicaciones
- Referencias
- Palabras clave
- Membresías
- Intereses
- Reconocimientos

Expediente curricular electrónico

Datos Personales

- CURP
- Nombre
- Fecha de nacimiento
- Lugar de nacimiento
- Sexo
- Domicilio actual
- Números telefónicos
- Tipo de sangre
- Contactos
- Actualización

Documentos probatorios

- Títulos de grado
- Certificados
- Constancias
- Idiomas
- Publicaciones
- Reconocimientos
- Experiencia laboral
- Otros

Expediente curricular electrónico

Documento en XML

Archivo DTD

Conclusiones y Aportaciones

- Definición de tarjeta inteligente para un contexto general
- Diseño del expediente curricular electrónico
- La tarjeta inteligente como un medio seguro y confiable de acceso al expediente curricular electrónico

Conclusiones y Aportaciones

- La importancia de la creación de entidades de certificación dentro de la arquitectura
- La utilización de Bases de Datos Distribuidas para el almacenamiento del expediente curricular electrónico
- Beneficios que proporcionaría la implementación del sistema

Recomendaciones

- Anticipar los problemas
 - Resistencia de adaptación
 - Complejidad en la reestructuración de los sistemas
- Tomar en cuenta el factor humano

Productos de investigación

- **Castillo, J., Flores, B., Ibarra, J. (2006, Octubre 20). *Tarjetas Inteligentes y sus Aplicaciones*. Taller impartido en el VI Simposium Internacional de Ingeniería Decivel. Facultad de Ingeniería, UABC. Mexicali, B.C., México.**
- **Castillo, J., Flores, B., Ibarra, J. (2006, Mayo 9). Grupo de Investigación en Tarjetas Inteligentes (GRINTAIN) – Estrategias y Resultados. Conferencia impartida durante la Semana de Computación e Informática en el XXV aniversario del Instituto de Ingeniería, UABC. Mexicali, B.C., México.**
- **Ibarra, J., Flores, B., Castillo, J. & Castro, U. (2006). Diseño de una Arquitectura para el Manejo de Expedientes Curriculares Electrónicos Utilizando Tarjetas Inteligentes. Congreso Internacional de Ingeniería en Electrónica ELECTRO 2006. Sección Sistemas Inteligentes. Vol. XXVIII. P.p 323-328. ISSN. 1405-2172. Creel, Chi., México.**

Productos de investigación

- Flores, B., Ibarra, J. & Castillo, J. (2005, Noviembre) La Problemática del Comercio Electrónico en Comprobantes Curriculares. Primer Simposium Internacional de Educación. Sección Educación a Distancia. Num. 48. Facultad de Ciencias Humanas, UABC. Mexicali, B.C., México.
- Castillo, J., Ibarra, J., Flores, B., “Introducción a las Tarjetas Inteligentes”. V Simposium Internacional Decivel. Facultad de Ingeniería, UABC. Mexicali, México. Octubre de 2005.
- Julio Castillo. Conferencia “Introducción a las Tarjetas Inteligentes y sus Aplicaciones”. Semana de Informática, CESUES. San Luis Río Colorado, Sonora. Octubre de 2005.

Productos de investigación

- **Castillo, J., Ibarra, J. & Flores, B. Publicación de cartel “Diseño de un Sistema para el Almacenamiento y Recuperación de Expedientes Curriculares Electrónicos utilizando Tarjetas Inteligentes”. Semana de Moprosoft. Facultad de Ingeniería, UABC. Mexicali, México. Junio de 2005.**
- **Sitio Web del grupo de Investigación en Tarjetas Inteligentes**
<http://www.grintain.com>

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA
FACULTAD DE INGENIERÍA



Maestría y Doctorado en Ciencias e Ingeniería

**“DISEÑO DE UN SISTEMA PARA EL ALMACENAMIENTO Y
RECUPERACIÓN DE EXPEDIENTES CURRICULARES
ELECTRÓNICOS UTILIZANDO TARJETAS INTELIGENTES”**

TESIS

QUE PARA OBTENER EL GRADO DE

Maestro en Ciencias

PRESENTA

Julio César Castillo Ramírez

DIRECTOR

M.C. Jorge Eduardo Ibarra Esquer

CODIRECTOR

M.C. Brenda Leticia Flores Ríos

Mexicali, Baja California, 8 de Junio de 2007