OS ESTUDIOS NACIONALES

PRIMER DIPLOMADO SUPERIOR EN EVALUACIÓN Y GESTIÓN DE PROYECTOS

TITULO DE LA MONOGRAFÍA

"Bases Jurídicas y Técnicas para un Proyecto de Creación de notarias digitales para migrantes"

Previa a la obtención del Título de:

DIPLOMADO SUPERIOR EN GESTIÓN Y EVALUACIÓN DE PROYECTOS

Elaborado por: Ing. Juan C. Benalcázar Z.

Tutora: Dra. Magdalena Granizo

Quito, 12 de mayo de 2008

Tabla de contenido

Introducción

Este trabajo está enfocado a tratar un gran problema social que desde hace algún tiempo ha pasado inadvertido, pero que poco a poco se ha ido constituyendo en una parte importante en el desarrollo sostenible de la economía nacional, como todos conocemos la migración es un problema social, político y económico que, como veremos en el desarrollo del presente trabajo, muestra otros aspectos que son importantes considerar como lo son el factor pscicológico y el familiar.

Como es lógico pensar, nuestros compatriotas en el exterior de una u otra forman se ven en la necesidad de realizar trámites legales en el Ecuador pero que debido a la distancia son encomendados a sus familiares, los mismos que deberán realizar todos los trámites necesarios en las notarias e instituciones públicas en el país que en muchos de los casos se constituyen en verdaderos retos debido a las trabas y problemas presentados en las diferentes instancias del proceso.

Adicionalmente, se presenta un alto grado de inseguridad ya que debido a la ausencia de los titulares y la entrega de poderes especiales se deja carta abierta a familiares y personas que pueden abusar de la confianza y cometer actos de mala fe y perjudicar en gran manera al migrante.

Por tal razón, aprovechando el desarrollo de las tecnologías de información y comunicaciones y basados en principios y marcos legales se propone la creación de notarias digitales para migrantes, la provisión de servicios notariales permitirá a la gran población de compatriotas que se encuentran fuera del territorio nacional efectuar de manera segura, rápida y fácil, diferentes trámites y servicios utilizando servicios web disponibles en el internet.

Lógicamente para poder implementar y llevar a cabo este proyecto es necesario efectuar un trabajo más extenso y profundo e involucrar a entidades gubernamentales y organizaciones especializadas, pero sin ninguna duda esta propuesta puede constituirse en un importante proyecto para contribuir al desarrollo de las TIC's y lo más importante brindar un espacio a nuestros hermanos migrantes para que estén de una u otra forma más cerca de nosotros.

Problemática

Una profunda crisis política y económica afectó al Ecuador con mayor intensidad en el año 2000 y sus resultados se continúan sintiendo en el País. Uno de ellos es la grave problemática de la migración de la población, especialmente de aquella perteneciente a sectores humildes, quienes salen del campo y ciudades pequeñas en su mayoría y con el afán de buscar mejores oportunidades laborales en países más desarrollados e industrializados, que de cierta manera ofrecen "estabilidad laboral y por ende la económica", de lo cual nuestro País es carente desde el agravamiento de sus crisis políticas y económicas.

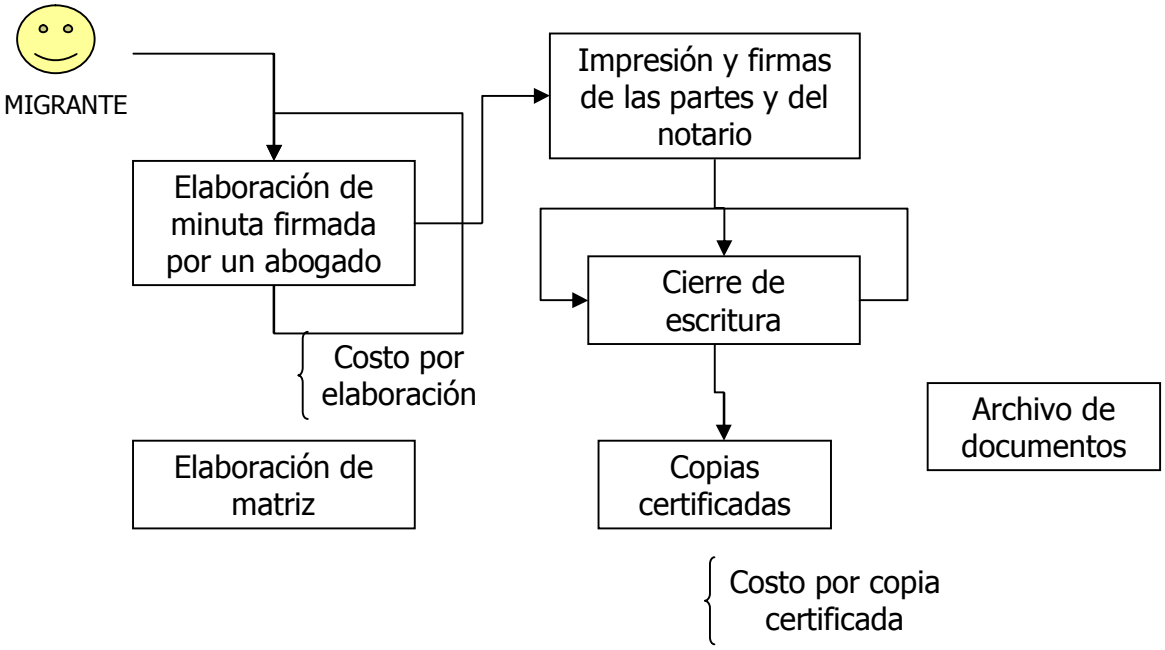
Esta situación sigue generando una problemática más grave que la económica, que es la social, ya que la migración ha causado el desarme de la institución familiar causando conflictos psico – emocionales por la desmembración de sus integrantes.

En los últimos diez años, alrededor de tres millones de ecuatorianos viven en el extranjero; de los cuales, al menos un millón y medio viven en Estados Unidos, un poco más de 500.000 viven en España y el otro medio millón de ecuatorianos viven en Italia, Alemania, Gran Bretaña, Colombia, Perú, entre otros países.

A pesar de que algunos de los migrantes ecuatorianos tienen legalizada su estadía, les es imprescindible realizar varios trámites legales que en su mayoría deben ser notarizados.

Los trámites notariales que generalmente tienen que realizar los migrantes están relacionados principalmente: con la emisión de poderes especiales y generales, autorizaciones de viaje para menores de edad, copias certificadas, reconocimiento de firmas, trámites para la doble nacionalidad, inscripción de divorcios, entre otros.
Dichos procesos resultan molestos y causan intranquilidad a los migrantes y sus familiares ya que son muy largos de realizar, además, dichos documentos una vez notarizados no están disponibles rápidamente para otros trámites ya sea en el Ecuador o en el extranjero dependiendo del lugar donde se hayan expedido.

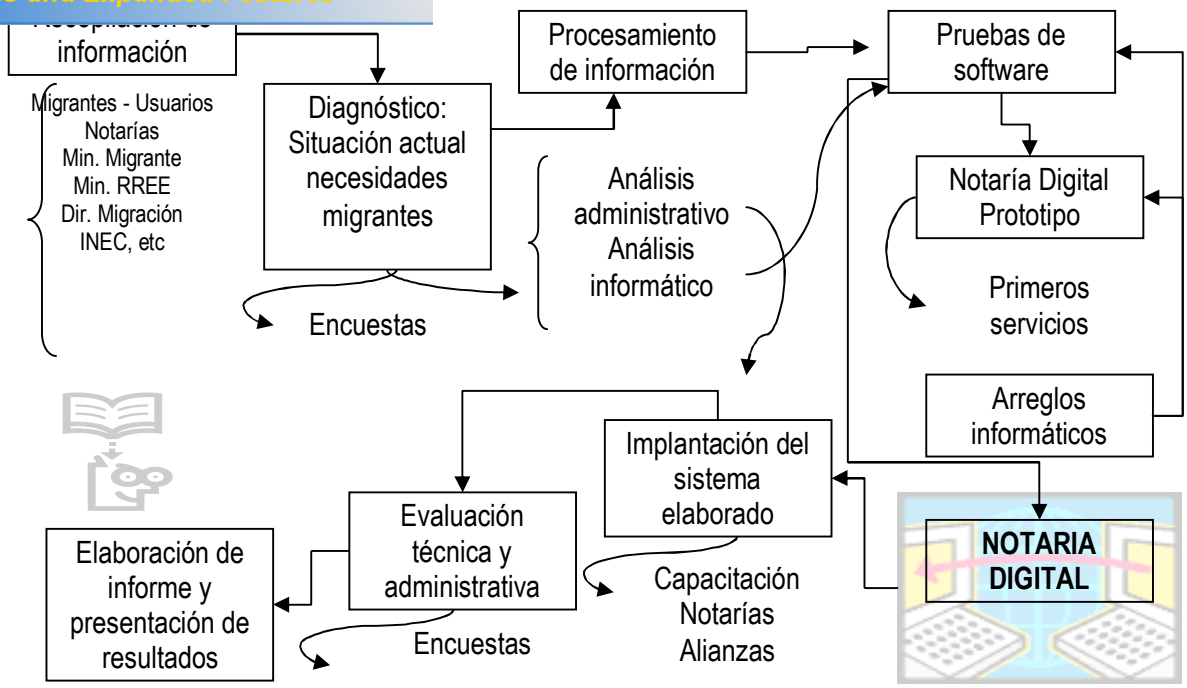
DIAGRAMA DEL PROCESO NOTARIAL ACTUAL



De acuerdo al cuadro anterior, se diagnosticará la situación actual en base a encuestas y al análisis de información obtenido de fuentes relacionadas con la problemática migratoria. Se identificarán los cuellos de botella en el proceso para notarización actual, los mismos que serán mejorados a través del sistema digital.

El equipo técnico trabajará en la estructuración del software para la creación de las notarías digitales, cuya arquitectura estará relacionada con los servicios y valores agregados para los migrantes – usuarios.

Con el prototipo de Notaría Digital se podrán prestar los primeros servicios con lo cual se realizarán los arreglos informáticos para poder implantar el nuevo sistema así como las estrategias para su utilización.



Por otra parte, el análisis administrativo llevará a cabo la coordinación del estudio en general así como la implantación y evaluación del mismo, que incluye: realizar las alianzas estratégicas necesarias, capacitación en notarías, elaboración, tabulación y análisis de encuestas, entre otros.

Cobertura y Localización

El proyecto se ejecutará desde Quito – Ecuador y la cobertura del mismo es mundial debido a la variedad de destinos que los ecuatorianos visitan diariamente.

Para preparar las bases tecnológicas del proyecto, se tomará en cuenta la información recopilada de acuerdo a los países de mayor flujo de ecuatorianos como: Estados Unidos, España, Colombia, Perú, entre otros; según información de la Dirección Nacional de Migración, del Instituto Ecuatoriano de Estadísticas y Censos - INEC, estudios de la FLACSO y del Programa Andino de Derechos Humanos. Dichos estudios han determinado que alrededor de 3 millones de ecuatorianos viven en el extranjero.

				2004	2005	2006	Oct-07	TOTAL PAÍSES
			6.575	175.799	201.667	218.925	210.487	1.212.194
2	ESPAÑA	157.579	144.912	88.588	87.156	147.247	123.194	748.676
3	COLOMBIA	54.295	65.775	83.158	76.32	85.323	80.736	445.607
4	PERU	21.164	19.718	93.212	105.273	95.548	93.023	427.938
5	CHILE	20.982	22.291	18.537	17.377	31.048	16.451	126.686
6	PANAMA	22.643	20.06	19.327	19.83	17.997	17.731	117.588
7	ARGENTINA	12.958	16.331	14.867	18.549	20.165	21.382	104.252
8	ITALIA	15.137	18.962	15.473	18.132	21.19	21.721	110.614
9	VENEZUELA	14.945	13.451			14.153	16.257	58.806
10	VARIOS PAISES			31.553	25.71			57.263
	TOTAL 10 PAÍSES	**528.444**	**518.074**	**540.514**	**570.014**	**651.596**	**600.982**	**3.409.623**
	TOTAL SALIDAS	**589.086**	**581.401**	**606.494**	**660.799**	**740.833**	**681.236**	**3.859.849**

Justificación

Siendo los migrantes ecuatorianos un segmento de la sociedad que crece día a día, generando el segundo ingreso económico del País, no cuentan con un proceso tecnológico que agilite sus trámites legales notariales ya que las notarías no prestan dicho servicio debido a muchos factores, entre ellos: no cuentan con una infraestructura tecnológica para brindar servicios notariales digitales, no existe el marco legal que sustente este tipo de servicios, no existe una comunicación con los migrantes para conocer sus necesidades a fondo.

En este aspecto, dada la gran cantidad de migrantes que tiene el Ecuador, surge la urgente necesidad de poner en funcionamiento una plataforma tecnológica para brindar servicios notariales digitales que ayuden a aliviar las cotidianas preocupaciones de los migrantes y sus familias, evitándoles llevar a cabo ciertos trámites engorrosos, con demoras y dificultades.

Es por esto que debemos considerar la creación de “Servicios Notariales Digitales”, convirtiéndose así esta propuesta en la herramienta idónea y eficiente para sobrellevar el problema de la notarización de los documentos, además de constituir un acercamiento con las múltiples necesidades legales de los migrantes al poder mantener una base de documentos disponibles para sus trámites en el Ecuador y en sus países de residencia a través de este desarrollo informático.

Objetivo General

El objetivo general del presente proyecto es el de proveer de Servicios Notariales Digitales para agilitar los trámites legales de los migrantes ecuatorianos, incentivando de esta manera el uso de nuevas tecnologías.

Objetivos Específicos

- Diseñar una plataforma tecnológica que permita brindar servicios notariales digitales para migrantes.
- Definir las normas técnicas, procesos, requerimientos legales y de capacitación para el funcionamiento de la plataforma tecnológica.
- Describir los modelos técnicos con sus respectivos sustentos legales.

Indicadores de resultado

- Ejecución de los primeros servicios notariales
- Puesta en funcionamiento de la plataforma tecnológica
- Guías desarrolladas y probadas en una Notaría Digital prototipo
- Reportes de trabajo obtenidos del sistema digital
- Encuestas de “satisfacción del servicio” de los usuarios

Matriz Marco Lógico

	LÓGICA DE LA INTERVENCIÓN	INDICADORES OBJETIVAMENTE VERIFICABLES	FUENTES DE VERIFICACIÓN	SUPUESTOS
OBJETIVO GENERAL	Proveer de servicios notariales a migrantes	En el primer año de ejecución del proyecto se atenderán por lo menos 100 solicitudes	Registro de recepción de documentos, registros financieros, entrega y cierre de solicitudes	
OBJETIVO ESPECÍFICO	Implementar en las Notarias servicios notariales para migrantes, bajo una adecuada plataforma tecnológica	1.- Definición de servicios disponibles, requisitos, procedimientos. 2.- Funcionamiento de plataforma tecnológica	Manuales técnicos, manuales de Procedimientos, manuales de usuario	Participación de Notarias. Selección de la plataforma tecnológica.
RESULTADOS	Notarias participantes brindan servicios notariales para migrantes	1.- Publicación de servicios notariales 2.- Definición de costos 3.- Definición de requisitos y procedimientos	Portal, página Web, prensa escrita	Establecer un marco jurídico adecuado para brindar el servicio y exista un beneficio para las notarias.
	Notarias participantes cuentan con una infraestructura tecnológica adecuada para brindar servicios notariales para migrantes	1.- Facturas de adquisición de equipos 2.- Inventarios 3.- Cableados de red 4.- Conexiones a Internet	Actas entrega recepción, registros contables e inventarios, mapa tecnológico, inspecciones, auditorias informáticas.	Inversión de notarias en tecnología
	Servicios Notariales para migrantes son ágiles, fáciles y rápidos de realizar.	1.- Encuestas de satisfacción de una muestra de 30% de usuarios. 2.- Los tiempos máximos para la atención de los servicios no podrán superar .os 15 días.	Encuestas de satisfacción, definición de tiempos máximos para la atención de los servicios, registros de auditoria	Establecer convenios, alianzas con embajadas en países donde residen los migrantes, con la finalidad de trabajar coordinada y mancomunadamente.
	Personal de Notarias participantes tienen los conocimientos tecnológicos necesarios para brindar un adecuado servicio notarial	1.- Aprobación de participantes con una nota mínima de 8 (16) puntos. 2.- Asistencia a los cursos del 95% de las horas programadas.	Registro de asistencia a capacitaciones, evaluaciones	Compromiso de personal involucrado en el proyecto (Ministerio, notarias, embajadas, proyectistas,etc)
ACTIVIDADES				

Cronograma de Actividades

	AÑO 1			MESES											
No	Actividad	Fecha inicio	Fecha fin	1	2	3	4	5	6	7	8	9	10	11	12
1	Recopilación de información	02/01/2008	01/03/2008	X	X	X									
2	Compra de equipos y materiales	02/01/2008	15/01/2008	X											
3	Análisis informático	01/02/2008	30/04/2008		X	X	X								
4	Análisis administrativo y legal	01/02/2008	30/09/2008		X	X	X	X	X	X	X	X			
5	Encuestas ex - ante	01/05/2008	30/06/2008					X	X						
6	Procesamiento de información	01/07/2008	31/10/2008							X	X	X	X		
7	Pruebas de software Notaría Digital prototipo	01/05/2008	30/11/2008					X	X	X	X	X	X	X	
8	Presentación de informe anual	01/11/2008	30/12/2008											X	X

	AÑO 2			MESES											
No.	Actividad	Fecha inicio	Fecha fin	1	2	3	4	5	6	7	8	9	10	11	12
1	Pruebas de software	02/01/2009	01/03/2009	X	X	X									
2	Arreglos informáticos	01/04/2009	30/06/2009				X	X	X	X					
3	Implantación del sistema elaborado	01/04/2009	30/11/2009				X	X	X	X	X	X	X	X	
4	Encuestas ex - post	01/07/2009	30/09/2009							X	X	X			
5	Evaluación técnica y administrativa	01/09/2009	30/11/2009									X	X	X	
6	Elaboración de informe final	01/10/2009	30/11/2009										X	X	
7	Presentación de resultados	01/11/2009	30/12/2009											X	X

Capitulo 2

Problemática de la Migración y Emigración

La migración y emigración, que hasta hace algunos años fue un fenómeno esporádico, toma hoy una importancia crucial para el país.

De un acto aislado, concentrado principalmente en algunas ciudades del austro, se convirtió en una estrategia social de supervivencia a nivel nacional.

Así, la emigración se presenta como un proceso nuevo, que afecta a todos los niveles de la sociedad ecuatoriana.

Sin embargo, este fenómeno no aparece exclusivamente en el Ecuador. Sino que se expande en varios países como elemento de un proceso aún más complejo, que es la globalización del sistema capitalista.

Ahora bien, dada la magnitud que el proceso migratorio ha adquirido en el país, no basta con examinar sus efectos. Una comprensión cabal del mismo exige el análisis exhaustivo de sus causas.

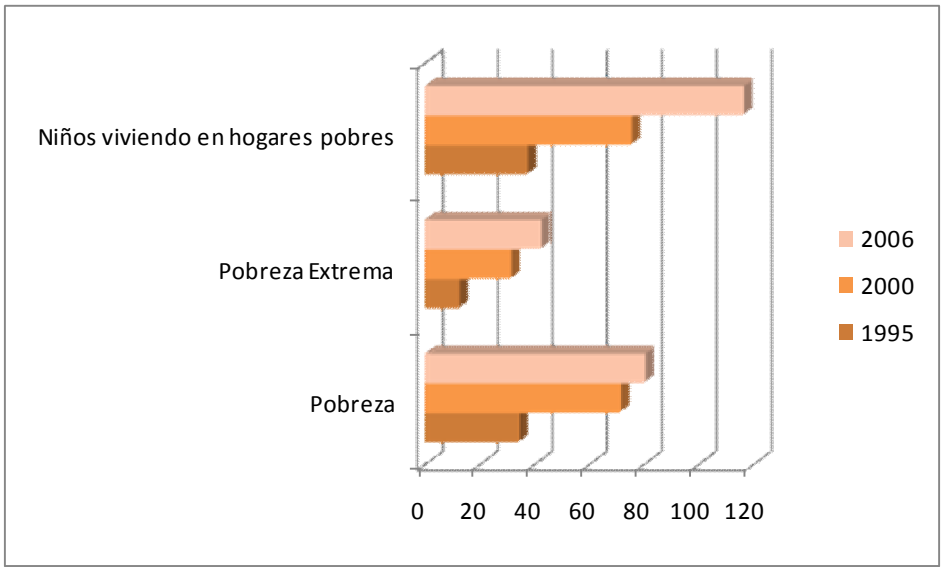
El objetivo de esta cartilla es precisamente desentrañar las principales causas del proceso migratorio ecuatoriano, partiendo del análisis de la realidad política, social, económica y cultural del país, conjugando también factores individuales, psicológicos y emocionales.

La crisis económica

La mayor crisis de la historia Ecuador, país latinoamericano, el más pequeño de la región andina y con una población de 12 millones de habitantes, concluyó el siglo XX con una crisis sin precedentes. Luego de un prolongado período de estancamiento desde 1982, al año 1999 se le recordará por registrar la mayor caída del PIB como se puede apreciar en el cuadro 1.

Este declinó en -30,1%, de 19.710 millones de dólares en 1998, pasó a 13.769 millones en 1999. El PIB por habitante se redujo en casi 32%, al desplomarse de 1.619 a 1.109 dólares.

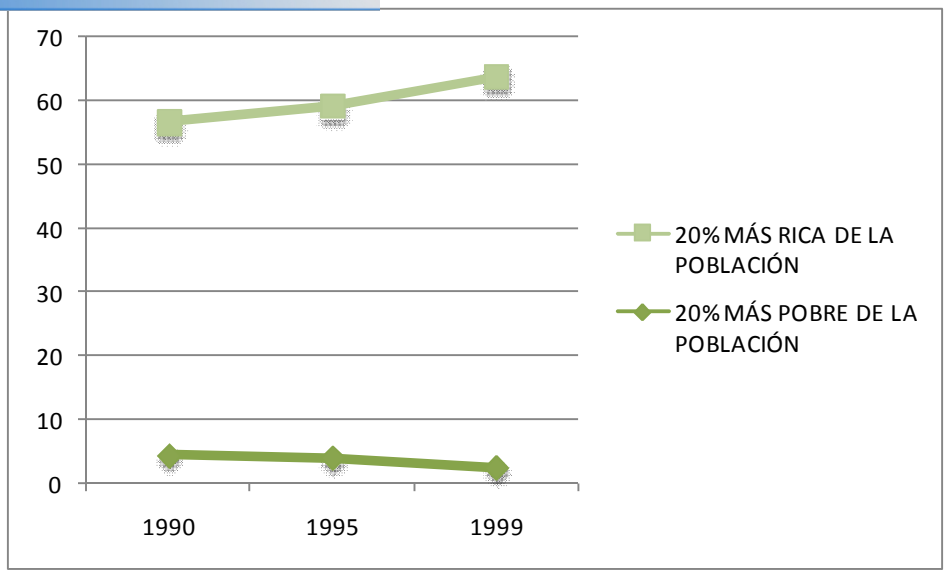
El país experimentó el empobrecimiento más acelerado en la historia de América Latina. Entre el año 1995 y el año 2000, el número de pobres creció de 3,9 a 9,1 millones, en términos porcentuales de 34% al 71%; la pobreza extrema dobló su número de 2,1 a 4,5 millones, el salto relativo fue del 12% a un 31% (ver cuadro 1).



Cuadro 1. Evolución de la pobreza
Elaborado por: el autor
Fuente: INEC

En estas condiciones, se registró un deterioro acelerado de los índices de bienestar. El ingreso por habitante del Ecuador alcanzó apenas un 43% del promedio latinoamericano.

Lo anterior vino acompañado de una mayor concentración de la riqueza. Como se puede ver en el cuadro 2, mientras en 1990 el 20% más pobre recibía el 4,6% de los ingresos, en el 2000 captaba menos de 2,5% (su participación cayó casi a la mitad). Entre tanto, el 20% más rico incrementaba su participación del 52% a más del 61%, un aumento de casi 10 puntos porcentuales. Esta inequidad es, sin duda alguna, una de las principales explicaciones de la pobreza. En efecto, la capacidad productiva del Ecuador podría satisfacer la demanda de bienes y servicios de toda la población, de existir una adecuada distribución del ingreso y de la riqueza.



Cuadro 2. Distribución del Ingreso Nacional
Elaborado por: el autor
Fuente: INEC

La consecuencia lógica de esta evolución fue el masivo desempleo y subempleo; la caída de los ingresos; la reducción de las inversiones sociales: salud, educación, desarrollo comunitario, vivienda; la creciente inseguridad ciudadana; el deterioro de la calidad de vida; y, la caída vertiginosa de la confianza en el país.

Ecuador entonces, al entrar en la mayor crisis de su historia, sumido en una espiral de deterioro económico y social, que produjo una grave inestabilidad política, todo lo cual inauguró un proceso inédito de emigración, cuyas consecuencias recién se empiezan a entender.

Las cifras sobre la emigración varían grandemente. Sin embargo, según datos del Plan Nacional de Ecuatorianos en el Exterior, en los últimos años, un millón y medio de ecuatorianos y ecuatorianas, más del 10% de la población, habrían salido del país.

Además otras organizaciones como Cáritas-España, destacan que, al contrario de otros casos, en el Ecuador no se produjo una emigración de las personas con la peor instrucción y preparación (característica de los sectores de bajos ingresos), sino mayoritariamente de esos sectores medios empobrecidos por la crisis.

Hoy se calcula que en el exterior, según el INEC, viven más de 2,5 millones de ecuatorianos y ecuatorianas, principalmente en los EEUU: cifras oficiales hablan de 600 mil personas en Nueva York, 100 mil en Los Angeles, 100 mil en Chicago y unos 60 mil en Washington. En España, se estima que el colectivo de ecuatorianos y ecuatorianas, que ocupaba un discreto décimo puesto entre las comunidades extranjeras en 1998, está disputando el primer lugar en la actualidad con más de 300 mil personas. En Italia las estimaciones hablan de entre 60 mil y 120 mil inmigrantes ecuatorianos y ecuatorianas.

Las cifras expuestas demuestran la gravedad de una situación dramática, explicable por una serie de factores coyunturales que se potenciaron mutuamente. El fenómeno de El Niño, la caída de los precios del petróleo, la desestabilización financiera internacional, el multimillonario salvataje bancario, el ajuste fondomonetarista, la corrupción galopante y la inestabilidad política - cinco gobiernos en cinco años-.

A más de estos problemas coyunturales, deben ser mencionados algunos de los puntos estructurales más sobresalientes, mutuamente interrelacionados, que se agravaron por los problemas antes mencionados.

La debilidad y fragilidad del mercado interno, a causa de las enormes desigualdades en la distribución de la riqueza, del bajo poder adquisitivo de las masas (pobreza) y de una creciente concentración del ingreso y los activos en pocas manos; concentración que motiva, también, la creciente pobreza.

- La presencia de sistemas de producción atrasados (con baja productividad de la fuerza de trabajo, pero con elevada productividad del capital) que caracteriza la heterogeneidad estructural del aparato productivo. En esta estructura se anclan la poca capacidad de absorción de la fuerza de trabajo y la desigualdad en la distribución del ingreso y los activos.
- La ausencia de políticas generadoras de empleos estables y de calidad.

- La carencia de una adecuada integración entre las diversas regiones del país y el débil desarrollo de las ciudades intermedias y pequeñas, agobiadas por varias manifestaciones de centralismo gubernamental y de concentración de la riqueza.
- Los escasos encadenamientos productivos y de consumo; a lo cual se suma la reducida vinculación sectorial, en particular de la agricultura con la industria y de las actividades de exportación con el resto de la economía.
- La inexistencia de una adecuada política fiscal y de una estructura tributaria equitativa y eficiente.
- La elevada propensión a importar, no sólo maquinaria, equipo y materias primas, sino, en especial, bienes de consumo duradero y no duradero; consecuencia de la consuetudinaria dependencia externa, en especial tecnológica y cultural.
- El mal manejo administrativo del Estado, una marcada arbitrariedad burocrática y una gran cantidad de ineficiencias acumuladas a lo largo de la historia.
- El irrespeto casi permanente a la institucionalidad democrática y a la misma Constitución, que ha aumentado la inestabilidad política y que deteriora la imagen internacional del país.
- Las masivas ineficiencias de sector privado, así como la falta de empuje y capacidad innovadora del segmento empresarial, infectado por la inercia del rentismo y de los clientelismos de antaño.
- La existencia de estructuras oligopólicas y aún monopólicas, así como la ausencia de transparencia que vuelven ineficientes a los mercados.

Esta crítica situación explosionó con el congelamiento de los depósitos bancarios en marzo de 1999, decreto que imposibilitaba al público el retiro de cualquier tipo de depósitos superiores a 550 dólares. Este congelamiento bancario tenía como fin evitar la quiebra masiva de bancos. Pero al restringir abruptamente el medio circulante, muchas pequeñas empresas se vieron imposibilitadas para cubrir sus deudas a corto plazo, e incluso para pagar a sus empleados, por lo que el resultado fue una quiebra generalizada de pequeñas empresas, acompañada de despidos masivos.

De inmediato, se presentó el pánico en la población, dando paso a procesos especulativos, que afectaron profundamente el poder adquisitivo de los sectores desfavorecidos.

A esto, se sumó la disminución de la inversión social, medida orientada a financiar el creciente servicio de la deuda externa. Así, mientras la sociedad, por un lado, era literalmente esquilmada para sanear la banca (concretamente para entregar recursos a los banqueros corruptos) por otro, se suspendió, en el año 1999, por varios meses, el pago de sueldos y salarios a maestros, enfermeras, médicos, policías y militares tratando de sostener el servicio de dicha deuda.

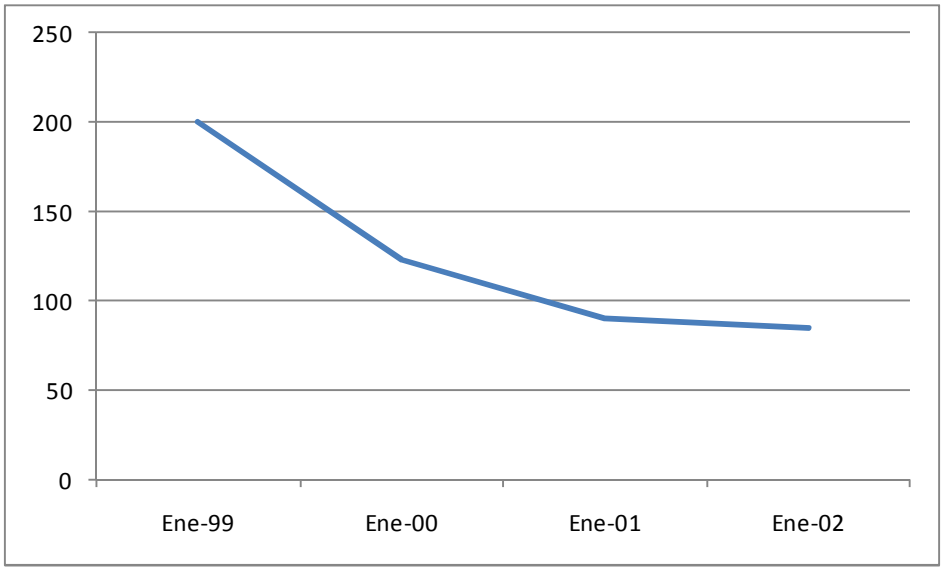
Este esfuerzo colapsó en agosto del año 1999 cuando el gobierno tuvo que suspender el servicio de la deuda externa. Fue una decisión tardía e inútil, al no estar enmarcada en una propuesta económica totalmente diferente a la seguida desde inicios de los años ochenta.

Y por cierto, otro de los factores que explican la crisis radica en el ajuste estructural y en las políticas de estabilización de inspiración fondomonetarista aplicadas en las últimas dos décadas, que tuvieron en la deuda externa y sus renegociaciones una gran palanca para su imposición.
Aunque hay quienes sostienen lo contrario, la economía ecuatoriana, como la de otros países de la región, ejecutó y sufrió el recetario del ajuste. Así, desde inicios de los años ochenta, con diversos grados de coherencia e intensidad, en el Ecuador se adoptó una concepción aperturista y liberalizadora de inspiración neoliberal, impuesta a través de múltiples mecanismos (incluidos chantajes externos e internos).

El objetivo de tales ajustes era la recuperación de los equilibrios macroeconómicos. Al mismo tiempo, se introducían cambios estructurales en la economía en función de las demandas de acumulación del capital transnacional.

Asimismo, no deben olvidarse los efectos nocivos de la dolarización. A los 3 años de su imposición, sus resultados, aún desde una perspectiva optimista, son pobrísimos. Y ateniéndose a las promesas iniciales, la dolarización fracasó en toda la línea. Basta recordar que la inflación y las tasas de interés en dólares se mantienen en niveles elevados, la recuperación económica se desvanece y los desequilibrios externos se vuelven insoportables.
Además, la rigidez del dólar ha perjudicado duramente la competitividad del país. En efecto, al permitir a los socios comerciales del Ecuador devaluar sus monedas en relación al dólar, los productos ecuatorianos y ecuatorianas se encarecen en el mercado internacional. Prueba de esto es

el sostenido deterioro del índice de tipo de cambio real, principal indicador de competitividad (ver cuadro 3).



Cuadro 3. Índice de tipo de cambio efectivo
Elaborado por: el autor
Fuente: Banco Central del Ecuador

Al mismo tiempo, en el país continúa agudizando la falta de industrialización, la distribución del ingreso y la riqueza no dejan de deteriorarse, la pobreza sigue en aumento, el poder económico continúa concentrándose y desnacionalizándose. Por último, se mantiene imparable la emigración de fuerza de trabajo calificada. Más del 45% de la población adulta ansía escapar de este "paraíso dolarizado".

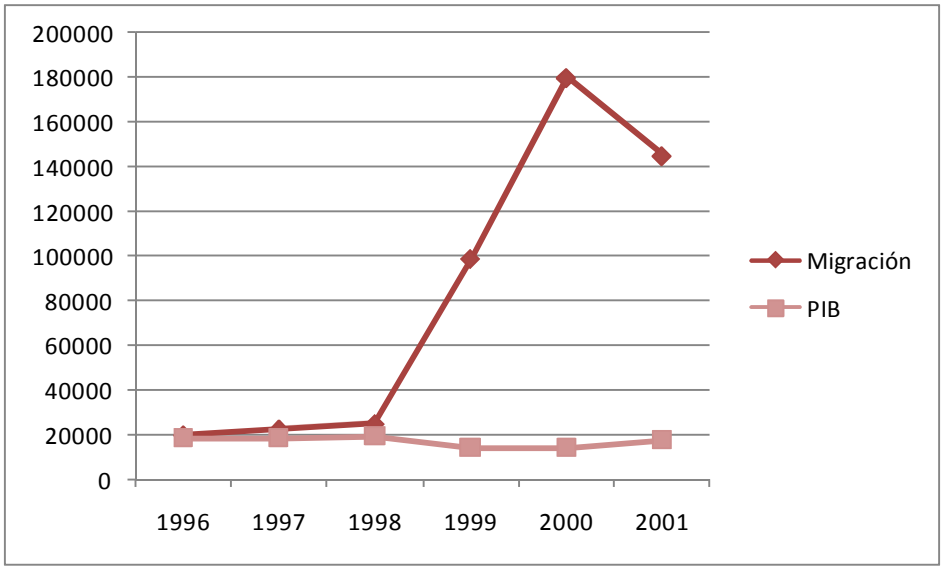
En síntesis, puede concluirse que la crisis económica se reflejó en:

- La quiebra de empresas
- La destrucción de empleos
- La pérdida del poder adquisitivo
- Las pésimas condiciones de trabajo
- El congelamiento de los depósitos
- La caída de las inversiones sociales
- El deterioro de los servicios públicos
- Un ambiente de inestabilidad política
- Creciente inseguridad

Ante tal crisis, los ecuatorianos y ecuatorianas decidieron reestructurar sus estrategias de reproducción social, integrando en éstas un nuevo factor de base: la emigración. Así, frente a la frágil situación nacional, el continuo deterioro económico y las limitadas posibilidades de reactivación, los ecuatorianos y ecuatorianas resolvieron aprovechar los beneficios de los países industrializados. Por ejemplo, mayores posibilidades de encontrar trabajo, remuneraciones superiores, horizontes culturales más amplios, etc. De esta manera, la emigración dejó de ser una aventura individual y se convirtió en un objetivo familiar e incluso colectivo.

Importancia del componente psicológico

Aunque el factor económico se constituye sin duda alguna en un elemento esencial en la explicación del proceso migratorio, no deben dejarse de lado otras variables determinantes para la comprensión de cualquier proceso social. En efecto, como puede verse en el cuadro 4, a pesar del crecimiento económico del 2001, que puso el PIB casi a niveles de 1998, el flujo migratorio se mantuvo en niveles elevados, aunque registró cierta disminución en relación al año 2000.



Cuadro 4. Migración y PIB
Elaborado por: el autor
Fuente: Banco Central del Ecuador, INEC

Cada decisión tomada por un ser humano constituye un acto consciente, determinado, entre otras cosas, por su percepción de la realidad, su estabilidad emocional y expectativas. Es decir, el ser humano tiene varias maneras de enfrentar dicha realidad, dependiendo en gran medida de la forma como percibe los hechos a su alrededor, de la interpretación que les da y de las conclusiones

que saca para sí. Estos elementos forman en las personas un conjunto de ideas que, junto con sus expectativas a futuro, determinarán sus estrategias tomadas para alcanzar el bienestar económico y social, tanto individual como colectivo. Este conjunto de percepciones y expectativas en torno a la crisis desatada en 1999, conformó una visión negativa del país, como un escenario sin oportunidades para el desarrollo de un proyecto de vida, estableciendo un nuevo motor para las decisiones migratorias.

La manera de pensar de los ecuatorianos después de la crisis

La crisis impuso en el Ecuador cierto pesimismo colectivo respecto al futuro. En efecto, como se puede ver en el cuadro 5, sólo el 8% de la población durante la crisis, cree en la posibilidad de un futuro mejor para sí. En menos de 3 años, desapareció la imagen del país como un espacio de oportunidades para el desarrollo social y laboral. Se deterioraron las bases políticas, económicas e institucionales, golpeando gravemente la confianza y legitimidad del gobierno.

Ecuatorianos creen que	
El gobierno les garantiza tranquilidad	7%
Hay posibilidad de encontrar empleo	10%
Control de la inflación por el gobierno	8%
Creen que el gobierno no es honrado	67%
Confían en el descenso de la corrupción	10%
Hay posibilidad de un futuro mejor para si	8%
Creen que el país puede salir adelante	7%
Índice de Bienestar General	12%

Cuadro 5. Componentes del Índice de Bienestar General
Elaborado por: el autor
Fuente: CEDATOS

Hasta hace apenas unos 7 años, la decisión migratoria partía de la voluntad individual de salir adelante. Pero a partir de la crisis de finales de los 90, con la pérdida de fe en el futuro del país, la emigración se transformó en una estrategia de supervivencia. Como se ve en el cuadro 5, apenas el 7% de la población cree que el país puede salir adelante. Así, las expectativas de realización de los proyectos individuales y colectivos de los ecuatorianos y ecuatorianas se trasladan hacia fuera del país.

Al transformarse la decisión migratoria, de un deseo individual de superación, en una estrategia familiar de subsistencia, se conforma una característica clave del proceso emigratorio ecuatoriano: la unidad primaria del proceso migratorio no es simplemente el individuo, sino las familias.

Los significados de la crisis en la decisión migratoria

En el nuevo concepto que los ecuatorianos y ecuatorianas tienen de su país, prima la idea de ausencia de oportunidades. Bajo tal criterio, la migración pasa a ser una opción racional para alcanzar el bienestar.

Se puede afirmar que los ecuatorianos y ecuatorianas entendieron la crisis de 2 maneras: Primero, como una drástica reducción del marco de oportunidades para la producción de los planes de vida en Ecuador. Y segundo, como un espacio para la innovación de estrategias familiares para la reproducción social y subsistencia.

a. Como reducción de oportunidades

En lo que se refiere a empleo y salario, apenas el 10% de ecuatorianos y ecuatorianas consideraban posible encontrar empleo, debido a la incertidumbre, y el cierre del campo laboral (quiebra de muchas empresas y fábricas). Además, la precariedad de las relaciones contractuales, la desvalorización social de la fuerza de trabajo, la flexibilización de las relaciones laborales (exacerbada por la llamada ley Trole 2) y la depreciación acelerada del ingreso real, acentuaron las condiciones de informalidad, inestabilidad y vulnerabilidad individual y grupal. Esto explica que los ecuatorianos y ecuatorianas hayan visto eliminadas sus oportunidades laborales. Tales factores, junto con los problemas de subsistencia (altos grados de pobreza) y búsqueda de reconocimiento, impulsan la decisión de emigrar.

Por otro lado, la cuestión de ética política, asociada con la corrupción, es considerada como una importante causa de la disminución del conjunto de posibilidades de supervivencia de la sociedad.

b. Como renovación de estrategias

Por la reducción de la confianza en su país como espacio de oportunidades para el desarrollo, los ecuatorianos y ecuatorianas ven deteriorada su imagen de lo laboral (empleo, salarios, legitimidad,

credibilidad en la gestión del gobierno, políticas económicas, etc). Por ello, están obligados a cambiar sus estrategias y acciones para alcanzar bienestar, lo que dispara la acción colectiva hacia la migración. Esta práctica se propaga dentro de la sociedad y pasa a formar parte de las estrategias para alcanzar desarrollo individual y colectivo. Así, la emigración se convierte en un instrumento de supervivencia y reconocimiento social. Esto hace que grupos nuevos emigren, ya no como resultado directo de las condiciones adversas del país, sino más bien como una opción normal para trabajar.

Expectativas de los ecuatorianos sobre la migración

Como se ha visto, el factor psicológico en la toma de decisiones es esencial. Este se complementa con los llamados "imaginarios sociales", que son ideas, verdaderas o no, que un grupo determinado tiene sobre un hecho, en este caso la migración. Tales ideas están basadas en elementos racionales e irracionales, objetivos y subjetivos, reales o ficticios.

Toda decisión contempla un objetivo y contiene cierto riesgo. El nivel de riesgo y dificultades aceptadas dependerá del grado de beneficio esperado por el individuo, basado en los imaginarios que se tenga al respecto.

Al ser la emigración una decisión drástica, por todo lo que ella implica (aventurarse en un país extraño dejando atrás familiares), es lógico pensar que el beneficio esperado es alto. Esta idea está sustentada junto a otros elementos, en un imaginario social: el mito del emigrante triunfador. Este consiste en la idea de que el emigrante automáticamente encuentra trabajo en el exterior, accediendo a un nivel de salario ampliamente superior al doméstico. Asimismo supone que el proceso de socialización, adaptación e integración es inmediato. De hecho, es raro que un emigrante acepte que atraviesa graves problemas, aún cuando así sea.

Existen otros imaginarios alternativos que nacen como respuesta a condiciones adversas y están vinculados a la búsqueda de otros horizontes donde proyectarse. Por ejemplo, está la idea de que saliendo del país, se encuentran automáticamente soluciones a futuro. Imaginario que es alimentado por la visión que llega a través de los medios (cine y televisión) sobre la vida en los países desarrollados.

Otros mitos se relacionan con los países de destino. Y en general, son concepciones relacionadas con desarrollo, progreso y bienestar. Los emigrantes saben de las diferencias salariales entre su país de origen y el de destino, y esperan beneficiarse de esta diferencia, así como de una mejor

calidad de vida (similar a la de los habitantes del país de destino), nuevos y mejores conocimientos. Estas ideas operan como mecanismos de atracción.

Factores culturales y emocionales

La decisión migratoria toma fuerza de otros elementos culturales, como las creencias religiosas. En efecto, las dudas y temores de los emigrantes y de sus familias encuentran consuelo en la fe religiosa, en la que se depositan también sus esperanzas de éxito: ¡todo saldrá bien, con ayuda de Dios!.

Un factor importante en la decisión es el miedo de los ecuatorianos y ecuatorianas al desempleo y a la inestabilidad laboral, lo que les impulsa a emigrar. Asimismo, está el temor, en los que ya viajaron, de decepcionar la confianza y las expectativas de la familia. Este temor constituye un incentivo para permanecer fuera del país, aceptando condiciones laborales desfavorables con el fin de salir adelante y pagar sus deudas de viaje.

De esta manera, la acción simultánea de ambos miedos genera una suerte de retroalimentación que impide el regreso: a la falta de recursos se suma la adquisición de una deuda de viaje. El miedo a la situación del país se conjuga con el miedo a fracasar al emigrar, y se fortalece la voluntad de permanencia en el exterior.

Sistemas de redes

Como se manifestó anteriormente, la reciente ola migratoria constituye un proceso social de carácter familiar. No surge como una decisión individual, sino más bien de una estrategia familiar de supervivencia. Más aún, toma cuerpo en un complejo sistema de lazos transnacionales que incluye elementos sociales, económicos, culturales y tecnológicos: las redes migratorias.

Para entender tales aspectos de este proceso multidimensional y complejo, deberán analizarse las formas en que operan los circuitos migratorios y cómo éstos dan a la emigración el carácter de transnacional. Asimismo, se revisará el funcionamiento de las redes familiares. Y finalmente, se examinarán los factores emocionales presentes dentro de las redes.

Circuitos migratorios

Debido a su dimensión, el fenómeno emigratorio ecuatoriano adoptó características particulares, constituyéndose en un verdadero sistema emigratorio. El amplio número de emigrantes mantiene

lazos permanentes con sus familiares en el país de origen (posibilitados por los avances en telecomunicaciones), creando un nuevo tipo de vínculo social: las familias transnacionales. No obstante, los vínculos no son sólo familiares. Los emigrantes contribuyen a la colocación laboral de nuevos potenciales emigrantes, disminuyendo el riesgo ligado a la emigración, y generando nuevas fuentes de ingreso para sí. Estos sistemas se conocen como redes.

A partir de las redes, la migración se convierte en un movimiento circular y continuo, generado por la acción efectiva de dichas redes que facilitan el desplazamiento de la población y refuerzan lazos económicos y sociales entre el país de origen y de destino. Esto hace que el proceso se facilite y se incremente.

Los riesgos de traslado, los costos de asentamiento, la búsqueda de empleo, etc, descansan en el sistema de redes y relaciones sociales, lo que facilita tanto el desplazamiento, como la inserción laboral del emigrante.

La interacción de las estrategias y redes consolidan, dan forma y explican el circuito migratorio. En efecto, la estrategia migratoria, que empieza con la salida de un miembro de la familia, se completa poco a poco con la migración progresiva del resto de miembros misma que se acelera gracias a la acción de las redes.

Funcionamiento de las redes

El Ecuador se caracteriza por la existencia de familias extensas; es decir que en la toma de decisiones, en las soluciones de problemas y en general en la vida cotidiana, toman parte activa los padres, hijos, abuelos, tíos e inclusive compadres del individuo. De ahí que para que el proceso emigratorio comience, se requiere un pacto previo entre los miembros de la familia.

Las acciones colectivas de la familia prevalecen sobre las acciones de cada uno, dejando a luz el carácter jerarquizado de la estructura familiar.

Una vez que el consenso se logra dentro de la familia, comienzan a desarrollarse un conjunto de estrategias para la obtención de recursos, para la exploración de oportunidades laborales, para la inserción en el país de destino, etc. Así, las unidades familiares se transforman en el eje articulador de la acción individual y colectiva en torno a la emigración.

Los recursos materiales para migrar se obtienen a través de dos mecanismos: el endeudamiento; y la hipoteca de los bienes inmuebles familiares. Para este fin se utiliza el apoyo de toda la familia, que actúa como prestamista del futuro viajero. Este financiamiento se puede realizar dentro de la familia

local, o se puede recurrir a préstamos de la familia en el extranjero. Así comienza a articularse el proceso migratorio con las redes familiares.

La familia espera que el que viaje ayude al resto, por lo que los préstamos son concebidos por ellos, como una inversión económica. Pero además del costo económico, también están los costos afectivos, como la separación de los cónyuges, los costos emocionales de los hijos y en los casos extremos la destrucción de hogares. Si bien el primer tipo de inversión es recuperable con el tiempo, los costos emocionales son más difíciles de cubrir.

Dentro de las redes que los emigrantes establecen, incluyen además de su familia, a compañeros de trabajo y a grupos de amigos establecidos ya en el exterior. Estos muchas veces son los que incentivan a que se inicie el proceso migratorio.

Las motivaciones migratorias también responden a conductas de imitación frente a los que ya se fueron. Los emigrantes que tuvieron éxito en el país extranjero, sugieren, fomentan, provocan y ayudan al proceso, dando información de cómo conseguir el dinero, de qué hacer cuando lleguen, etc.

Por otro lado, cuando el acto migratorio es una realidad y el emigrante ya se encuentra en el país de destino, las estrategias familiares siguen funcionando para facilitar el proyecto familiar. En efecto, si al llegar al país extranjero el emigrante no encuentra trabajo, la familia juega un papel central, porque es ella la que colabora para su subsistencia, hasta que él pueda establecerse.

Como se ve las redes familiares fomentan, proveen los recursos, facilitan y ayudan al emigrante, esto sucede debido a que, en las redes hay un alto grado de solidaridad no solo dirigido al viajero, sino a su familia que queda en el país ya que ayudan a su subsidencia hasta que el emigrante se establezca. Además el apoyo familiar, también se expresa en la responsabilidad que asumen, ya sea, en el cuidado de los hijos que quedan en el país, o en el ámbito jurídico, a través de poderes legales ***(para ejecutar transacciones a nombre del emigrante, para la legalización de los documentos en el Ecuador para la inserción laboral en España, etc)***

Pero las redes no solo se limitan a las familias y amigos, sino también se ligan a ellas instituciones que ayudan al emigrante, por ejemplo en España la iglesia católica asila temporalmente a los recién llegados que no encuentran empleo.

La pertenencia a las redes permite al emigrante el acceso a determinados flujos de información, intercambios y posicionamientos sociales (mercado de trabajo, vivienda, condiciones de inserción, etc). Esto no solo facilita la migración, sino que la incentiva.

Factores emocionales de la migración dentro de las redes

Dentro de las redes familiares emergen causas emocionales y subjetivas, las cuales ayudan a explicar la continuidad de los flujos migratorios sin considerar como causal los efectos de factores estructurales vinculados a la crisis económica.

De esta forma una vez establecida las redes, operan por si mismas con independencia a las condiciones políticas, sociales y económicas del país. El proceso migratorio dentro de las redes es autosustentado por otras motivaciones. Por ejemplo, la necesidad de reagrupación con la pareja, hace que los celos, la desconfianza respecto a la actitud del cónyuge en el exterior o el temor a la ruptura del matrimonio sean motivaciones para viajar.

Otros factores dentro de las redes migratorias son elementos que tienen que ver con la comunicación que permiten un contacto con el emigrante en tiempo real, está complementado con el intercambio de fotos, cartas y documentos, hacen que la ausencia física sea contrarrestada con la presencia imaginada.

Además las redes migratorias también cuentan con la ayuda de varias ONG y asociaciones de apoyo al emigrante, las cuales prestan servicios asistenciales, intentan mejorar las condiciones de acogidaal emigrante, buscan reinvidicación política para los emigrantes e inclusive organizan actividades sociales, deportivas y culturales, los cuales hacen el proceso y la decisión migratoria más fácil.

Estos factores (desarrollo tecnológico de las comunicaciones, ayuda de asociaciones) permiten establecer nuevos canales de interacción dentro del circuito migratorio.

En las redes familiares circulan todo tipo de información con una carga de construcciones simbólicas que le dan sentido al proceso migratorio. Se produce un contagio social y se forman nexos permanentes entre los emigrantes y sus familias, estableciendo espacios pluri-locales (a través del permanente intercambio de bienes materiales, culturales y simbólicos) que facilitan y estimulan la decisión migratoria.

Abusos dentro de las redes

Si bien las redes se caracterizan por incentivar y facilitar el proceso migratorio, brindando ayuda al emigrante y su familia, dentro de ellas también existen abusos en algunos casos. Por ejemplo, para poder financiar el viaje, en ciertos casos, el dinero se consigue hipotecando los bienes inmuebles del

emigrante y su familia. Pero en otros, se acude a los llamados “chulqueros” (usureros). Éstos, desde la ilegalidad, hacen de prestamistas y valiéndose de los temores de los futuros emigrantes, perfilan prácticas abusivas en todos los niveles de la contratación.

Para llegar a su destino, el emigrante acude en la mayoría de casos a agencias de viaje para comprar el pasaje, en lugar de comprarlo directamente en las compañías de aviación. Debido a esto, han proliferado las agencias de viaje dedicadas exclusivamente a ofrecer servicios completos y “combos promocionales” para migrar.

En algunos casos, las agencias trabajan de acuerdo a la ley y brindan precios justos, facilitando el viaje.

En otros casos, al igual que los coyoteros, utilizan métodos irregulares y además de venderles el pasaje, les dan el dinero de la bolsa de viaje requerida por las autoridades migratorias, comprobantes de hoteles para hacerse pasar por turistas, asesoría sobre las actitudes y forma de vestir al ingresar al país, e inclusive falsifican contratos de trabajo para facilitar el ingreso, cobrando sumas exageradas de dinero a tasas de intereses altísimas.

Estas agencias no sólo trabajan a nivel nacional, incluso se han detectado redes de tráfico de trabajadores que operan a nivel internacional.

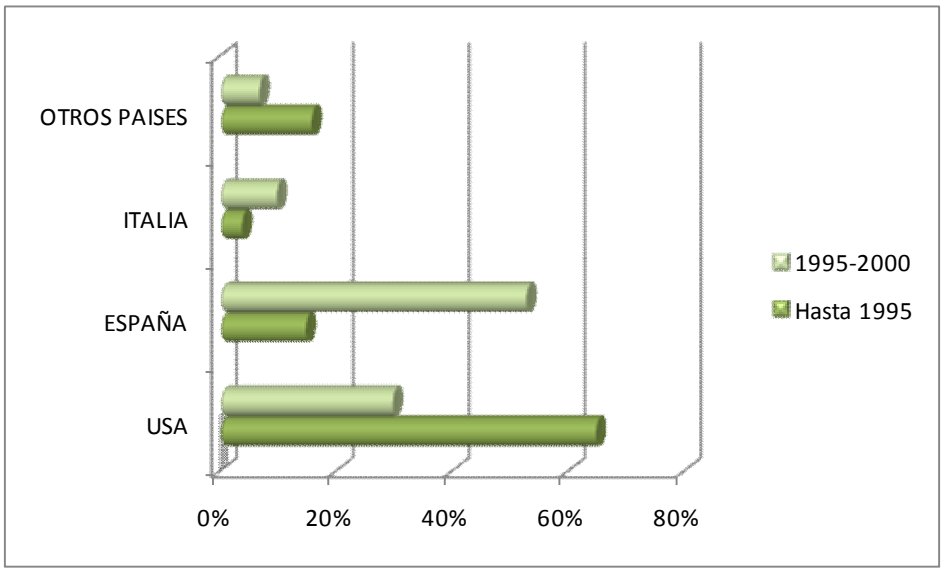
Por otro lado, si bien es cierto que al emigrante recién llegado, los amigos pueden ayudarlo, aún prestándole dinero hasta que logre conseguir trabajo, en otros no sucede eso. Bajo la lógica costo/beneficio, puede ocurrir que el recién llegado se convierta en un subarrendatario del amigo o del compadre, obligándolo a pagar los servicios prestados.

En este sentido, este tipo de red cumple una función ambigua. Facilita la migración en su primera etapa, como mecanismo de imitación y de contagio, pero puede resultar contradictorio en el momento de llegada.

La realidad española

En la reciente ola migratoria se han detectado cambios en cuanto al destino de emigrantes. En efecto como se ve en el cuadro 6, España que hasta 1995 recibía al 15% de los emigrantes ecuatorianos y ecuatorianas, en la actualidad acoge a más del 50%, convirtiéndose en el principal destino de los ecuatorianos y ecuatorianas. Según Cáritas-España, aunque no hay estadísticas completamente fiables, se calcula que son más de 350.000 los ecuatorianos y ecuatorianas que han migrado en busca de trabajo hacia España, de los cuales 150.000 habrían legalizado su situación en

verano del 2002. Lo que deja 200.000 personas viviendo en el territorio español en situación irregular. ¿Qué es lo que determina este cambio en el comportamiento migratorio? ¿Por qué a España?



Cuadro 6. Destino de los emigrantes
Elaborado por: el autor
Fuente: INEC

El cambio en la tendencia migratoria tiene relación con componentes coyunturales, debido a que se origina en un período crítico del país. Esto, junto a estrategias familiares, imaginarios, funcionamiento de las comunidades transnacionales y redes migratorias, marcaron una mayor presencia de flujos migratorios a partir de 1998, la cual se duplicó en 1999 y se aceleró en el segundo semestre del 2000.

Esta tendencia migratoria a España como fenómeno nuevo en el Ecuador, puede explicarse por diversas razones las cuales son tratadas a continuación.

Oportunidades en el mercado de trabajo español

En España se ha producido un incremento general de bienestar, aumento de nivel educativo y de las expectativas de movilidad social entre los españoles, lo que ha provocado que los españoles no ocupen ciertos trabajos como los de servicios y los relacionados a la construcción.

Esto junto con el incremento del mercado informal y de trabajos atípicos, forma un nicho para los inmigrantes, los cuales van en busca de trabajo de cualquier tipo. En el cuadro 7 se ve con más

claridad la tendencia de trabajos realizados por los emigrantes legales; el 30,4% se ubica en servicio doméstico, el 23,66% en servicios en general y el 19,2% en la construcción.

Sector de Actividad	Porcentaje
Servicio doméstico	30.40%
Servicios	23.60%
Construcción	19.20%
Hostelería	8.00%
Otros	10.00%
Comercio	2.60%
Transporte	2.20%
Industria	1.60%
Agricultura, ganadería, pesca	2.40%
Total	100.00%

Cuadro 7. Resoluciones de solicitudes de permisos favorables
Elaborado por: el autor
Fuente: INEC

Otros elementos que impulsan a los emigrantes ecuatorianos

En el caso de los emigrantes ecuatorianos y ecuatorianas se incorporan otros elementos que facilitan la emigración a España.

El primero, es el idioma que posibilita la integración de los emigrantes en la sociedad española.

En la misma línea, como resultado de la conquista española, se tiene como herencia: similar cultura y religión. Lo que agiliza la adaptación de los emigrantes.

Otro elemento es que, a diferencia de Estados Unidos, segundo lugar de destino desde 1996, para viajar a España no es todavía necesaria la exención del permiso visado (visa), lo que facilita el viaje. Ventaja que se perdería de aprobarse la propuesta de imponer una visa para ingresar a la Unión Europea.

Por último, debe mencionarse que las diferencias salariales entre Ecuador y España constituyen otro importante aliciente del flujo migratorio.

El número de ecuatorianos y ecuatorianas en España es tan elevado que ha hecho que los dos países amplíen sus relaciones bilaterales en cuestión de política migratoria, con el objetivo de crear instrumentos jurídicos para regular, dirigir y limitar la oleada migratoria hacia España.

En general, esta política intenta establecer una política de migración selectiva, controlada por las agencias estatales españolas; y establecer mecanismos para frenar la migración irregular de ecuatorianos y ecuatorianas.

En este marco legal, el Estado ecuatoriano, que no ha priorizado a la persona en su política de migración, es cómplice del Gobierno Español por no negociar en favor de los emigrantes ecuatorianos y ecuatorianas; y en lugar de eso, fomentar políticas inadecuadas y confusas que ponen en riesgo la estabilidad y la seguridad misma del emigrante.

Principios Básicos de la Certificación Digital

Infraestructura de Clave Pública

Para entender los principios básicos relacionados con la certificación digital, es esencial conocer la estructura, servicios, elementos y demás características concernientes a una Infraestructura de Clave Pública, también conocida como Infraestructura de Firma Digital o PKI[1] por sus siglas en inglés.

El desarrollo tecnológico y el aumento en los servicios por Internet, han cambiado dramáticamente la forma en que las organizaciones y las personas se comunican y realizan transacciones de negocios tanto privados como públicos.

Una Infraestructura de Clave Pública le permite a una organización contar con un sistema de autenticación, controles de acceso, confidencialidad y no repudiabilidad para sus aplicaciones, usando tecnología avanzada, tales como firmas digitales, criptografía, certificados digitales, entre otros.

Este tipo de infraestructura se basa, en el cifrado RSA[2] o DSA[3] de llaves o claves públicas, siendo el algoritmo RSA el primero en patentarse por la empresa RSA Data Security Inc. y que junto a su filial certificadora Verisign, se constituyeron en una de las alianzas más importantes en el desarrollo e

[1] *PKI.- Public Key Infrastructure*
[2] *RSA Algoritmo de encriptación asimétricos de llaves públicas (Rivest, Shamir, Adleman), 1978*
[3] *DSA Digital Signature Algorithm – Algoritmo de Firmas Digitales*

implementación de Infraestructuras de Claves Públicas, más adelante se profundizará en la situación actual y las características de los algoritmos asimétricos. (Diffie-Hellman[4], PGP[5])

Definición

Una Infraestructura de Clave Pública, puede definirse como *"un sistema de información compuesto de hardware, software, canales de comunicación, procedimientos y recursos humanos entrenados que provee un marco de seguridad y confianza a los documentos digitales y mensajes de datos mediante la realización de actividades vinculadas con la creación, administración, almacenamiento, distribución y revocación de certificados digitales de clave pública."*[6]

Analizando esta definición se precisa que la adecuada combinación entre los productos de software, hardware, políticas, comunicaciones, procedimientos y recurso humano, determinará el nivel de seguridad con el que se podrán realizar las transacciones electrónicas a través de redes públicas o privadas; se menciona también a los certificados digitales, los cuales actúan como pasaportes electrónicos vinculando a un usuario de firma digital con su clave pública, los que se consideran como identificadores digitales.

Dentro de la cadena de seguridad que impone una *Infraestructura de Clave Pública* es substancial el papel de identificación de la persona, para ello, es necesario la creación de Autoridades Certificantes, que registren a las personas y emitan los así llamados Certificados (datos de identidad y clave pública de la persona, firmados digitalmente por la Autoridad Certificadora), garantizando la vinculación entre la persona real o institución y su clave pública.

La PKI también es considerada por algunos especialistas como una norma que trata de describir los procesos organizativos necesarios para la gestión de certificados digitales de claves públicas para el intercambio seguro de información, que permite firmar digitalmente un documento electrónico (un

[4] *Algoritmo de clave pública desarrollado por Diffie-Hellman 1976*
[5] *Pretty Good Privacy, algoritmo de clave pública desarrollado por OpenPGP, IETF RFC 2440*
[6] *Ley No.126-02 Sobre Comercio Electrónico, Documentos Y Firmas Digitales, Agenda Regulatoria del INDOTEL*

mail, el código de un programa, una transacción bancaria, unos análisis médicos, transacciones on-line, dinero digital, entre otros) o permite identificar a una persona o institución en Internet o permite acceder a un recinto virtual o servicio restringido o su vez todas ellas.

Misión

Su misión debe ser la de garantizar la acreditación, el no repudio, la integridad y la confidencialidad de los datos, así como también su auditabilidad.

Servicios

La implementación funcional de PKI permite como mínimo proporcionar los siguientes servicios:

a. Servicios de Certificación .- Garantías de autenticidad, confidencialidad e integridad de los datos a través de una plataforma de certificación, gestión de usuarios, control de revocados, entre otros.
b. Servicios de certificación temporal y timbre o fechado digital[7].
c. Disponer de un conjunto heterogéneo y compatible de soluciones criptográficas.
d. Asesoramiento y apoyo en cuanto a soluciones disponibles ante problemas que surjan en la implementación de otros proyectos.

Estos servicios podrán variar según la naturaleza de la institución o empresa en la que se vaya a implementar, así como también de acuerdo a sus objetivos.

Mecanismos Básicos de Seguridad

Criptografía

[7] *Time-stamping .- servicio de fechado digital.*

Siempre se ha asociado a la Criptografía con algo secreto y misterioso utilizado por el espionaje en todas las guerras y, por otro lado, con una matemática indescifrable, compleja y no abordable para la mayoría de los mortales.

De hecho la Criptografía toma su denominación del griego y se puede traducir como "La manera de escribir raro" (Criptos, extraño; Graphos, escritura).

Las dos técnicas más básicas de cifrado en la criptografía clásica son la ***sustitución*** que supone el cambio de significado de los elementos básicos del mensaje las letras, los dígitos o los símbolos y la ***transposición*** que supone una reordenación de las mismas; la gran mayoría de las cifras clásicas son combinaciones de estas dos operaciones básicas.

Si bien su origen tiene carácter militar, en la actualidad su interés ha desbordado ampliamente dicho campo, para introducirse en las áreas donde la información es valiosa, como la informática.

La criptografía comprende dos procesos bien definidos para la transformación de la información: (**Ver figura 1**)

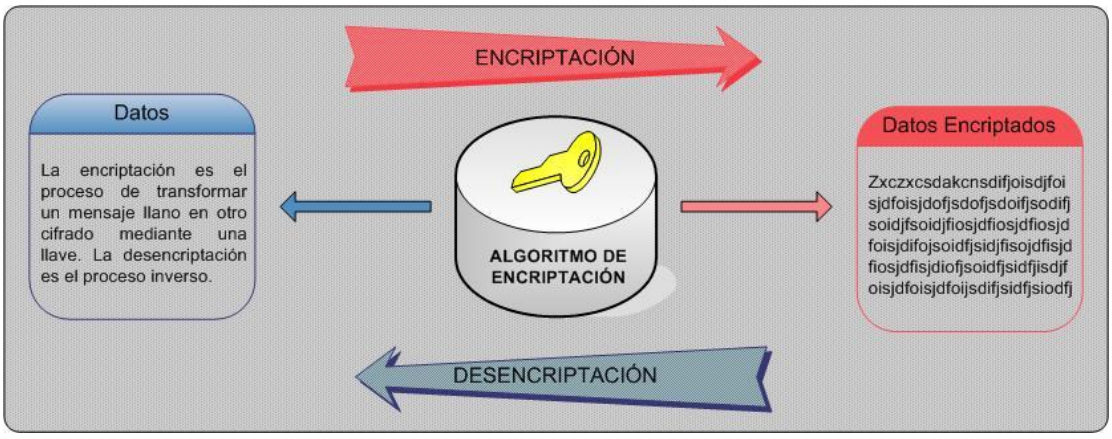


Figura 1. Procesos de la Criptografía
Elaborado por: el autor

1. Encriptación: Proceso mediante el cual un conjunto de datos se transforman en un conjunto cifrado de datos mediante una función de transformación y una llave de codificación. Transforma la información en una forma no legible asegurando la privacidad.

2. Desencriptación: Proceso inverso a la encriptación, en el cual el conjunto cifrado de datos se convierte en el texto original mediante una segunda función de transformación y una llave de desencriptación. La llave puede ser la misma para ambos procesos o distinta.

Todas estas tecnologías usan técnicas matemáticas sofisticadas. Por ejemplo, para mantener la seguridad dentro del Sistema de Nombres de Dominio (DNS dinámico)[8] se consideró la autentificación de usuarios por medio de un nombre (login) y contraseña (password). Los usuarios inicialmente se conectarían al servidor (DNS dinámico) y si el usuario teclea una combinación válida, podrían llevarse modificaciones dentro del servidor; de lo contrario, no se tendría acceso al mismo.

Esta forma de autentificación es una seguridad "débil" por las siguientes razones:

1. Privacidad: El nombre y contraseña del cliente pueden ser capturados por un intruso y leídos sin mayor problema.
2. Verificación: No hay ninguna garantía que el nombre y contraseña del cliente no hayan sido enviados por un impostor (hacerse pasar por un cliente).

El principal problema con un simple nombre y contraseña de un cliente es el hecho de que no pueden ser verificados; por lo tanto, es necesario aplicar un mecanismo para identificar a todos los clientes que intenten conectarse al servidor (DNS dinámico) así como verificar que los clientes son realmente los que dicen ser y no sean impostores.

Se han implementado dos algoritmos criptográficos para llevar a cabo el mecanismo antes mencionado:

a. Llave simétrica o secreta.- Utiliza una misma llave para encriptar y desencriptar la información enviada a través de la red; pero el problema que se presenta es que tanto quien envía como quien recibe la información deben tener la misma llave asegurándose que nadie

[8] *DNS.- Base de datos jerárquica y distribuida que contiene asignaciones de nombres de dominio para varios tipos de datos, como direcciones IP.*

más pueda obtenerla porque si intercepta la información pudiera desencriptarla y leerla fácilmente. Supongamos que necesitamos enviar un mensaje entre dos lugares muy separados, y que éste es confidencial o secreto, por lo que se requiere que nadie lo lea. Para esto se deberá "encriptar o cifrar" el mensaje mediante un procedimiento matemático (algoritmo), que hará que el texto se deforme para que no sea descifrable por un tercero desconocido o no autorizado.

Estos algoritmos necesitan una "contraseña" o "clave" para la encriptación, por lo que, si se ha encriptado el texto original con una clave, el destinatario necesitará la misma clave y el mismo algoritmo para que el mensaje pueda descifrarse y ser leído. Este proceso se llama encriptación simétrica.

Ahora bien, el problema se suscita en la transferencia de esta contraseña o clave al destinatario del mensaje, por lo que se necesita un canal seguro, protegido contra la intercepción, sin lo cual la clave podría ser conocida por un tercero ajeno al proceso. Pero surge la paradoja que si ya se posee un canal seguro para comunicarse con el destinatario del mensaje, no se necesitaría la criptografía para comunicarse en forma segura.

La realidad es que existen pocos canales seguros ya que los servicios de información mundiales, las escuchas telefónicas y otros métodos de interceptación son moneda corriente en nuestros días y por lo cual habría que encontrarse personalmente, supuesto imposible si ambas partes se hallan a una distancia considerable y sobre todo si para cada comunicación segura en Internet habría que repetir estos encuentros.

Este tipo de algoritmo es aun muy utilizado debido a su rapidez.

La fortaleza de los algoritmos de llaves simétricas depende de los siguientes factores:

- Confidencialidad de la llave.
- Dificultad de adivinar la llave.

- Dificultad de forzar el algoritmo de encriptación.
- Ausencia de puertas traseras, es decir huecos de seguridad que permitan desencriptar el mensaje sin tener la llave.
- La posibilidad de desencriptar un mensaje si se conoce una parte de él (ataque de piedra roseta).

Lamentablemente es muy difícil probar la fortaleza criptográfica. Generalmente se prueba la debilidad de un algoritmo que a veces ya se encontraba difundido como seguro. La verdadera seguridad criptográfica está en publicar el algoritmo y esperar a que no se le encuentren errores Los ataques más comunes que reciben este tipo de sistemas son algunos de los siguientes:

- Ataque de búsqueda de llaves (fuerza bruta): Si el violador de códigos tiene la capacidad de reconocer el resultado de utilizar la llave correcta, entonces el método más simple de violar la encriptación es probar todas las llaves posibles. Casi todas fallarán pero al final alguna tendrá éxito.. La forma de protegernos contra este tipo de ataques es que el universo de llaves posibles sea suficientemente grande para evitar que se prueben todas. Por ejemplo. En Internet se utilizan, generalmente llaves de 128 bits. Esto permite 2128 (3.4 x 1038) llaves posibles, un número suficientemente grande como para evitar que alguien se ponga probar de a una. Hasta con ayuda de procesadores que intenten violar el código se tomaría varios miles de años hasta descifrar el código.
- Criptoanálisis: La mayoría de los algoritmos de encriptación pueden ser vencidos mediante la combinación de matemáticas y poder de cómputo. Por lo que casi nunca es necesario, para violar un código, el intentar el método de la fuerza bruta.

Un criptoanalista (persona que rompe códigos) puede descifrar el texto encriptado sin necesidad de tener la llave y sin saber el código de encriptación. Un tipo de criptoanálisis es el ataque de piedra roseta en el que el violador tiene parte del mensaje desencriptado y la misma parte encriptada; con este tipo de ataque el violador obtendrá primero el algoritmo de encriptación, el que luego puede utilizar para intentar inferir el algoritmo de desencriptación para así descifrar el mensaje.

- Ataques basados en el sistema: Esta forma de ataque se basa en buscar debilidades en el sistema que utiliza el algoritmo criptográfico sin atacar al algoritmo en sí. Un ejemplo es el caso de una violación en la seguridad de Netscape que utiliza una llave aleatoria14. Pero el generador de números aleatorios de Netscape no era un buen generador por lo que se podía alterar la semilla del generador y predecir el número aleatorio generado, pudiendo así adivinar la llave.

b. Llave asimétrica o pública.- La solución para resolver el problema presentado por la llave simétrica, surgió en un trabajo publicado en noviembre de 1976, bajo el título "Nuevas Direcciones en Criptografía" de los entonces jóvenes investigadores de la Universidad de Stanford, Whitfield Diffie y Martin Hellman, quienes desarrollaron una metodología de encriptación llamada encriptación asimétrica o pública.

Es un método de transmisión de información en donde el que recibe la información puede estar seguro de la identidad de quien la envió. La idea básica de este método es el uso de un par de llaves:

- Llave privada: Solamente su dueño la conoce y se usa para desencriptar la información enviada por otras personas.
- Llave pública: Esta se publica y se usa por cualquier persona para encriptar la información antes de enviarla a su destino (dueño).

El par de llaves se generan simultáneamente, usando algoritmos especiales en donde los mensajes que se encriptan con la llave pública de una persona puedan ser desencriptados solamente con la llave privada de esa misma persona y viceversa. Por lo tanto, para establecer una comunicación segura ya no es necesario compartir primeramente una llave privada.

Esta transmisión es segura en el sentido de que nadie más que reciba la información podrá leerla porque no sabe el valor de la llave privada.

Con la utilización del par de llaves los sujetos que desean intercambiar mensajes pueden intercambiarse la llave pública encriptadora de forma no segura y conservar la llave desencriptadora. Este principio es el mismo que se usa en las firmas digitales. El problema más grave de este sistema es que es muy lento, entre "*diez y cien veces más que el sistema de llaves simétricas*"[9].

Ha habido mucho menos desarrollo de algoritmos de llave pública que de llave simétrica ya que para crear un algoritmo de llave simétrica sólo hace falta idear una forma de hacer la revoltura de datos, de forma confiable y suficientemente intrincada como para que no sea fácil deducir el algoritmo de desencriptación.

En cambio, los algoritmos de llave pública se basan en la teoría numérica por lo que el desarrollo de un algoritmo nuevo implica encontrar un paradigma matemático de características especiales.

Los ataques más comunes que reciben este tipo de sistemas son los siguientes:

[9] ***"TECNICAS DE PROTECCIÓN CONTRA PIRATERÍA EN DISCOS COMPACTOS",*** *Ing. Ana Azucena Evangelista, Tesis de Maestría en Ciencias, Telemática, página 31*

- Ataques de factorización: Intentan derivar la llave secreta a partir de la llave pública, de la que el atacante tiene una copia. Este ataque necesita resolver problemas matemáticos de alta dificultad como la factorización de números grandes.
- Ataques algorítmicos: Este tipo de ataque consiste en encontrar una falla o debilidad fundamental en el algoritmo en que se basa el problema matemático.

El problema con este tipo de algoritmos es que un defecto en los mismos no necesariamente tiene que ser publicado, lo cual no significa que no exista o no se conozca.

Existe un problema que reside en el hecho de que la llave pública no puede ser verificada. Cómo se que la llave pública realmente es suya y no una llave pública generada por algún impostor que desee interceptar sus mensajes. Este problema es más serio cuando es usado para verificar automáticamente la comunicación entre dos "hosts", tales como un cliente ("browser") y un servidor (DNS dinámico). Aquí es donde intervienen los certificados.

c. Criptosistemas híbridos público / privado: Este sistema se basa en una llave de sesión, que es una llave pública aleatoria que se utiliza para crear un sistema de llaves simétricas. Cada vez que se inicie un intercambio de datos, la llave aleatoria habrá cambiado y se generará una nueva llave simétrica. Este sistema es uno de los más utilizados ya que combina las ventajas de ambos sistemas.

d. Funciones de compendio de mensaje: Este tipo de encriptación genera un patrón de bits único para cada entrada específica. Son como huellas digitales para archivos.

Firma Digital

Con la invención de la criptografía de llaves públicas, Es posible otro proceso conocido como firma digital. Una firma digital es equivalente a una firma manual, la cual proporciona la prueba que el que firma es el autor original del mensaje (Autenticación). Si se desea firmar el mensaje que será

enviado a un destinatario, el mensaje se cambia por medio de una función matemática (conocida como función hash) para lo cual hace un resumen del mensaje (código hash). Este resumen es único para cada mensaje y es equivalente a una huella digital. Luego este resumen o código hash se encripta con la llave privada y se adjunta la final de mensaje. Este código adjunto es conocido como firma digital. El destinatario puede verificar luego que el mensaje fue enviado por una persona que tiene una firma digital haciendo uso de la llave pública a través de una función hash similar. Si los dos códigos hash son similares entonces el que envió el correo firmado fue la persona correcta (no repudio) y no fue alterado (integridad). Todo esto suena complicado pero en la práctica todo lo que se tiene que hacer es dar un clic en un icono que hace referencia a la firma digital, en la pantalla del computador.

Función HASH

Junto a la criptografía asimétrica se utilizan en la firma digital las llamadas funciones hash o funciones resumen. Los mensajes que se intercambian pueden tener un gran tamaño, hecho éste que dificulta el proceso de cifrado. Por ello, no se cifra el mensaje entero sino un resumen del mismo obtenido aplicando al mensaje una función hash.

Partiendo de un mensaje determinado que puede tener cualquier tamaño, dicho mensaje se convierte mediante la función hash en un mensaje con una dimensión fija (generalmente de 160 bits). Para ello, el mensaje originario se divide en varias partes cada una de las cuales tendrá ese tamaño de 160 bits, y una vez dividido se combinan elementos tomados de cada una de las partes resultantes de la división para formar el mensaje-resumen o hash, que también tendrá una dimensión fija y constante de 160 bits. Este resumen de dimensión fija es el que se cifrará utilizando la clave privada del emisor del mensaje.

La firma digital funciona en documentos electrónicos como una firma manuscrita en un documento impreso. La firma es una parte de la información infalsificable que identifica a la persona que lo envió y puede demostrar que está de acuerdo con el documento en el que puso su firma. Actualmente, la firma digital brinda un más alto grado de seguridad que la firma manuscrita. El receptor del mensaje digital puede verificar que el mensaje ha sido originado por la persona cuya firma se encuentra añadida y que el mensaje no ha sido alterado (de forma maliciosa o accidental) desde que fuera firmado. Es por esto que las firmas digitales seguras no pueden repudiarse. El firmante del documento no puede alegar que la firma era falsa. En otras palabras, las firmas digitales permiten la autenticación de los mensajes, asegurándole al receptor la identidad del emisor y la integridad del mensaje.

Para una mejor comprensión de la utilización de una firma digital se plantearan algunos ejemplos:

Supongamos que un sujeto A, distribuye una llave pública a prueba de alteración. Como esta llave sólo sirve para comprobar si la llave privada que el sujeto A conserva es realmente la llave privada del sujeto A, sí alguien intercepta la llave pública no le serviría de nada, por lo tanto el sujeto A podría distribuir la llave pública por cualquier medio. (**Ver Figura 2**)

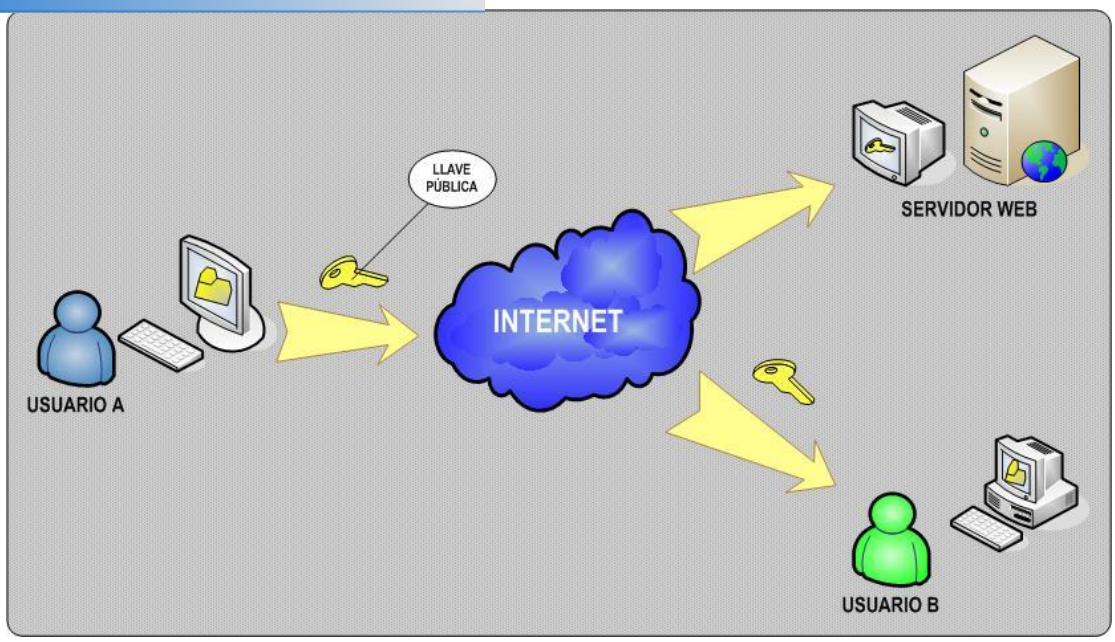


Figura 2. Distribución de la llave pública
Elaborado por: el autor

Supongamos ahora que un sujeto B, necesita corroborar que el sujeto A ha leído un documento X, para esto envía el documento X por mail al sujeto A, el sujeto A recibe el documento X lo lee y anexa su firma generada con la llave secreta. El sujeto A reenvía el documento firmado al sujeto B que mediante la llave pública corrobora la legitimidad de la firma. (**Ver Figura 3**)

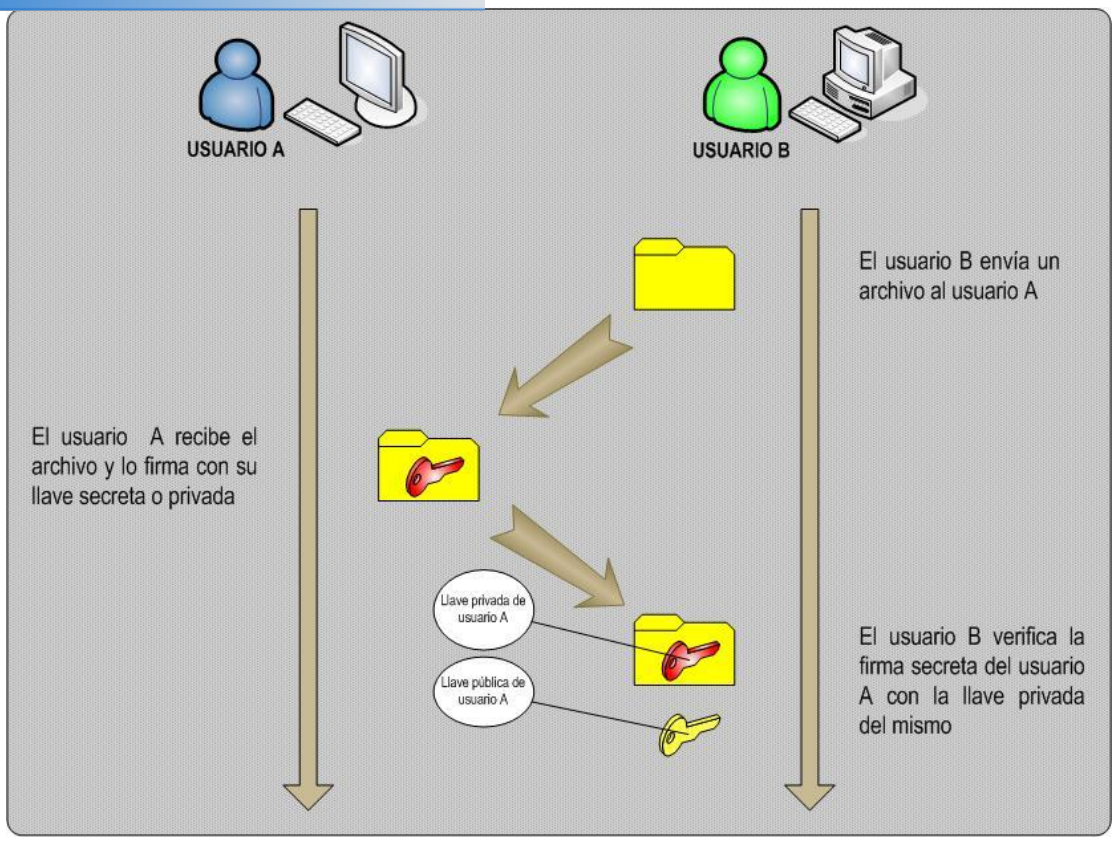


Figura 3. Uso de la Firma Digital para verificar la identidad
Elaborado por: el autor

Los siguientes son los medios físicos en los que soportan la tecnología de llave digital para realizar firmas.

- Llave encriptada almacenadas en disco duro: esta es la forma más sencilla de almacenar la llave, aunque vulnerable a usuarios de la computadora y a programas hostiles.
- Llave encriptada en medio removible: es un poco más seguro guardar la llave privada en un disquete, disco compacto u otro medio removible. Pero para utilizar la llave privada la computadora debe desencriptarla y copiar la memoria, por lo que aún sigue siendo vulnerable a programas hostiles.

- Llave almacenada en un dispositivo inteligente: estos dispositivos son una tarjeta con un microprocesador que almacena la llave privada transfiriéndola directamente sin cargarla en memoria por lo que es inmune a un programa hostil que intente capturarlo. La desventaja de este tipo de dispositivo es su fragilidad y la posibilidad de ser robadas o extraviadas.

A continuación mencionaremos algunas desventajas que presenta utilizar una infraestructura de llaves públicas.

1. La mayor parte de las transacciones de comercio en Internet se basan en las tarjetas de crédito, sin utilizar la tecnología de firmas digitales.
2. Las firmas digitales facilitan la prueba de identidad pero no la aseguran, todo lo que comprueban es que una persona tiene acceso a una llave privada específica que complemente a una llave pública específica que está firmada por una autoridad certificadora específica.
3. Al no existir estándares que regulen a las autoridades certificadoras no es posible evaluar la confiabilidad de las mismas, no es posible saber si la autoridad certificadora quebranta sus propias reglas emitiendo documentos fraudulentos. También es difícil comparar una autoridad certificadora con otra y más difícil aún hacerlo de forma automática.
4. El certificado no posee los datos suficientes como para identificar de forma legal a su poseedor.
5. La tecnología de firma digital no permite la divulgación selectiva de datos

Generalmente, una clave expira tras un período de tiempo de aproximadamente un año. Un documento firmado con una firma caducada no debe ser aceptado. No obstante, existen varios supuestos en los que un documento firmado es considerado legalmente válido por un período superior a dos años; por ejemplo los alquileres a largo plazo y los contratos. Al realizar un contrato

con el servico de "sello de tiempo digital", la firma tiene validez incluso después del vencimiento de la clave. Si todas las partes que intervinieron en el contrato guardan una copia de el sello de tiempo, pueden verificar que el contrato se firmó con claves válidas. De ahí que el sello de tiempo pueda garantizar la validez de la operación posteriormente el periodo de validez de la clave. Todo documento firmado digitalmente puede tener sello de tiempo.

Certificados Digitales

Un certificado digital es un equivalente electrónico del pasaporte. Este contiene información que puede ser usada para verificar la identidad del dueño. Una parte principal del contenido de la información del certificado digital es la llave pública del usuario. Una llave pública puede ser usada para poder realizar una comunicación encriptada entre dos usuarios que tengan certificados digitales.

Los Certificados electrónicos son documentos digitales que sirven para asegurar la veracidad de la Clave Pública perteneciente al propietario del certificado ó de la entidad, con la que se firman digitalmente documentos que puedan proporcionar la más absoluta garantía de seguridad respecto a cuatro elementos fundamentales:

- La autentificación del usuario/entidad (es quien asegura ser).
- La confidencialidad del mensaje (que sólo lo podrá leer el destinatario).
- La integridad del documento (nadie los ha modificado).
- El no repudio (el mensaje una vez aceptado, no puede ser rechazado por el emisor).

Es, por tanto, muy importante estar realmente seguros de que la Clave Pública que manejamos para verificar una firma o cifrar un texto, pertenece realmente a quien creemos que pertenece.

Sería nefasto cifrar un texto confidencial con una Clave Pública de alguien, que no es nuestro intencionado receptor. Si lo hiciéramos la persona a quién pertenece la clave pública con la que lo

hemos cifrado, podría conocer perfectamente el contenido de este, si tuviera acceso al texto cifrado. De la misma forma, si manejáramos una clave pública de alguien que se hace pasar por otro, sin poderlo detectar, podríamos tomar una firma fraudulenta por válida y creer que ha sido realizada por alguien que realmente no es quien dice ser.

Otro dato a tener en cuenta, es que un certificado no puede falsificarse ya que van firmados por la Autoridad de Certificación. Si algún dato se modificase la firma no correspondería con el resumen (hash) que se obtendría de los datos modificados.

Por tanto al utilizarlo, el software que los gestiona daría un menaje de invalidez. Un certificado electrónico contiene una clave pública, y una firma digital. Para su correcto funcionamiento, los certificados contienen además la siguiente información:

- Un identificador del propietario del certificado, que consta de su nombre, sus apellidos, su dirección e-mail, datos de su empresa como el nombre de la organización, departamento, localidad, provincia y país, etc.
- Otro identificador de quién asegura su validez, que será una Autoridad de Certificación.
- Dos fechas, una de inicio y otra de fin del período de validez del certificado, es decir, cuándo un certificado empieza a ser válido y cuándo deja de serlo, fecha a partir de la cual la clave pública que se incluye en él, no debe utilizarse para cifrar o firmar.
- Un identificador del certificado o número de serie, que será único para cada certificado emitido por una misma Autoridad de Certificación. Esto es, identificará inequívocamente a un certificado frente a todos los certificados de esa Autoridad de Certificación.
- Firma de la Autoridad de Certificación de todos los campos del certificado que asegura la autenticidad del mismo.

Los navegadores actuales gestionan y almacenan las Claves Públicas de los certificados que permiten al emisor de mensajes firmarlos y encriptarlos utilizando las claves públicas de los destinatarios. Para complementar la seguridad en cualquier transacción es necesario utilizar, otro tipo de herramientas y protocolos.

Además de servir como mecanismo confiable y seguro de identificación en la red, su certificado de identidad digital le permite disfrutar de otra serie de beneficios: puede enviar y recibir información confidencial, asegurándose que sólo el remitente pueda leer el mensaje enviado; puede acceder a sitios Web de manera segura con su identidad digital, sin tener que usar el peligroso mecanismo de passwords; puede firmar digitalmente documentos, garantizando la integridad del

contenido y autoría del documento; y todas aquellas aplicaciones en que se necesiten mecanismos seguros para garantizar la identidad de las partes y confidencialidad e integridad de la información intercambiada, como comercio electrónico, declaración de impuestos, pagos provisionales, uso en la banca, etc.

La utilización de los Certificados Digitales conjuntamente con los sistemas de encriptación, así como también estrictos procedimientos de verificación de identidades, proporciona una eficaz alternativa de solución en cuanto a la seguridad, por cuanto es posible asegurar que todas las partes involucradas en una transacción son quienes dicen ser y que la información se transmite con integridad, es importante mencionar y considerar que ninguna herramienta o infraestructura asegura el 100% de confiabilidad y seguridad.

Las tiendas virtuales, la banca electrónica y otros servicios electrónicos se están convirtiendo en lugares de encuentro que ofrecen al cliente un servicio flexible y personalizado 24 horas al día, directamente en su casa. No obstante, la preocupación acerca de la privacidad y la seguridad puede limitar el aprovechamiento de estas nuevas formas de intercambio. Por sí sólo, el sistema de encriptación no es suficiente, porque no ofrece prueba alguna sobre la identidad del remitente que

envió la información encriptada. Sin ninguna garantía especial, se arriesga a que un tercero se haga pasar por usted en línea. Los Certificados Digitales solucionan este problema, ofreciendo un medio electrónico para verificar la identidad de una persona. Al utilizar los Certificados Digitales en conjunto con el sistema de encriptación, se proporciona una solución más completa para la seguridad, asegurando la identidad de todas las partes involucradas en una transacción.

Igualmente, un servidor seguro debe tener un Certificado Digital para asegurar que el servidor está administrado por la organización que dice poseerlo y para asegurar que el contenido que ofrece es auténtico.

Cuando usted recibe mensajes firmados digitalmente puede verificar que el firmante del mensaje es quien dice ser y que no se está produciendo una suplantación, siempre y cuando en la practica, durante el proceso de asignación de los certificados se haya constatado y verificado la identidad del individuo, así como también, información que permita disminuir el riesgo de suplantación. Los navegadores de Internet reconocen a muchas de estas autoridades certificadoras automáticamente y permiten agregar manualmente a las que no reconocen.

El "ciclo de vida" de un certificado comprende la emisión, renovación y revocación, siendo esta última ocasionada si la llave privada del tenedor ha sido violada, si la persona ha dado datos incorrectos o si hay copias falsas de ésa llave, entonces el certificado puede ser revocado. Las llaves revocadas que aún no están vencidas son colocadas en una Lista de Revocación de Certificados (CRL), estas listas tienden a crecer con rapidez pero su actualización es lenta.

A continuación, se muestra dos certificados uno emitido por VeriSing una Autoridad Certificadora reconocida a nivel internacional y un certificado emitido por la Superintendencia de Bancos y Seguros. (**Ver Figura 4**)

Figura 4. Certificado válido y emitido por la Autoridad Certificadora **SBS AC** de la Superintendencia de Bancos y Seguros.

Elaborado por: el autor

Tipos de certificados

A continuación veremos los distintos tipos de certificados disponibles hoy en día, dependiendo del uso que se vaya a dar al certificado y de qué persona o entidad lo solicita, las Autoridades Certificadoras han dividido los certificados en varios tipos. Del tipo de certificado a emitir van a depender las medidas de comprobación de los datos y el precio del mismo.

Los certificados, según las comprobaciones de los datos que se realizan, se dividen en cuatro clases:

- Certificados de Clase 1: corresponde a los certificados más fáciles de obtener e involucran pocas verificaciones de los datos que figuran en él: sólo el nombre y la dirección de correo electrónico del titular.
- Certificados de Clase 2: en los que la Autoridad Certificadora comprueba además el DNI o permiso de conducir, el número de la Seguridad Social y la fecha de nacimiento.
- Certificados de Clase 3: en la que se añaden a las comprobaciones de la Clase 2 la verificación de crédito de la persona o empresa mediante un servicio del tipo Equifax o Duns&Bradstreet.
- Certificados de Clase 4: que a todas las comprobaciones anteriores suma la verificación del cargo o la posición de una persona dentro de una organización (todavía no formalizados los requerimientos; está en estudio).

Desde el punto de vista de la finalidad, los certificados electrónicos se dividen en:

1. Certificados SSL para cliente: usados para identificar y autentificar a clientes ante servidores en comunicaciones mediante el protocolo Secure Socket Layer, y se expiden normalmente a una persona física, bien un particular, bien un empleado de una empresa.
2. Certificados SSL para servidor: usados para identificar a un servidor ante un cliente en comunicaciones mediante el protocolo Secure Socket Layer, y se expiden generalmente a nombre de la empresa propietaria del servidor seguro o del servicio que éste va a ofrecer, vinculando también el dominio por el que se debe acceder al servidor. La presencia de éste certificado es condición imprescindible para establecer comunicaciones seguras SSL.

3. Certificados S/MIME: usados para servicios de correo electrónico firmado y cifrado, que se expiden generalmente a una persona física. El mensaje lo firma digitalmente el remitente, lo que proporciona Autentificación, Integridad y No Repudio. También se puede cifrar el mensaje con la clave pública del destinatario, lo que proporciona Confidencialidad al envío.
4. Certificados para la firma de código: usados para identificar al autor de ficheros o porciones de código en cualquier lenguaje de programación que se deba ejecutar en red (Java, JavaScript, CGI, etc). Cuando un código de éste tipo puede resultar peligroso para el sistema del usuario, el navegador lanza un aviso de alerta, en el que figurará si existe certificado que avale al código, con lo que el usuario puede elegir si confía en el autor, dejando que se ejecute el código, o si por el contrario no confía en él, con lo que el código será rechazado.
5. Certificados para AC: que identifican a las propias Autoridades Certificadoras, y es usado por el software cliente para determinar si pueden confiar en un certificado cualquiera, accediendo al certificado de la AC y comprobando que ésta es de confianza.

Toda persona o entidad que desee obtener un certificado debe pagar una cuota a las Autoridades de Certificación, cuota que irá en función de la clase del certificado y del uso que se le vaya a dar al mismo (ambas están relacionadas). A mayor nivel de comprobación de datos (clase mayor), más costará el certificado. La vigencia de cada uno de ellos será determinada por la Autoridad Certificadora emisora, que deberá considerar las necesidades del negocio.

A continuación se presentan ejemplos de certificados digitales:

- Certificado digital clase 3 caducado (no válido) emitido por VeriSing (**Ver Figura 5**).

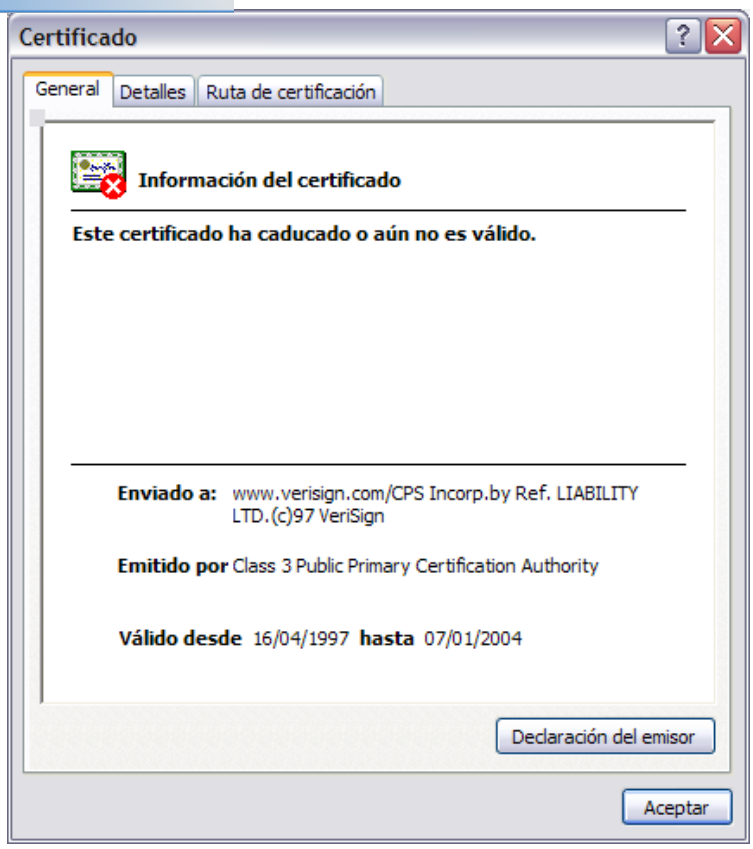


Figura 5. Mensaje de advertencia cuando un certificado ha caducado o aún no ha entrado en vigencia.

Elaborado por: el autor

Certificación cruzada

También conocido como subordinación cualificada, la Certificación Cruzada permite colocar restricciones en las autoridades de certificación (CAs) subordinadas y en los certificados expedidos por éstas y crea confianza entre las CAs de distintas jerarquías. El soporte de Certificación Cruzada mejora la eficiencia de la administración de la clave de infraestructura pública. La certificación cruzada es el acto de compartir niveles de confianza entre dos o mas organizaciones o autoridades de certificación. Esto quiere decir que 2 o mas CAs intercambian información de llaves criptográficas

para la confianza entre sus respectivas llaves, esto permite definir relaciones de confianza entre dominios gestionados por diferentes Autoridades de Certificación. Estas relaciones de confianza pueden ser jerárquicas, de modo que una CA puede permitir CAs subordinadas que expandan la infraestructura, o también pueden establecerse relaciones entre CAs raíces, que son totalmente independientes; estas relaciones de confianza se denominan certificación cruzada “peer-to-peer”.

Time stamping

El servicio de Sello de Tiempo Digital (DTS, Digital Time-Stamping) emite fechas ciertas relacionando una fecha y hora con un documento digital en un sistema criptográfico robusto. El sello de tiempo digital puede utilizarse posteriormente para verificar que el documento electrónico fue creado o modificado el día que figura en el sello de tiempo. Por ejemplo, un físico puede escribir una brillante idea en un procesador de texto y sellar con sello de tiempo dicho documento. Ambos, conjuntamente, pueden probar con posteridad que el científico se merece el Premio Nobel, aún cuando un investigador rival lo haya publicado antes.

Supongamos que Alicia desea firmar un documento con sello de tiempo. Alicia utiliza una función numérica segura para procesar el documento y enviarlo al DTS, que le devuelve un sello de tiempo digital, es decir el mensaje numérico y una fecha y una hora. Como el mensaje numérico no revela ninguna información sobre el contenido del documento, el servicio de sello de tiempo digital (DTS) no puede indagar en el documento. Por eso Alicia puede presentar el documento y el sello de tiempo en forma conjunta para probar la fecha en que se realizó el documento. Un verificador procesa el mensaje numérico del documento, se asegura que coincida con el sello de tiempo y luego verifica la firma del servicio de sello de tiempo digital (DTS) sobre el sello de tiempo. Para ser creíble, el sello de tiempo debe ser infalsificable. Considere los requisitos que debe cumplir el servicio de sello de tiempo digital:

1. El servicio de sello de tiempo digital (DTS) debe tener una clave larga para que el sello de tiempo sea fiable durante décadas.
2. La clave privada del DTS debe guardarse con total seguridad, en un hardware cerrado a posibles modificaciones.
3. La fecha y hora deben provenir de un reloj, dentro de un hardware a prueba de modificaciones, que no puede ser reseteado y que guardará la fecha exacta durante años e incluso décadas.
4. Debe ser imposible crear un sello de tiempo sin utilizar el reloj que se encuentra dentro del hardware a prueba de modificaciones.

El servicio de sello de tiempo digital (DTS) combina esencialmente los valores numéricos de los documentos en una estructura de datos denominada árboles binarios, cuyos valores de "raíz" se publican periódicamente. El sello de tiempo consiste en un par de valores numéricos que permiten a un verificador procesar nuevamente la raíz del árbol. Como las funciones numéricas poseen un solo sentido, no puede falsificarse la validación de los valores numéricos. La fecha relacionada con el documento por el sello de tiempo, es la fecha de publicación de dicho documento.

El uso del servicio de sello de tiempo digital (DTS) es extremadamente importante o esencial, para mantener la validez del documento durante años. Pongamos por caso un contrato de alquiler por tiempo de 20 años. Las claves públicas que se utilizaron para firmar el contrato de alquiler expiran poco después de la firma. Una solución consistiría en firmar el acuerdo cada dos años con nuevas claves, pero esto requeriría que la sociedad dure varios años tras la firma original. En caso que una de las partes no esté satisfecha con el contrato, puede rechazar la sociedad. La solución es registrar el contrato de alquiler con los servicios de sello de tiempo digital (DTS) en la fecha de la firma

original. Luego, ambas partes recibirán una copia del sello de tiempo, que puede ser utilizada varios años después para exigir el cumplimiento del contrato original.

En el futuro, el servicio de sello de tiempo digital (DTS) será utilizado para multitud de actividades, desde los contratos cuya vigencia alcance un largo periodo de tiempo hasta diarios personales y cartas. Actualmente, si un historiador descubre una carta perdida de Cervantes, su autenticación se realiza a través de medios físicos. Pero un descubrimiento parecido puede ocurrir dentro de 100 años en los archivos informáticos de un autor actual; y el sello de tiempo puede ser la única manera de dar validez al descubrimiento.

Elementos de una Infraestructura de Clave Pública

La siguiente figura, se muestra en forma macro los elementos mínimos requeridos en una Infraestructura de Clave Pública y que serán estudiados en este documento. (**Ver Figura 6**)

Figura 6. Visión macro de una PKI.
Elaborado por: el autor

Para poder realizar un adecuado estudio, es preciso identificar claramente los conceptos y estándares utilizados en la implementación de una PKI, su uso e importancia.

Autoridad Certificadora

También llamadas Autoridades Certificadoras (AC) son entidades de confianza quienes tienen la responsabilidad principal de certificar la autenticidad de los usuarios.

Una autoridad certificadora es aquella que presta servicios de emisión, revocación u otros servicios inherentes a la certificación digital, pudiendo también asumir las funciones de una autoridad de Registro (AR) o verificación.

Es decir una AC es la tercera parte fiable que acredita la ligazón entre una determinada clave y su propietario real. Actúa como una especie de notario electrónico que extiende un certificado de claves el cual esta firmado con su propia clave, para así garantizar la autenticidad de dicha información.

La AC, es quien firma digitalmente los certificados, asegurando su integridad y certificando la relación existente entre la Clave Pública contenida y la identidad del propietario. La firma de la AC es la que garantiza la validez de los certificados.

La confianza de los usuarios la Autoridad de Certificación es fundamental para el buen funcionamiento del servicio. El entorno de seguridad (control de acceso, cifrado, etc.) de la AC ha de ser muy fuerte, en particular en lo que respecta a la protección de la Clave Privada que utiliza para firmar sus emisiones. Si este secreto se viera comprometido, toda la infraestructura de Clave Pública (PKI) se vendría abajo.

Las autoridades de certificación realizan las siguientes tareas:

- Emisión de los certificados de usuarios registrados y validados por la Autoridad de Registro (AR).

- Revocación de los certificados que ya no sean válidos (CRL[10]). Un certificado puede ser revocado por que los datos han dejado de ser válidos, la clave privada ha sido comprometida o el certificado ha dejado de tener validez dentro del contexto para el que había sido emitido.
- Renovación de certificados.
- Publicar certificados en el directorio repositorio de certificados.
- Definir tipos de certificados y su aplicación según su jerarquía.
- Definir Políticas y Procedimientos necesarios para la Certificación.
- Definir las funciones de la o las autoridades de registro si las hubiera.

La emisión de certificados y la creación de claves privadas para firmas digitales acostumbran a depender de una pluralidad de entidades que están jerarquizadas de una manera que las de nivel inferior obtienen su capacidad de certificación de otras entidades de nivel superior. Finalmente, en la cúspide de la pirámide suele hallarse una autoridad certificadora, que puede pertenecer al Estado. (**Ver figura 7)**

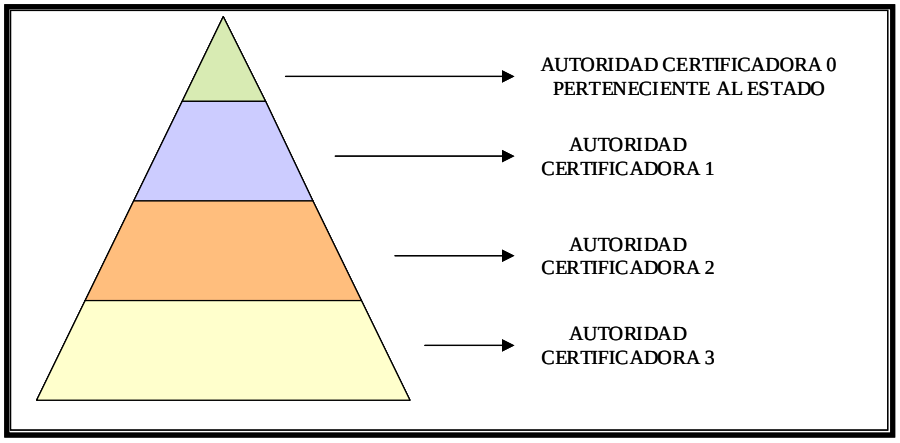


Figura 7. Autoridades Certificadoras que certifiquen a otras.
Elaborado por: el autor

[10] *CRL .- Lista de certificados revocados* o, *en inglés, Certificate Revocation List*

Los certificados indican la autoridad certificadora que lo ha emitido, identifican al firmante del mensaje o transacción, contienen la clave pública del firmante, y contienen a su vez la firma digital de la autoridad certificadora que lo ha emitido.

De esta manera, las partes que intervienen en una transacción aportan como credencial los certificados de su correspondiente entidad certificadora. Para llegar a ser una entidad certificadora deberá mediar una solicitud a una autoridad certificadora de nivel superior, que podrá denegar la licencia si el solicitante no ofrece la fiabilidad o los conocimientos necesarios, ni cumple los requisitos establecidos en la ley.

Existen varias Autoridades Certificadoras, que tengan la facultad de certificar o verificar la identidad de otra Autoridad Certificadora y así sucesivamente; pero habrá un punto en que una Autoridad no tendrá quién la certifique, en este caso, el certificado es firmado por uno mismo ("self-signed""), por lo tanto, la Autoridad Certificadora es verificada o confiada por ella misma (Generalmente la última Autoridad Certificadora es el Estado por medio de alguna Institución).

Las Autoridades Certificadoras (o notarios electrónicos) deben ser entes fiables y ampliamente reconocidos que firman las claves públicas de las personas, certificando con su propia firma la identidad del usuario. Por lo tanto, si se desea establecer una Autoridad Certificadora, éstas deben tomar extremadas precauciones para evitar que sus claves caigan en manos de intrusos, lo cual comprometería todo el sistema. Para ello tendrá que utilizar claves largas y dispositivos especiales para su almacenamiento. Además, cuando emiten un certificado, deben estar seguros de que lo hacen a la persona adecuada. No podemos olvidar que la Autoridad Certificadora es la responsable, en última instancia, de todo el proceso, con una serie de responsabilidades legales y que basa su "negocio" en la credibilidad que inspire en sus potenciales clientes. Una Autoridad Certificadora con autentificaciones erróneas no tendrá más remedio que cerrar ya que los usuarios no considerarán sus certificados de la suficiente "calidad".

Varias compañías se han establecido como Autoridades Certificadoras. Entre las cuales destacan:

- VeriSign, Inc. [http://www.verisign.com]
- Thawte Certification. [http://www.thawte.com]
- Xcert Sentry CA. [http://www.xcert.com]
- Entrust. [http://www.entrust.net]
- Cybertrust. [http://www.baltimore.com]

Autoridad de Registro

La Autoridad de Registro (AR) es la entidad encargada de identificar de manera inequívoca a los usuarios que solicitan un certificado a la Autoridad de Certificación (AC), así como de gestionar los certificados.

Las autoridades de registro realizan las siguientes tareas:

- Validar solicitudes de certificado en base a determinados procedimientos de identificación, apropiados a los niveles de seguridad que ofrece cada categoría de certificado (políticas de seguridad).
- Mandar las peticiones de generación de certificados a la Autoridad de Certificación (CA), para que esta los firme con su clave privada.
- Recibir los certificados solicitados a la Autoridad de Certificación (CA).
- Entregar físicamente los certificados a los solicitantes, por cualquier medio (e-mail, disquete)
- Informar a los usuarios de la necesidad de la renovación de su certificado.
- Petición de revocación de un certificado (también puede solicitarlo el propio usuario).

En toda PKI deben establecerse los mecanismos para que los usuarios soliciten su propio certificado, de tal forma que se asegure la identidad de dicho usuario. A este procedimiento se le denomina "Proceso de Registro" y se realiza a través de la denominada "Autoridad de Registro".

Existen dos tipos principales de registro:

- Registro Clásico.- El solicitante acude en persona a una "Oficina de Registro", donde, tras acreditar su identidad, se le proporciona de forma segura su clave privada y su certificado.
- Registro Remoto.- El usuario, a través de Internet, realiza una solicitud de certificado. Para esto empleará un software (p.e. un navegador, Lotus/Notes) que generará el par de claves y enviará su clave pública a la Autoridad de Registro para que sea firmada por la Autoridad Certificadora y le sea devuelto su certificado.

La validez de la Firma Digital estará condicionada por la calidad del proceso de registro, siendo obligatorio para asegurar la validez legal de la firma, algún tipo de registro "Cara a Cara", ya que es el único que asegura la identidad del solicitante. Por otra parte, la validez de la firma digital también estará condicionada a la firma manuscrita de un "contrato" por el que el solicitante acepta su certificado y las condiciones de uso del mismo.

La Autoridad de Registro se compondrá de una serie de elementos tecnológicos (hardware y software específico) y unos medios humanos (los Operadores de Registro). Es el punto de comunicación entre los usuarios de la PKI y la Autoridad Certificadora.

Políticas de Certificación

Deben diseñarse una serie de políticas y procedimientos operativos, que rigen el funcionamiento de la PKI y establecen los compromisos entre la Autoridad Certificadora y los Usuarios Finales.

Estos documentos tendrán un carácter tanto técnico como legal. Dentro de una PKI, las Autoridades de Certificación y Registro tienen mucha importancia y por ello, la seguridad toma un cariz de máxima importancia. Si por cualquier motivo, se compromete la clave privada de alguno de estos sistemas, la PKI utilizada no tendrá ninguna garantía de validez.

Por ello, una solución PKI debe garantizar:

- El secreto de las claves privadas de la Autoridad de Certificación (AC) y la Autoridad de Registro (AR), que se almacenarán cada una en un módulo de seguridad a prueba de manipulaciones.
- El acceso a la AR y a la AC debe realizarse previa autenticación tanto de usuarios como de administradores, utilizando cualquier mecanismo seguro como pueden ser las tarjetas inteligentes.
- La existencia de un operador o administrador de AR que apruebe las distintas peticiones de certificación destinadas a la AC.
- La integridad y confidencialidad de todas las peticiones de certificación que se cursen dentro del sistema, para evitar la generación de posibles "peticiones intrusas" de terceras entidades.

Las políticas de certificación establecen y definen la dirección que debería seguir la organización respecto de la seguridad de su información considerando también los procesos y principios establecidos para el uso de medios criptográficos. También incluye documentos de cómo la organización deberá manejar sus claves a fin de establecer el nivel de control deseado de acuerdo a los riesgos existentes. Típicamente, todos estos aspectos son agrupados en lo que es conocido como Certification Practice Statements – CPS – Este documento es donde se detallan los procedimientos operacionales, como son el funcionamiento de la autoridad certificadora, las actividades de administración de los certificados, las características de los certificados, etc.

La finalidad de este documento es detallar las políticas y prácticas de emisión y gestión de certificados digitales por parte de una Autoridad Certificadora (AC), además, se incluyen las políticas y prácticas de las Autoridades de Registro acreditadas por esta AC.

Para conformar este sistema se requiere de una serie de componentes que procedemos a detallar a continuación:

En el contenido de este manual se debe considerar los siguientes puntos importantes:

- Usuarios Informados,
- Ambiente de Operación Seguro,
- Responsabilidad bien definida,
- Operaciones bien efectuadas,
- Autenticación correcta de identidad.

Repositorio de Certificados o Directorios

Los repositorios de Certificados o Directorios son las estructuras encargadas de almacenar la información relativa a la PKI. Los dos repositorios más importantes son el repositorio de certificados y el repositorio de listas de revocación de certificados.

En una lista de revocación de certificados se incluyen todos aquellos certificados que por algún motivo han dejado de ser válidos antes de la fecha establecido dentro del mismo certificado, más concretamente se almacenan los números de serie de los certificados que han sido revocados o que ya no son válidos y en los que no debe confiar ningún sistema de usuario, este generalmente es un archivo de texto encriptado que se encuentra dentro de las carpetas de configuración del CA.

Cuando una autoridad de certificación emite un certificado digital, lo hace con un periodo máximo de validez que oscila entre tres y cinco años. El objetivo de este periodo de caducidad es obligar a la renovación del certificado para adaptarlo a los cambios tecnológicos. Disminuyendo el riesgo de que el certificado quede comprometido por un avance tecnológico. La fecha de caducidad viene indicada en el propio certificado digital. Cabe anotar que entre más corto sea este periodo de validez más seguro será el certificado, pero la carga operativa aumentará.

Sin embargo, existen otras situaciones que pueden invalidar el certificado digital aún cuando no ha caducado, de manera inesperada:

- El usuario del certificado cree que su clave privada ha sido robada.
- Desaparece la condición por la que el certificado fue expedido. Por ejemplo, el cambio de apoderado de una entidad jurídica.
- El certificado contiene información errónea o información que ha cambiado. Por ejemplo, una errata en los apellidos.
- Una orden judicial, etc.

He aquí la importancia de que las herramientas cuenten con algún mecanismo para comprobar la validez de un certificado antes de su caducidad. Las CRL son uno de estos mecanismos.

Profundizando un poco más en el tema, una CRL es una lista de números de serie de certificados digitales revocados por una autoridad de certificación concreta. Dicha lista está firmada digitalmente por la propia autoridad de certificación.

Cuando un tercero desea comprobar la validez de un certificado debe descargar una CRL actualizada desde los servidores de la misma autoridad de certificación que emitió el certificado en cuestión. A continuación comprueba la autenticidad de la lista gracias a la firma digital de la autoridad de certificación. Después debe comprobar que el número de serie del certificado cuestionado está en la lista. En caso afirmativo, no se debe aceptar el certificado como válido.

Estrictamente hablando, no es necesario descargar una CRL cada vez que se verifica un certificado. Solamente es necesario cuando no se dispone de la CRL de una entidad de certificación concreta, y cuando dicha lista tiene una cierta antigüedad que aconseja su renovación.

La única ventaja de las CRL es que se pueden consultar sin necesidad de una conexión de datos permanente con cada autoridad de certificación. Basta establecer dicha conexión con cierta periodicidad para descargar las CRL actualizadas.

Sin embargo, las desventajas de las CRL son varias:

- Existe el peligro de que un certificado haya sido revocado, pero no aparezca en la CRL del tercero que comprueba su validez. Esto se debe a que la CRL utilizada podría no estar actualizada.
- Si existe responsabilidad legal por el uso de un certificado revocado, no hay forma de demostrar quién es el culpable: el tercero por no comprobar la validez, o la autoridad de certificación por no incluirlo en la CRL a tiempo.
- Las CRL solamente crecen en tamaño, resultando ineficientes para su tratamiento directo.

Además es muy importante realizar un análisis profundo y exhaustivo de las implicaciones que pueden producirse según los esquemas o arquitecturas utilizadas en los casos prácticos.

Generalmente, las aplicaciones comerciales proveen de un software que permite la verificación de las CRL's, otras en cambio utilizan dispositivos de hardware previamente configurados para realizar una verificación evitando la participación del usuario, cualquiera de las dos formas anotadas anteriormente tendrían sus desventajas en cuanto a la disponibilidad de la información (actualización) ya que lo ideal sería que estás verificaciones se las realicen en línea.

El protocolo usado con mayor frecuencia para publicar los CRL's es el Protocolo de Acceso Ligero a Directorio, mejor conocido como LDAP, está basado en el estándar X.500, pero significativamente más simple y adecuado de mejor manera para satisfacer las necesidades del usuario. A diferencia de X.500 LDAP soporta TCP/IP, que es necesario para el acceso a Internet.

Seguridades y Estándares Técnicos

A continución se presentan una serie de estándares definidos por algunas de las siguientes organizaciones:

1. Estándares internacionales dictados por la Internet Engineering Task Force (IETF)
2. Unión Internacional de Telecomunicaciones (UIT)

3. Las Request For Comments (RFC) que son un conjunto de notas técnicas y organizativas donde se describen los estándares o recomendaciones de Internet

❖ **Seguridad Criptográfica**

- Requerimientos de seguridad para módulos criptográficos, para la publicación de estándares del procesamiento de información de las entidades públicas (tomando como referencia el FIPS 140-1 del gobierno de los Estados Unidos).
- Realizar una evaluación para la garantía criptográfica y los respectivos programas de evaluación.

❖ **Estándares de Algoritmos Criptográficos**

Algoritmos Simétricos:

- **DES** (Data encryption Standar), 64 bits, fue aprobado como estándar federal en noviembre de 1976, y publicado el 15 de enero de 1977 como FIPS PUB 46, autorizado para el uso no clasificado de datos. Fue posteriormente confirmado como estándar en 1983, 1988 (revisado como FIPS-46-1), 1993 (FIPS-46-2), y de nuevo en 1998 (FIPS-46-3), El 26 de mayo de 2002, DES fue finalmente reemplazado por AES (Advanced Encryption Standard), tras una competición pública[11]. DES continúa siendo ampliamente utilizado.
- **3DES** (Triple Data encryption Estándar) se llama al algoritmo que hace triple cifrado del DES. También es conocido como TDES, fue desarrollado por IBM en 1978.
- Algunos de los algoritmos para sustituir a DES fueron: **CAST-256** de Entrust Technologies, Inc., **CRYPTON** de Future Systems, Inc., **DEAL** de Richard Outerbridge, Lars Knudsen, **DFC de CNRS** – Centre National pour la Recherche Scientifique – Ecole Normale Superieure, **E2 de NTT** – Nippon Telegraph and Telephone Corporation, **FROG** de TecApro International, S.A., **HPC** de Rich Schroeppel, **LOKI97** de Lawrie Brown, Josef Pieprzyk,

[11] *http://es.wikipedia.org/wiki/Data_Encryption_Standard*

Jennifer Seberry, **MAGENTA** de Deutsche Telekom AG, **MARS** de IBM, **RC6** de RSA Laboratories, **RIJNDAEL de John Daemen, Vincent Rijmen**[12], **SAFER+** de Cylink Corporation, **SERPENT** de Ross Anderson, Eli Biham, Lars Knudsen, **TWOFISH** de Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson

Algoritmos Asimétricos:

- El sistema criptográfico con clave pública RSA es un algoritmo asimétrico cifrador de bloques, que utiliza una clave pública, la cual se distribuye (en forma autenticada preferentemente), y otra privada, la cual es guardada en secreto por su propietario.

Algoritmos de Resumen (HASH):

- MD5 es un de algoritmo de reducción criptográfico diseñado por el profesor Ronald Rivest del MIT (Massachusetts Institute of Technology, Instituto Tecnológico de Masachusets).
- SHA-1 es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el National Institute of Standards and Technology (NIST).

En la actualidad se conoce que, en ambos sistemas se han descubierto colisiones o han sido rotos por algunos investigadores.[13]

Algoritmos de firma digital:

- DSA (Digital Signature Algorithm, en español Algoritmo de Firma digital) Es un estándar del Gobierno Federal de los Estados Unidos de América o FIPS para firmas digitales. Fue un Algoritmo propuesto por el Instituto Nacional de Normas y Tecnología de los Estados Unidos para su uso en su Estándar de Firma Digital(DSS), especificado en el FIPS 186 . DSA se hizo público el 30 de agosto de 1991, este algoritmo como su nombre lo indica, sirve para

[12] *El algoritmo Rijndael ganó la competición pública para reemplazar al algoritmo DES y en Noviembre de 2001 se publicó FIPS 197 donde se asumía oficialmente.*
[13] *http://en.epochtimes.com/news/7-1-11/50336.html, http://www.schneier.com/blog/archives/2005/02/sha1_broken.html*

firmar y para cifrar información. Una desventaja de este algoritmo es que requiere mucho más tiempo de cómputo que RSA.

❖ **Protocolos de Comunicaciones y formatos de datos**

- RFC 1777 LDAP (Protocolo de acceso ligero a directorios)
- ISO/IEC 8824 y 8825
- Especificación de mensajes S/MIME : PKCS Servicios de seguridad para formatos MIME.
- PEM (Privacidad en el correo electrónico)
- MSP (protocolo de seguridad de mensajes)
- Unidad de protección independiente de los datos (IDUP)
- GSS API, RFC 1508
- Protocolo para verificación del estado de un certificado en línea (OCSP[14])
- SSH (Secure SHell) sirve para acceder a máquinas remotas a través de una red, permitiendo copiar datos de forma segura.
- HTTPS es la versión segura del protocolo HTTP[15] utiliza un cifrado basado en las Secure Socket Layers (SSL) para crear un canal cifrado.
- FTPS (FTP/SSL) es un nombre usado para abarcar un número de formas en las cuales el software FTP puede realizar transferencias de ficheros seguras. Cada forma conlleva el uso de una capa SSL/TLS debajo del protocolo estándar.
- SSL (Seguridad de la Capa de Transporte), protocolo criptográfico que proporciona comunicaciones seguras en Internet.

[14] *Online Certificate Status Protocol, este protocolo se describe en RFC 2560*
[15] *HyperText Transfer Protocol, es el protocolo usado en cada transacción de la Web (WWW)*

- SET Secure Electronic Transaction (Transacción electrónica segura) es un protocolo estándar para proporcionar seguridad a una transacción con tarjeta de crédito en redes de computadoras inseguras, en especial Internet.

❖ **Infraestructura para almacenamiento de certificados**

Servicios de directorio X.500, y soporte para otros directorios o repositorios que tengan interfase LDAP.

❖ **Infraestructura de llave pública**

- Certificados X.509 v3
- Especificaciones para interoperabilidad mínima para componentes
- Protocolo de intercambio seguro (SEP)
- Mecanismos simples de llaves publicas GSS-API, RFC 2078

Consideraciones para la implementación de la PKI

En resumen las consideraciones que se deberán tomar en cuenta para evaluar la futura implementación de la PKI:

Flexibilidad y Compatibilidad

Una parte importante en la optimización del uso de una PKI, es que todos sus componentes sean compatibles con los diversos estándares y RFCs que definen cada uno de ellos. De esta forma la PKI, debe ser compatible con LDAP y X.500 para la comunicación con servidores de directorios.

Por otra parte, debe ofrecer la posibilidad de realizar tanto un nuevo registro de usuario como peticiones (de certificación, de revocación o renovación de certificados) por distintas vías : correo electrónico, navegador web o cualquier otro dispositivo de comunicación en red.

Según la finalidad a la que se destine el PKI, puede ser muy interesante tratar las peticiones por lotes, debido a su gran número. De esta forma, se exigirá a la Infraestructura de Clave Pública un proceso automatizado en la comunicación entre AR y AC.

Aunque los principios con los que funciona un sistema de PKI pueden ser complicados, su gestión no debe serlo. La PKI debe permitir a personal no especializado, manejarla con confianza. Estos operadores no tienen por qué entender las complicaciones de los algoritmos criptográficos, claves y firmas.

Debe resultar tan fácil como pulsar iconos y dejar a la aplicación de software que se encargue del resto. El interfaz debe ser gráfico e intuitivo, ayudando a la tarea de gestión, en lugar de dificultarla con complejos registros de la base de datos.

Sencillez

Las características más importantes de un sistema PKI, serán la flexibilidad y la sencillez en el manejo del mismo. Ello conllevará ventajas apreciables en todos los aspectos concernientes a la formación, el mantenimiento, la configuración del sistema, la integración de los distintos componentes y la posibilidad de crecimiento en el número de usuarios.

Pero como todo, tiene el inconveniente del coste asociado a la optimización de estas dos características. Hay que llegar a un equilibrio razonable entre ambos aspectos: el funcional y el económico.

Interoperabilidad

El escenario ideal para que exista una interoperabilidad en una o varias PKIs debería ser, cuando las entidades emisoras emitan un conjunto de certificados de interoperabilidad plena, basándose en un protocolo estándar de solicitud de certificados, solo así las aplicaciones dependientes podrán ser evaluados adecuadamente y no existiría ambigüedad, ni sintáctica, ni semántica en la interpretación durante la duración del proceso.

Como es natural en el desarrollo de nuevas herramientas tecnológicas, es difícil conseguir el grado de interoperabilidad mencionado anteriormente, pero como es lógico a medida que se da un mayor número de aplicaciones que utiliza la tecnología basada en claves públicas, es más factible alcanzar una interoperabilidad sin problemas, esto es atribuible a la relativa madurez de esta tecnología.

Es importante tener muy claro que los estándares de Internet no aseguran la interoperabilidad, aunque resulten de una gran ayuda, como ocurre frecuentemente en los mercados de desarrollo tecnológico la falta de colaboración de las empresas hace que la estandarización sea mucho más complicado, y la tecnología de llaves públicas y certificados digitales no puede ser la excepción; actualmente la IETF tiene múltiples grupos de trabajo desarrollando activamente los estándares propuestos para la tecnología basada en claves públicas. Sin embargo, muchas de las posibles aplicaciones beneficiarias de estos estándares están ya integradas en productos comerciales. Además, ningún estándar puede anticipar todos los requisitos y dependencias de las aplicaciones. Incluso los estándares más completos no se aprovechan al máximo al implementarse. La interoperabilidad, entonces, es el resultado de los estándares atenuados por la realidad del mercado.

El grupo de trabajo IETF encargado de la definición de bases para lograr la interoperabilidad de PKI es PKIX (X.509). Después de casi tres años de trabajo, la arquitectura básica está establecida y la especificación, "Internet Public Key Infrastructure X.509 Certificate and CRL Profile, Part 1"[16] sigue el proceso de convertirse en estándar.

En IETF se están haciendo muchos esfuerzos que pueden tener impacto significativo en la compatibilidad de la PKI. Éstos se deben a las necesidades de las aplicaciones basadas en claves públicas, especialmente TLS, S/MIME e IPSec. En cada caso, estas aplicaciones se han visto en la necesidad de definir un subconjunto de PKIX que satisfaga sus necesidades o a menudo sustituyen

[16] *http://www.ietf.org/ids.by.wg/pkix.html*

la funcionalidad PKIX definida. Aunque podría parecer que esto trunca el proceso, en realidad crea un ciclo de sugerencias para los diseñadores de PKI.

También hay una "obligación moral" inminente para conseguir la interoperabilidad de la PKI. El National Institute of Standards (NIST) ha creado un grupo de trabajo acerca de interoperabilidad compuesto por AT&T, CertCo, Certicom, Cylink, Digital Signature Trust, Dynacorp, Entrust, Frontier Technologies, GTE, ID Certify, MasterCard, Microsoft, Motorola, Spyrus, VeriSign y Visa. El objetivo de este proyecto es asegurar la interoperabilidad mínima entre las implementaciones de los miembros de PKIX parte 1. NIST piensa que este grupo resolverá todas las ambigüedades y errores del nuevo estándar de PKIX.

Otro factor en la definición de los estándares de la PKI está completamente fuera de IETF.

Hay un conjunto de estándares[17] de hecho de mensajes cifrados (“PKCS”), desarrollados y mantenidos por RSA Laboratories, que se distribuyen ampliamente con los productos. Los estándares PKCS, publicados por primera vez en 1990, incluyen la sintaxis para los mensajes cifrados. Los estándares más relevantes para la PKI son PKCS-7, "Estándar de sintaxis de mensajes cifrados" y PKCS-10, "Estándar de sintaxis de solicitud de certificados". La importancia de estos estándares RSA radica en que proporcionan un marco básico, aunque bien definido, para la interoperabilidad. De hecho, cuando el grupo de trabajo PKIX propuso otro estándar para administración de certificados, el grupo S/MIME creó una propuesta propia basada en PKCS. Esta respuesta es típica de las prácticas de IETF y refleja su conocimiento del mercado. Los estándares de hecho son, a menudo, la mejor alternativa para maximizar así la interoperabilidad.

Es razonable esperar que los estándares se completen, aunque a fin de cuentas sólo un subconjunto de ellos se integra en los productos que crean los fabricantes para proporcionar soluciones

[17] *http://www.rsa.com/rsalabs/html/standards.html*

interoperables. Un buen ejemplo de la fuerza de los mercados en la determinación de la interoperabilidad de claves públicas es el funcionamiento de los modelos de confianza.

Escalabilidad

La escalabilidad es una característica necesaria definida por el crecimiento paulatino del sistema. Se puede aplicar a diversos "campos" dentro de la Infraestructura de Clave Pública:

- Número de usuarios;
- Número y tipo de certificados emitidos;
- Número de CRLs almacenadas;
- Tipos de mecanismos de registro;
- Número de ACs y ARs en ejecución;
- Número de aplicaciones soportadas.

Confianza en la AC/AR

Una de las formas por las que se establece la confianza en una AC para un usuario consiste en la "instalación" en el ordenador del usuario (tercero que confía) del certificado autofirmado de la AC raíz de la jerarquía en la que se desea confiar. El proceso de instalación puede hacerse, en sistemas operativos de tipo Windows, haciendo doble click en el fichero que contiene el certificado e iniciando así el "asistente para la importación de certificados". Por regla general el proceso hay que repetirlo por cada uno de los navegadores que existan en el sistema, tales como Opera (navegador), Firefox o Internet Explorer, y en cada caso con sus funciones específicas de importación de certificados.

Si está instalada una AC en el repositorio de ACs de confianza de cada navegador, cualquier certificado firmado por dicha AC se podrá validar, ya que se dispone de la clave pública con la que verificar la firma que lleva el certificado. Cuando el modelo de AC incluye una jerarquía, es preciso establecer explícitamente la confianza en los certificados de todas las cadenas de certificación en las

que se confíe. Para ello, se puede localizar sus certificados mediante distintos medios de publicación en internet, pero también es posible que un certificado contenga toda la cadena de certificación necesaria para ser instalado con confianza.

Marcos Legales sobre Certificación Digital

Marco Legal Internacional

Existen sólo diecisiete países en el mundo con un marco legal establecido por sus respectivos gobiernos en el desarrollo de tecnología PKI. Esto da una idea de la situación en la que se encuentra la utilización de la Infraestructura de Clave Pública en el mundo.

España fue uno de los primeros países pioneros en la implementación de la firma digital y certificación digital, así como también han dado un gran aporte tecnológico al desarrollo de nuevas tecnologías orientadas a la seguridad informática.

La Unión Europea y Estados Unidos son los primeros que han definido modelos de estrategias globales para el desarrollo de Tecnologías de Información y Comunicaciones, y han sido para los demás países ejemplos a seguir en este campo.

La Infraestructura Nacional de la Información[18] es el modelo norteamericano impulsado por el gobierno de Bill Clinton, mientras que la conocida *Sociedad de la Información*[19] es el modelo adoptado por la Comunidad Europea, cada uno de estos modelos presentan características muy particulares, pero dentro de una concepción más general coinciden en señalar a la empresa privada como el motor que debe impulsar el desafío del cambio y a los gobiernos con la imperiosa necesidad de participación, fijando las pautas generales para crear un escenario propicio para el desarrollo de la investigación, encaminada a alcanzar un nuevo horizonte.

La situación en Europa es muy distinta de la estadounidense. En Estados Unidos reina una mayor libertad de mercado, porque las reglas no siempre son claras. Por el contrario, en Europa la Directiva

[18] *The National Information Infrastructure (NII)*
[19] *The Information Society (IS)*

de Firma Electrónica y las correspondientes leyes nacionales sobre la materia han restringido el ámbito en el que se pueden mover los prestadores de servicios de certificación y los proveedores de estas tecnologías.

Además, en los países de la Unión Europea suele haber una autoridad auspiciada por el gobierno con vocación de establecerse como prestador de servicios genérico para facilitar el acceso a la firma electrónica por parte de los ciudadanos, como el **Proyecto Ceres**[20] en España o las fábricas de moneda y timbre de cada país.

Como es de suponerse, el sector privado ha sido el más interesado en el desarrollo de estas herramientas, presionando a los gobiernos a definir los marcos legales y regulatorios indispensables para su normal desenvolvimiento, pero como todo lo que brilla no es oro, los fabricantes de tecnología PKI que se crearon confiando en el boom de final del siglo pasado se han dado un buen tropiezo debido a varios factores entre los que se encuentran el antagonismo de la adopción masiva del comercio electrónico y el Ecuador no ha sido la excepción muchas empresas privadas esperan muy atentas a que este mercado sea realmente rentable.

¿Pero como puede el Estado construir el escenario necesario para que este mercado sea aprovechado por los empresarios?

Esta es una de las interrogantes que se han hecho muchos de los países en América Latina, y que las Naciones Unidas con el propósito de fomentar la armonización y unificación del derecho mercantil internacional y el progreso del comercio internacional de los países en desarrollo, el 16 de diciembre de 1996 la ***Comisión de las Naciones Unidas para el Derecho Mercantil Internacional*** **(CNUDMI)** aprobó la ***Ley Modelo sobre Comercio Electrónico,*** así como también la elaboración de una ***Guía para la Promulgación de la Ley Modelo.*** Estos documentos, se elaboraron con la intención de ayudar a los gobiernos a fortalecer la legislación que rige la implementación de las

[20] *http://www.csi.map.es/csi/tecnimap/tecnimap1998/sp7.htm*

nuevas tecnologías de información y comunicaciones, elementos que sustituyen a los medios manuscritos utilizados actualmente.

Como se había anotado anteriormente, la Comisión de las Naciones Unidas elaboraron un formato de **LEY SOBRE COMERCIO ELECTRÓNICO** para facilitar a los países que poco o nada conocían sobre el tema, la modificación o incorporación en sus legislaciones de una Ley que permita crear un marco jurídico coherente a las necesidades del uso del comercio electrónico en cada uno de las naciones, con la finalidad de proporcionar las reglas necesarias para sortear los obstáculos jurídicos que puedan presentarse en el ejercicio del mismo, de igual forma conscientes de la complejidad y dificultad que podría presentarse para los Estados que no estaban familiarizados con las técnicas de comunicación presentadas en este documento, elaboraron una **GUIA** en base a la recopilación de sus primeras experiencias en el desarrollo de esta Ley, la que orientaría a los usuarios de los medios electrónicos de comunicación en los aspectos jurídicos de su empleo y a la implementación de las herramientas por parte de los estudios en el tema.

Otro de los aspectos considerados por la comisión es el de establecer un formato de **LEY** que permita en un futuro cercano, fomentar el comercio electrónico internacional, creando en cada uno de los países una legislación similar lo que permitiría llegar a tener un **entorno legal neutro** o como se conocería en la parte técnica estandarizar la ley para que las comunicaciones, convenios, entre otros, permitan facilitar el uso del comercio electrónico haciéndola más rápida, segura y eficiente.

Una vez que la Comisión de las Naciones Unidas proporcionaron la herramienta y su correspondiente manual de uso, realizaron una serie de sugerencias a gobiernos, estudiosos del tema, investigadores para que consideren esta normativa en sus actividades y hagan referencia al mismo con la intención de promulgar la estandarización del marco legal sobre uso del comercio electrónico, además como es lógico pensar recomiendan también utilizar a esta **LEY MODELO** como la base para aplicarla a los regímenes internos ya que podrá ser modificada según el marco

jurídico en el que se pretenda establecer, existen también algunas consideraciones muy importantes como la **neutralidad tecnológica,** la **equivalencia funcional** y las **reglas de derecho supletorio o imperativo.**

Como se ha mencionado al inicio de este capítulo, los gobiernos cumplen un rol fundamental en el desarrollo de estas nuevas tecnologías de información y comunicaciones, una de estas herramientas que permiten que este cambio sea realidad es la Infraestructura de Llave Pública (PKI), ya que en ella se sustenta toda la **confianza** de este modelo al asegurar la autenticidad, integridad, no repudio, confidencialidad y auditabilidad de la información, bajo este esquema de seguridad que debidamente legalizado y regulado constituyen una gran aporte para el desarrollo comercial local e internacional de las naciones, de igual forma la empresa privada, el sector público pueden vislumbrar un futuro muy prometedor y la solución a muchos de sus problemas.

Pero es necesario destacar el compromiso de las naciones que conforman la Unión Europea, al agotar todos los esfuerzos necesarios para llegar a establecer consensos que han permitido conseguir un gran avance en materializar su **"Sociedad de la Información",** a pesar de las diferencias que puedan existir entre sus países han trabajado de forma conjunta para alcanzar los objetivos propuestos y proporcionar a sus pueblos de instrumentos valiosos para el desarrollo comercial, social y humano.

Este es el ejemplo a seguir pero lo debemos hacer con inteligencia no adoptando sus leyes o regulaciones por que lógicamente no somos iguales, sino haciendo un trabajo consiente en determinar cuales son nuestras fortalezas y debilidades, creando nuevas oportunidades y disminuyendo las amenazas que puedan presentarse en la implementación o utilización de las mismas, pero como poder conseguir este sueño, pues yo creo que la única manera es la de comenzar a trabajar de forma conjunta en poner en práctica lo que nos enseñan estas naciones,

como mencionada el *Dr. Miguel Angel Davara Rodríguez*[21] *"El desarrollo tecnológico es una realidad, y el derecho debe estar presente para que exista equilibrio en el uso de la tecnología, el hecho de que existan o no las normas que permitan regular su funcionamiento no frena el desarrollo y uso de la tecnología."*

Desarrollar nuevas tecnologías que permitan solucionar problemas en nuestras instituciones públicas, con la finalidad de disminuir el riesgo que puedan presentarse en transferencias de comercio electrónico o de información por medios poco seguros, creando un esquema de certificación que pueda ser regulado y en el que se puedan establecer reglas y políticas claras y seguras, y tener el coraje de poder romper los paradigmas del cambio son algunas de las cosas que nos permitirán sacar adelante a nuestro país.

En lo que se refiere a los gobiernos esta es la lista de los que tienen iniciativas en este campo:

- Argentina: www.pki.arg.gov
- Australia: Government Public Key Infrastructure
- Austria: Supervisory Authority for Electronic Signatures
- Bélgica: Service public fédéral Technologie de l'Information et de la Communication (FEDICT) ó Centre d'Information sur la Signature Electronique
- Brasil: ICP-Brasil - Infra-estrutura de Chaves Públicas Brasileira
- Canadá: GOC Public Key Infrastructure
- EEUU: Federal Public Key Infrastructure Steering Committee ó NIST PKI Program ó Department Of Defense PKI
- España: Fábrica Nacional de Moneda y Timbre - Proyecto CERES

[21] *Doctor en Derecho Informático e impulsador de la Ley de Firma Electrónica en España.*

- Francia: Le site du programme d'action gouvernemental pour la société de l'information ó Agence pour les Technologies de l'Information et de la Communication dans l'Administration
- Holanda: Dutch government PKI Task Force
- Hong Kong: Digital Certificate and Public Key Infrastructure
- Italia: Autorità per l'informatica nella Pubblica Amministrazione
- Nueva Zelanda: Secure Electronic Environment PKI
- Panamá: Proyecto Firma Digital y Comercio Electrónico (SENACYT)
- Reino Unido: HMG Public Key Infrastructure (PKI) ó Government Gateway
- República de Corea: Korea Certification Authority Central
- Singapur: Controller of Certification Authorities

Fuente: www.pki.gov.ar

Marco Legal Nacional

A partir del 17 de abril del 2002, existe en el país la "Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos" expedida, así como también su respectivo Reglamento lo cual permite sustentar el proyecto dentro de un marco legal adecuado.

También existe un "Reglamento para la Acreditación, Registro y Regulación de Entidades Habilitadas para prestar Servicios de Certificación de Información y Servicios Relacionados" emitido por el CONATEL encamina al uso de firma electrónica, registro de datos y sellado de tiempo entre otras actividades relacionadas con el presente proyecto. Este es el último documento regulado por el Consejo Nacional de Telecomunicaciones, que tiene como finalidad llamar a una Audiencia Pública para calificar a todas las Entidades Públicas o Privadas como Autoridades Habilitantes de Servicios de Certificación de Información.

Este reglamento establece las normas y procedimientos aplicables a la prestación de Servicios de Certificación, así también como los deberes y derechos de los prestadores de estos servicios y de sus usuarios.

Por otra parte, muchas instituciones en el ámbito internacional han adoptado soluciones similares para mejorar sus seguridades informáticas; por ser la Superintendencia de Bancos y Seguros, una institución que maneja información muy sensible del Sistema Financiero, es prioridad y obligación de la misma hacer los esfuerzos necesarios por aumentar los niveles de seguridad en sus servicios de transferencias y aplicaciones.

Análisis de Servicios Notariales

PROCEDIMIENTO PARA LA ATENCIÓN DE SERVICIOS NOTARIALES DESCRITOS EN LA LEY.

1.- Hablar con el consul
2.- El consul elabora el documento
3.- Adjuna documentos habilitantes
4.- Envia a notaria (Ecuador)
5.- El notario solicita al fedatario su presencia
6.- En presencia del notario, el fedatario desmaterializa y da fe de la validez del documento
7.- El notario concluye el proceso de la declaración
8.- Se envía una copia por correo usuario (Exterior)

SERVICIOS NOTARIALES	APLICACIÓN
1.- Autorizar los actos y contratos a que fueren llamados y redactar las correspondientes escrituras, salvo que tuvieren razón o excusa legítima para no hacerlo;	SI APLICA
2.- Protocolizar instrumentos públicos o privados por orden judicial o a solicitud de parte interesada patrocinada por abogado, salvo prohibición legal;	SI APLICA
3.- Autenticar las firmas puestas ante el en documentos que no sean escrituras públicas;	ANALIZAR
4.- Dar fe de la supervivencia de las personas naturales;	NO APLICA
5.- Dar fe de la exactitud, conformidad y corrección de fotocopias y de otras copias producidas por procedimientos o sistemas técnico - mecánicos, de documentos que se les hubieren exhibido, conservando una de ellas con la nota respectiva en el Libro de Diligencias que llevarán al efecto;	SI APLICA
6.- Levantar protestos por falta de aceptación o de pago de letras de cambio o pagarés a la orden particularizando el acto pertinente conforme a las disposiciones legales aplicables, actuación que no causará impuesto alguno;	NO APLICA
7.- Intervenir en remates y sorteos a petición de parte e incorporar al Libro de Diligencias las actas correspondientes, así como las de aquellos actos en los que hubieren intervenido a rogación de parte y que no requieran de las solemnidades de la escritura pública.	NO APLICA
8.- Conferir extractos en los casos previstos en la Ley; y,	SI APLICA (OJO COMPRAVENTAS REGISTRO DE LA PROPIEDAD)
9.- Practicar reconocimiento de firmas.	SI APLICA (OJO CASO FIRMA ELECTRÓNICA Y DIGITAL)

10.- Receptar la declaración juramentada del titular de dominio, con la intervención de dos testigos idóneos que acrediten la necesidad de extinguir o subrogar, de acuerdo a las causales y según el procedimiento previsto por la Ley, el patrimonio familiar constituido sobre sus bienes raíces, en base a lo cual el Notario elaborará el acta que lo declarará extinguido a subrogado y dispondrá su anotación al margen de la inscripción respectiva en el Registro de la Propiedad correspondiente;	SI APLICA (CONSIDERAR LA COMPARECENCIA DE TESTIGOS)
En los casos en que el patrimonio familiar se constituye como mandato de la Ley, deberá adicionalmente contarse con la aceptación de las instituciones involucradas;	
11.- Receptar la declaración juramentada del titular de dominio con intervención de dos testigos idóneos que acrediten que la persona que va a donar un bien, tenga bienes suficientes adicionales que garanticen su subsistencia, lo cual constará en acta notarial, la que constituirá suficiente documento habilitante para realizar tal donación.	SI APLICA (CONSIDERAR LA COMPARECENCIA DE TESTIGOS)
12.- Receptar la declaración juramentada de quienes se creyeren con derecho a la sucesión de una persona difunta, presentando la partida de defunción del de cujus y las de nacimiento u otros documentos para quienes acrediten ser sus herederos, así como la de matrimonio o sentencia de reconocimiento de la unión de hecho del cónyuge sobreviviente si los hubiera. Tal declaración con los referidos instrumentos, serán suficientes documentos habilitantes para que el Notario conceda la posesión efectiva de los bienes pro indiviso del causante a favor de los peticionarios, sin perjuicio de los derechos de terceros. Dicha declaración constará en acta notarial y su copia será inscrita en el Registro de la Propiedad correspondiente;	SI APLICA
13.- Tramitar la solicitud de disolución de la sociedad de gananciales de consuno de los cónyuges, previo reconocimiento de las firmas de los solicitantes ante el Notario, acompañando la partida de matrimonio o sentencia de reconocimiento de la unión de hecho. Transcurridos diez días de tal reconocimiento el Notario convocará a audiencia de conciliación en la cual los cónyuges, personalmente o por medio de apoderados ratificarán su voluntad de declarar disuelta la sociedad de gananciales formada por el matrimonio o unión de hecho. El acta respectiva se protocolizará en la Notaría y su copia se subinscribirá en el Registro Civil correspondiente, particular del Cual se tomará	SI APLICA (Interviene Registro Civil envío correo electrónico) Marginación
14.- Autorizar la venta en remate voluntario de bienes raíces de personas menores que tengan la libre administración de sus bienes cumpliendo las disposiciones pertinentes de la Sección Décima Octava del Título Segundo del Código de Procedimiento Civil;	REVISAR
15.- Receptar informaciones sumarias y de nudo hecho;	SI APLICA
16.- Sentar razón probatoria de la negativa de recepción de documentos o de pago de tributos por parte de los funcionarios públicos o agentes de recepción;	NO APLICA
17.- Protocolizar las capitulaciones matrimoniales, inventarios solemnes, poderes especiales, revocatorias de poder que los comerciantes otorgan a sus factores y dependientes para administrar negocios; y,	SI APLICA
18.- Practicar mediante diligencia notarial, requerimientos para el cumplimiento de la promesa de contrato como para la entrega de cosa debida y de la ejecución de obligaciones.	NO APLICA
De registrarse controversia en los casos antes mencionados, el notario se abstendrá de seguir tramitando la petición respectiva y enviará copia auténtica de todo lo actuado a la oficina de sorteos del cantón de su ejercicio, dentro del término de tres días contados a partir del momento en que tuvo conocimiento del particular, por escrito o de la oposición de la persona interesada, para que después del correspondiente sorteo se radique la competencia en uno de los jueces de lo Civil del Distrito.	
19.- Proceder a la apertura y publicación de testamentos cerrados. Para el efecto, el que tenga o crea tener interés en la sucesión de una persona, puede solicitar al notario, ante quien el causante otorgó el testamento y lo haya conservado en su poder, proceda a exhibirlo para su posterior apertura y publicación en la fecha y hora que para tal propósito señale. En su petición el interesado indicará adicionalmente, el nombre y dirección de otros herederos o interesados que conozca, y que se disponga de una publicación, en un medio de prensa escrito de amplia circulación local o nacional, para los presuntos beneficiarios. Trascurridos no menos de treinta días, en la fecha y hora señalados, previa notificación a los testigos instrumentales, el notario levantará un acta notarial en la que dejará constancia del hecho de haberlo exhibido a los peticionarios la cubierta del testamento, declarando si así corresponde, adicionalmente junto con los comparecientes, que en su concepto la cerradura, sellos	NO APLICA
En la diligencia notarial, a la que se permitirá el acceso a todo interesado que justifique un presunto interés en el contenido del testamento, de presentarse oposición a la práctica de esta diligencia, el notario oirá la exposición. En este evento, elaborará un acta con los fundamentos de la oposición y la enviará a conocimiento de juez competente, cumpliendo el procedimiento de ley, ante quien se deberá llevar a efecto el juicio de apertura y publicación de testamento cerrado de conformidad con las normas previstas en los Códigos Civil y de Procedimiento Civil.	
De no presentarse oposición, el notario procederá a efectuar el reconocimiento de firmas y rúbricas de los testigos instrumentales, así como de que la cubierta y el sobre que contiene el testamento cerrado del testador, es el mismo que se presentó para su otorgamiento al notario. De no presentarse todos los testigos instrumentales, el notario abonará las firmas de los testigos faltantes con una confrontación entre las que aparecen en la carátula con las que constan en la copia de la misma que debe reposar en los protocolos de la notaría, según lo dispone el artículo 25 de la Ley Notarial. El notario actuante confrontará la firma del notario que ejercía el cargo al momento de su otorgamiento con su firma constante en otros instrumentos notariales incorporados en el protocolo.	
En el caso de que la cubierta del testamento presentare notorias alteraciones que haga presumir haberse abierto, el notario luego de proceder a la apertura y publicación del testamento, levantará el acta pertinente haciendo constar estos particulares y remitirá todo lo actuado al juez competente. En estos casos el testamento únicamente se ejecutará en virtud de sentencia ejecutoriada que así lo disponga.	
La diligencia concluye con la suscripción del acta de apertura y lectura del testamento, al cabo de lo cual todo lo actuado se incorporará al protocolo del notario, a fin de que otorgue las copias respectivas;	

20.- Será facultad del notario proceder al registro de firmas de funcionarios y representantes de personas jurídicas, siempre y cuando haya petición de parte y el notario tenga conocimiento pleno de quien registra su firma. El documento que contenga la certificación de firma en virtud de este procedimiento de registro, gozará de autenticidad, pero no tendrá los efectos probatorios de instrumento público, para cuyo efecto se procederá de conformidad con lo previsto en el artículo 194 del Código de Procedimiento Civil.	NO APLICA
Nota: Numeral 7 reformado por Ley No. 62, publicada en Registro Oficial 406 de 28 de Noviembre del 2006. (CONTINUA).	
Art. 18.- (CONTINUACION)	
21.- Autorizar los actos de amojonamiento y deslinde en sectores rurales, que a petición de las partes, siempre que exista acuerdo, tengan por objeto el restablecimiento de los linderos que se hubieren oscurecido, desaparecido o experimentado cualquier cambio o alteración, o en que se deban fijar por primera vez la línea de separación entre dos o más inmuebles, con señalamiento de linderos. Al efecto, se señalará fecha y hora para la diligencia, a la que concurrirán las partes, que podrán designar perito o peritos, quienes presentarán sus títulos de propiedad y procederán a señalar e identificar lugares, establecer linderos y dar cualquier noticia para esclarecer los hechos.	NO APLICA
De esta diligencia se levantará un acta, siempre y cuando exista conformidad de todas las partes, la que se agregará al protocolo del notario y de la cual se entregará copias certificadas a las mismas para su catastro municipal e inscripción en el Registro de la Propiedad correspondiente.	
De presentarse oposición, el notario procederá a protocolizar todo lo actuado y entregará copias a los interesados, para que éstos, de considerarlo procedente, comparezcan a demandar sus pretensiones de derecho ante los jueces competentes;	
22.- Tramitar divorcios por mutuo consentimiento, únicamente en los casos en que los cónyuges no tengan hijos menores de edad o bajo su dependencia. Para el efecto, los cónyuges expresarán en el petitorio, bajo juramento, lo antes mencionado y su voluntad definitiva de disolver el vínculo matrimonial, mismo que deberá ser patrocinado por un abogado en libre ejercicio, cumpliendo adicionalmente en la petición, lo previsto en el artículo 107 del Código Civil. El notario mandará que los comparecientes reconozcan sus respectivas firmas y rúbricas y fijará fecha y hora para que tenga lugar la audiencia, dentro de un plazo no menor de sesenta días, en la cual los cónyuges deberán ratificar de consuno y de viva voz su voluntad de divorciarse. El notario levantará un acta de la diligencia en la que declarará disuelto el vínculo matrimonial, de la que debidamente protocolizada, se entregará copias certificadas a las partes y se oficiará al Registro Civil para su marginación respectiva; el Registro Civil a su vez, deberá sentar la razón correspondiente de la marginación en una copia certificada de la diligencia, que deberá ser devuelta al notario e incorporada en el protocolo respectivo. El sistema de correo electrónico podrá utilizarse para el trámite de marginación señalada en esta disposición. Los cónyuges podrán comparecer directamente o a través de procuradores especiales. De no realizarse la audiencia en la fecha designada por el notario, los cónyuges podrán solicitar nueva fecha y hora para	SI APLICA
23.- Proceder a la liquidación de sociedad de bienes o de la sociedad conyugal, para este efecto, sin perjuicio de la facultad jurisdiccional de los jueces de lo civil, los cónyuges o ex-cónyuges, o los convivientes vinculados bajo el régimen de la unión de hecho, según el caso, podrán convenir mediante escritura pública, una vez disuelta la sociedad conyugal o la sociedad de bienes que se haya formado como consecuencia de la unión de hecho, la liquidación de la sociedad de bienes. Este convenio se inscribirá en el Registro de la Propiedad correspondiente cuando la liquidación comprenda bienes inmuebles, y en el Registro Mercantil cuando existieren bienes sujetos a este Registro. Previamente a la inscripción, el notario mediante aviso que se publicará por una sola vez en uno de los periódicos de circulación nacional en la forma prevista en el artículo 82 del Código de Procedimiento Civil, hará conocer la liquidación de la sociedad conyugal o de la sociedad de bienes de la unión de hecho, para los efectos legales consiguientes. Transcurrido el término de veinte días desde la publicación y de no existir oposición, el notario sentará la respectiva razón notarial y dispondrá su inscripción en el registro o registros correspondientes de los lugares en los que se hallaren los inmuebles y bienes objeto de esta liquidación. De presentarse oposición, el notario procederá a protocolizar todo lo actuado y entregará	SI APLICA (INVOLUCRA COMPLICACIONES EN EL PROCESO SRI)
24.- Autorizar la emancipación voluntaria del hijo adulto, conforme lo previsto en el artículo 309 del Código Civil. Para este efecto, los padres comparecerán ante el notario a dar fin a la patria potestad, mediante declaración de voluntad que manifieste esta decisión, la que constará en escritura pública, donde además se asentará la aceptación y consentimiento expreso del hijo a emanciparse. A esta escritura pública se agregará como habilitantes los documentos de filiación e identidad respectivos, y las declaraciones juramentadas de dos testigos conformes y sin tacha, que abonen sobre la conveniencia o utilidad que percibiría el menor adulto con esta emancipación. El notario dispondrá la publicación de la autorización, por una sola vez en la prensa, cuya constancia de haberse publicado se incorporará en el protocolo, con lo cual entregará las copias respectivas para su inscripción en los Registros de la Propiedad y Mercantil del cantón en el que se hubiere hecho la emancipación;	NO APLICA
25.- Tramitar la petición de declaratoria de interdicción para administrar los bienes de una persona declarada reo por sentencia ejecutoriada penal; para el efecto se adjuntará la sentencia ejecutoriada. En el acta que establezca la interdicción, se designará un curador;	NO APLICA

26.- Solemnizar la declaración de los convivientes sobre la existencia de la unión de hecho, previo el cumplimiento de los requisitos establecidos en el artículo 222 del Código Civil. El Notario levantará el acta respectiva, de la que debidamente protocolizada, se conferirá copia certificada a las partes; y,	SI APLICA
27.- Declarar la extinción de usufructo, previa la justificación instrumental correspondiente y de acuerdo con las reglas del Código Civil, a petición del nudo propietario en los casos siguientes:	
a) Por muerte del usufructuario;	NO APLICA
b) Por llegada del día o cumplimiento de la condición prefijados para su terminación; y,	SI APLICA
c) Por renuncia del usufructuario.	SI APLICA
Nota: Numerales 5 y 6 agregados por Decreto Supremo No. 2386, publicado en Registro Oficial 564 de 12 de Abril de 1978.	
Nota: Numerales 7, 8 y 9 agregados por Ley No. 35, publicado en Registro Oficial 476 de 10 de Julio de 1986.	
Nota: Artículo reformado por Ley No. 000, publicada en Registro Oficial Suplemento 64 de 8 de Noviembre de 1996.	
Nota: Artículo reformado por Ley No. 62, publicada en Registro Oficial 406 de 28 de Noviembre del 2006.	

Capitulo 3

Modelos de soluciones propuestas

Las herramientas informáticas que se actualizan cada día, constituyen la fortaleza de este proyecto, ya que se las utilizará para el mejoramiento de los procesos notariales.

La implementación de este sistema de Notarias Digitales es un campo no explotado en su total dimensión, sin embargo, proporciona grandes ventajas:

- Simplificará el manejo de datos e información
- Se obtendrá una confianza en el servicio junto a una administración, gestión y promoción de las notarías
- Se obtendrá una eficiente función notarial al otorgar un servicio eficiente
- Se automatizarán procesos sencillos pero repetitivos
- Se tendrá una rápida recuperación de datos
- Se podrán minimizar errores
- Permitirá el intercambio seguro de correo electrónico, garantizando la integridad y confidencialidad del mismo.

En este sentido, hemos definido el uso de la seguridad de la plataforma tecnológica en base a tres modelos tecnológicos para que puedan ser usados conforme al nivel de madurez tecnológico y nivel preparación para el uso de los servicios notariales digitales por parte de los proveedores de servicios y de los migrantes

Modelo Propuesto 1: Uso de firma electrónica con fedatario

Los migrantes podrán enviar sus solicitudes y documentos firmados de manera manuscrita tradicional y desmaterializados como mensaje de datos. En el país serán materializados por un fedatario que dará fe de su autenticidad.

Procedimiento

El migrante junto con su abogado de confianza preparará el documento que requiere notarizar, este deberá ser convertido a documento PDF con seguridad. El documento es firmado electrónicamente (entendiéndose como firma electrónica a la firma escaneada del migrante en este caso) el

documento será enviado vía correo electrónico al notario de confianza del migrante, el notario lo recibirá en su correo quien en presencia del fedatario juramentado procederá a descargar el correo electrónico que contendrá el documento en PDF, el fedatario sentará razón de la descarga y materialización del documento.

Una vez que el documento este materializado el notario procederá a notarizar el documento y de igual manera en presencia del fedatario juramentado se procederá a la desmaterialización del mismo para ser enviado vía correo electrónico al migrante.

Viabilidad Legal

Para llevar a cabo los procesos con fedatario juramentado, es necesario llevar a cabo reformas especialmente a la **ley notarial**, donde se establezca la creación de la figura del fedatario, los requisitos para ser uno y donde se deberá llevar a cabo su inscripción, así como detallar las actividades que llevaran a cabo.

Viabilidad Técnica

Respecto al requisito tecnológico este es muy básico pues para llevar a cabo el proceso con la ayuda del fedatario juramentado únicamente se necesita un computador con Internet y cargado programa para creación de documentos PDF.
El notario deberá contar con algún sistema de creación de marcas de agua o sello que identifique al documento como notarizado.

Ventajas y desventajas

La ventaja es la rapidez de llevar a cabo el trámite y la facilidad de hacerlo.
La desventaja es la falta de seguridades y riesgos de que el documento pueda ser interceptado por un tercero.
Es un modelo que se basa en la absoluta confianza tanto del migrante como de los notarios y fedatarios para llevar a cabo el proceso.

Modelo Propuesto 2: Uso de firma electrónica con consulado

El mismo caso anterior pero enviado desde un consulado a través de la firma digital del cónsul.

El sistema de firma digital se maneja a través de claves, públicas y privadas para el envío y desmaterialización de los documentos notarizados.

Esto permitirá la seguridad y la confiabilidad en este sistema. El ente fedatario en este caso el embajador del Ecuador en los países donde se aplica el sistema, será quien valide el trámite.

Procedimiento

Una opción consistiría en que el usuario concurre al consulado más próximo a objeto que el cónsul le redacte el documento que necesite notarizar, se firma por el usuario dicho documento, se escanea o desmaterializa, y el Cónsul con su firma digital envía el documento desmaterializado a la respectiva notaria en el Ecuador.

Una segunda opción es que el usuario una vez firmado el respectivo documento, se desmaterializa, pero esta vez se envía con la firma digital del usuario a la notaria respectiva en el Ecuador, ambos con la asistencia del Cónsul.

Viabilidad Legal

A este respecto hay que aclarar que la Ley de Comercio Electrónico, no señala o faculta a los Notarios para protocolizar documentos electrónicos o ser Notarios digitales, esto sin perjuicio de lo que señala el artículo 18 numeral 2 de la Ley Notarial, el que señala: " Son atribuciones de los notarios, además de las contenidas **en otras leyes**: 2.- Protocolizar instrumentos públicos (con lo cual también se aplicaría a los instrumentos públicos electrónicos) o privados por orden judicial o a solicitud de parte interesada patrocinada por abogado, salvo prohibición legal". Esto a su vez, en relación con el articulo 1 de la Ley de registro, sobre el objeto del Registro, señala: "La inscripción de los instrumentos públicos, títulos y demás documentos **que la ley exige** o permite que se inscriban en los registros correspondientes, tiene principalmente los siguientes objetos:"

A su vez respecto a las atribuciones de los Cónsules las que están determinadas en la Ley Orgánica del Servicio Exterior, en su articulo 65 letra C, señala: "En el cumplimiento de sus atribuciones, los funcionarios consulares intervendrán en especial en aquellos actos que deban surtir sus efectos en el Ecuador, sean ecuatorianos o extranjeros los interesados en dichos actos.

Con tal propósito, intervendrán los funcionarios consulares en los siguientes asuntos, autorizándoles debidamente: c) Funciones notariales y de registro...". Con lo cual se estarían sometiendo también a lo establecido por la Ley Notarial, específicamente con el artículo 18.

Adicionalmente, en el Reglamento a la Ley de Comercio Electrónico, a diferencia de la Ley, si habla de los notarios, como por ejemplo en su artículo 4, sin embargo, por la jerarquización de las leyes, el Reglamento no puede o no tiene la suficiente fuerza para ampliar las atribuciones de los notarios, a no ser que esto se realice mediante otra ley, como ya sucedió con la Ley Reformatoria Nº 62 del 28 de noviembre del 2006, con la cual se ampliaron las funciones o atribuciones de los notarios.

Además de lo anteriormente expuesto, hay que tomar en consideración los posibles cambios que pudieran provenir de la Asamblea Constituyente, en la cual se discute el carácter público de las notarias, y en caso que así fuere, podrían realizar todo aquello que no esté prohibido por la Ley, pero aún esto es especulación.

Como conclusión, y con el objeto de evitar demoras, lo más conveniente es legislar en el sentido de ampliar las funciones de los Notarios, esto es ampliar el artículo 18 de la ley Notarial, incluyendo los contratos, y documentos electrónicos, o bien dictar disposiciones respecto a la creación y funcionamiento de las notarias virtuales o digitales.

Viabilidad Técnica

Se requeriría la utilización de firmas digitales, computadores aptos para la recepción de los correos relativos al tema, y licencias.

Ventajas y desventajas

Las ventajas: agilita totalmente el trámite respecto de las personas que se encuentran a ciertas distancia del Ecuador y no pueden movilizarse, elimina el papel, no necesita un espacio para el archivo físico de documentos, reduce considerablemente los problemas de falsificación de documentos, etc.

Las desventajas: el hecho que la gente tiene que capacitarse en cuanto al tema, lo que puede provocar un poco de rechazo, por el hecho de enfrentar un cambio.

Modelo Propuesto 3: Servicios digitales mediante el uso de certificado de firma electrónica

Dicha firma es entregada por las entidades de certificación debidamente registrada en Ecuador conforme a la Ley de Comercio Electrónico.

Funciones y responsabilidades (como autoridad certificadora)

Es la encargada de emitir y revocar certificados. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.

La autoridad de registro (o, en inglés, RA, Registration Authority): es la responsable de verificar el enlace entre los certificados (concretamente, entre la clave pública del certificado) y la identidad de sus titulares.

Los repositorios: son las estructuras encargadas de almacenar la información relativa a la PKI. Los dos repositorios más importantes son el repositorio de certificados y el repositorio de listas de revocación de certificados. En una lista de revocación de certificados (o, en inglés, CRL, Certificate Revocation List) se incluyen todos aquellos certificados que por algún motivo han dejado de ser válidos antes de la fecha establecida dentro del mismo certificado.

La autoridad de validación (o, en inglés, VA, Validation Authority): es la encargada de comprobar la validez de los certificados digitales.
La autoridad de sellado de tiempo (o, en inglés, TSA, TimeStamp Authority): es la encargada de firmar documentos con la finalidad de probar que existían antes de un determinado instante de tiempo.

Funciones y responsabilidades (como autoridad de registro)

Es la responsable de verificar el enlace entre los certificados (concretamente, entre la clave pública del certificado) y la identidad de sus titulares.

Se encargan de la verificación de la validez y veracidad de los datos del que pide un certificado, y gestionan el ciclo de vida de las peticiones hacia las AC's.

Viabilidad Económica y Financiera

El presente proyecto es de tipo social por lo que la principal función es buscar el bienestar de la sociedad – objetivo, en este caso, del segmento de migrantes ecuatorianos.

Sin embargo, se realiza aproximaciones de los flujos de fondos para una notaría tipo en el País, los mismos que demuestran que las 4 alternativas que se propone, resultan viables y definen al proyecto como auto sustentable.

Estas alternativas de negociación se desarrollarían en el transcurso del proyecto de acuerdo al nivel de negociación con las organizaciones pertinentes

APROXIMACIÓN DEL FLUJO DE FONDOS PARA LA ALTERNATIVA 1

	AÑO 0 2009		AÑO 1 2010		AÑO 2 2011		AÑO 3 2012		AÑO 4 2013		AÑO 5 2014	
	PRECIO	DEMANDA	PRECIO	DEMANDA	PRECIO	DEMANDA	PRECIO	DEMANDA	PRECIO	DEMANDA	PRECIO	DEMANDA
	1,125	30	1,238	36	1,362	43	1,498	52	1,648	62	1,812	75
INGRESOS												
Ingresos por servicios de capacitación a notarías		33,760.34		44,563.64		58,824.01		77,647.69		102,494.95		135,293.34
TOTAL INGRESOS		33,760.34		44,563.64		58,824.01		77,647.69		102,494.95		135,293.34
	SUBTOTAL		SUBTOTAL		SUBTOTAL		SUBTOTAL		SUBTOTAL		SUBTOTAL	
EGRESOS												
COSTOS DEL PROYECTO		378,876.96										
GASTOS FIJOS		0.00		2,000.00		2,000.00		2,000.00		2,000.00		2,000.00
Mantenimiento de software			2,000.00		2,000.00		2,000.00		2,000.00		2,000.00	
TOTAL EGRESOS		378,876.96		2,000.00		2,000.00		2,000.00		2,000.00		2,000.00
TOTAL FLUJO (I - E)		**-345,116.62**		**42,564**		**56,824**		**75,648**		**100,495**		**133,293**
FLUJOS ACUMULADOS		-345,116.62		-302,552.98		-245,728.97		-170,081.28		-69,586.32		63,707.02

INDICADORES FINANCIEROS		
%	10%	0.1
TIR	14.03%	
VAN	$ -46,564.63	
PUNTO EQUILIBRIO	346 notarías	
PER. RECUPERACION	4.30 años	

APROXIMACIÓN DEL FLUJO DE FONDOS PARA LA ALTERNATIVA 2

	AÑO 0 2009		AÑO 1 2010		AÑO 2 2011		AÑO 3 2012		AÑO 4 2013		AÑO 5 2014	
	PRECIO	DEMANDA	PRECIO	DEMANDA	PRECIO	DEMANDA	PRECIO	DEMANDA	PRECIO	DEMANDA	PRECIO	DEMANDA
		57	0	63	0	69	0	76	0	83	0	92
INGRESOS por prestación de serv dig												
Poder general	80	4,545.45	80	5,000.00	80	5,500.00	80	6,050.00	80	6,655.00	80	7,320.50
Poder especial	80	4,545.45	80	5,000.00	80	5,500.00	80	6,050.00	80	6,655.00	80	7,320.50
Autorización de viaje menores	80	4,545.45	80	5,000.00	80	5,500.00	80	6,050.00	80	6,655.00	80	7,320.50
Reconocimiento de firmas	11	625.00	11	687.50	11	756.25	11	831.88	11	915.06	11	1,006.57
Información sumaria	11	625.00	11	687.50	11	756.25	11	831.88	11	915.06	11	1,006.57
Protocolizaciones	22	1,250.00	22	1,375.00	22	1,512.50	22	1,663.75	22	1,830.13	22	2,013.14
Copias certificadas	5	284.09	5	312.50	5	343.75	5	378.13	5	415.94	5	457.53
TOTAL INGRESOS		16,420.45		18,062.50		19,868.75		21,855.63		24,041.19		26,445.31
	SUBTOTAL		SUBTOTAL		SUBTOTAL		SUBTOTAL		SUBTOTAL		SUBTOTAL	
EGRESOS												
GASTOS ADMINISTRATIVOS		14,812.38		14,300.00		15,730.00		17,303.00		19,033.30		20,936.63
Remuneraciones personal	12,000.00		13,200.00		14,520.00		15,972.00		17,569.20		19,326.12	
Capacitación Notarías Digitales	1,812.38											
Suministros y materiales	1,000.00		1,100.00		1,210.00		1,331.00		1,464.10		1,610.51	
GASTOS GENERALES		1,200.00		1,320.00		1,452.00		1,597.20		1,756.92		1,932.61
Pagos agua, luz, teléfono	1,200.00		1,320.00		1,452.00		1,597.20		1,756.92		1,932.61	
GASTOS FIJOS		0.00		750.00		825.00		907.50		998.25		1,098.08
Infraestructura		500.00	550.00		605.00		665.50		732.05		805.26	
Mantenimiento de software			200.00		220.00		242.00		266.20		292.82	
TOTAL EGRESOS		16,512.38		16,370.00		18,007.00		19,807.70		21,788.47		23,967.32
TOTAL FLUJO (I - E)		**-91.92**		**1,692.50**		**1,861.75**		**2,047.93**		**2,252.72**		**2,477.99**
FLUJOS ACUMULADOS		-91.92		1,600.58		3,462.33		5,510.25		7,762.97		10,240.96

INDICADORES FINANCIEROS		
%	10%	0.1
TIR		
VAN	6,910	
PUNTO EQUILIBRIO	38	usuarios
PER. RECUPERACION	0	años

APROXIMACIÓN DEL FLUJO DE FONDOS PARA LA ALTERNATIVA 3

	AÑO 0 2009		AÑO 1 2010		AÑO 2 2011		AÑO 3 2012		AÑO 4 2013		AÑO 5 2014	
	PRECIO	DEMANDA	PRECIO	DEMANDA	PRECIO	DEMANDA	PRECIO	DEMANDA	PRECIO	DEMANDA	PRECIO	DEMANDA
		57	0	63	0	69	0	76	0	83	0	92
INGRESOS por prestación de serv dig												
Poder general	80	4,545.45	80	5,000.00	80	5,500.00	80	6,050.00	80	6,655.00	80	7,320.50
Poder especial	80	4,545.45	80	5,000.00	80	5,500.00	80	6,050.00	80	6,655.00	80	7,320.50
Autorización de viaje menores	80	4,545.45	80	5,000.00	80	5,500.00	80	6,050.00	80	6,655.00	80	7,320.50
Reconocimiento de firmas	11	625.00	11	687.50	11	756.25	11	831.88	11	915.06	11	1,006.57
Información sumaria	11	625.00	11	687.50	11	756.25	11	831.88	11	915.06	11	1,006.57
Protocolizaciones	22	1,250.00	22	1,375.00	22	1,512.50	22	1,663.75	22	1,830.13	22	2,013.14
Copias certificadas	5	284.09	5	312.50	5	343.75	5	378.13	5	415.94	5	457.53
TOTAL INGRESOS		16,420.45		18,062.50		19,868.75		21,855.63		24,041.19		26,445.31
	SUBTOTAL		SUBTOTAL		SUBTOTAL		SUBTOTAL		SUBTOTAL		SUBTOTAL	
EGRESOS												
GASTOS ADMINISTRATIVOS		14,642.05		16,106.25		17,716.88		19,488.56		21,437.42		23,581.16
Remuneraciones personal	12,000.00		13,200.00		14,520.00		15,972.00		17,569.20		19,326.12	
Capacitación Notarías Digitales	1,642.05		1,806.25		1,986.88		2,185.56		2,404.12		2,644.53	
Suministros y materiales	1,000.00		1,100.00		1,210.00		1,331.00		1,464.10		1,610.51	
GASTOS GENERALES		1,200.00		1,320.00		1,452.00		1,597.20		1,756.92		1,932.61
Pagos agua, luz, teléfono	1,200.00		1,320.00		1,452.00		1,597.20		1,756.92		1,932.61	
GASTOS FIJOS		300.00		530.00		583.00		641.30		705.43		775.97
Infraestructura	300.00		330.00		363.00		399.30		439.23		483.15	
Mantenimiento de software			200.00		220.00		242.00		266.20		292.82	
TOTAL EGRESOS		16,142.05		17,956.25		19,751.88		21,727.06		23,899.77		26,289.75
TOTAL FLUJO (I - E)		**278.41**		**106.25**		**116.88**		**128.56**		**141.42**		**155.56**
FLUJOS ACUMULADOS		278.41		384.66		501.53		630.10		771.52		927.08

INDICADORES FINANCIEROS		
%	6%	
TIR	6%	
VAN	$ 819	
PUNTO EQUILIBRIO	42	usuarios
PER. RECUPERACION	0	años

Supuestos utilizados para el cálculo

Los supuestos a continuación se han considerado para apreciar flujos de fondos conservadores.

Alternativa 1: Cobro por servicio notarial digital otorgado (transacción)

Para realizar la aproximación del flujo de efectivo, se considera los siguientes rubros:

Para los ingresos:

- El cobro de la capacitación por el número de notarías en el País que contratarían el servicio de Notarías Digitales.
- Consideramos también que al menos el 87% de las notarías contratarían la capacitación; se pronostica una demanda inicial de 30 notarías con un incremento anual del 30%.
- El precio de la capacitación de año a año tiene un incremento del 10%.

Para los egresos:

- El costo total del proyecto.
- El costo de mantenimiento del Sistema Notarial Digital.

VIABILIDAD

Al tratarse de un proyecto de ayuda social el financiamiento se lo puede efectuar a través de una entidad gubernamental u ONG.

VENTAJAS Y DESVENTAJAS PARA LA INSTITUCIÓN PROMOTORA

La ventaja consiste en que la entidad auspiciante recuperaría directamente el costo del proyecto para emplearlo en otros proyectos de ayuda social.

La desventaja es que el tiempo de recuperación dependería del precio de la capacitación y mientras exista un precio más alto la mayoría de notarías no desearían obtener la capacitación.

Alternativa 2: Venta de servicios, cobro mensual de los servicios previa entrega de tecnología

Se ofrecería directamente a las notarías el servicio de la plataforma digital.

En este caso se calcula solo el periodo de recuperación y el punto de equilibrio sobre el posible costo de capacitación y entrega de la plataforma tecnológica que tendrían que pagar las notarías.

Debido a que los datos financieros de las notarías son confidenciales, constan en la aproximación de este flujo de fondos los costos incurridos por una pequeña empresa que inicia sus actividades.

Para los ingresos:

- El número de usuarios es tomado de acuerdo al estudio realizado por la Fundación Rumiñahui que estima que existe 1 de cada 3 migrantes demandantes del servicio. A este dato consideramos un castigo para poder aproximarnos al dato de usuarios potenciales para cada notaría.
- La tasa incremental de usuarios la consideramos en el 10%, para mantener un flujo conservador, ya que no se cuentan con datos históricos de la demanda.
- Tomamos como referencia el precio de los principales servicios notariales publicados por el Ministerio de Relaciones Exteriores.

Para los egresos:

- El costo de la adquisición del paquete tecnológico que se considera para el año 0.
- El costo de mantenimiento del software a partir del año 1.
- Se toma una breve aproximación de los posibles gastos de una notaría ya que la información financiera de las notarías es confidencial.
- Los egresos considerados tienen un incremento del 10% anual en el horizonte del proyecto.

VIABILIDAD

Esta alternativa dependería de la negociación entre la institución promotora del proyecto, con la Asociación de Notarías en lo referente al ofrecimiento del servicio y al cobro de la capacitación en el nuevo sistema digital.

VENTAJAS Y DESVENTAJAS PARA LA INSTITUCIÓN PROMOTORA

Otra ventaja es que el precio de la capacitación que las notarías pagarían sería de una vez al año y solo se consideraría un pequeño costo de mantenimiento.

La desventaja es que mientras exista un precio alto de capacitación algunas notarías no desearían obtener el servicio.

Alternativa 3: Implementación de normas y tecnologías a cambio de una tasa porcentual por transacción

Se cobraría una tasa porcentual por cada transacción que las notarías realicen luego de la entrega del servicio.

La aproximación del flujo de fondos de las notarías para esta alternativa es similar a la anterior pero en los egresos se considera el 10% de comisión por transacción que las notarías deberían pagar.

VIABILIDAD

Para el cobro del porcentaje por transacciones que las notarías realicen sería necesario especificar en un reglamento de los “cobros de los servicios notariales”, el pago de este servicio.

VENTAJAS Y DESVENTAJAS PARA LA INSTITUCIÓN PROMOTORA

La ventaja es que las notarías no necesitarían un monto de dinero para obtener el servicio sino que pagarían de acuerdo a las transacciones que realicen.

La desventaja es que mientras no exista un reglamento donde se especifique el posible convenio entre las partes para el cobro del servicio mediante esta alternativa, la plataforma tecnológica no funcionaría.

Indicadores económicos y sociales (TIR, VAN y Otros)

Los indicadores económicos están relacionados con los resultados obtenidos en la elaboración de los flujos de fondos aproximados.

Como estos rubros y valores constituyen una aproximación a los flujos, consideramos los cálculos de los indicadores económicos del TIR, el VAN, el punto de equilibrio y el período de recuperación de la inversión, están sujetos a los cambios que se presenten en los valores de los flujos de fondos.

	ALTERNATIVA 1	ALTERNATIVA 2	ALTERNATIVA 3
DEMANDA	383 notarìas	57 usuarios	57 usuarios
PRECIO	$ 1.08	$ 80	$ 72
TASA REQUERIDA	6%	6%	6%
TIR	14,03 %	14,34%	6%
VAN	$ 96.93	$ 8.59	$ 819
PUNTO EQUILIB.	344 notarìas	37 usuarios	41 usuarios
PER. RECUPER.	3.97 años	0 años	0 años

A modo general podemos darnos cuenta que es un proyecto auto sustentable de acuerdo a todas las alternativas presentadas considerando también que las aproximaciones a los flujos son conservadoras ya que es un servicio necesario para la satisfacción de una necesidad de los migrantes y para la modernización de los procesos notariales en el País.

La TIR en los flujos, sobrepasa la tasa esperada de rendimiento del 14%, tomando en cuenta que el interés pasivo en el mercado es del 6% en promedio.

El VAN en los flujos es positivo lo que indica la viabilidad del proyecto, sin tomar en cuenta que estamos realizando aproximaciones para flujos conservadores.

El punto de equilibrio es necesariamente menor a la demanda estimada en cada caso. El período de recuperación es mínimo y aceptable.

En cuanto a los indicadores sociales, están relacionados con el nivel de satisfacción de las necesidades de la población objetivo, en este caso del segmento de los migrantes ecuatorianos, quienes se verán beneficiados por:

- La obtención de un servicio eficiente, rápido, seguro y confiable
- Sus costos se verán reducidos
- Se podrá contar con una base de apoyo de los documentos legalizados que estarán disponibles para sus trámites tanto en el Ecuador como en el extranjero
- Se mantendrá la tranquilidad para el migrante – usuario como para su familia en el País, debido a la ejecución rápida y segura de sus trámites.
- Reinserción del migrante en las actividades productivas del País, debido a la realización de trámites económicos como la compra – venta o creación de empresas
- Posibilidad de realizar el voto electrónico para los migrantes

Estos datos se analizarán con precisión en la evaluación social luego de implementado el proyecto.

Análisis de Sostenibilidad

Análisis de impacto ambiental y de riesgos

En la actualidad, resulta imprescindible la implantación de gestiones electrónicas que aceleren los procesos en todos los sectores de la sociedad.

Con la implementación de un sistema Notarial Digital se podrán realizar transacciones electrónicas con el mismo nivel de seguridad y confianza que las transacciones persona a persona, ya que dichas transacciones al ser creadas poseerán registros electrónicos para no ser alteradas o confundidas, que se logran con complejos sistemas matemáticos.

Es comprensible que al ser herramientas informáticas tienen un grado de riesgo pero al mismo tiempo proveen de herramientas ya utilizadas con éxito en otros países así como de estrategias para la seguridad de los servicios, en este caso de la Notaria Digital, que estamos proponiendo.

Por otra parte, al ser un sistema notarial digital de uso fácil, rápido, que minimiza errores, podemos decir, que ayuda a reducir los costos no solo para los usuarios sino también para las notarías principalmente por la reducción de consumo de papel y las consiguientes situaciones ambientales.

Sostenibilidad social: equidad, género, participación ciudadana

El tipo de proyecto es social, ya que va dirigido al segmento de migrantes ecuatorianos que requieran realizar trámites legales notariales a quienes se les ofrecerá un servicio rápido, seguro y confiable, que reducirá sus preocupaciones y además, sus costos.

Es imprescindible la participación activa de los organismos estatales vinculados con la problemática migratoria, las notarías y sus funcionarios y la ciudadanía en general para desarrollar el conocimiento de este nuevo sistema de Notaría Digital, para impulsar el nuevo sistema y para obtener las sugerencias que pueden ayudar a mejorarlo para beneficio de todos.

Además de los beneficios del sistema de notarías digitales para los usuarios en el sentido técnico y económico, este sistema puede ser de gran ayuda ya que se podrá mantener un contacto mas real de las necesidades de los migrantes - usuarios del sistema, con lo que será más oportuna la implantación de políticas de ayuda dirigidas a este segmento de migrantes ecuatorianos.

Podríamos decir, que la visión de este proyecto social estaría encaminada a la "reinserción de la población migrante" a las actividades productivas del País en el sentido de su participación activa en procesos que no solo se refieren a trámites notariales sino también a trámites económicos como la compra – venta o creación de empresas.

Otro punto importante que permite la sostenibilidad social del proyecto es que debido a la facilidad, rapidez y confiabilidad en la ejecución de trámites legales a través del sistema de notarías digitales, estos servicios también estarán disponibles para toda la sociedad ecuatoriana que requiere este tipo de trámites incluso dentro del País.

Estrategias de seguimiento y evaluación

Evaluación de resultados e impactos

El área de coordinación planteará las estrategias para la evaluación del proyecto.

Entre sus trabajos constará la realización de encuestas principalmente enfocadas a la "Satisfacción del servicio" que serán realizadas a la población objetivo previo los respectivos estudios y luego de la implantación del proyecto.

Capitulo 4

Conclusiones

El desarrollo de las Tecnologías de Información y su utilización permiten brindar soluciones a problemas relacionados con la gran población mundial de migrantes, sus trámites, solicitudes, entre otros servicios podrán prestarse a través de internet y podrán estar a disposición de todos sin importar su condición social o cultural. Para esto se deberá coordinar todos los esfuerzos y tecnologías para alcanzar una mayor eficiencia en los servicios propuestos en este trabajo.

En lo relacionado al marco legal, técnico y operativo, las leyes y reglamentos establecidos en el país permiten operar sin ningún problema cualquiera de las alternativas propuestas en el trabajo, es importante anotar que hasta la realización de este trabajo todavía no se han presentado empresas que brinden ofrezcan este servicio.

Los análisis económicos, financieros, técnicos y legales presentados en este trabajo, determinan la factibilidad y sustentabilidad del mismo.

Recomendaciones

La utilización de las Tecnologías de Información y Comunicación en el país es muy importante, el desarrollo de las mismas sin lugar a duda permite el crecimiento y desarrollo de nuevas herramientas para combatir problemas sociales, mejorando la educación y disminuyendo las brechas de conocimientos tecnológicos.

Es importante estar atentos a las regulaciones y modificaciones que puedan presentarse en la Asamblea Constituyente a la Ley y Reglamento de Comercio Electrónico, Firmas electrónicas y mensajes de datos, ya que los cambios podrían afectar las soluciones propuestas.

Debido a que estas tecnologías no han sido frecuentemente utilizadas en el país es necesario que se mantenga la supervisión del mismo por parte de personal que ha tenido experiencia en el tema (Certificación Digital), lo que garantizará la sinergia en el cumplimiento de los objetivos propuestos.

Es importante recalcar que es fundamental para el éxito del proyecto las relaciones y coordinaciones con organismos específicos en el tema, por ejemplo, Consulados, Notarias, Ministerio del Migrante, entre otras.

Referencias Bibliograficas

- **"Comercio Electrónico y Firma Digital",** Dr. Mauricio Devoto, Editorial La Ley S.A., Buenos Aires – Argentina, 2001, 486 págs.
- "Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos", 10 de abril del 2002.
- "Reglamento a La Ley De Comercio Electrónico", Decreto Ejecutivo No. 3496. RO/ 735 de 31 de Diciembre del 2002.
- "Reglamento para la Acreditación, Registro y Regulación de Entidades Habilitadas para prestar servicios de Certificación de Información y servicios relacionados", Resolución No.584-23-CONATEL-2003.