Universidad de Lima

Facultad de Ingeniería y Arquitectura

Carrera de Ingeniería Industrial

DESARROLLO E IMPLEMENTACIÓN DEL SISTEMA DE FIRMAS ELECTRÓNICAS Y CERTIFICADOS DIGITALES DEL ESTADO E IMPLANTACIÓN DE LA AUTORIDAD ADMINISTRATIVA COMPETENTE

Trabajo de suficiencia profesional para optar el Título Profesional de Ingeniero Industrial

Carlos Ruben Bernardino Vermejo Ruiz

Código 19801006

Asesor

Ana Elizabeth Valdez Ampuero

Lima – Perú

Setiembre de 2020

UNIVERSIDAD DE LIMA
MCMLXV
SCIENTIA ET PRAXIS

Development and implementation of the system for Electronic Signatures and Digital Certificates of the State and Implementation of the Competent Administrative Authority

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo consiste en proveer e implementar la infraestructura oficial del Sistema Nacional de Firma Electrónica y Certificados Digitales para realizar transacciones electrónicas confiables y con ello contribuir a la modernización y descentralización del Estado.

La Autoridad Administrativa Competente que es el órgano rector del Sistema Nacional de Firma Electrónica y Certificados Digitales estará encargada de aprobar los estándares y normas nacionales del sistema; iniciará su operación en INDECOPI, además se implementará una entidad de Emisión y Registro de Certificados del Estado en Reniec, y luego de acuerdo a las necesidades del Estado, otras instituciones públicas participarán en el sistema ya sea como Entidades de Certificación o Entidades de Registro o Verificación.

El ámbito del proyecto es básicamente el estatal, aunque con la implementación del ente rector, la Autoridad Administrativa Competente, se generaran Entidades Emisoras y de Registro del sector privado, las cuales emitirán certificados digitales que tendrán efecto legal al ser generados dentro de la infraestructura oficial de firma digital.

Palabras Clave: PKI, Certificados Digitales, Firma Digital, Autoridad Administrativa Competente, Infraestructura Oficial de Firma Digital.

ABSTRACT

The present work consists of providing and implementing the official infrastructure of the National System of Electronic Signature and Digital Certificates to carry out reliable electronic transactions and thereby contribute to the modernization and decentralization of the State.

The Competent Administrative Authority that is the governing body of the National System of Electronic Signature and Digital Certificates will be in charge of approving the national standards and norms of the system; It will start its operation at INDECOPI, in addition, an authority will be implemented to issue and register Digital Certificates for the government at Reniec, and then according to the needs of the State, other public institutions will participate in the system, either as Certification Entities or Registration or Verification Entities.

The scope of the project is basically to the public sector, although with the implementation of the governing body, the Competent Administrative Authority, Issuing and Registration Entities of the private sector will be created, which will issue digital certificates that will have legal effect when generated within the official infrastructure of digital signature.

Keywords: PKI, Digital Certificates, Digital Signature, Competent Administrative Authority, Official infrastructure of Digital Signature.

CAPÍTULO 1: ANTECEDENTES DEL PROYECTO

1.1 Breve Descripción del proyecto, la institución y reseña histórica.

El proyecto consiste en proveer la infraestructura de seguridad requerida para realizar transacciones electrónicas confiables y con ello contribuir a la modernización y descentralización del Estado.

La Autoridad Administrativa Competente que es el órgano rector del Sistema Nacional de Firma Electrónica y encargado de aprobar los estándares y normas nacionales del sistema iniciará su operación en INDECOPI además se implementará una entidad de Emisión y Registro de Certificados del Estado, y luego de acuerdo a las necesidades del Estado, otras instituciones públicas participarán en el sistema ya sea como Entidades de Certificación o Entidades de Registro o Verificación del Estado.

El ámbito del proyecto básicamente es el Estatal, sin embargo, con la implementación del ente regulador, la Autoridad Administrativa Competente, en el sector privado se generarán otras Entidades de Certificación y otras Entidades de Registro o Verificación, que contribuirán con los medios de seguridad indispensables para la realización de transacciones confiables dentro el ámbito privado. Su cobertura geográfica es nacional

La institución encargada de este estudio fue el Programa de Modernización y Descentralización del Estado (PMDE) que nació del contrato de préstamo No. 1437/OC/PE suscrito entre el Gobierno del Perú y el Banco Interamericano del Desarrollo con fecha 12 de Septiembre de 2004 su operación se describe en el manual de operación del Programa de Modernización y Descentralización del Estado Recuperado de (Programa de Modernización y Descentralización del Estado. *Manual Operativo del contrato de préstamo No. 1437/OC/PE suscrito entre el Gobierno del Perú y el Banco Interamericano del Desarrollo*. 2004)

Para su ejecución, se separaron los componentes de Modernización del Estado a cargo de PCM, y el de Descentralización a cargo del Consejo Nacional de Descentralización.

El componente 3 de modernización fue el referido al Gobierno Electrónico, el cual fue dividido en varios sub-componentes, el sub-componente 1 fue el encargado para realizar el Desarrollo e implementación del Sistema de Firmas Electrónicas y Certificados Digitales del Estado e Implantación de la Autoridad Administrativa Competente.

El propósito de este proyecto es el de implementar el Sistema Nacional de Firma Digital, que nace con la ley No. 27269 del 29 de Mayo de 2000 (ley muy bien planteada) que incluso apoyo en las preparaciones iniciales del modelo del marco legal de firma digital propuesto por la Comisión de las Naciones Unidas para el Derecho Mercantil (CNUDMI. *Ley Modelo de la CNUDMI sobre las Firmas Electrónicas*. 2001).

La justificación de este proyecto tiene como marco restrictivo la justificación del proyecto marco de Gobierno Electrónico cuyo propósito consiste en acercar el Estado al ciudadano, en ese sentido se planteó que para que la iniciativa de Gobierno Electrónico tenga éxito, se requiere poder realizar transacciones electrónicas seguras y para ello tecnológicamente se requiere de los certificados digitales. A pesar que en el Benchmarking detectamos por ejemplo que en el Asia la adopción de estos sistemas se sustentó en el aumento de la eficiencia del Estado, y en el caso de Estados Unidos se sustentó por competitividad.

El estudio realizado siguió la metodología del Sistema Nacional de Inversión Pública (SNIP), y pasó por el proceso de aprobación de la Oficina de Programación de Inversiones del Ministerio de Economía y Finanzas, siendo aprobado como estudio de pre-inversión debido al cambio en el enfoque de la formulación por sub-componentes.

La formulación del estudio de factibilidad de éste sub-componente la realizó el Programa de Modernización y Descentralización del Estado, el beneficiario fue la Oficina Nacional de Gobierno Electrónico, dependiente de la Secretaría de Gestión Pública de la Presidencia del Consejo de Ministros contratando para ello una consultoría individual para realizar la formulación desde noviembre del 2004 hasta finales del 2005.

1.2 Descripción del sector.

A nivel del estado, aparecen algunos esfuerzos individuales por colocar servicios en línea a los ciudadanos, en el estudio de la demanda, en las entrevistas exploratorias a las instituciones públicas más relevantes a nivel transaccional se pudo identificar el efecto

favorable de los servicios en línea realizado por Registros Públicos en la zona registral No. IX – Sede Lima con la venta de las consultas de la publicidad registral en línea, fue la primera iniciativa de gran impacto y que afirmó el éxito estratégico del lanzamiento de nuevas tecnologías a través de aplicaciones concretas.

Si revisamos algunos indicadores sobre esta aplicación nos puede ayudar a formar un criterio válido.

Tenemos las siguientes cifras antes y después de lanzar el servicio de consultas electrónicas y copias de las fichas y registros de la SUNARP, Baltazar Caballero, Jorge Luis (2002). Sistematización de los procesos de inscripción y publicidad registral (tesis para optar el título profesional de Ingeniero Industrial). Universidad Nacional Mayor de San Marcos:

Tabla 1.1

SUNARP Impacto de los servicios electrónicos en línea

Rubro	**1997**	**1998**
Consultas	949,702	1,286,665
Inscripciones	252,879	479,503

Fuente: Baltazar Caballero, Jorge Luis (2002). *Sistematización de los procesos de inscripción y publicidad registral.* (p. 28).

Tabla 1.2

SUNARP Crecimiento Anual luego de lanzar servicio electrónico

Rubro	**1997 - 1998**
Incremento anual de las consultas e inscripciones	46,85%
Reducción de tiempos en los trámites	de 60 días a un rango entre 2 y 9 días dependiendo del servicio
Tarifa por consulta.	S/. 5.00
Ingresos por servicio de consultas web	Suficiente para mantener el Sistema a Nivel Nacional y más

Fuente: Baltazar Caballero, Jorge Luis. (2002). *Sistematización de los procesos de inscripción y publicidad registral.* (p. 10,28).

Al cambiar el tipo de atención de consultas e inscripciones en forma electrónica, estas crecieron en un 46.85% anual obteniéndose ingresos importantes por este servicio, estos ingresos permitieron que el Sistema se amplíe a una cobertura Nacional, estos ingresos actualmente son tan importantes que varios de los servicios de consultas se están brindando sin costo.

Los resultados observados en el Benchmarking de China, Estados Unidos y Europa también nos llevaron a reconocer las siguientes ventajas:

Con respecto a China, la aplicación más impactante ha sido la de comercio exterior del puerto de Hong Kong (Government Electronic Trading Services) llevada a cabo por Tradelink, desde mediados de 1999 se estableció el objetivo de pasar todo los trámites del puerto de Hong Kong en forma electrónica a partir del 1 de enero de 2000. El proyecto fue un éxito logrando realizar la operación electrónica del puerto por un valor de 360 billones de dólares el año 2000, el año 2018 este comercio realizado electrónicamente en su totalidad ascendió a 1,200 billones de dólares americanos y su modelo de negocio desde el 2005 fue replicado en toda Asia y Francia.

1.3 Definición del problema y sus causas

El problema por resolver en el proyecto es definido como:

“Reducida seguridad en la atención al ciudadano en los servicios en línea del estado”.

Se trata de un problema determinante para el éxito de proyectos de Gobierno Electrónico, es uno de los factores que destaca a la hora que el ciudadano hace uso de las nuevas tecnologías al relacionarse con el Estado. Es un problema que debe ser asumido por el Estado asignando capacidades y recursos necesarios para resolverlo. Su solución pasa por la implementación de un sistema que provea al Estado, así como a los ciudadanos y empresas, de los elementos tecnológicos y políticas que generen la confianza necesaria y la percepción de transparencia de las acciones del Gobierno. Ello coadyuvará a los

esfuerzos del gobierno para la modernización y descentralización del Estado. Una vez determinados los medios fundamentales para solucionar el problema identificado, se procedió a determinar las acciones necesarias para concretar dichos medios y de esta manera alcanzar el objetivo central del proyecto. Se plantearon acciones concretas orientadas a lograr cada uno de los medios fundamentales ya definidos en la base del árbol de objetivos.

CAPÍTULO 2: OBJETIVOS DE LA INVESTIGACION

2.1 Objetivo del Proyecto

El producto del proyecto es el Certificado Digital con valor Oficial emitido dentro de la Infraestructura Oficial de Firmas Electrónicas que proporcionará al Estado la capacidad de realizar transacciones electrónicas seguras.

El servicio faculta la realización de transacciones seguras en un escenario de confianza provisto y garantizado por el Estado.

La Infraestructura Oficial de Firmas Electrónicas, provee el respaldo técnico y legal tangible, por medio del cumplimiento estricto por parte de las Entidades Certificadoras acreditadas de los requisitos funcionales, administrativos y técnicos determinados y supervisados por la Autoridad Administrativa Competente del País.

El empleo de prácticas estándares internacionales permiten que los Certificados Digitales puedan ser validados en línea en cualquier instante, así mismo el Sistema garantiza que se ha utilizado procedimientos normalizados en todo el ciclo de vida del Certificado Digital.

El uso de Certificados Digitales en las transacciones electrónicas le otorgan los siguientes atributos:

- Autenticidad: Es la certeza de que cuando se establece una comunicación con alguien, ese alguien es realmente quien dice ser.
- Confidencialidad: Es la seguridad de que la información será develada únicamente a aquella persona a quien va dirigida.
- Integridad: Es la seguridad de que la información del documento electrónico no ha sido alterado desde su firmado digital.
- No Repudio: Si se dan las condiciones de autenticidad, confidencialidad e integridad, no se podrá argumentar carencia de responsabilidad en la transacción electrónica.

2.2 Medios fundamentales y acciones del proyecto

A continuación se muestra el cuadro de medios y acciones del proyecto.

Tabla 2.1

Cuadro de medios fundamentales y acciones del Proyecto

MEDIOS DIRECTOS	**Adecuada Infraestructura de Servicios en línea seguros**		**Socialización de los Servicios en Línea**	
MEDIOS FUNDAMENTALES	**MF.1.1.**	**MF.1.2.**	**MF.2.1**.	**MF.2.2**.
	Seguridad en las transacciones electrónicas en línea con el Estado.	Control sobre los medios de seguridad en los servicios en línea.	Difusión de Servicios en línea ofertados por el Estado utilizando certificados digitales.	Programas de capacitación a los empleados del Estado, para ofertar servicios en línea seguros.
ACCIONES	**Acción MF.1.1.1.**	**Acción MF.1.2.1**.	**Acción MF.2.1.1**.	**Acción MF.2.2.1.**
	Implementación de la Autoridad de Emisión y Registro de Certificados del Estado para su empleo en las aplicaciones y servicios del Estado en Línea AERC-RENIEC.	Implementación de la Autoridad Administrativa Competente en cumplimiento de lo estipulado por Ley (AAC1)	Programas de Difusión de la seguridad ofrecida por la tecnología de Certificados Digitales.	Programas de capacitación al personal de las entidades estatales sobre la tecnología de Certificados Digitales.
	Acción MF.1.1.2.	**Acción MF.1.2.2.**	**Acción MF.2.1.2.**	**Acción MF.2.2.2.**
	Implementación de Entidad o Entidades de Emisión y Registro de Certificados Digitales del Estado.	Implementación de la Autoridad Administrativa Competente modelado por la ONGEI-PCM (AAC2)	Programas de Difusión de la oferta de servicios públicos en línea utilizando certificados digitales.	Programas de capacitación al personal de las entidades estatales para la mejor prestación de servicios públicos en línea seguros, empleando Certificados Digitales.

(continúa)

(continuación)

MEDIOS DIRECTOS	Adecuada Infraestructura de Servicios en línea seguros	Socialización de los Servicios en Línea
	Acción MF.1.2.3.	
ACCIONES	Implementación de la Entidad de Certificación Raíz del Estado Peruano para su empleo en las aplicaciones y servicios del Estado en Línea ECREP-RENIEC.	

Elaboración propia.

8

CAPÍTULO 3: SITUACIÓN INICIAL

El diagnóstico de la situación actual se realizó, en primer lugar, desarrollando un acápite conceptual de enfoque del problema, a fin de determinar un esquema de análisis en el contexto de los servicios de Gobierno Electrónico, y mediante el empleo de una entrevista y encuesta a las entidades del estado que realizan una mayor cantidad de transacciones con la ciudadanía y que son las que han desarrollado iniciativas de Gobierno Electrónico, Luego de la identificación de varios problemas para la ejecución de las transacciones electrónicas, desarrollamos un diagnóstico; a continuación, se elabora una enumeración consolidada de los problemas identificados.

3.1 Lista de problemas identificados

En el diagnóstico se ha realizado una investigación explorativa mediante el uso de entrevistas y encuestas con las entidades estatales con más transacciones, luego de un análisis, se identificaron los siguientes problemas:

Los trámites presenciales consumen mucho tiempo y dinero del Ciudadano.

Los Servicios del Estado no han sido diseñados pensando en las necesidades del Ciudadano sino en las necesidades de la institución estatal.

Las Instituciones Estatales otorgan pocos recursos e importancia para el desarrollo de los portales web.

Se reportan cantidades importantes de errores en los trámites presenciales.

Existe poca experiencia en el uso de la tecnología de Firmas Digitales.

Carencia de una entidad supervisora que permita absolver reclamos sobre la emisión de Certificados Digitales sin las garantías suficientes.

Ausencia de los procesos de acreditación oficial para las Entidades de Certificación que permitirían corregir procedimientos errados en la administración de Certificados Digitales.

Ausencia de una Autoridad Supervisora de Certificados Digitales para coordinar procesos de interoperación y reconocimiento mutuo con otras entidades similares a nivel nacional e internacional.

Se han detectado procedimientos con trámites duplicados o innecesarios que restan competitividad a las Entidades Públicas, las empresas y el Ciudadano.

Se han detectado procesos Estatales no integrados entre las diferentes entidades estatales que dificultan el servicio y consumen tiempo y dinero al Ciudadano.

Los pocos servicios en línea, son difíciles de utilizar debido a que en muchos casos el diseño web no ha tomado en cuenta el punto de vista del usuario.

Carencia de estadísticas sobre la performance y disponibilidad de los servicios web de las instituciones estatales, impidiendo el monitoreo seguimiento para su mejora.

No existen estadísticas de comportamiento de los usuarios cuando navegan dentro del portal web, con el objetivo de mejorar las páginas web, los contenidos y sus estructuras.

No se toman las medidas adecuadas de seguridad para la realización de transacciones electrónicas con efecto legal y económico.

Incipiente conocimiento de la aplicación de la tecnología de Certificados Digitales.

Reducida percepción de transparencia debido a la poca publicación de toda la información existente publicable en las Entidades Estatales.

Empleo de insuficientes herramientas de seguridad de la información.

Carencia de una política de Seguridad Informática de la Entidad Estatal.

Carencia de sanciones explicitas ante infracciones a la política de seguridad.

Implementación del estándar de seguridad ISO 17799 no terminada, ni optimizada.

Marco legal carente de sanciones para las infracciones a las políticas y procedimientos dentro del Sistema de Firmas electrónicas y Certificados Digitales del Estado.

Escaso personal especializado disponible en temas de seguridad informática.

Carencia de conocimiento sobre la operación y uso de los Certificados Digitales, incluyendo su verificación.

Muchos Ciudadanos ignoran la oferta de servicios que las Entidades Estatales han implementado vía web.

Muchos Ciudadanos no saben cómo emplear la tecnología de Certificados Digitales para realizar sus transacciones electrónicas.

3.2 Diagnóstico del sector público

Luego de la identificación de los problemas, realizamos un diagnóstico del conjunto de entidades públicas que prestan servicios por Internet como iniciativas de Gobierno Electrónico, respecto a los elementos o factores que promueven o estimulan su difusión en la sociedad, podemos llegar a las siguientes conclusiones:

- La mayor parte de entidades que prestan servicios públicos en línea a través de un sitio Web se limitan a la oferta de información institucional difundible con la finalidad de lograr una percepción de transparencia institucional por parte de los ciudadanos o empresas usuarias del servicio. Esta información está generalmente accesible por sistemas de consulta a bases de datos, aunque en algunos casos no se da información importante para el usuario y no está actualizada. Por lo general ofrecen gran parte de su información, la restante no se encuentra en línea debido a la escasez de recursos, a la falta de prioridad, políticas de seguridad y difusión internas o decisión institucional.

Aún no se ofrecen opciones o canales de comunicación que promuevan la solución de conflictos o la participación ciudadana, contribuyendo con sus ideas, participando en la toma de decisiones o contactando directamente con sus representantes políticos, fortaleciendo la democracia e incrementando el sentido cívico de la sociedad.

Es aún muy reducido el grado de difusión de los servicios en línea, éstos requieren de campañas de publicidad y marketing que insumen recursos que posiblemente no estén disponibles. Igualmente, son escasos los programas de promoción del conocimiento de estos nuevos canales de comunicación y capacitación a los ciudadanos en el uso de los servicios públicos en línea. Estas acciones permiten incrementar el número de usuarios del servicio favoreciendo su difusión al resto de la sociedad, creando una masa crítica que permita la implementación de nuevos servicios.

Es evidente aún la sensación de desprotección y vulnerabilidad de los usuarios de los servicios en línea, respecto a su privacidad y protección de la información personal. El marco legal vigente no garantiza la protección del usuario, es necesario que se establezcan mecanismos de control, administrativos y judiciales, que garanticen la aplicación de las leyes. Así mismo, es necesario que dicho marco legal se armonice con el internacional, para que dicha protección jurídica sea independiente de la nacionalidad del sitio Web.

Los sitios Web que ofrecen servicios basados en transacciones electrónicas, no disponen aún de sistemas de seguridad transaccional que permitan garantizar la autenticidad, confidencialidad, integridad y no repudio de las operaciones realizadas. No se dispone de la tecnología de firma digital y las que lo aplican no cuentan con la certificación oficial que debe provenir de la Autoridad Administrativa Competente. La mayor parte de entidades utilizan sistemas de seguridad transaccional basadas en códigos de usuario y password que ofrecen una seguridad muy limitada.

En la actualidad es imposible ofertar servicios públicos en línea que permitan la realización de transacciones electrónicas auténticas, confidenciales, integras y no repudiables. Limitación muy grande que frena el desarrollo del Gobierno Electrónico.

Se ha constatado que la mayor parte de páginas Web de los sitios de servicios público en línea, tienen un alto grado de amigabilidad (usabilidad según norma ISO 9241-11) lo cual permite una navegación sencilla y de fácil comprensión del contenido. Sin embargo, en algunos casos es necesario promover un mejor diseño que considere las limitaciones preceptúales del ser humano, la ayuda y el soporte en línea.

Se hace evidente que no existe mecanismos de medida de la satisfacción de los usuarios de los servicios en línea, sistemas de retroalimentación que permitan monitorear el éxito de los servicios implementados e ir corrigiendo los defectos y generar el mayor valor añadido posible.

Conclusión

Es evidente que la confianza del usuario del servicio en línea y la disponibilidad del sistema público de emisión de Firmas Electrónicas y Certificados Digitales oficiales del Estado, constituyen actualmente el principal freno para el éxito de las iniciativas de Gobierno Electrónico, implementados y por implementar.

3.3 Sector privado

Con respecto al sector privado, a pesar de existir muchas iniciativas especialmente del sector financiero de realizar transacciones seguras por internet, localmente aún no se puede adquirir Certificados Digitales generados oficialmente con valor legal, lo que frena el desarrollo de transacciones y servicios por internet.

Mayor detalle sobre la situación del sector privado la puede obtener del Anexo No. 6

CAPÍTULO 4: ALCANCE Y LIMITACIONES DE LA INVESTIGACION

4.1 Alcance

El alcance del proyecto es Nacional, el objetivo es implantar el Sistema Nacional de Firma Digital llamado en términos legales la Infraestructura Oficial de Firma Digital y por extensión la Infraestructura Oficial de Firma Electrónica. Son elementos del proyecto el ente regulador nacional que es la Autoridad Administrativa Competente a implementarse en Indecopi, y la Entidad Reguladora del Estado y de Emisión y Registro del Estado Peruano, los cuales supervisan a las Entidades Certificadoras y a las entidades de Registro o Verificación que son las encargadas de emitir los certificados digitales con valor oficial.

4.2 Limitantes

El estudio realizado es parte de un proyecto más grande y hereda de él las siguientes restricciones:

- El objetivo principal del proyecto macro es implantar el Gobierno Electrónico
- La justificación del Proyecto es la de acercar el Estado al ciudadano
- Existe presión y pugna entre las dos autoridades participantes principales, Reniec e Indecopi.

Adicionalmente por las propias características de lo que se quiere realizar encontramos las siguientes limitantes:

- Es un producto con muchos detalles muy técnicos a tomar en cuenta
- Es un producto novedoso
- Existen múltiples beneficios muy difíciles de cuantificar como por ejemplo la tangibilidad de los documentos en el desarrollo de un juicio.

4.3 Marco conceptual

4.3.1 Introducción

El marco conceptual es necesario, porque para que la tecnología de certificados digitales pueda producir valor legal requiere una serie de elementos funcionales como las entidades de registro, las entidades de certificación, la autoridad administrativa competente que adopta los estándares vigentes y que acredita y supervisa a las entidades antes mencionadas, un marco legal y unos estándares técnicos de verificación y de firmado, así como un repositorio de publicación, todos esos elementos en su conjunto se denominan Infraestructura Oficial de Firma Digital.

Para implantar la infraestructura oficial (el sistema que hace que todo funcione y pueda lograrse el efecto legal) se requiere además unos equipos, una infraestructura tecnológica de hardware y software que cumplan unos estándares técnicos y que requiere una inversión y un retorno, de eso trata esta investigación.

Con respecto al marco conceptual, hemos incorporado en el Anexo 7 algunos conceptos técnicos adicionales necesarios para comprender el proyecto, así como un glosario de términos en el Anexo 1.

CAPÍTULO 5: JUSTIFICACIÓN DE LA INVESTIGACION

5.1 Introducción

Tomando en cuenta el diagnóstico realizado en las principales entidades del estado que participarán en el sistema recogido de las entrevistas realizadas con ellas y tomando en cuenta las restricciones del proyecto se elaboró el Marco Lógico.

5.2 Marco lógico

Producto del diagnóstico desarrollado en acápites anteriores se ha encontrado una lista de causas relacionadas con el problema presunto, las cuales están referidas a la deficiente atención de los servicios públicos al ciudadano y con mayor énfasis a los servicios en línea ofertados por el Estado.

Luego, dichas causas fueron caracterizadas como directas o indirectas según una relación de causalidad. Estas causas ayudaron a definir nuestro problema principal, el cual queda expresado de la siguiente manera:

REDUCIDA SEGURIDAD EN LA ATENCION AL CIUDADANO EN LOS SERVICIOS EN LINEA DEL ESTADO

5.2.1 Análisis de causas

El análisis de causas nos conduce a establecer dos vertientes de causas que están referidas a las limitaciones de infraestructura, y una reducida difusión y capacitación en el uso de certificados digitales en los servicios públicos en línea.

Una de estas causas directas identificadas es la **Limitada infraestructura de servicios en línea seguros**, que se manifiesta por que no se cuenta en el sector público con la adecuada infraestructura tecnológica, organizacional y legal que brinde la seguridad necesaria a los servicios en línea del Estado.

Esta causa a su vez se deriva, entre otras, de las causas indirectas que se describen a continuación:

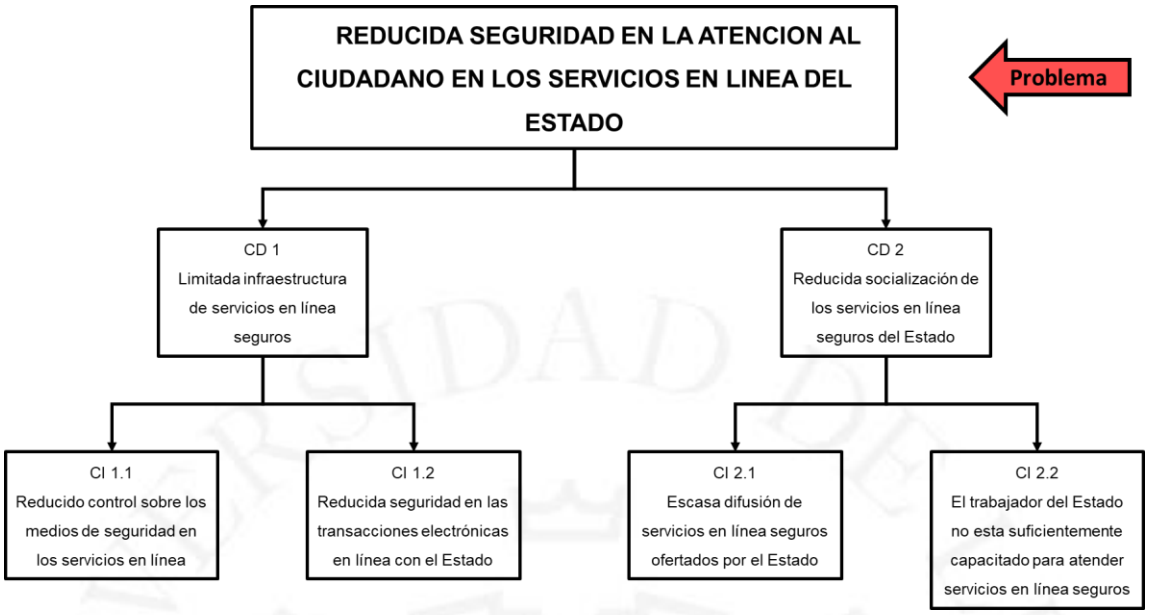
- Reducida seguridad en las transacciones electrónicas en línea con el Estado, debido a que no se cuenta con la tecnología adecuada para realizar transacciones electrónicas con efecto legal y económico que garanticen la integridad, autenticidad, confidencialidad y no-repudiación de las transacciones
- Reducido control sobre los medios de seguridad en los servicios en línea, porque no se cuenta con una entidad que posea la autoridad, capacidad normativa y de control que garantice la seguridad de los mecanismos y procedimientos en los servicios en línea del Estado.

Una segunda causa directa quedaría expresada en la ***reducida difusión y capacitación en el uso de certificados digitales en los servicios públicos en línea***, explicada debido al evidente desconocimiento por parte de los ciudadanos y empresas sobre las capacidades y ventajas del uso de certificados digitales en los servicios en línea ofertados por el estado y la falta de capacitación y experiencia por parte de los servidores públicos en la prestación de servicios en línea utilizando certificados digitales.. Esta causa directa a su vez proviene, entre otras, de las siguientes causas indirectas:

- Escasa difusión de servicios públicos en línea ofertados por el Estado utilizando certificados digitales de valor oficial, puesto que se ha observado que solo algunos de los servicios en línea de las instituciones evaluadas han realizado campañas de difusión de sus servicios a los usuarios.
- Reducida experiencia y capacitación del servidor del Estado en la prestación de servicios en línea utilizando certificados digitales de valor oficial. Se ha observado que no existen programas de capacitación con este enfoque de servicios en línea, lo que contribuye a generar dificultades en la prestación del servicio en línea seguro.

Figura 5.1

Árbol de Causas



Elaboración propia

5.2.2 Análisis de efecto

Si las causas analizadas previamente persisten y no son abordados por un proyecto, estos tendrán efectos en la sociedad, por lo que es necesario analizar el escenario sin proyecto. De igual manera que las causas, los efectos fueron divididos por niveles. Los efectos directos, que están íntimamente ligados con el problema central y son consecuencia directa de éste; los efectos indirectos, que se derivan de los anteriores; y por último, el efecto final, que produce una deficiencia de orden general

Uno de los efectos directamente ligados con el problema central es la **limitación para emitir certificados digitales oficiales**, debido a que aún no se cuenta con infraestructura oficial que se encargue de proveer dicho producto a los que requieren realizar transacciones con él. Este efecto produce el siguiente efecto indirecto:

- Imposibilidad de realizar transacciones electrónicas seguras con efecto legal y económico. La ausencia de certificados digitales oficiales que garanticen la integridad, autenticidad, confidencialidad y no repudio de transacciones electrónicas, hace prácticamente imposible emitir certificados digitales de carácter oficial.

Un segundo efecto directamente ligado al problema central es el **limitado número de usuarios de los servicios públicos en línea que brinda el Estado**, se refiere al efecto que produce los servicios públicos prestados inadecuadamente (inseguros) que no incentivan su uso por la sociedad, es decir, no genera la masa crítica que justifique el desarrollo de estos servicios. Este efecto, a su vez, ocasiona los efectos indirectos siguientes:

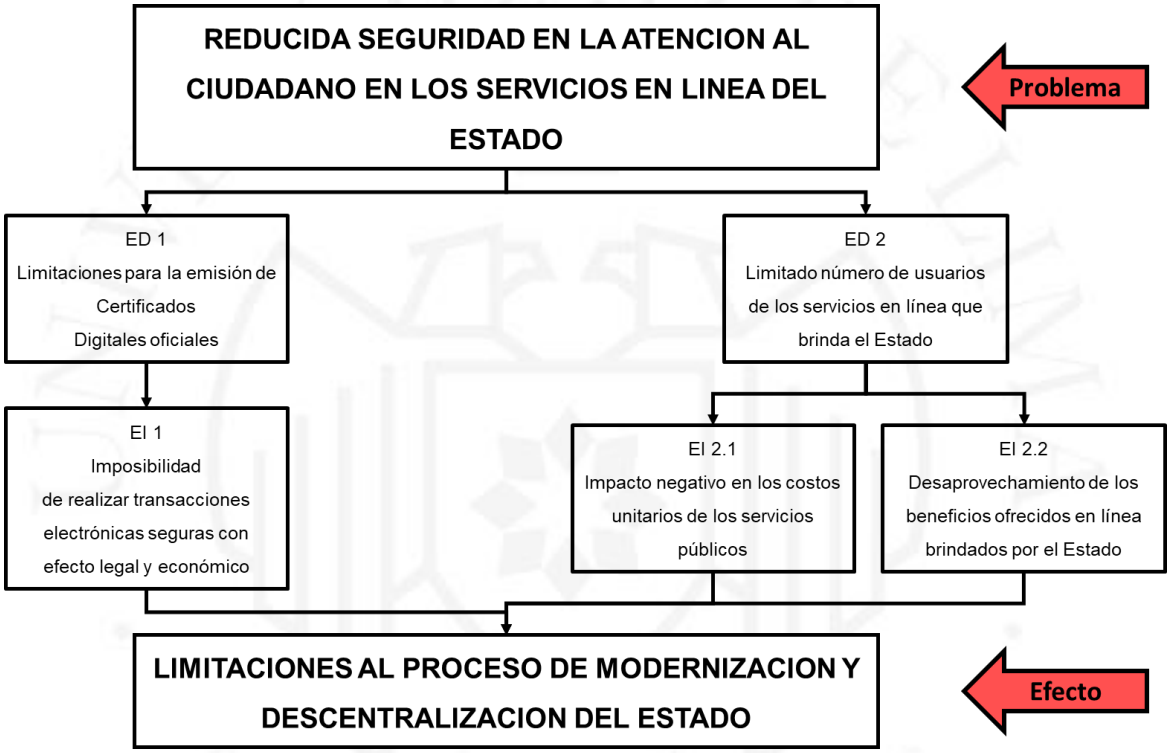
- Impacto negativo en los costos unitarios de los servicios públicos. En efecto, el limitado número de usuarios de los servicios públicos eleva los costos unitarios de los mismos, desaprovechando las economías de escala que son inherentes a los proyectos de esta naturaleza.
- Desaprovechamiento de los beneficios ofrecidos por los servicios en línea brindados por el Estado, lo que asimismo contribuye a que existan reducidas opciones para el desarrollo de nuevos servicios públicos en línea.

En consecuencia los efectos analizados nos producen el siguiente efecto final:

LIMITACIONES AL PROCESO DE MODERNIZACION Y DESCENTRALIZACION DEL ESTADO

Figura 5.2

Árbol de Efectos



Elaboración propia

5.2.3 Objetivo central o propósito del proyecto (medios)

El análisis de las causas y efectos del problema nos lleva al planteamiento de los siguientes medios que buscan la solución del problema y definen el objetivo central del proyecto que puede expresarse como:

AMPLIACION Y MEJORAMIENTO DE LA SEGURIDAD EN LA ATENCION AL CIUDADANO EN SERVICIOS EN LINEA DEL ESTADO

A continuación de describe los medios de primer nivel y fundamentales que permitirán el logro del objetivo central.

- Adecuada infraestructura de servicios en línea seguros. Que permitirán al Estado ofrecer servicios en línea con integridad, confidencialidad, autenticidad y no repudio entre las partes. Esto será posible si disponemos de los siguientes medios fundamentales:

- Seguridad en las transacciones electrónicas en línea con el Estado, que se logrará implementando entidades certificadoras para la emisión de certificados digitales.
- Control sobre los medios de seguridad en los servicios en línea, que se logrará mediante la implementación y entrada en operación de la Autoridad Administrativa Competente, la que se encargará de regular, supervisar y acreditar a las Entidades Certificadoras que emiten los Certificados Digitales.

- Socialización de los Servicios en Línea, referidos a acciones que están encaminadas a incrementar la utilización de los servicios en línea seguros utilizando certificados digitales, en base a las acciones de difusión hacia los usuarios y capacitación de los servidores del estado en el uso y atención de estos servicios en línea. Esto será posible si disponemos de los siguientes medios fundamentales

- Difusión de servicios en línea ofertados por el estado utilizando certificados digitales. Se refiere a los programas de difusión de los servicios en línea para su adopción masiva y utilización por la ciudadanía y empresas.

- Programas de capacitación a los empleados estatales para que puedan brindar nuevos servicios en línea seguros utilizando certificados digitales

Figura 5.3

Árbol de Medios

Elaboración propia

5.2.4 Análisis de fines

Los fines del proyecto son las consecuencias positivas que se espera lograr con la solución del problema. A su vez, éstos determinarán el fin último u objetivo de desarrollo del proyecto.

A continuación se describen los fines directos e indirectos del proyecto.

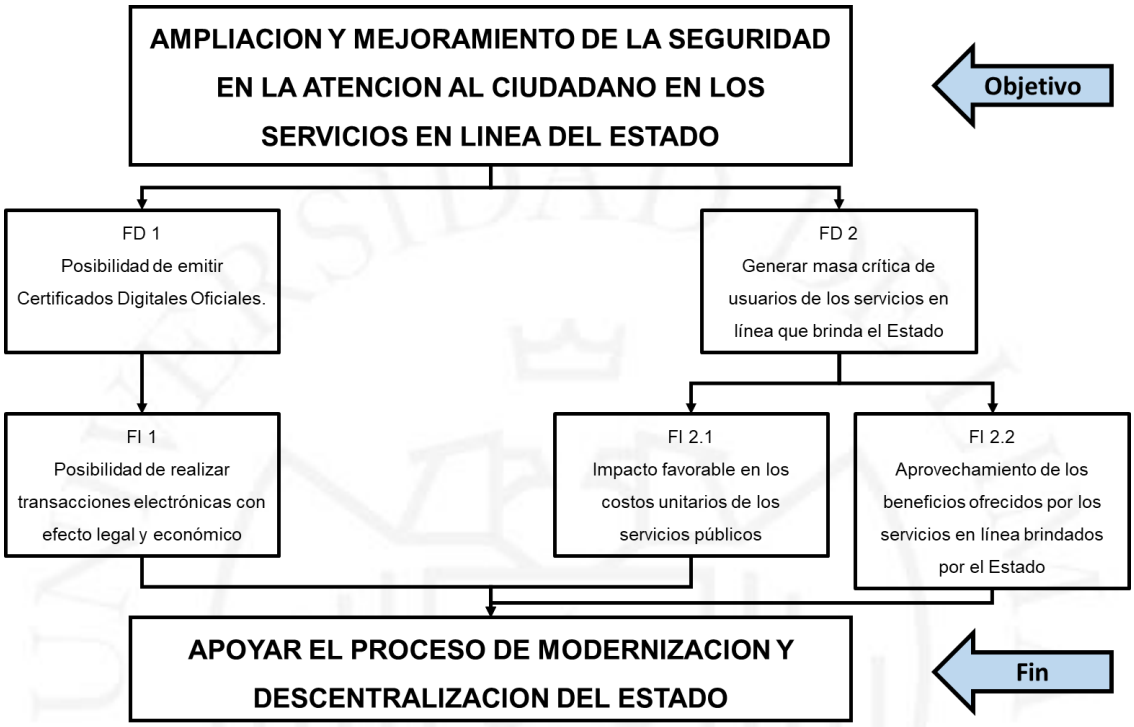
- **Posibilidad de emitir Certificados Digitales Oficiales**, las Entidades Certificadoras podrán emitir Certificados Digitales que serán empleados para poder realizar transacciones seguras en línea, el fin indirecto relacionado es que esto permitirá dar efectos económicos y legales en las transacciones que se realicen en línea.
- **Generar masa crítica de usuarios de los servicios en línea seguros que brinda el Estado**, relacionado con el incremento de la cantidad de usuarios debido al aumento de la confianza en los Servicios en línea del Estado. El efecto indirecto es el impacto favorable en los costos unitarios de los servicios públicos, además permitirá el aprovechamiento de las capacidades de los servicios en línea seguros brindados por el Estado.

El fin último de desarrollo del proyecto es:

APOYAR EL PROCESO DE MODERNIZACION Y DESCENTRALIZACIÓN DEL ESTADO

Figura 5.4

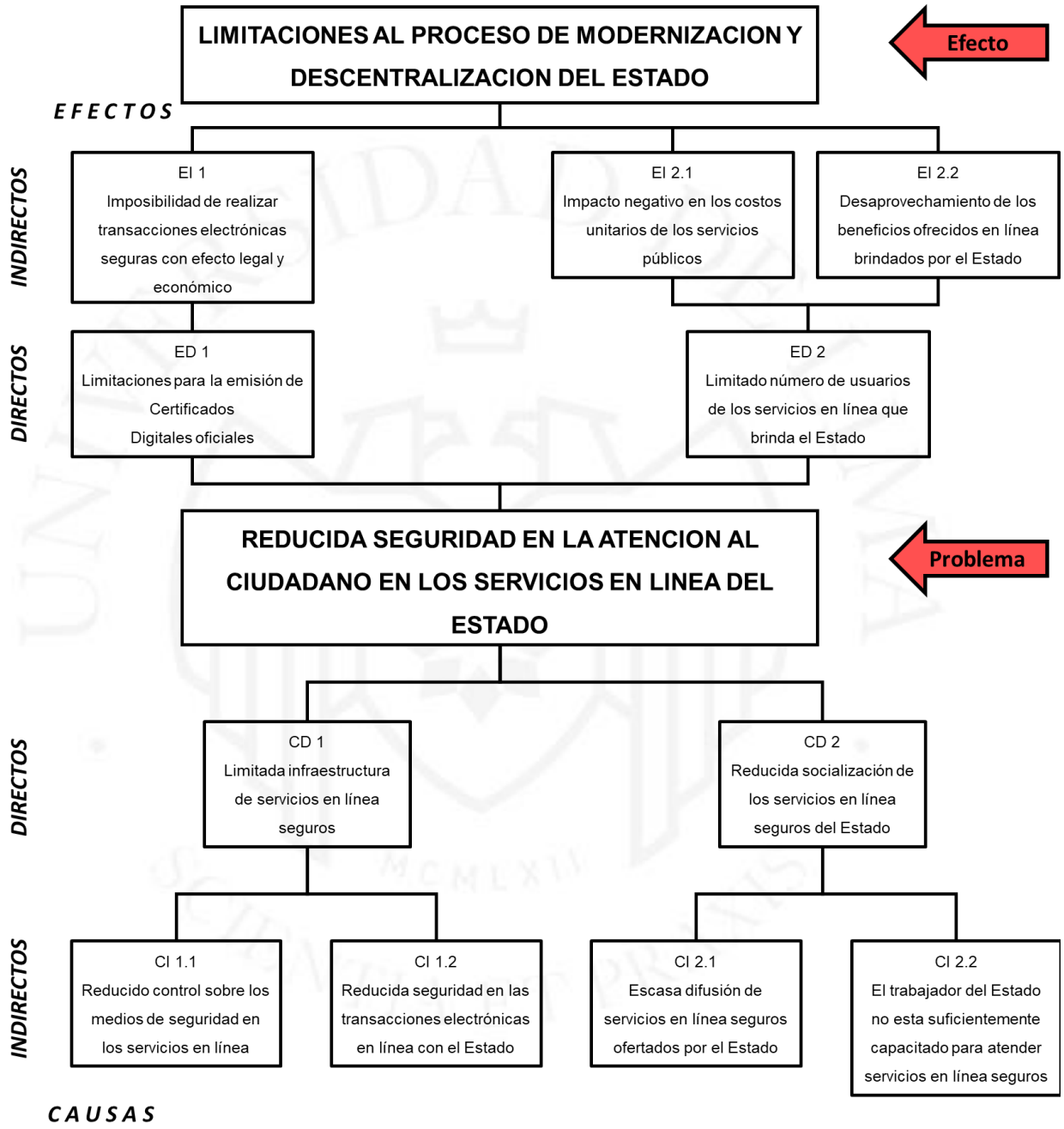
Árbol de Fines



Elaboración propia

Figura 5.5

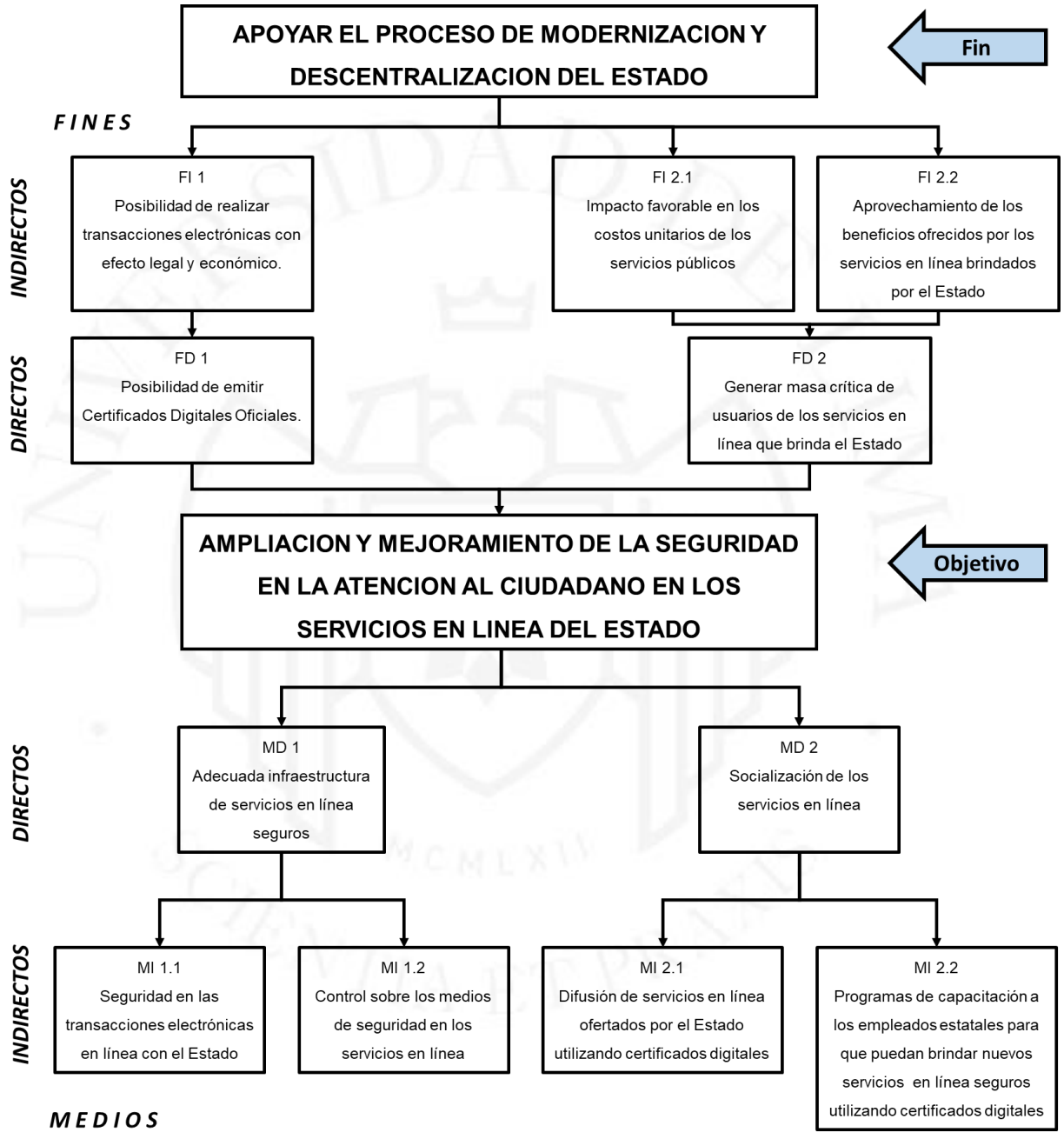
Árbol de Causas y Efectos



Elaboración propia

Figura 5.6

Árbol de Medios y Fines



Elaboración propia

5.2.5 Matriz del Marco Lógico

“DESARROLLO E IMPLEMENTACION DEL SISTEMA DE FIRMAS ELECTRÓNICAS Y CERTIFICADOS DIGITALES DEL ESTADO E IMPLEMENTACION DE LA AUTORIDAD ADMINISTRATIVA COMPETENTE”

Tabla 4.1

Marco Lógico del proyecto

	NIVEL DE OBJETIVO	INDICADORES	MEDIOS DE VERIFICACIÓN	SUPUESTOS
Fin	Apoyar el proceso de modernización y descentralización del Estado.	La percepción de los funcionarios públicos, ciudadanos y empresas respecto a la seguridad en las transacciones electrónicas con el Estado se incrementa en un 30 % cada año, a partir de la operación de la infraestructura oficial de firmas electrónicas.	Encuestas de opinión a funcionarios públicos, ciudadanos y empresas usuarias de los sistemas.	(Sostenibilidad) Apoyo político a las iniciativas de Gobierno Electrónico implementadas por la PCM. Ingresos recibidos por valor añadido a los servicios de emisión de firmas electrónicas y certificados digitales. Ahorros efectivos en la administración pública, por la simplificación administrativa y sustitución de transacciones presenciales por virtuales seguras.

(continúa)

(continuación)

	NIVEL DE OBJETIVO	INDICADORES	MEDIOS DE VERIFICACIÓN	SUPUESTOS
	Ampliada y mejorada la seguridad en la atención al ciudadano en los servicios en línea del Estado.	Cobertura de usuarios de firmas electrónicas y certificados digitales emitidos dentro de la infraestructura oficial de firmas electrónicas, a partir de la operación del sistema, se incrementa: 25% el primer año. 50% al segundo año 75% al tercer año	Registros de emisión y anulación de certificados digitales. Registros sobre Entidades Públicas que prestan servicios utilizando firmas electrónicas y certificados digitales. Registros de acciones realizadas por la Autoridad Autónoma Competente, para garantizar un entorno de transacciones electrónicas seguras. Encuestas a usuarios de los sistemas.	Apoyo político y compromiso real de las instituciones involucradas en el sistema (INDECOPI, RENIEC, PCM). Autoridades nacionales y los funcionarios públicos participan activamente en la instrumentalización e institucionalización del gobierno electrónico. Marco legal compatible con el desarrollo del sistema. Provisión oportuna y suficiente de fondos para la ejecución, operación y monitoreo del proyecto.
Propósito		Cobertura de entidades públicas que prestan servicios en un entorno de transacciones electrónicas, utilizando firmas electrónicas y certificados digitales, emitidas por la infraestructura oficial de firma electrónica a partir de la operación del sistema, se incrementa: 50 % el primer año 100 % al segundo año		

(continúa)

(continuación)

	NIVEL DE OBJETIVO	INDICADORES	MEDIOS DE VERIFICACIÓN	SUPUESTOS
	Seguridad en las transacciones electrónicas en línea con el Estado.	Infraestructura oficial de firmas electrónicas implementada y operativa al inicio del segundo año de operación del proyecto	Informes del sistema de monitoreo del proyecto.	Apoyo político y compromiso real de las instituciones involucradas en el sistema (INDECOPI, RENIEC, PCM, BID).
	Control sobre los medios de seguridad en los servicios en línea.	Autoridad Administrativa Competente del sistema implementado y operativo funcionalmente a los 6 meses de iniciado la fase operativa del proyecto.		Marco legal compatible con el desarrollo del sistema.
	Difusión de los servicios en línea ofertados por el Estado utilizando certificados digitales.	Programas de difusión masivas por medios escritos, radiales, televisivos y por Internet, sobre los servicios en línea y las ventajas y seguridad del uso de certificados digitales en las transacciones electrónicas con el Estado, a partir del tercer mes de iniciado la fase de operación del proyecto, hasta el tercer año.		Provisión oportuna y suficiente de fondos para la ejecución, operación y monitoreo del proyecto
Resultado	Programas de capacitación a los empleados estatales para que puedan brindar nuevos servicios seguros en línea utilizando certificados digitales.	Programas de capitación continúa en línea (e-learning) a funcionarios y empleados estatales respecto a la tecnología de certificados digitales y la prestación de servicios en línea utilizando dicha tecnología.		Receptividad de la Población ante campañas de difusión
				Actitud positiva del funcionario público ante Programas de Capacitación.

(continúa)

(continuación)

	NIVEL DE OBJETIVO	INDICADORES	MEDIOS DE VERIFICACIÓN	SUPUESTOS
	1.1. Implementación de la Autoridad de Emisión y Registro de Certificados del Estado para su empleo en las aplicaciones y servicios del Estado en Línea.		Informes del sistema de monitoreo del proyecto.	Apoyo político y compromiso real de las instituciones involucradas en el sistema (INDECOPI, RENIEC, PCM).
	2.1. Implementación de la Autoridad Administrativa Competente			Marco legal compatible con el desarrollo del sistema.
	3.1. Programa de difusión de la seguridad ofrecida por la tecnología de certificados digitales.			Ambientación y seguridad física proveída por las entidades involucradas.
Actividades	3.2. Programas de difusión de la oferta de servicios publicaos en línea utilizando certificados digitales.			Provisión oportuna y suficiente de fondos para la ejecución, operación y monitoreo del proyecto (MEF; BID).
	4.1. Programas de capacitación al personal de las entidades estatales sobre la tecnología de certificados digitales.			
	4.2. Programas de capacitación al personal de las entidades estatales para la mejor prestación de servicios públicos en línea seguros, empleando certificados digitales.			

Elaboración propia

CAPÍTULO 6: PROPUESTAS Y RESULTADOS

6.1 Propuesta

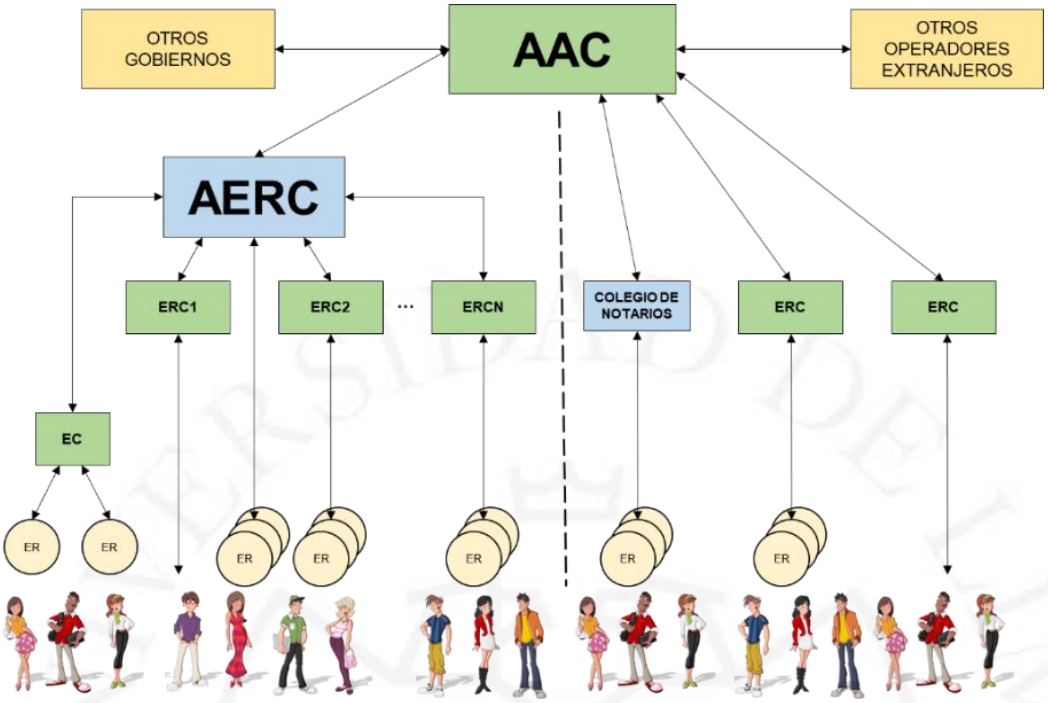
6.2 Descripción de la alternativa Seleccionada

La alternativa A que es la seleccionada se basa en la implementación de la Autoridad Administrativa Competente (AAC) como lo estipula la Ley de Firmas y Certificados Digitales vigente, y la creación de una nueva Autoridad que no se encuentra en la Ley, que es la Autoridad de Emisión y Registro de Certificados del Estado Peruano (AERC), cuya finalidad sería la de coordinar todas las Emisiones de Certificados del Estado y erigirse como puente de las Entidades Certificadoras del Estado garantizando de esta forma la interoperabilidad en el ámbito estatal y coordinando todos los esfuerzos estatales, complementada con programas de difusión y capacitación que refuercen las acciones mencionadas, una característica importante de esta alternativa es que respeta las funciones de acreditación, supervisión y regulación que ejerce la AAC, y la segunda característica también muy importante es que la AERC emitirá la gran mayoría de los Certificados Digitales a nivel nacional para el Estado.

Se elaboraron tres alternativas, la alternativa B no empleaba una entidad de emisión y registro del Estado, esta alternativa se desechó debido a que en la evaluación financiera se perdían los ingresos por emisión y verificación de certificados lo que la hacía inviable económicamente y y el uso de ésta tecnología generaría costos adicionales para el sector público, la alternativa C le daba el rol a la ONGEI para ser la entidad de emisión y registro de certificados digitales, esta también se desechó debido a que esta institución no contaba con locales a nivel nacional, se tendría que invertir en infraestructura adicional para hacer la labor de registro lo que aumenta enormemente la inversión reduciendo su beneficio, adicionalmente, existía la voluntad política y el interés de Reniec en participar en forma sustancial en el sistema.

Figura 6.1

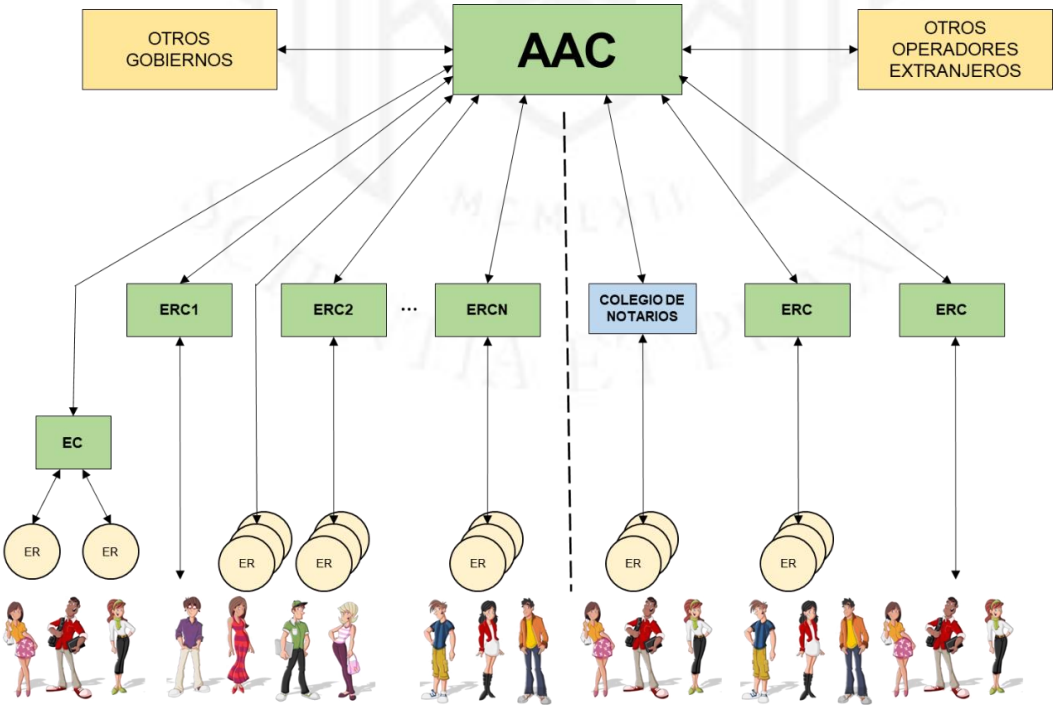
Arquitectura del Sistema Nacional de Firma Digital alternativa A



Elaboración propia

Figura 6.2

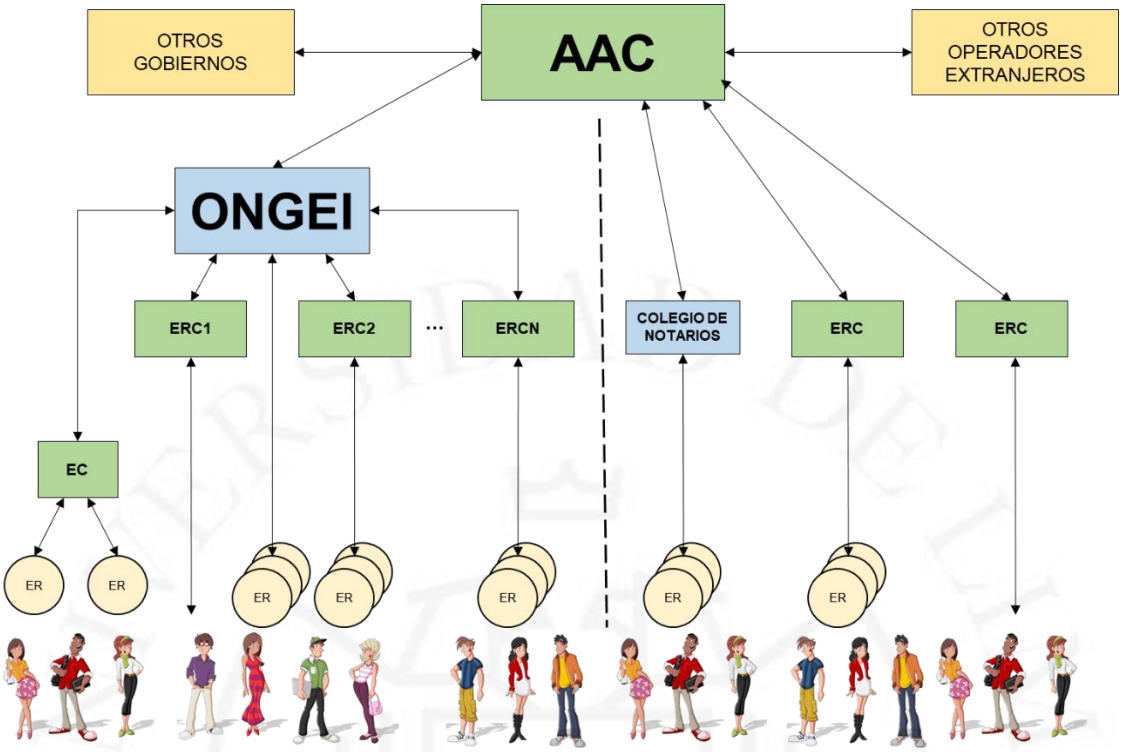
Arquitectura del Sistema Nacional de Firma Digital alternativa B



Elaboración propia

Figura 6.3

Arquitectura del Sistema Nacional de Firma Digital alternativa C



Elaboración propia

6.2.1 Características Funcionales de la Alternativa Seleccionada

La alternativa A está compuesta de la Autoridad Administrativa Competente, encargada exclusivamente en la acreditación regulación y supervisión de las Entidades Certificadoras y de las Entidades de Registro o Verificación. Así mismo, constará de la Autoridad de Emisión y Registro de Certificados del Estado, cuya principal misión será la de ser la Entidad de Emisión de Certificados Digitales del Estado, y encargada de coordinar los esfuerzos de Emisión de Certificados dentro del Estado y de la Emisión masiva de Certificados Digitales a nivel nacional. En caso de ser necesario se crearán algunas Entidades Certificadoras que también emitirán Certificados Digitales, y trabajarán en forma coordinada con las Entidades de Registro o Verificación del Estado, Todas estas entidades cumplen con la ley 27269 de Firmas y Certificados Digitales, su reglamento y disposiciones complementarias.

6.2.1.1 Funciones de la Autoridad Administrativa Competente

La Autoridad Administrativa Competente tiene las siguientes funciones:

- Servicio de Acreditación de Entidades de Certificación y Entidades de Registro.
- Servicio de Emisión de Certificados Raíz a las entidades de Certificación que lo requieran.
- Adopción de los estándares internacionales sobre Firmas Electrónicas y Certificados Digitales que serán válidos en el Perú.
- Establecimiento de las políticas necesarias sobre la funcionalidad, los requisitos de verificación. La estructura de datos de los Certificados, los Algoritmos o protocolos de encriptación, y los protocolos de administración de Certificados.
- Aceptar o rechazar las relaciones cruzadas entre otras las Entidades de Certificación o las Entidades de Registro.
- Aceptar o rechazar a las Entidades de Acreditación externas y sus Certificados.
- Aceptar la interoperabilidad del Sistema de Firmas y Certificados Digitales Nacional, con otro similar a nivel internacional.
- Capacidad para establecer nuevas reglas de juego para la acreditación y supervisión auditada.
- Capacidad de establecer sanciones y aplicarlas a las entidades reguladas si no cumplen con las obligaciones obtenidas en el proceso de acreditación.
- Definir y coordinar junto con otros participantes, los detalles de implantación de la estructura del árbol de directorio del estado, así como de su funcionalidad adicional requerida.

6.2.1.2 Funciones de la Autoridad de Emisión y Registro de Certificados del Estado

La Autoridad de Emisión y Registro de Certificados del Estado, se encarga de las siguientes funciones:

- Emisión y Registro de los Certificados Digitales a ser empleados por el Estado.
- Servir de puente entre las diferentes Entidades Certificadoras del Estado que puedan ser nombradas para ese fin.

- Servir de Entidad Certificadora de otras Entidades de Registro del Estado o para el Estado.
- Recopilar los Certificados digitales de todas las Entidades de Certificación que trabajen con el Estado para su uso por las aplicaciones pertinentes.

6.2.1.3 Funciones de las Entidades de Certificación (EC)

Las Entidades de Certificación (EC), se encargan de las siguientes funciones:

- Emisión y Firmado de Certificados Digitales.
- Publicación de Certificados Digitales y CRLs en el servidor de directorio LDAP propio o envío via web.
- Revocación de Certificados Digitales.
- Mantenimiento de un Servicio en Línea de Verificación de la validez del Certificado utilizando el protocolo OCSP o uno mejor.
- Coordinar con las Entidades de Registro para aceptar su interface de operación con la EC.
- Cumplir con sus declaraciones de prácticas y pasar previamente el proceso de acreditación y los costes con la Autoridad Administrativa Competente.

6.2.1.4 Funciones de las Entidades de Registro o Verificación (ER)

Las Entidades de Registro o Verificación (ER), se encargan de las siguientes funciones:

- Inicio del proceso de emisión de certificados, siendo obligatorio la verificación de la identidad del usuario en persona, la Autoridad Administrativa Competente determinará si es necesario guardar la documentación sustentatoria de la verificación.
- Generar o proveer los medios para que el usuario final genere su llave privada y con ella firme la solicitud que contendrá la llave pública que será aprobada por la Entidad de Registro previa verificación
- Además de firmar la solicitud electrónica después de la verificación, debe enviarla a la Entidad Certificadora para que esta a su vez la firme.

- Una vez que la Entidad Certificadora la firma debe recibirla para entregarla al usuario final a través de un medio seguro.

A nivel técnico la Autoridad Administrativa Competente cuenta con una infraestructura básica para la Emisión de Certificados Digitales en cantidades limitadas, pero cuenta con Servidores de Publicación dimensionados para soportar una carga superior para cumplir con la finalidad de ser un puente nacional que pueda realizar Certificaciones cruzadas con Organismos Internacionales similares de acuerdo a los requerimientos técnicos de interoperabilidad aceptados por la comunidad Internacional en su mayoría y que han sido propuestos por la Organización de APEC. Además realizará los acuerdos de reconocimiento mutuos con otras Entidades de Certificación y eventualmente también emitirá Certificados Digitales Raíz de otras Entidades Certificadoras Nacionales.

6.3 Herramientas de Ingeniería empleadas

Para el estudio de factibilidad se emplearon las siguientes herramientas, Benchmarking, Análisis explorativo, Árbol de causas y efectos, Marco lógico, estimación de la demanda, propuesta técnica y su dimensionamiento, Organización, Procesos, Evaluación financiera.

6.4 Benchmarking

El Benchmarking se realizó para los países de la región, Estados Unidos, Europa, Australia y China, llegando a las siguientes conclusiones:

- Autoridad Reguladora: Usualmente este rol es ocupado por entidad de estándares nacionales.
- Estrategia: Las adopciones más exitosas han estado relacionadas con el lanzamiento del sistema a través de aplicaciones masivas e impactantes.
- Dueño del Negocio: La entidad encarga de desarrollar el ecosistemas es usualmente la entidad encargada del desarrollo del Gobierno Electrónico.
- Grados de madurez: El sistema cuenta con un esquema de madurez y proceso de mejora continua.
- Lenta adopción en sistemas normativos optativos y aplicaciones de back-office deficientes.
- La justificación Principal para la implantación de éstos sistemas e invertir es por Aumento de la eficiencia y por el Aumento de competitividad.
- El uso principal y mayor beneficio de los certificados digitales es por Firmado Electrónico.
- Existe un peligro de pensar que esta tecnología solo tiene un uso exclusivo para autenticación.
- El siguiente peligro es no comprender los aspectos y detalles técnicos correctamente pudiendo hacer implantaciones erróneas.

6.5 Análisis explorativo

El análisis explorativo permitió diagnosticar y analizar la problemática de las entidades involucradas, dando como resultado el análisis de Causa y Efecto; y el Análisis de los medios y fines y con ello permitir construir el marco lógico, el resultado de ésta parte se puede apreciar en el punto 2.1.

6.6 Árbol de causa y efectos

El árbol causa y efecto y el de medios y fines fueron la base para la construcción del marco lógico y lo pueden ver en el punto 4.2

6.7 Marco lógico

El marco lógico ya desarrolla adicionalmente supuestos e indicadores para el seguimiento del proyecto, se puede apreciar al final del punto 4.2

6.8 Estimación de demanda

Para la estimación de demanda, se hizo un relevamiento de los principales servicios transaccionales de las entidades involucradas y se estimó su conversión paulatina a su publicación por internet, a esto se añadió una estimación de adopción paulatina de la tecnología, con esta estimación se realizó el plan de producción y se proyectaron los ingresos que tienen los siguientes rubros:

Autoridad Administrativa Competente:

Tabla 6.1

Ingresos por Autoridad Administrativa Competente

Item	Ingresos AAC
1	Ventas de Servicios de Acreditación
2	Trámite Administrativo
3	Ingresos por supervisión
4	Emisión de Certificados Raíz
5	Venta de Servicios de Valor Añadido

Elaboración Propia

Autoridad de Emisión y Registro de Certificados:

Tabla 6.2

Ingresos por Autoridad de Emisión y Registro de Certificados

Item	Ingresos AERC
1	Venta de Certificados Digitales
2	Venta de Servicio en Línea para Verificación
3	Venta de Certificados Raíz
4	Venta de Servicios de Valor Añadido

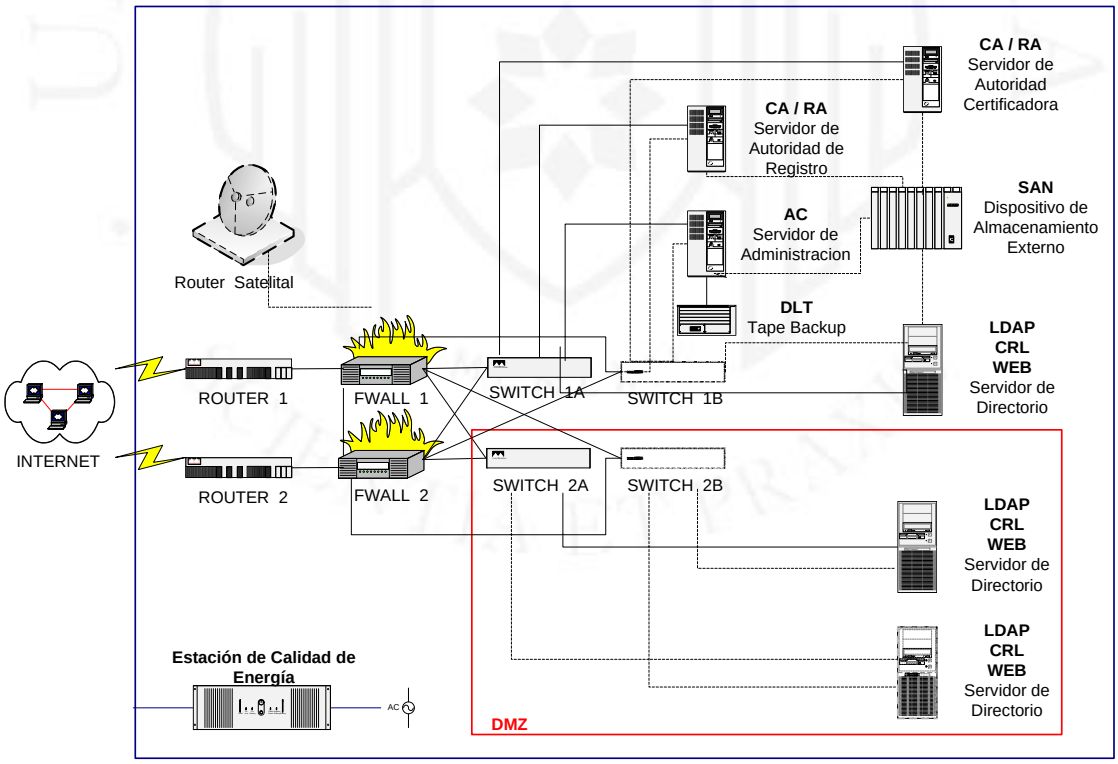
Elaboración Propia

6.9 Propuesta técnica

La propuesta técnica incluyó el dimensionamiento, las especificaciones técnicas del hardware y del software a adquirir, y la distribución física y las obras civiles en los lugares aparentes a ser instalados, a continuación se muestra un extracto del mismo:

Figura 6.4

Infraestructura de la Autoridad Administrativa Competente

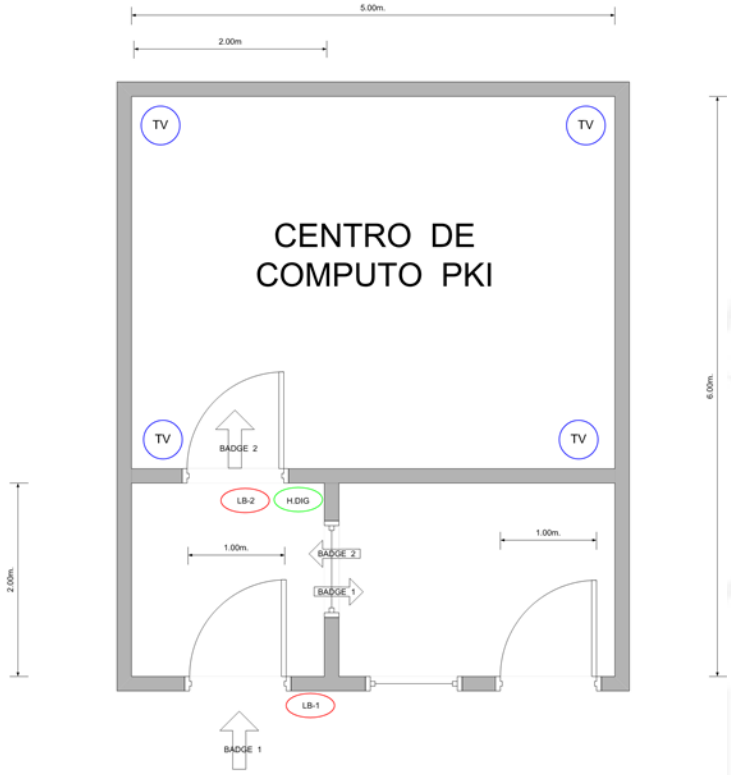


Elaboración propia

Propuesta para la Seguridad Física de la Autoridad Administrativa Competente Indecopi.

Figura 6.5

Seguridad Física para la Autoridad Administrativa Competente



Elaboración propia

Para acceder al centro de cómputo PKI, se accede con una tarjeta (Badge) en el lector LB-1 luego en la antecámara cambian su credencial por otra tarjeta que acciona el lector LB-2, su ingreso se registra tanto con hora de entrada y salida, al salir se entrega el Badge-2 y le devuelven el Badge-1.

Tabla 6.3

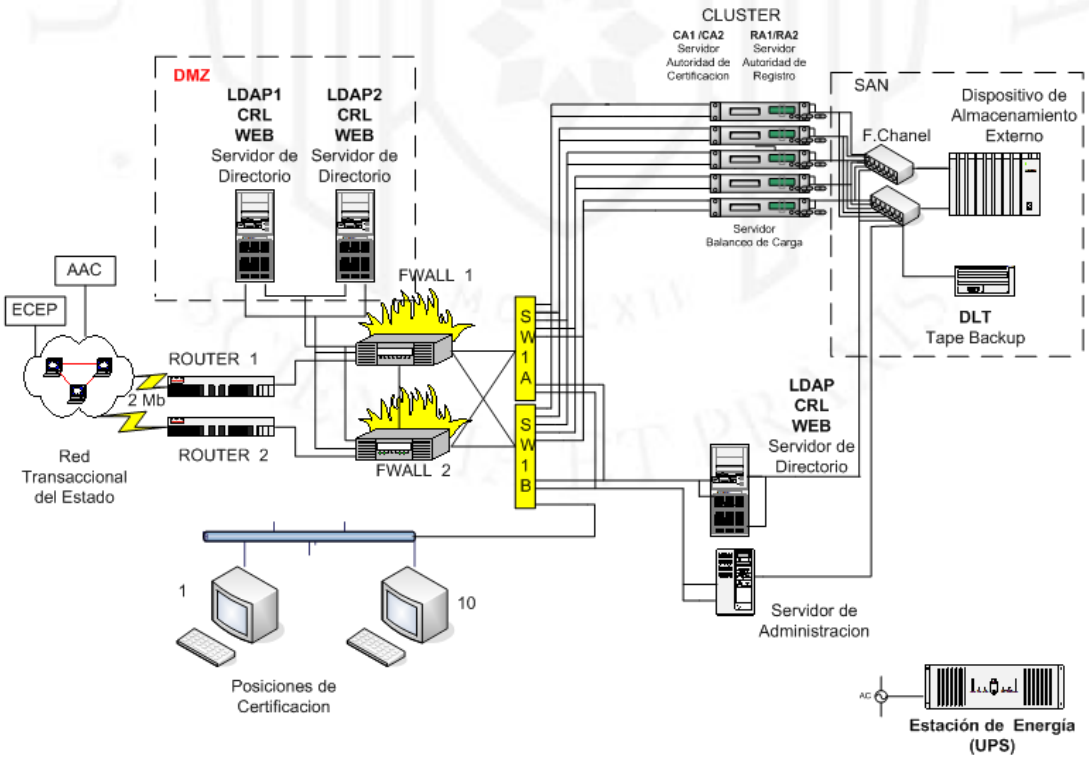
Infraestructura de seguridad física de la AAC

OBRAS CIVILES	**EQUIPAMIENTO**
Demoler 17 mt de pared de madera	Dos (02) Lectores de Banda Magnética
Construir 18 metros de ladrillos y cemento	Un (01) Lector de huella digital (Activado por el lector de Banda Magnética)
Tres (03) Puertas de Seguridad	Cuatro (04) Camaras de Circuito Cerrado
Dos (02) Ventanas de Vidrio Templado de 1 mt	Un (01) Equipo de DVR
OPERACIÓN	
Estos equipos requieren el mantenimiento recomendado por sus fabricantes	
Esta alternativa genera costos operacionales adicionales al tener que contratar servicio de seguridad.	
EVALUACIÓN	
Esta alternativa entrega un nivel de seguridad mayor que es requerido por la aplicación	
Existen otras alternativas evaluadas más económicas pero que no proveen el nivel de seguridad necesario.	

Elaboración propia

Figura 6.6

Infraestructura de la AERC del Estado



Elaboración propia

Propuesta para la seguridad Física de la Autoridad de Emisión y Registro de Certificados

Para el alojamiento de la plataforma de cómputo y de Red del sistema AERC se ha considerado la siguiente distribución:

Tabla 6.4

Área dimensionada para la AERC

Distribución de área por Elemento	**Mtrs Cuadrados**
Rack de Comunicaciones	2
Rack de Servidores	2
Rack de Arreglo de discos	3
Consola del Sistema	2
Espacio para un UPS	3
Espacio para mantenimiento	9
Considerando crecimiento	6
Alojamiento de la bóveda de seguridad	2
Compartimiento de los cartuchos de cinta y otros	3
Total Sala de Equipos	**32**
Área Personal de Operación	**32**
Área total	**64**

Elaboración propia

Se requiere 32 Mt^2 de Área cuya estructura de seguridad debe estar construido con material noble y recomendable reforzado el perímetro con malla de acero y deberá contar con falso piso y falso techo para la circulación de Aire Acondicionado.

Se ha considerado un área adicional de 32 Mts cuadrados para el personal encargado de la administración, operación del sistema.

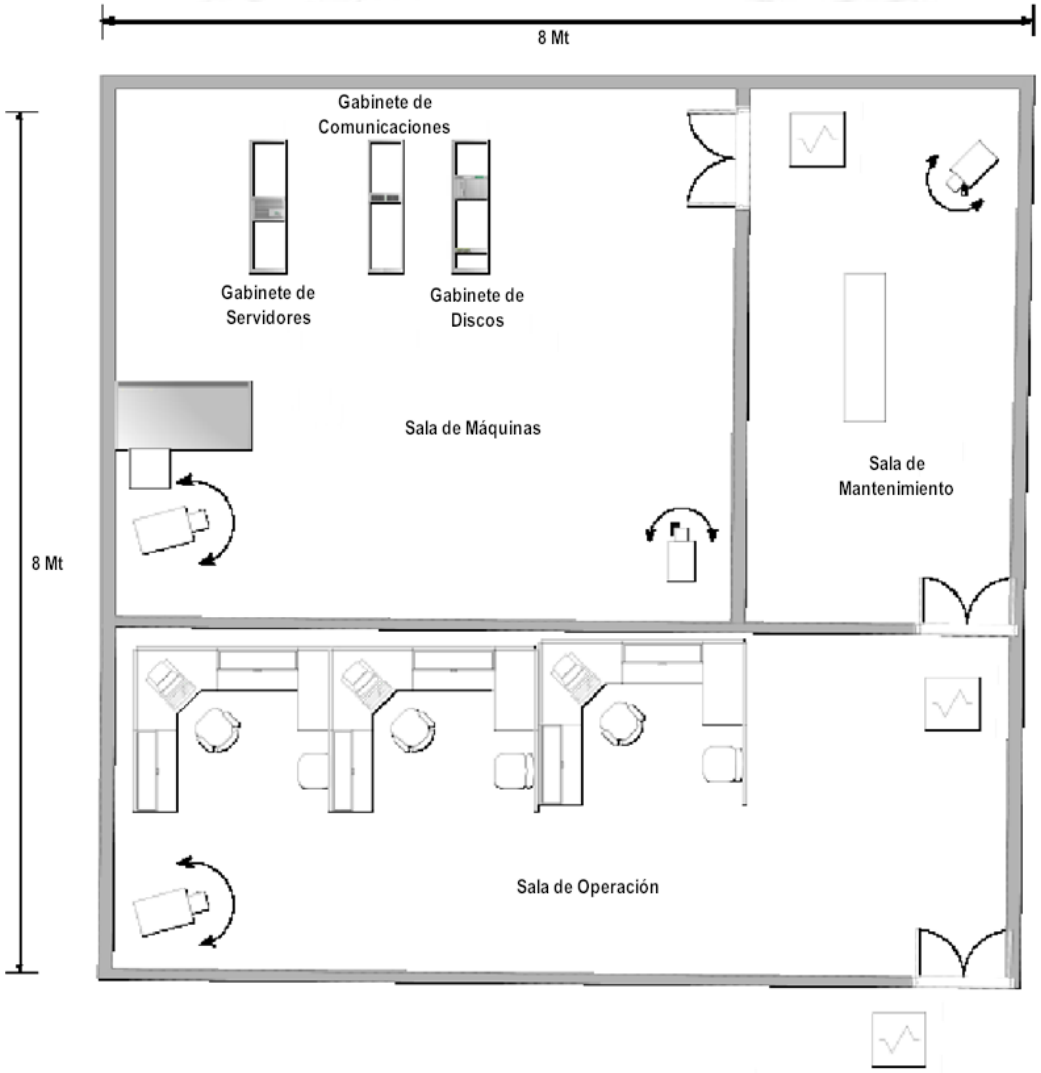
El cableado estructurado deberá ser instalado con una canalización adecuada por el falso piso siguiendo los estándares EIA/TIA 568.

El Centro de computo AERC debe contar con un sistema UPS de 15 KVA con una capacidad de autonomía de 30 minutos como mínimo y un grupo electrógeno con un tablero de control de transferencia automática para garantizar la continuidad del servicio. Se recomienda un aislamiento eléctrico con un pozo de tierra mínimo a 5 Mts de profundidad con una resistividad menor o igual a 3 Ohms.

En la siguiente página se muestra el diseño del centro de cómputo de la AERC.

Figura 6.7

Distribución Física de la AERC



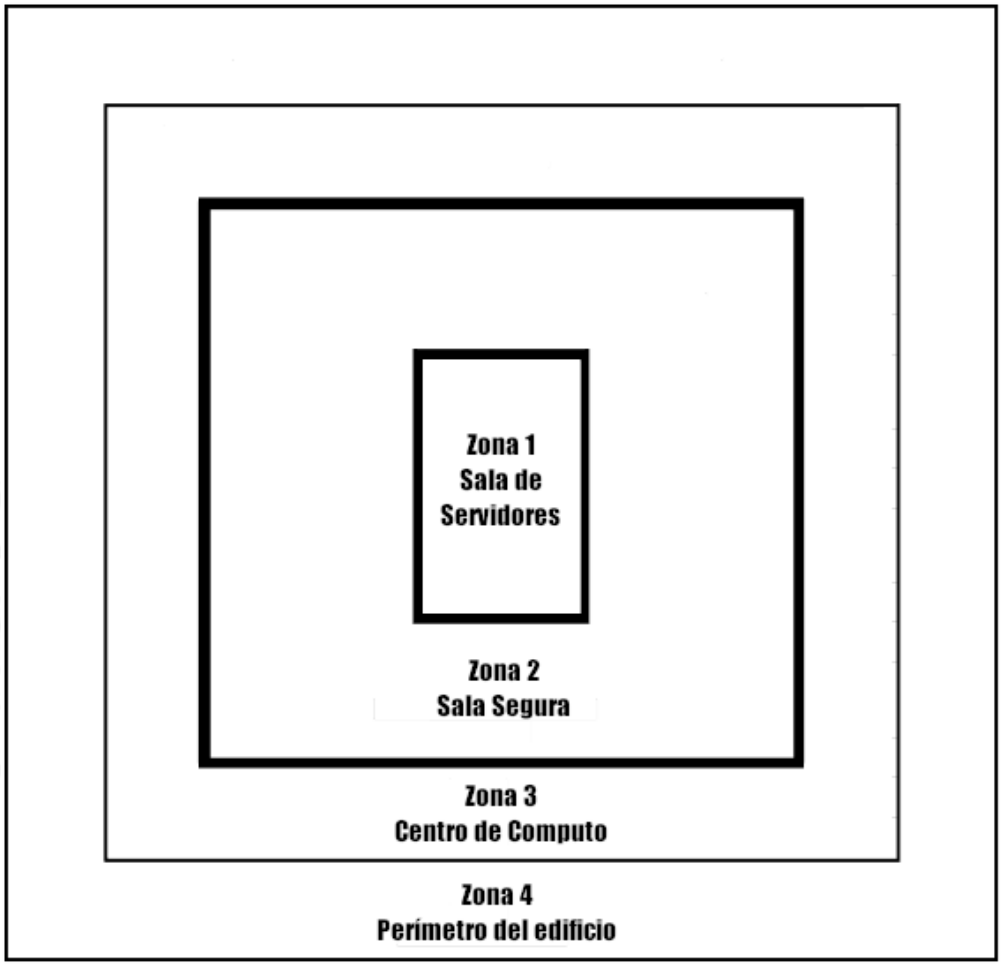
Elaboración propia

Acceso a las Instalaciones:

Se ha considerado 4 zonas de seguridad la cual se explica en el diagrama siguiente:

Figura 6.8

Zonas de seguridad de la AERC



Elaboración propia

Zona 4 que es el perímetro del edificio del local de la RENIEC deberá estar resguardado por un servicio de vigilancia 7X24, control de acceso foto ID y además debe contar con sistemas centralizado de alarmas con detectores de movimiento, circuito cerrado de TV

Zona 3 que corresponde al Centro de cómputo de la RENIEC, deberá tener una seguridad estructural y control acceso Vigilado 7X24.

Zona 2 Sala Segura de la AERC estará limitado solo a aquellos empleados que atienden directamente los requerimientos de los clientes es decir los administradores y

operadores del sistema de Certificación Digital deberá contar con un sistema de acceso biométrico , detector de movimiento circuito cerrado de TV.

Zona 1 Es el área nuclear de la sala segura punto crítico del sistema por lo tanto la seguridad de esta área se debe preservar mediante la implantación de los siguientes mecanismos:

Sistema de control de acceso biométrico.

Sistema cerrado de cámaras de video y detectores de movimiento,

Además, estos cuartos estarán electrónicamente protegidos, requiriendo un mínimo de 2 personas autorizadas presentes para lograr acceso.

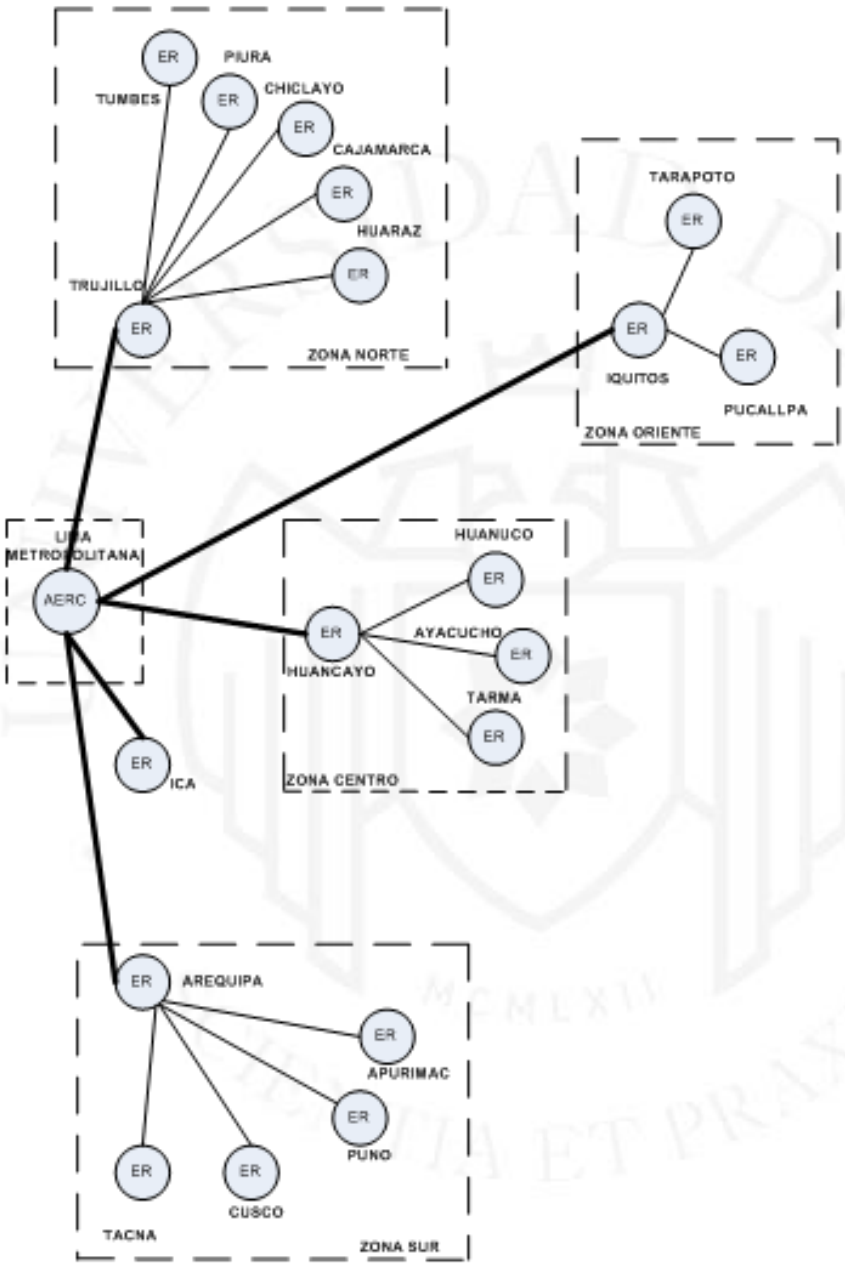
Se ha incluido el dimensionamiento del equipamiento en el Anexo 4 y el dimensionamiento de los servicios de comunicación en el Anexo 5.

6.9.1 Extensión de atención red WAN de la AERC

Se prevé que para la atención al público a nivel nacional, se requiere incorporar Entidades de Registro en las diferentes capitales de departamento y concentrar el trabajo en agrupaciones para de ahí conectarse a la infraestructura central en Lima. A continuación se muestra el Diagrama de la Red WAN interna de la AERC

Figura 6.9

Diagrama de Red WAN de la AERC



Elaboración propia

6.10 Organización

Para la organización se coordinó con ambas instituciones, Indecopi y Reniec para ver en sus cuadros organizativos como podría incorporarse como se muestra a continuación:

Autoridad Administrativa Competente

Para la Organización y Gestión de la Autoridad Administrativa Competente, se ha conversado en varias oportunidades con el interlocutor válido de Indecopi y en forma conjunta hemos elaborado el siguiente esquema organizacional que es como sigue:

6.10.1 Funciones

- **Comisión de Reglamentos Técnicos y Comerciales (CRT).-** Mediante Decreto Supremo Nro. 019-2002-JUS el INDECOPI fue designado como Autoridad Administrativa Competente (AAC) para acreditar entidades de certificación de firmas digitales y entidades de verificación/registro. En sesión de fecha 25 de julio de 2002, el Directorio de INDECOPI designó a su Comisión de Reglamentos Técnicos y Comerciales (CRT) como su representante para cumplir las funciones de la AAC. La CRT (un cuerpo colegiado formado por cinco personas) tiene la responsabilidad de suscribir la resolución administrativa que otorga o deniega la acreditación.

Comité Consultivo.- Organismo externo a la CRT, conformado por representantes de:

- El Organismo Supervisor de la Inversión Privada en Telecomunicaciones – OSIPTEL.
- El Ministerio de Justicia – MINJUS.
- La Presidencia del Consejo de Ministros - PCM.
- Los organismos acreditados (cuando los haya).

  El Comité Consultivo absuelve las consultas que pueda presentarle la CRT. Su opinión no obliga a esta última.

  Nota.- La pertenencia al Comité Consultivo no da derecho a percibir ninguna retribución económica.

- **Secretaría Técnica de la CRT.-** Órgano de enlace entre la CRT y la estructura orgánica de INDECOPI, que presta a la CRT el apoyo necesario para su funcionamiento. Comprende, entre otras, al Área Legal y a la Unidad de Firmas

Digitales. El Secretario Técnico presenta a la CRT el proyecto de resolución que otorga o deniega la acreditación.

Área Legal.- Órgano de la Secretaría Técnica de la CRT que elabora el proyecto de resolución que otorga o deniega la acreditación y lo entrega al Secretario Técnico de la CRT. Se basa en:

- Las conclusiones técnicas elaboradas por el Comité de Acreditación.
- El análisis de las políticas de certificación de la entidad solicitante, su cumplimiento de los requisitos señalados en la Ley de Firmas Digitales, en el Reglamento de Firmas Digitales, en las Disposiciones Complementarias al Reglamento de Firmas Digitales, en las normas legales sobre micro grabación y demás normas pertinentes.

Asimismo, investiga las eventuales infracciones a las normas de acreditación, propone a la CRT el inicio de procedimientos sancionadores, y conduce tales procedimientos.

Nota.- Hoy, dos personas componen el Área Legal de la Secretaría Técnica de la CRT, de las cuales una es un practicante. El Área Legal asiste jurídicamente al Área de Normalización (Normas Técnicas), al Área de Acreditación de Organismos de Evaluación de la Conformidad (cuyo tema es distinto al de Acreditación de Certificadoras de Firmas Digitales), al Área de Restricciones Para-arancelarias y en las consultas y controversias vinculadas a Metrología Legal. Para que el Área Legal pueda prestar asistencia jurídica a la nueva Unidad de Firmas Digitales de la Secretaría Técnica de la CRT sin menoscabar la atención que presta a las demás áreas de la S.T., es imprescindible que por lo menos cuente con una persona adicional. La Gerencia de Administración de INDECOPI podría asignar esta persona a la Secretaría Técnica de la CRT en calidad de Asistente Legal Junior.

- **Comité de Acreditación.-** Órgano técnico que evalúa los resultados del procedimiento de acreditación (incluyendo las auditorías de los evaluadores) y como consecuencia recomienda (o no) a la CRT la acreditación del organismo solicitante.

Nota.- La pertenencia al Comité de Acreditación no da derecho a percibir ninguna retribución económica.

Evaluador.- Persona técnicamente calificada que lleva a cabo auditorías sobre los organismos solicitantes y produce un informe que entrega al Comité de Acreditación.

Nota.- Los honorarios del Evaluador provienen exclusivamente de la entidad que solicita su acreditación.

Unidad de Firmas Digitales.- Organo de la Secretaría Técnica de la CRT que se crearía para conducir los procedimientos de acreditación de entidades de certificación de firmas digitales y de entidades de verificación/registro.

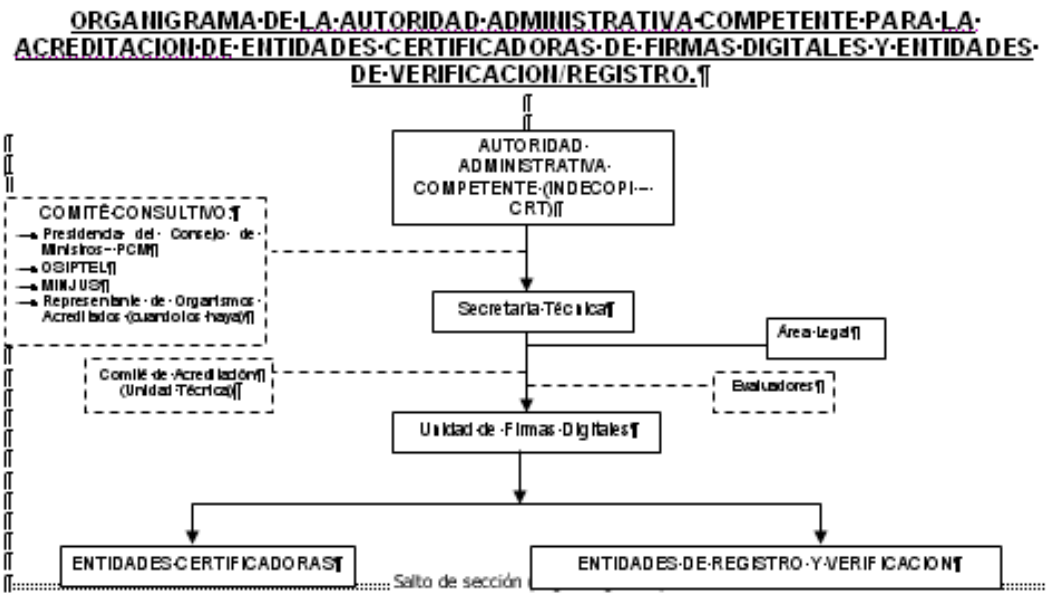
Nota.- Para crear esta unidad al interior de la Secretaría Técnica de la CRT es necesario contratar, por lo menos a tiempo parcial (inicialmente), a un ingeniero especializado en Infraestructura de Clave Pública (PKI). Ninguno de los ingenieros que trabaja actualmente en la Secretaría Técnica de la CRT tiene especialización en PKI. Además, sus jornadas laborales están copadas con las funciones que desempeñan en las Áreas de Normalización, Acreditación de OEC, y Metrología Legal.

6.10.1.1Organigrama Propuesto:

6.10.1.2Estructura organizacional de la AAC

Figura 6.10

Organigrama propuesto de la AAC



Elaboración propia

Autoridad de Emisión y Registro de Certificados

Para la Organización y Gestión de la Autoridad de Emisión y Registro de Certificados del Estado, se ha estimado sin la colaboración de Reniec debido a sus cambios de opiniones sobre su participación en el proyecto que es como sigue:

El estamento central de La Autoridad de Emisión y Registro de Certificados (AERC) del Estado Peruano debe contar para su funcionamiento con el siguiente personal como mínimo: para atender el servicio de certificación digital.

Tabla 6.5
Funciones del personal de la AERC

Puestos	**Funciones**
Jefe de Oficina AERC	• Gestionar y Gerenciar, la Oficina de la Autoridad de Emisión y Registro de Certificados (AERC) del Estado Peruano. • Representar a la RENIEC ante la Autoridad Administrativa Competente.
Secretaria	• Cumplir con las funciones administrativas, control , Archivo y trámite documentario en apoyo al Jefe de Oficina y Personal técnico
Administrador de Certificados digitales	• Reporta al Jefe de Oficina, • Coordinar con las autoridades de Certificación y Registro dentro del Dominio de la AERC • Firmar los Certificados , Revocar los certificados • Publica los Certificados y las listas de Certificados Revocados en el directorio LDAP • Es el responsable de la seguridad de la clave Privada de la Entidad Certificadora Raíz. • Es una de las personas que tiene acceso a la Sala segura. La otra será designada por el Jefe de Oficina. • Lleva el control estadístico de certificados y revocaciones. • Apoya al Administrador del Sistema PKI,
Administrador de Sistemas PKI y BD.	• Gestión del sistema PKI, a través de la consola Principal. • Controla los Cambios y configuraciones, realiza afinamiento para optimizar el sistema, • Realiza el mantenimiento preventivo y correctivo del sistema • Administra la Base de datos LDAP, realiza los respaldos programados a la Base de datos. • Revisa y verifica las incidencias del sistema de seguridad y toma las acciones preventivas y correctivas. • Lleva el control de las incidencias y documenta la solución.

(continúa)

(continuación)

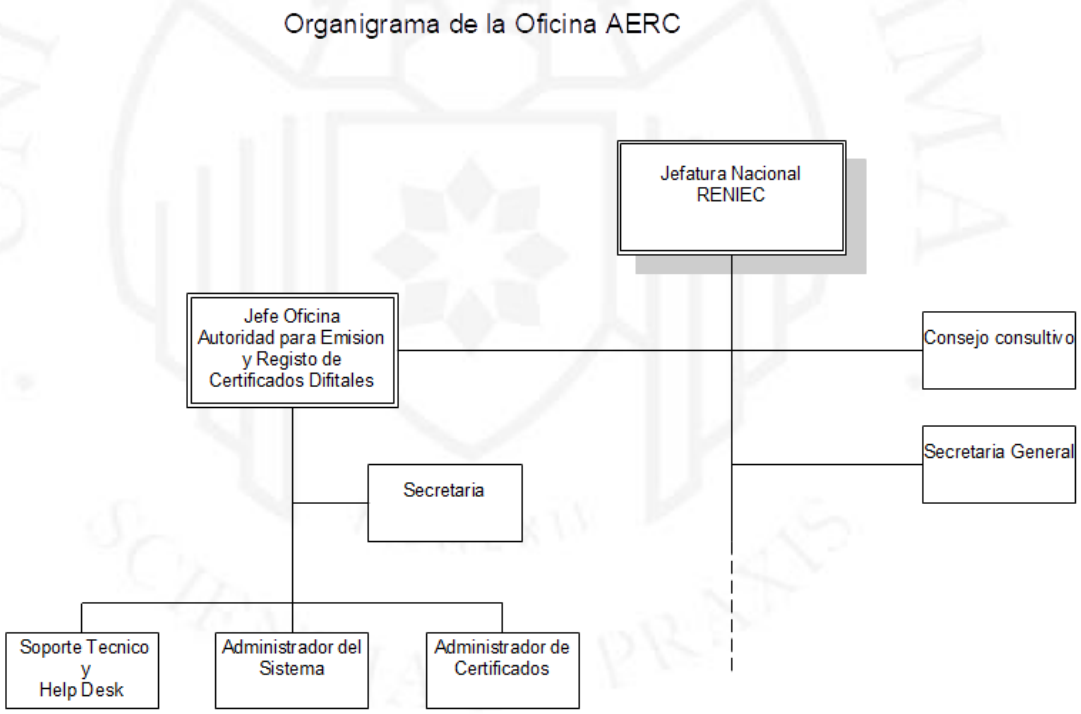
Especialista de soporte técnico y Help Desk	• Atención de incidencias y problemas de Comunicaciones , • Diagnostica y resuelve los problemas de enlace, y la Red TCP/IP. • Apoya a los Operadores en la asistencia remota a los usuarios del sistema • Lleva el control de incidencias, y documenta la solución.
Operadores	• Atienden el proceso de registro, verificación y validación de las solicitudes de certificados digitales para la firma de la autoridad de Certificación. Coordina con el supervisor de la oficina

Elaboración propia

6.10.1.3Estructura organizacional de la AERC.

Figura 6.11

Organigrama propuesto de la AERC



Elaboración propia

Perfil del personal para cubrir los roles definidos para la AERC

Tabla 6.6

Perfil personal de los roles para la AERC

Descripción de Puesto	Cantidad	Perfil
Jefe de la Oficina AERC	1	Título Profesional en Ingeniería de Sistemas, Industrial o Electrónica 05 Años de Experiencia en administración y Gestión de Tecnologías de Información. Especialización en seguridad de Tecnologías de Información. Deseable Inglés Escrito y Hablado
Secretaria	1	Certificado de Institución de prestigio Experiencia y buen conocimiento de Windows OFFICE y correo electrónico.
Administrador de Certificados digitales	1	Titulo Profesional en Ingeniería de Sistemas o electrónica. 03 años de experiencia en seguridad de Tecnologías de Información. Especialización en Sistema PKI Certificación en Administración de Sistemas UNIX o Linux
Administradores de Sistemas PKI y BD.	1	Bachiller en Ingeniería de Sistemas o electrónica. 03 años de experiencia en seguridad de Tecnologías de Información en Ambientes UNIX. Especialización en Sistema PKI Certificación en Administración de Sistemas UNIX o Linux... Certificación en Administración de BD
Especialista de soporte técnico y Help Desk	1	Bachiller en Ingeniería de Sistemas , electrónica o carreras afines: 03 años de experiencia en soporte y administración de Redes TCP/IP. Conocimiento de Sistemas PKI. Amplio conocimiento de Protocolos LAN, WAN,VPN, IPSEC. Protocolos de Enrutamiento RIP, EIGRP, BGP. Conocimiento en configuración y soporte de Firewalls
Operadores (*)	10	Bachiller en Ingeniería de Sistemas, o Instituto Tecnológico de Prestigio. 01 año de Experiencia en ambientes Unix . Buen conocimiento en scripts Unix, Conocimiento sobre Procesos en Batch, Backup y Restore.

(*) De acuerdo a necesidad del servicio
Elaboración propia

Los administradores y los especialistas deberán cumplir con los perfiles del puesto y estar debidamente entrenados para operar y administrar el servicio.

6.11 Procesos

Se vieron varios procesos para la emisión y verificación de certificados, así como para su uso, estos se pueden apreciar en el Anexo 8

6.12 Evaluación financiera

La evaluación financiera se realizó haciéndolo de acuerdo a la metodología de costo-beneficio, la cual evalúa el impacto con el proyecto y sin el proyecto.

A continuación se muestra primero el cuadro de parámetros que se han tomado para realizar la evaluación, luego los cuadros de presupuestos de inversión, de costos de operación, ingresos, gastos financieros, flujo de caja, fuljo de beneficios y costos, costo – beneficio, sensibilidad del VAN con costo de inversión y con tarifa de producto 2 y sostenibilidad financiera.

6.12.1 Cuadro de Parámetros:

Tabla 6.7

Parámetros de evaluación financiera

Costos de Inversión de la AAC

Sub-Ítem	Nombre del Bien o Servicio Conexo	Breve descripción	Cantidad	Costo Unit. US$	Valor Referencial US $
Hardware					
1	Servidores de Oper.	Servidores Intel de 32 bits	3	4,760.00	14,280.00
2	Servidores de Publicación	Servidores de 64 bits	2	11,900.00	23,800.00
3	Firewalls	Firewall Appliances	2	17,850.00	35,700.00
4	Routers	Routers	2	1,487.50	2,975.00
5	Switches Administrables	Switches Administrables	2	2,082.50	4,165.00
6	Dispositivo de Almacenamiento Externo	Dispositivo de Almacenamiento Externo incluyendo 4 tarjetas FC para servidores	1	45,220.00	45,220.00
7	Dispositivos de Back-Up Externo	Dispositivos de Back-Up Externo incluyendo Cartuchos de Datos y de limpieza	1	2,975.00	2,975.00
8	Cableado	Cableado Categoría 5e	12	23.80	285.60
TOTAL Hardware					129,400.60
Software					
9	Software de PKI	Software de PKI	1	35,700.00	35,700.00
10	Software de Directorio LDAP	Software de Directorio LDAP	Lic. para 1000 Entradas	1.19	1,190.00
11	Software de Administración de Seguridad	Software de Administración de Seguridad	Lic. para 4 Servidores	2,499.00	22,491.00
12	Software de Back-Up	Software de Back-Up	Lic. para 4 Servidores	1,190.00	10,710.00
13	Sistemas Operativos	Sistemas Operativos	5	1,487.50	7,437.50
TOTAL Software					77,528.50
Adecuación					
19	Servicio de Implantación	Servicio de Implantación	1	21,240.00	21,240.00
21	Cableado de Fibra Óptica	Cableado de Fibra Óptica	4	59.50	238.00
22	Racks de 42 U	Racks de 42 U	1	1,785.00	1,785.00
23	UPS de 15 KVA	UPS de 10 KVA	1	11,900.00	11,900.00
24	Adecuación ambiente de Seguridad	Adecuación ambiente de Seguridad	1	35,700.00	35,700.00
TOTAL Adecuación					70,863.00
TOTAL de la Inversión					277,792.10

(continúa)

(continuación)
Costos de Inversión de la AERC

Sub-Ítem	Nombre del Bien o Servicio Conexo	Breve descripción	Cantidad	Costo Unit. US$	Valor Referencial US $
Hardware					
1	Servidores de Operación	Servidores Intel de 32 bits	7	4,760.00	33,320.00
2	Servidores de Publicación	Servidores de 64 bits	3	11,900.00	35,700.00
3	Switch de Fibre Channel	Switch de Fibre Channel	2	17,850.00	35,700.00
4	Firewalls	Firewall Appliances	2	17,850.00	35,700.00
5	Routers	Routers	2	1,487.50	2,975.00
6	Switches Administrables	Switches Administrables	2	2,082.50	4,165.00
7	Dispositivo de Almacenamiento Externo	Dispositivo de Almacenamiento Externo incluyendo 4 tarjetas FC para servidores	1	57,120.00	57,120.00
8	Dispositivos de Back-Up Externo	Dispositivos de Back-Up Externo incluyendo Cartuchos de Datos y de limpieza	1	14,875.00	14,875.00
9	Módulo de Seguridad Física de Clave Privada Raíz	Módulo de Seguridad Física de Clave Privada Raíz	2	10,710.00	21,420.00
10	Impresora de Tarjetas SmartCards	Impresora de Tarjetas SmartCards	3	2,380.00	7,140.00
11	Equipamiento Sucursales	PCs y Equipos de Comunicación			298,720.00
12	Estaciones de Trabajo	Estaciones de Trabajo	20	1,190.00	23,800.00
TOTAL Hardware					570,635.00
Software					
12	Software de PKI	Software de PKI	1	35,700.00	35,700.00
13	Software de Directorio LDAP	Software de Directorio LDAP	1	1,190.00	1,190.00
14	Software de Administración de Seguridad	Software de Administración de Seguridad	20	2,499.00	49,980.00
15	Software de Back-Up	Software de Back-Up	10	1,190.00	11,900.00
16	Sistemas Operativos	Sistemas Operativos	9	1,785.00	16,065.00
17	Software de Impresión de Smartcards	Software de Impresión de Smartcards	3	1,190.00	3,570.00
18	Kit de desarrollo para Smartcards	Kit de desarrollo para Smartcards	1	5,355.00	5,355.00
TOTAL Software					123,760.00
Adecuación					
19	Servicio de Implantación	Servicio de Implantación	1	42,480.00	42,480.00
20	Cableado Estructurado Cat. 5	Cableado Estructurado Cat. 5	40	35.70	1,428.00
21	Cableado de Fibra Óptica	Cableado de Fibra Óptica	20	59.50	1,190.00

(continúa)

(continuación)

Costos de Inversión de la AERC

Sub-Ítem	Nombre del Bien o Servicio Conexo	Breve descripción	Cantidad	Costo Unit. US$	Valor Referencial US $
22	Racks de 42 U	Racks de 42 U	3	1,785.00	5,355.00
					(continúa)
23	UPS de 15 KVA	UPS de 15 KVA	1	17,850.00	17,850.00
24	Adecuación ambiente de Seguridad	Adecuación ambiente de Seguridad	1	35,700.00	35,700.00
	TOTAL Adecuación				104,003.00
	TOTAL de la Inversión				798,398.00

Elaboración propia

Organización AAC	No	Sueldos	Total
Secretario Técnico	1	$ 4,000.00	$ 4,000.00
Asesor Legal	1	$ 3,000.00	$ 3,000.00
Unidad de Certificados Digitales	1	$ 2,000.00	$ 2,000.00
Asistente Legal Junior	1	$ 1,000.00	$ 1,000.00
Asistente	1	$ 500.00	$ 500.00
TOTAL	5		$ 10,500.00

Elaboración propia

Organización AERC	No	Sueldos	Total
Gerente	1	$ 4,000.00	$ 4,000.00
Soporte Técnico	1	$ 2,000.00	$ 2,000.00
Administrador del Sistema	1	$ 2,500.00	$ 2,500.00
Especialista en Tecnología PKI	1	$ 2,500.00	$ 2,500.00
Secretaria	1	$ 500.00	$ 500.00
Operadores Registrales	9	$ 1,000.00	$ 9,000.00
Supervisor de Operadores	1	$ 2,000.00	$ 2,000.00
Registradores Operativos	10	$ 1,200.00	$ 12,000.00
TOTAL	15		$ 34,500.00

Elaboración propia

Organización ECREP	No	Sueldos	Total
Secretario Técnico	1	$ 4,000.00	$ 4,000.00
Asesor Legal	1	$ 3,000.00	$ 3,000.00
Unidad de Certificados Digitales	1	$ 2,000.00	$ 2,000.00
Asistente Legal Junior	1	$ 1,000.00	$ 1,000.00
Asistente	1	$ 500.00	$ 500.00
TOTAL	5		$ 10,500.00

Elaboración propia

Otros parámetros	No	Costo Unit.	Total
Línea de Comunicación de 2 Mb		$ 1,500.00	Mensual
Líneas de Comunicación de AERC		$ -	Mensual
Consumo Energía mes AAC	10,800	$ 1,101.60	$ 0.10
Consumo Energía mes AERC	144,000	$ 14,688.00	$ 0.10
Consumo Energía mes ECREP	10,800	$ 1,101.60	$ 0.10

Servicio de Seguridad Externa AAC	$ 3,000.00	
Servicio de Seguridad Externa AERC	$ 12,000.00	
Servicio de Seguridad Externa ECREP	$ 3,000.00	
Trámite Administrativo de Acreditación	$ 1,000.00	
Porcentaje Ley de Entidades Privadas por supervisión	0.80%	
Tasa anual de Perdida de Certificados el primer año	10.00%	
Tasa anual de Perdida de Certificados el segundo año	8.00%	
Servicios de Verificación vendidos por Reniec al año	1,000,000	
Precio de Venta del Certificado Digital	$ 1.52	
Servicio de Acreditación AAC	$ 20,000.00	
Servicio de Acreditación AERC	$ 10,000.00	
Precio de Emisión de Certificado Raíz AAC	$ 5,000.00	
Precio de Emisión de Certificado Raíz AERC	$ 2,500.00	
Costo de la consulta de verificación en línea de Reniec	$ 1.00	
Supervisión de la ECREP en % de Facturación	0.80%	
Certificados Emitidos por Entidades Estatales fuera de Reniec	2,500,000	
Primer préstamo BID para la AAC	$ 230,000	
Primer préstamo BID para la AERC	$ 570,000	
Tasa de Interés primer préstamo BID	6.00%	
Periodos del préstamo	20	
Costo de Personal de Sucursales	2,940,000	anual
Costo enlaces de comunicación	-	anual

Elaboración propia

Intangibles

Descripción		Monto
Evaluación de Marco Normativo	**$**	**42,000.00**
Estudio Definitivo (Bases AAC)	**$**	**4,000.00**
Estudio Definitivo (Bases AERC)	**$**	**4,000.00**
Total Intangibles	**$**	**50,000.00**

Elaboración propia

- Acción MF.2.1.1. Programas de Difusión de la seguridad ofrecida por la tecnología de Certificados Digitales $300,000
- Acción MF.2.1.2. Programas de Difusión de la oferta de servicios públicos en línea utilizando certificados digitales
- Acción MF.2.2.1. Programas de capacitación al personal de las entidades estatales sobre la tecnología de Certificados Digitales $200,000
- Acción MF.2.2.2. Programas de capacitación al personal de las entidades estatales para la mejor prestación de servicios públicos en línea seguros, empleando Certificados Digitales

Elaboración propia

6.12.2 Presupuesto de Inversión

Tabla 6.8

Presupuesto de Inversión

Inversión AAC en US$	**Año 0** **2005**	**Año 1** **2006**	**Año 2** **2007**	**Año 3** **2008**	**Año 4** **2009**	**Año 5** **2010**	**Año 6** **2011**	**Año 7** **2012**	**Año 8** **2013**	**Año 9** **2014**	**Año 10** **2015**
Hardware	129,401			135,871			142,664			142,664	
Software	77,529			81,405			85,475			85,475	
Adecuación	70,863			14,173			14,173			14,173	
Ampliaciones de Hardware			6,470			6,794					
Ampliaciones de Software			3,876			4,070					
Inversión Total AAC	**277,792**	**-**	**10,346**	**231,448**	**-**	**10,864**	**242,312**	**-**	**-**	**242,312**	**-**
Depreciación de Hardware		32,350	32,350	33,968	67,935	35,585	37,284	71,332	37,364	37,364	71,332
Depreciación de Software		25,840	25,840	27,132	28,424	28,424	28,489	29,845	29,845	28,489	28,489
Depreciación de Adecuación		7,086	7,086	7,086	7,086	7,086	7,086	7,086	7,086	7,086	7,086
Depreciación Total AAC		**65,277**	**65,277**	**68,186**	**103,446**	**71,096**	**72,859**	**108,264**	**74,296**	**72,940**	**106,907**
Mantenimiento de HW		12,940	12,940		13,587	13,587		14,266	14,266		14,266
Mantenimiento de SW		15,506	15,506		16,281	16,281		17,095	17,095		17,095
Mantenimiento de Adecuación		14,173	14,173		14,173	14,173		14,173	14,173		14,173
Gasto de Manto. Total AAC	**-**	**42,618**	**42,618**	**-**	**44,041**	**44,041**	**-**	**45,534**	**45,534**	**-**	**45,534**

(continúa)

(continuación)

Inversión AERC en US$	**Año 0**	**Año 1**	**Año 2**	**Año 3**	**Año 4**	**Año 5**	**Año 6**	**Año 7**	**Año 8**	**Año 9**	**Año 10**
INVERSION AERC	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**
Hardware	570,635			599,167			629,125			629,125	
Software	123,760			129,948			136,445			136,445	
Adecuación	104,003			20,801			20,801			20,801	
Ampliaciones de Hardware			28,532			29,958					
Ampliaciones de Software			6,188			6,497					
Inversión Total AERC	**798,398**	**-**	**34,720**	**749,915**	**-**	**36,456**	**786,371**	**-**	**-**	**786,371**	**-**
Depreciación de Hardware		142,659	142,659	149,792	299,583	156,925	164,414	314,563	164,771	164,771	314,563
Depreciación de Software		41,249	41,249	43,312	45,374	45,374	45,477	47,643	47,643	45,477	45,477
Depreciación de Adecuación		10,400	10,400	10,400	10,400	10,400	10,400	10,400	10,400	10,400	10,400
Depreciación Total AERC		**194,308**	**194,308**	**203,504**	**355,358**	**212,699**	**220,292**	**372,606**	**222,814**	**220,648**	**370,440**
Mantenimiento de HW		57,064	57,064		59,917	59,917		62,913	62,913		62,913
Mantenimiento de SW		24,752	24,752		25,990	25,990		27,289	27,289		27,289
Mantenimiento de Adecuación		20,801	20,801		20,801	20,801		20,801	20,801		20,801
Gasto Manto. Total AERC	**-**	**102,616**	**102,616**	**-**	**106,707**	**106,707**	**-**	**111,002**	**111,002**	**-**	**111,002**

(continúa)

(continuación)

Inversión Total Alternativa1 en US$	**Año 0 2005**	**Año 1 2006**	**Año 2 2007**	**Año 3 2008**	**Año 4 2009**	**Año 5 2010**	**Año 6 2011**	**Año 7 2012**	**Año 8 2013**	**Año 9 2014**	**Año 10 2015**
Hardware	700,036	-	-	735,037	-	-	771,789	-	-	771,789	-
Software	201,289	-	-	211,353	-	-	221,921	-	-	221,921	-
Adecuación	174,866	-	-	34,973	-	-	34,973	-	-	34,973	-
Ampliaciones de Hardware	-	-	35,002	-	-	36,752	-	-	-	-	-
Ampliaciones de Software	-	-	10,064	-	-	10,568	-	-	-	-	-
Inversión Total	**1,076,190**	**-**	**45,066**	**981,364**	**-**	**47,320**	**1,028,683**	**-**	**-**	**1,028,683**	**-**
Depreciación de Hardware	-	175,009	175,009	183,759	367,519	192,510	201,698	385,895	202,135	202,135	385,895
Depreciación de Software	-	67,089	67,089	70,444	73,798	73,798	73,966	77,488	77,488	73,966	73,966
Depreciación de Adecuación	-	17,487	17,487	17,487	17,487	17,487	17,487	17,487	17,487	17,487	17,487
Depreciación Total	**-**	**259,585**	**259,585**	**271,690**	**458,804**	**283,795**	**293,150**	**480,870**	**297,110**	**293,588**	**477,347**
Mantenimiento de HW	-	70,004	70,004	-	73,504	73,504	-	77,179	77,179	-	77,179
Mantenimiento de SW	-	40,258	40,258	-	42,271	42,271	-	44,384	44,384	-	44,384
Mantenimiento de Adecuación	-	34,973	34,973	-	34,973	34,973	-	34,973	34,973	-	34,973
Gasto de Manto. Total	**-**	**145,234**	**145,234**	**-**	**150,748**	**150,748**	**-**	**156,536**	**156,536**	**-**	**156,536**

Elaboración propia

6.12.3 Presupuesto de Costos de Operación

Tabla 6.9

Presupuesto Costos de Operación

Costos de Operación en US$	Año 0 2005	Año 1 2006	Año 2 2007	Año 3 2008	Año 4 2009	Año 5 2010	Año 6 2011	Año 7 2012	Año 8 2013	Año 9 2014	Año 10 2015
AAC											
Mano de Obra	73,500	147,000	147,000	147,000	147,000	147,000	147,000	147,000	147,000	147,000	147,000
Línea de Comunicación	9,000	18,000	18,000	18,000	18,000	18,000	18,000	18,000	18,000	18,000	18,000
Energía Eléctrica	6,610	13,219	13,219	13,219	13,219	13,219	13,219	13,219	13,219	13,219	13,219
Servicios de Seguridad Externa	18,000	36,000	36,000	36,000	36,000	36,000	36,000	36,000	36,000	36,000	36,000
Total AAC	**107,110**	**214,219**	**214,219**	**214,219**	**214,219**	**214,219**	**214,219**	**214,219**	**214,219**	**214,219**	**214,219**
AERC											
Mano de Obra	1,711,500	3,423,000	3,423,000	3,423,000	3,423,000	3,423,000	3,423,000	3,423,000	3,423,000	3,423,000	3,423,000
Línea de Comunicación	-	-	-	-	-	-	-	-	-	-	-
Energía Eléctrica	88,128	176,256	176,256	176,256	176,256	176,256	176,256	176,256	176,256	176,256	176,256
Servicios de Seguridad Externa	72,000	144,000	144,000	144,000	144,000	144,000	144,000	144,000	144,000	144,000	144,000
Pago de Supervisión AAC	-	56,720	110,304	21,779	64,502	154,080	13,024	60,611	154,080	8,160	56,720
Total AERC	**1,871,628**	**3,799,976**	**3,853,560**	**3,765,035**	**3,807,758**	**3,897,336**	**3,756,280**	**3,803,867**	**3,897,336**	**3,751,416**	**3,799,976**
Total Alternativa 1	**1,978,738**	**4,014,195**	**4,067,779**	**3,979,254**	**4,021,978**	**4,111,555**	**3,970,499**	**4,018,086**	**4,111,555**	**3,965,635**	**4,014,195**

Elaboración propia

6.12.4 Presupuesto del Plan de Producción

Tabla 6.10

Presupuesto del Plan de Producción

Plan de Producción	Año 0 2005	Año 1 2006	Año 2 2007	Año 3 2008	Año 4 2009	Año 5 2010	Año 6 2011	Año 7 2012	Año 8 2013	Año 9 2014	Año 10 2015
AAC											
Acreditaciones	-	3	4	3	3	4	3	3	4	3	3
Supervisiones	-	-	3	7	10	10	10	10	10	10	10
Emisión de Certificados Raíz	-	2	3	2	2	3	2	2	3	2	2
Servicios de Valor añadido	-	-	-	-	-	-	-	-	-	-	-
AERC											
Emisión de Certificados Digitales Nuevos	-	4,000,000	8,000,000	-	-	4,000,000	-	-	-	-	-
Renovación de Certificados por perdida primer año	-	-	400,000	800,000	-	-	400,000	-	-	-	-
Renovación de Certificados por perdida Segundo año	-	-	-	320,000	640,000	-	-	320,000	-	-	-
Renovación de Certificados por Expiración	-	-	-	-	4,000,000	8,000,000	-	4,000,000	12,000,000	-	4,000,000
Total Emisión de Certificados	**-**	**4,000,000**	**8,400,000**	**1,120,000**	**4,640,000**	**12,000,000**	**400,000**	**4,320,000**	**12,000,000**	**-**	**4,000,000**
Servicios en Línea para Verificación	-	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000
Emisión de Certificados Raíz	-	2	4	4	2	4	4	2	4	4	2
Servicios de Valor añadido	-	-	-	-	-	-	-	-	-	-	-
Plan de Producción Alternativa 1											
Total Emisión de Certificados	**-**	**4,000,000**	**8,400,000**	**1,120,000**	**4,640,000**	**12,000,000**	**400,000**	**4,320,000**	**12,000,000**	**-**	**4,000,000**

Elaboración propia

6.12.5 Presupuesto de Ingresos

Tabla 6.11

Presupuesto de Ingresos

Ingresos en US$	Año 0 2005	Año 1 2006	Año 2 2007	Año 3 2008	Año 4 2009	Año 5 2010	Año 6 2011	Año 7 2012	Año 8 2013	Año 9 2014	Año 10 2015
AAC											
Ventas de Servicios de Acreditación	-	60,000	80,000	60,000	60,000	80,000	60,000	60,000	80,000	60,000	60,000
Trámite Administrativo	-	3,000	4,000	3,000	3,000	4,000	3,000	3,000	4,000	3,000	3,000
Ingresos por supervisión	-	56,720	110,304	21,779	64,502	154,080	13,024	60,611	154,080	8,160	56,720
Emisión de Certificados Raíz	-	10,000	15,000	10,000	10,000	15,000	10,000	10,000	15,000	10,000	10,000
Venta de Servicios de Valor Añadido	-	-	-	-	-	-	-	-	-	-	-
Total Ingresos	**-**	**129,720**	**209,304**	**94,779**	**137,502**	**253,080**	**86,024**	**133,611**	**253,080**	**81,160**	**129,720**
AERC											
Venta de Certificados Digitales	-	6,080,000	12,768,000	1,702,400	7,052,800	18,240,000	608,000	6,566,400	18,240,000	-	6,080,000
Venta de Servicio en Línea para Verificación	-	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000
Venta de Certificados Raíz	-	10,000	20,000	20,000	10,000	20,000	20,000	10,000	20,000	20,000	10,000
Venta de Servicios de Valor Añadido	-	-	-	-	-	-	-	-	-	-	-
Total Ingresos	**-**	**7,090,000**	**13,788,000**	**2,722,400**	**8,062,800**	**19,260,000**	**1,628,000**	**7,576,400**	**19,260,000**	**1,020,000**	**7,090,000**
Ingresos Totales Alternativa 1											
Total Ingresos	**-**	**7,219,720**	**13,997,304**	**2,817,179**	**8,200,302**	**19,513,080**	**1,714,024**	**7,710,011**	**19,513,080**	**1,101,160**	**7,219,720**

Elaboración propia

6.12.6 Presupuesto de Gastos Financieros

Tabla 6.12

Presupuesto de Gastos financieros

Gastos Financieros	Año 0 2005	Año 1 2006	Año 2 2007	Año 3 2008	Año 4 2009	Año 5 2010	Año 6 2011	Año 7 2012	Año 8 2013	Año 9 2014	Año 10 2015
AAC											
Préstamo	230,000	-	-	-	-	-	-	-	-	-	-
Amortización	-	23,000	23,000	23,000	23,000	23,000	23,000	23,000	23,000	23,000	23,000
Deuda	230,000	207,000	184,000	161,000	138,000	115,000	92,000	69,000	46,000	23,000	-
Intereses	13,800	12,420	11,040	9,660	8,280	6,900	5,520	4,140	2,760	1,380	-
AERC											
Préstamo	570,000	-	-	-	-	-	-	-	-	-	-
Amortización	-	57,000	57,000	57,000	57,000	57,000	57,000	57,000	57,000	57,000	57,000
Deuda	570,000	513,000	456,000	399,000	342,000	285,000	228,000	171,000	114,000	57,000	-
Intereses	34,200	30,780	27,360	23,940	20,520	17,100	13,680	10,260	6,840	3,420	-
Gastos Financieros de Alternativa 1											
Préstamo	800,000	-	-	-	-	-	-	-	-	-	-
Amortización	-	80,000	80,000	80,000	80,000	80,000	80,000.0	80,000	80,000	80,000	80,000
Deuda	800,000	720,000	640,000	560,000	480,000	400,000	320,000	240,000	160,000	80,000	-
Intereses	48,000	43,200	38,400	33,600	28,800	24,000	19,200	14,400	9,600	4,800	-

Elaboración propia

6.12.7 Presupuesto de Flujo de Caja

Tabla 6.13

Presupuesto de Flujo de Caja

Alternativa 1 AAC	**Año 0 2005**	**Año 1 2006**	**Año 2 2007**	**Año 3 2008**	**Año 4 2009**	**Año 5 2010**	**Año 6 2011**	**Año 7 2012**	**Año 8 2013**	**Año 9 2014**	**Año 10 2015**
Ingresos											
Préstamo BID	230,000										
Otros Prestamos de Inversión											
Prestamos de Corto Plazo											
Ventas de Servicios de											
Acreditación	-	60,000	80,000	60,000	60,000	80,000	60,000	60,000	80,000	60,000	60,000
Trámite Administrativo	-	3,000	4,000	3,000	3,000	4,000	3,000	3,000	4,000	3,000	3,000
Ingresos por supervisión	-	56,720	110,304	21,779	64,502	154,080	13,024	60,611	154,080	8,160	56,720
Emisión de Certificados Raíz	-	10,000	15,000	10,000	10,000	15,000	10,000	10,000	15,000	10,000	10,000
Venta de Servicios de Valor Añadido	-	-	-	-	-	-	-	-	-	-	-
Total Ingresos	**230,000**	**129,720**	**209,304**	**94,779**	**137,502**	**253,080**	**86,024**	**133,611**	**253,080**	**81,160**	**129,720**
Egresos											
Infraestructura	277,792	-	10,346	231,448	-	10,864	242,312	-	-	242,312	-
Costos de Operación	107,110	214,219	214,219	214,219	214,219	214,219	214,219	214,219	214,219	214,219	214,219
Amortización	-	23,000	23,000	23,000	23,000	23,000	23,000	23,000	23,000	23,000	23,000
Costo Financiero	13,800	12,420	11,040	9,660	8,280	6,900	5,520	4,140	2,760	1,380	-
Costos de Capacitación y Entrenamiento											
Costos de Promoción y Difusión											
Total Egresos	**398,702**	**249,639**	**258,606**	**478,327**	**245,499**	**254,983**	**485,051**	**241,359**	**239,979**	**480,911**	**237,219**
Saldo del Ejercicio	**(168,702)**	**(119,919)**	**(49,302)**	**(383,548)**	**(107,997)**	**(1,903)**	**(399,027)**	**(107,748)**	**13,101**	**(399,751)**	**(107,499)**
Saldo Acumulado	**(168,702)**	**(288,621)**	**(337,923)**	**(721,471)**	**(829,468)**	**(831,370)**	**(1,230,398)**	**(1,338,146)**	**(1,325,045)**	**(1,724,796)**	**(1,832,295)**

Elaboración propia

Alternativa 1 AERC	**Año 0 2005**	**Año 1 2006**	**Año 2 2007**	**Año 3 2008**	**Año 4 2009**	**Año 5 2010**	**Año 6 2011**	**Año 7 2012**	**Año 8 2013**	**Año 9 2014**	**Año 10 2015**
Ingresos											
Préstamo BID	570,000										
Otros Préstamos de Inv.											
Prestamos de Corto Plazo											
Ventas de Certificados Digitales	-	6,080,000	12,768,000	1,702,400	7,052,800	18,240,000	608,000	6,566,400	18,240,000	-	6,080,000
Venta de Servicio en Línea para Verificación	-	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000
Venta de Certificados Raíz	-	10,000	20,000	20,000	10,000	20,000	20,000	10,000	20,000	20,000	10,000
Venta de Servicios de Valor Añadido	-	-	-	-	-	-	-	-	-	-	-
Total Ingresos	**570,000**	**7,090,000**	**13,788,000**	**2,722,400**	**8,062,800**	**19,260,000**	**1,628,000**	**7,576,400**	**19,260,000**	**1,020,000**	**7,090,000**
Egresos											
Infraestructura	798,398	-	34,720	749,915	-	36,456	786,371	-	-	786,371	-
Costos de Operación	1,871,628	3,799,976	3,853,560	3,765,035	3,807,758	3,897,336	3,756,280	3,803,867	3,897,336	3,751,416	3,799,976
Amortización	-	57,000	57,000	57,000	57,000	57,000	57,000	57,000	57,000	57,000	57,000
Costo Financiero	34,200	30,780	27,360	23,940	20,520	17,100	13,680	10,260	6,840	3,420	-
Costos de Capacitación y Entrenamiento											
Costos de Promoción y Difusión											
Total Egresos	**2,704,226**	**3,887,756**	**3,972,640**	**4,595,891**	**3,885,278**	**4,007,892**	**4,613,331**	**3,871,127**	**3,961,176**	**4,598,207**	**3,856,976**
Saldo del Ejercicio	**(2,134,226)**	**3,202,244**	**9,815,360**	**(1,873,491)**	**4,177,522**	**15,252,108**	**(2,985,331)**	**3,705,273**	**15,298,824**	**(3,578,207)**	**3,233,024**
Saldo Acumulado	**(2,134,226)**	**1,068,018**	**10,883,378**	**9,009,888**	**13,187,409**	**28,439,518**	**25,454,186**	**29,159,459**	**44,458,283**	**40,880,076**	**44,113,100**

Elaboración propia

Alternativa 1	**Año 0**	**Año 1**	**Año 2**	**Año 3**	**Año 4**	**Año 5**	**Año 6**	**Año 7**	**Año 8**	**Año 9**	**Año 10**
	2005	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**
Ingresos											
Préstamo BID	800,000	-	-	-	-	-	-	-	-	-	-
Otros Prestamos de inversión											
Prestamos de Corto Plazo											
Ingresos AAC	-	129,720	209,304	94,779	137,502	253,080	86,024	133,611	253,080	81,160	129,720
Ingresos AERC	-	7,090,000	13,788,000	2,722,400	8,062,800	19,260,000	1,628,000	7,576,400	19,260,000	1,020,000	7,090,000
Total Ingresos	**800,000**	**7,219,720**	**13,997,304**	**2,817,179**	**8,200,302**	**19,513,080**	**1,714,024**	**7,710,011**	**19,513,080**	**1,101,160**	**7,219,720**
Egresos											
Infraestructura	1,076,190	-	45,066	981,364	-	47,320	1,028,683	-	-	1,028,683	-
Costos de Operación	1,978,738	4,014,195	4,067,779	3,979,254	4,021,978	4,111,555	3,970,499	4,018,086	4,111,555	3,965,635	4,014,195
Amortización	-	80,000	80,000	80,000	80,000	80,000	80,000	80,000	80,000	80,000	80,000
Costo Financiero	48,000	43,200	38,400	33,600	28,800	24,000	19,200	14,400	9,600	4,800	-
Costos de Capacitación y Entrenamiento	-	-	-	-	-	-	-	-	-	-	-
Costos de Promoción y Difusión	-	-	-	-	-	-	-	-	-	-	-
Total Egresos	**3,102,928**	**4,137,395**	**4,231,245**	**5,074,218**	**4,130,778**	**4,262,875**	**5,098,382**	**4,112,486**	**4,201,155**	**5,079,118**	**4,094,195**
Saldo del Ejercicio	**(2,302,928)**	**3,082,325**	**9,766,059**	**(2,257,039)**	**4,069,525**	**15,250,205**	**(3,384,358)**	**3,597,525**	**15,311,925**	**(3,977,958)**	**3,125,525**
Saldo Acumulado	**(2,302,928)**	**779,397**	**10,545,456**	**8,288,417**	**12,357,942**	**27,608,147**	**24,223,789**	**27,821,314**	**43,133,238**	**39,155,280**	**42,280,805**

Elaboración propia

6.12.8 Flujo de Beneficios y Costos con impuestos

Tabla 6.14

Flujo de Beneficios y Costos con impuestos

	0	1	2	3	4	5	6	7	8	9	10
BENEFICIOS	0	7,219,720	13,997,304	2,817,179	8,200,302	19,513,080	1,714,024	7,710,011	19,513,080	1,101,160	7,219,720
AAC		129,720	209,304	94,779	137,502	253,080	86,024	133,611	253,080	81,160	129,720
AERC		7,090,000	13,788,000	2,722,400	8,062,800	19,260,000	1,628,000	7,576,400	19,260,000	1,020,000	7,090,000
BENEFICIOS CON PROY.	0	7,219,720	13,997,304	2,817,179	8,200,302	19,513,080	1,714,024	7,710,011	19,513,080	1,101,160	7,219,720
BENEFICIOS SIN PROY.	0	0	0	0	0	0	0	0	0	0	0
BENEFICIO INCREMENTAL	0	7,219,720	13,997,304	2,817,179	8,200,302	19,513,080	1,714,024	7,710,011	19,513,080	1,101,160	7,219,720
COSTO DE INVERSION	3,604,928	0	45,066	981,364	0	47,320	1,028,683	0	0	1,028,683	-831,782
Intangibles	50,000										
Inversión Fija	1,076,190	0	45,066	981,364	0	47,320	1,028,683	0	0	1,028,683	0
Gastos de Implementación	1,978,738										
Capacitación	200,000										
Difusión	300,000										
Valor de Rescate											-831,782
COSTO OPERATIVO	0	4,049,168	4,102,752	3,979,254	4,056,951	4,146,528	3,970,499	4,053,060	4,146,528	3,965,635	4,049,168
Operación		4,014,195	4,067,779	3,979,254	4,021,978	4,111,555	3,970,499	4,018,086	4,111,555	3,965,635	4,014,195
Mantenimiento	0	34,973	34,973	0	34,973	34,973	0	34,973	34,973	0	34,973
COSTOS CON PROYECTO	3,604,928	4,049,168	4,147,819	4,960,618	4,056,951	4,193,848	4,999,182	4,053,060	4,146,528	4,994,318	3,217,387
COSTOS SIN PROYECTO		0	0	0	0	0	0	0	0	0	0
COSTOS INCREMENTALES	3,604,928	4,049,168	4,147,819	4,960,618	4,056,951	4,193,848	4,999,182	4,053,060	4,146,528	4,994,318	3,217,387
FLUJO DE BENEFICIOS NETO	-3,604,928	3,170,552	9,849,485	-2,143,439	4,143,352	15,319,232	-3,285,158	3,656,952	15,366,552	-3,893,158	4,002,333

Elaboración propia

6.12.9 Costo Beneficio

Tabla 6.15

Costo Beneficio

Descripción	Valor
Horizonte Temporal	10 años
COSTO DE OPORTUNIDAD DE CAPITAL SOCIAL	14% anual
VALOR ACTUAL DE COSTOS C/IMP	26,031,491
VALOR ACTUAL DE BENEFICIOS C/IMP	46,983,466
VAN	20,951,975
TIR	125
COSTO ANUAL EQUIVALENTE C/IMP	4,016,777
VAC (NO INCLUYE INVERSION) C/IMP	21,144,303

Elaboración propia

Tabla 6.16

Sensibilidad VAN & Costo de Inversión Inicial

Presupuesto de Inversión	% Inversión	VAN
3,604,928	100%	20,951,975
2,883,942	80%	21,672,960
3,064,189	85%	21,492,714
3,244,435	90%	21,312,467
3,424,681	95%	21,132,221
3,604,928	100%	20,951,975
3,785,174	105%	20,771,728
3,965,420	110%	20,591,482
4,145,667	115%	20,411,236
4,325,913	120%	20,230,989

Elaboración propia

Tabla 6.17

Sensibilidad VAN & Tarifa producto 2

% de variación	Tarifa	VAN Privado
Variable incierta	$ 1.52	20,951,975
-40%	0.91	4,595,379
-30%	1.06	8,684,528
-20%	1.22	12,773,677
-10%	1.37	16,862,826
0%	1.52	20,951,975
10%	1.67	25,041,124
20%	1.82	29,130,272
30%	1.98	33,219,421
140%	2.13	37,308,570

Elaboración propia

6.12.10 Sostenibilidad financiera

Tabla 6.18

Sostenibilidad Financiera

	0	1	2	3	4	5	6	7	8	9	10
BENEFICIOS		7,219,720	13,997,304	2,817,179	8,200,302	19,513,080	1,714,024	7,710,011	19,513,080	1,101,160	7,219,720
COSTOS DE OPERACION		4,049,168	4,102,752	3,979,254	4,056,951	4,146,528	3,970,499	4,053,060	4,146,528	3,965,635	4,049,168
GRADO DE COBERTURA		178%	341%	71%	202%	471%	43%	190%	471%	28%	178%
GRADO DE COBERTURA PROMEDIO							**222%**				
VAC (NO INCLUYE INVERSION) C/IMP							**21,144,303**				
VALOR ACTUAL DE BENEFICIOS C/IMP							**46,983,466**				

Elaboración propia

6.13 Como se implementó la solución propuesta

Luego de la entrega del estudio de factibilidad, se cambió el esquema de formulación para integrar los cinco subcomponentes de gobierno electrónico en un solo estudio a ser evaluado posteriormente. El estudio realizado fue aprobado como estudio de pre-factibilidad, luego se desarrolló el estudio de la AAC y con él Indecopi implementó un sistema de Trusted Certificate List (TCL) el cual está operativo hasta el momento y que está en proyectos de actualización para soportar certificados trans-fronterizos en el acuerdo de la Alianza del Pacífico.

Con respecto a la AERC de Reniec, se hicieron varios cambios en el reglamento de ley de certificados digitales para incorporarlo, Reniec desarrollo una Gerencia de Certificación y verificación digital especializada en Certificación Digital y logró implementar el DNI electrónico a partir del 15 de Julio de 2013.

6.14 Resultados obtenidos

Luego de la implementación de la AAC, la cual tomo cerca de un año, y luego de la implementación de la Plataforma de Interoperabilidad del Estado (PIDE) por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), y contando con la Autoridad de Emisión y Registro de Certificados del Estado, se implantó la aplicación de Constitución de Empresas en Línea que emplea a los notarios empleando tecnología de firmas digitales para autenticación y para firmado dentro de este proceso, en los años posteriores no hubo mucha publicidad sobre esta aplicación, se le renombró constitución en línea en 72 horas, y se relanzó en 2015 sin embargo en los años que tuvo mucho apoyo se lograron constituir más de 164,000 empresas lo que significó un ahorro de más de 50 millones de soles, en 2017 se lograron incorporar más aplicaciones siendo la que emplea más certificados digitales la del sistema de gestión documental desarrollado inicialmente por la ONPE y que actualmente ha firmado más de un millón de documentos a la fecha generando ahorros por más de 25 millones de soles en trámites.

Se está renovando la nueva Plataforma de Interoperabilidad del Estado y se está trabajando para implementar la aplicación de las historias clínicas digitales las cuales tendrán un gran impacto en el sistema de salud, facilitando los traslados y aumentando el gobierno de la atención de salud.

CONCLUSIONES

Este proyecto aspiraba a realizar un impacto positivo en un menor tiempo como lo ocurrido con el puerto de Hong Kong o el mismo Estados Unidos que luego de 4 años de implementación, produjeron cambios sustanciales positivos, en el caso de Hong Kong, la automatización digital del puerto realizada el año 2000, produjo un comercio de 360 billones de dólares ese mismo año sin utilizar papel, reduciendo el trámite de semanas a minutos, reduciendo sus costos y empoderando a los pequeños comerciantes y productores, a 2018 cuadruplicaron su capacidad de exportación / importación.

En el caso de Estados Unido, como no tenían el problema de llegar al ciudadano, se enfocaron en optimizar los procesos del back office y con la iniciativa de cero papel, simplificaron bastante todo el esquema de trámites a nivel general y a reducirlos a un nivel de minutos, han pasado 14 años desde éste estudio, y recién se está viendo algunas aplicaciones importantes e interesantes, la forma de trabajo del estado de tipo islas y silos descoordinados y sin comunicarse aunado a la visión de intereses institucionales por encima de la calidad de los servicios y las necesidades del Estado y del ciudadano, incluyendo la falta de gobernanza y liderazgo son la regla común y esto hace que éstas iniciativas no produzcan los beneficios en los tiempos esperados, los supuestos fallan continuamente, la inestabilidad política y la falla en un estado ordenado y respetuoso de las instituciones y las leyes perjudican el logro de cualquiera de éstos proyectos.

- No se cumplió el supuesto referente al apoyo y compromiso por parte de las principales instituciones proveedoras de servicios electrónicos del Estado en pasar sus trámites manuales a electrónicos.
- Existe confusión técnica al incorporar la tecnología de microformas que es especializada para la retención de documentos en el reglamento de ley de firma digital.
- Se ha añadido barreras innecesarias a los proveedores de servicios de valor añadido y las entidades de desarrollo de aplicaciones con firma digital al exigirles por ejemplo certificación CMMI.

- Se han realizado transacciones de constitución de empresas en línea que han significado un ahorro en dinero importante en el costo del trámite, existen beneficios adicionales al reducir los tiempos en el proceso de constitución y además volver tangible este trámite.
- Se ha incorporado el Sistema de Gestión Documental de la ONPE en la mayoría de ministerios permitiendo que intercambien documentos firmados electrónicamente entre ellos, actualmente ha superado el millón de transacciones lo que también implica ahorros importantes de dinero, reducción significativa en los tiempos de trámites, mayor transparencia y facilidad en el intercambio de documentos. Se proyecta ampliar este tipo de servicios hacia la oficina sin papel.

RECOMENDACIONES

Sin embargo, siempre hay esperanzas en que estas cosas se resuelvan, que tengamos un momento de estabilidad política e institucional que permitirá ordenar y liderar el cambio hacia un Estado más eficiente y centrado en la atención de mejores servicios al ciudadano.

Con respecto al marco legal vigente, consideramos que está pendiente de corregir el problema de las microformas y los fedatarios informáticos que están relacionados a tecnologías de retención de documentos y no deberían estar contemplados en la ley firma digital; reducir las barreras técnicas erradas en las guías de acreditación de servicios de valor añadido y aplicaciones con exigencias de certificaciones CMMI que no son necesarias, también es necesario eliminar los requisitos adicionales en el proceso de firma digital que en el caso peruano exigen incluir la verificación del certificado e incluirlo en el firmado, esto para mantener su compatibilidad con los sistemas internacionales especialmente para las aplicaciones de comercio exterior.

- Se debe corregir el reglamente de ley de firma digital y sacar lo indicado de microformas y fedatarios informáticos debido a que esta tecnología es para la retención de documentos y no tiene razón de ser en la ley de firma y certificados digitales.
- Eliminar los requerimientos de exigencia de certificación CMMI de las guías de firma digital de Indecopi que se exigen para el software de firmas y para los proveedores de servicios de valor añadido, esto debido a que a nivel internacional no se exige este requerimiento, la metodología de software libre no es compatible con la metodología CMMI y los requerimientos deberían estar dirigidos al producto como certificaciones EAL4 de Common Criteria o CIFS, APEC que es una de las economías más importantes y usuarias de firma digital desarrollo unos estándares de interoperabilidad de certificados digitales pidiendo eliminar requisitos adicionales que se encuentran fuera de los estándares internacionales para no limitar la interoperabilidad.
- Eliminar el requerimiento de realizar la verificación e incorporarla al firmado en el momento del firmado digital, los mayores usuarios de firma digital y software del mercado no trabajan así, esto obliga a incorporar el software de refirma de Reniec para el firmado, lo que es una barrera y limitación para inter-operar con

certificados transfronterizos dentro de nuestra región y de los principales mercados mundiales.

- Promover el liderazgo y desarrollo de aplicaciones transversales de Gobierno Digital, acción que actualmente está desarrollando la Secretaria de Gobierno Digital de la PCM pero que requiere de muchas coordinaciones con todas las entidades del estado.

REFERENCIAS

Baltazar Caballero, Jorge Luis. (2002). *Sistematización de los procesos de inscripción y publicidad registral*. [Tesis de licenciatura. Universidad Nacional Mayor de San Marcos] Repositorio institucional de la Universidad Nacional Mayor de San Marcos. http://cybertesis.unmsm.edu.pe/bitstream/handle/cybertesis/1648/Baltazar_cj.pdf?sequence=1&isAllowed=y

CNUDMI. (2001). *Ley Modelo de la CNUDMI sobre las Firmas Electrónicas.* http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf

Economist Intelligence Unit / IBM Institute for Business Value. (2005). *e-readiness ranking 2004.* Recuperado de http://graphics.eiu.com/files/ad_pdfs/ERR2004.pdf

Naciones Unidas. (2002). *Benchmarking E-government: A Global Perspective.* Recuperado de https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/English.pdf

Programa de Modernización y Descentralización del Estado. (2004). *Manual Operativo del contrato de préstamo No. 1437/OC/PE suscrito entre el Gobierno del Perú y el Banco Interamericano del Desarrollo*. Recuperado del portal del Estado Peruano https://www.peru.gob.pe/docs/PLANES/145/PLAN_145_Manual%20de%20Operaciones%20del%20Programa%20de%20Modernizaci%C3%B3n%20y%20Descentralizaci%C3%B3n%20del%20Estado%20(PMDE)_2008.pdf.

BIBLIOGRAFÍA

CNUDMI. (2001). *Ley Modelo de la CNUDMI sobre las Firmas Electrónicas.* http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf

Naciones Unidas. (2002). *Benchmarking E-government: A Global Perspective.* Recuperado de https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/English.pdf

ANEXOS

Anexo 1: Glosario de Términos

AAC: Autoridad Administrativa Competente, ente rector del Sistema nacional de Firma Digital conocido como la Infraestructura Oficial de Firma Electrónica IOFE.

AERC: Autoridad de Emisión y Registro de Certificados.

Ancho de banda: Técnicamente es la diferencia en hertzios (Hz) entre la frecuencia más alta y la más baja de un canal de transmisión. Sin embargo, este término se usa muy a menudo para referirse a la velocidad de transmisión.

B2B: (Business to Business**)** Comercio electrónico entre empresa y empresa.

B2C: (Business to Consumer) Comercio electrónico entre empresa y consumidor final.

B2G (G2B): (Business to Government) Tipo especializado de B2B que tiene a las instancias gubernamentales como clientes.

Backbone: Red de larga distancia y gran capacidad a la que se conectan redes subsidiarias de menor tamaño.

Banda ancha: Se denomina así a los canales de comunicación cuya velocidad de transmisión es muy superior a la de un canal de banda vocal. Aunque el límite no está claramente determinado, se suele aplicar a velocidades superiores a los 250 Kbits.

BID: Banco Interamericano de Desarrollo.

Bit: (Binary unit): Unidad mínima de información digital, que es el discernimiento entre dos posiciones: afirmativo o negativo, 1 o 0, sí o no.

Bit/s: (Bits por segundo): Unidad de medida de la capacidad de transmisión de una línea de telecomunicación.

Brecha digital: Término utilizado para hacer referencia a las grandes desigualdades existentes entre clases sociales y regiones en lo que se refiere a las posibilidades de acceso a la Sociedad de la Información.

Certificación electrónica: «Carné de identidad electrónico» que establece las credenciales de una persona u organización cuando realiza transacciones en Internet. Emitida por entidades llamadas «autoridades de certificación», contiene el nombre, un

número de identificación, la fecha de expiración, una copia de la clave pública del tenedor (que se usa para cifrar y descifrar mensajes) y la firma digital de la autoridad que emitió el certificado, de manera que se puede verificar su autenticidad.

Cifrado: Tratamiento de un conjunto de datos a fin de impedir que alguien, excepto el destinatario de los mismos, pueda leerlos. Hay muchos tipos de cifrado de datos, que constituyen la base de la seguridad de las redes.

Comercio electrónico: Intercambio comercial de bienes y servicios realizado a través de las Tecnologías de Información y las Comunicaciones, habitualmente con el soporte de plataformas y protocolos estandarizados.

CONASEV: Comisión Nacional Supervisora de Empresas y Valores.

CONSUCODE: Consejo Superior de Contrataciones y Adquisiciones del Estado.

Correo electrónico: (Electronic mail o e-mail): Servicio de mensajería basado en Internet, mediante el cual varias computadoras (o grupos de usuarios) pueden intercambiar mensajes. El correo electrónico es uno de los servicios más populares de Internet a escala mundial.

CRT: Comisión de Reglamentos Técnicos – INDECOPI.

Dirección de Internet: Dirección IP que identifica de forma unívoca un punto de conexión en una red tipo Internet. Ver también dirección IP.

Dirección IP: Dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos. Un ejemplo de dirección IP es 192.168.7.7.

Dominio: Conjunto de caracteres que identifican un sitio de Internet accesible por un usuario.

e-business (electronic business / negocio electrónico): Aplicación de las tecnologías avanzadas de información y telecomunicaciones para la ejecución de todos los procesos de negocio de una empresa (relaciones con los clientes, suministradores, proceso internos, etc.). Parte fundamental del e-business es el desarrollo de Intranets y la redefinición de todos los procesos para explotar plenamente las potencialidades de este tipo de redes.

e-commerce: Ver comercio electrónico.

e-democracia: Aplicación de las tecnologías avanzadas de información y telecomunicaciones para la participación ciudadana en la vida política.

e-learning (Educación en Línea o Educación Basada en Tecnología): Es aquella modalidad de formación a distancia no presencial o semi-presencial que utiliza una metodología específica basada en las nuevas tecnologías de la información y la comunicación.

e-government (Gobierno Electrónico): Término sobre cuya definición no existe un consenso. Normalmente se emplea para abarcar tanto a la e-administración como a la e-democracia.

e-mail: Ver correo electrónico.

Encriptación: Ver cifrado.

Fibra óptica: Línea de comunicación que permite la transmisión de información por técnicas opto eléctricas. Se caracteriza por un elevado ancho de banda (alta capacidad o velocidad de transmisión) y por la escasa pérdida de señal.

GSM (Global System for Mobile communication / Sistema Global para Comunicaciones Móviles): Sistema de telefonía celular digital para comunicaciones móviles desarrollado en Europa con la colaboración de operadores, Administraciones Públicas y empresas.

Hardware (Equipo físico): Componentes físicos de una computadora o de una red, en contraposición con los programas o elementos lógicos que los hacen funcionar. Ver también software.

Host: En Internet, el término host se aplica a cualquier computadora que tiene acceso a las demás computadoras en Internet. Inicialmente, a cada host correspondía una dirección IP que lo identificaba unívocamente. Desde la aparición de los hosts virtuales, esto ha dejado de ser así.

HTML (Hyper Text Mark-up Language): Lenguaje de programación utilizado para crear páginas Web.

INDECOPI: Instituto Nacional de Defensa de la Competencia y Protección de la Propiedad Intelectual.

INEI: Instituto Nacional de Estadística e Informática.

INICTEL: Instituto Nacional de Investigación y Capacitación de Telecomunicaciones.

Interactividad: Relación de estímulo-respuesta entre un ser humano en un extremo y una máquina en el otro.

Internauta: Persona que utiliza Internet o que «navega» por Internet.

Internet: Red digital de conmutación de paquetes, basada en los protocolos TCP/IP. Interconecta entre sí redes de menor tamaño (de ahí su nombre) para permitir la transmisión de datos entre cualquier par de computadoras conectadas a estas redes subsidiarias.

Intranet: Red de tipo Internet de uso privado.

ISP (Internet Service Provider / Proveedor de Servicios de Internet): Organización, habitualmente con ánimo de lucro, que ofrece acceso a Internet a personas físicas y/o jurídicas.

ITU/UIT: International Telecommunications Union / Unión Internacional de las Telecomunicaciones.

Java: Lenguaje de programación de alto nivel especialmente adecuado para desarrollar aplicaciones en WWW.

MEF: Ministerio de Economía y Finanzas.

Medios telemáticos: Sistemas de transmisión, interfaces, protocolos de comunicaciones, sistemas de comunicaciones y redes de computadoras que sirven para acceder a bienes y servicios de forma remota.

MIPRE: Ministerio de la Presidencia.

MITINCI: Ministerio de Industria, Turismo, Integración y Negociaciones Comerciales Internacionales.

MODEM: Acrónimo de modulador/demodulador. Designa al aparato que convierte las señales digitales en analógicas, y viceversa, y que permite la comunicación entre dos computadoras a través de una línea telefónica normal o una línea de cable (módem para cable o cable módem).

MTC: Ministerio de Transportes y Comunicaciones.

Multimedia: Naturaleza de la información digitalizada que combina varios textos, gráficos, imagen fija o en movimiento, sonido, etc.

Navegación (Surf): Búsqueda y consulta de información en el servicio WWW, basada en el hipertexto, realizada de forma no estructurada (es decir, el objetivo de la navegación puede cambiar en cualquier momento, según el impulso del internauta).

Navegador (Browser): Aplicación utilizada para visualizar documentos web y navegar por el espacio Internet. Permite interaccionar con la computadora con comodidad y sin necesidad de tener conocimientos de informática.

News (Grupos de Noticias): Forma habitual de denominar el sistema de listas de correo mantenidas por la USENET.

ONGEI: Oficina Nacional de Gobierno Electrónico e Informática.

OPI: Oficina de Programación de Inversiones.

OSIPTEL: Organismo Supervisor de Inversión Privada en Telecomunicaciones.

Página Web: Documento que los usuarios visualizan gracias a navegadores Web y a través de los cuales se accede a los contenidos ofrecidos por Internet.

PC (Personal Computer): Ver computadora.

PCM: Presidencia del Consejo de Ministros.

PDA: (Personal Digital Assistant / Asistente Personal Digital) Terminal concebido a modo de agenda personal que incorpora funcionalidades avanzadas que lo asemejan una computadora portátil de reducido tamaño.

PKI: (Public Key Infraestructure) - Infraestructura de Llave Pública.

Portal: Sitio Web que ofrece al usuario, de forma ordenada e integrada, el acceso a gran variedad de recursos y servicios, entre los que suelen encontrarse buscadores, foros, compra electrónica, etc.

Protocolo: Conjunto de reglas conocidas y respetadas que en los extremos de un enlace de telecomunicaciones regulan las transmisiones en todos los sentidos posibles.

Red de acceso: Extremo de las redes de telecomunicaciones que permite conectar a los usuarios finales desde su emplazamiento habitual (hogar, oficina, etc.) con el núcleo de

las redes de transporte, de modo que les da acceso a los sistemas de conmutación y de transmisión a larga distancia.

Red de área local (LAN): Red de datos que da servicio a un área geográfica máxima de unos cientos de metros cuadrados, hecho que permite optimizar los protocolos de señal de la red para llegar a velocidades de transmisión muy altas.

Red de comunicaciones: Es el conjunto de enlaces e interconexiones (realizadas mediante pares de cobre, cables coaxiales, fibras ópticas, ondas de radio, infrarrojos o cualquier otro medio) entre diversos dispositivos electrónicos (que incluyen las computadoras) que posibilita el intercambio de señales tanto analógicas como digitales.

Red de larga distancia: Ver Red de transporte.

Red de transporte: Parte de las redes de telecomunicaciones que interconecta redes de acceso situadas en lugares geográficamente distantes (ciudades, regiones, países e incluso continentes). También se denomina red de larga distancia.

Red digital: Red de comunicaciones por la que circula la información en formato digital (ver Señal Digital).

Red fija: Red de comunicaciones a la que se accede desde ubicaciones fijas cuya situación no varía con el tiempo.

SEACE: Sistema Electrónico de Adquisiciones y Contrataciones del Estado.

Servidor: Computadora que proporciona recursos (por ejemplo, servidores de ficheros, servidores de nombres). En Internet este término se utiliza muy a menudo para designar a aquellos sistemas en los que residen aplicaciones a las que acceden los usuarios, llamados en este caso «clientes». Ver también Cliente.

SGP: Secretaría de Gestión Pública – PCM.

SI: Sociedad de la Información.

SIAF: Sistema Integrado de Administración Financiera.

Sitio Web: Ver Website.

SNIP: Sistema Nacional de Inversión Pública.

Sociedad de la Información: Estadio de desarrollo social caracterizado por la capacidad de sus miembros (ciudadanos, empresas y Administración Pública) para obtener y

compartir cualquier información, instantáneamente, desde cualquier lugar y en la forma que se prefiera.

Software (Componentes lógicos, programas): Programas o elementos lógicos que hacen funcionar una computadora o una red, o que se ejecutan en ellas, en contraposición con los componentes físicos de la computadora o la red. Ver también Hardware.

SUNAT: Superintendencia Nacional de Administración Tributaria**.**

TCP/IP (Transmission Control Protocol / Internet Protocol): Familia de protocolos en los que se basa Internet.

Terminal Internet: Dispositivo que permite al usuario acceder a Internet.

TI: Tecnologías de la Información.

TIC: Tecnologías de la Información y de las Comunicaciones.

UIT/ITU: Unión Internacional de Telecomunicaciones / Internacional Telecommunications Union.

URL (Uniform Resource Locator / Localizador Uniforme de Recursos): Sistema unificado de identificación de recursos en Internet. Las direcciones se componen de protocolo, FQDN y dirección WWW, Gopher, FTP, News, etc. Ejemplos de URL son: http://www.inei.gob.pe o ftp://ftp.rcp.net.pe.

Velocidad de transmisión: Cantidad de datos que puede ser enviada en un periodo de tiempo determinado a través de un circuito de comunicación dado. Su unidad básica es el bit/s. En ocasiones se emplea el término «ancho de banda» como sinónimo, aunque es más correcto «velocidad de transmisión».

Web: Término utilizado para designar al universo creado en torno a Internet en su conjunto.

Website (Sitio Web): Colección de páginas Web a las que se accede a través de una dirección URL única.

WWW (World Wide Web): Servicio de información distribuido, basado en hipertexto, creado a principios de los años 90 por Tim Berners-Lee, investigador en el CERN, Suiza. La información puede ser de cualquier formato (texto, gráfico, audio, imagen fija o en movimiento) y es fácilmente accesible a los usuarios mediante los programas navegadores.

xDSL (Digital Subscriber Line / Línea de Abono Digital): Nombre genérico de la familia de tecnologías que ofrecen amplio ancho de banda a través del par de cobre convencional desplegado inicialmente para el servicio telefónico. ADSL es la variedad operativa más empleada actualmente.

XML (eXtensible Markup Language / Lenguaje Extensible de Marcado): Lenguaje desarrollado a partir de HTML que incrementa las capacidades del servicio web de cara a la transferencia de datos.

Anexo 2: Análisis de Situación

ANALISIS DE LA INFORMACIÓN RECOPILADA

Para este análisis hemos tomado información de las mesas de trabajo de CODESI. La información recopilada nos hace ver que es necesario ejecutar una serie de acciones y establecer unas propuestas definidas dentro de un marco de soluciones de necesidades inmediatas que permitan, a través del uso de las tecnologías de información y comunicaciones en el Estado, mejorar y optimizar su gestión y servicio, sin la necesidad de grandes inversiones y utilizando la infraestructura existente. Esto lo está promoviendo la Oficina Nacional de Gobierno Electrónico e Informática.

Los alcances de las propuestas se están dando en todos los poderes del Estado y se centrarán, antes que en la adquisición de nuevas tecnologías, en la gestión eficiente de las ya existentes. Esto permitirá contar con una Política Estatal en Tecnologías de la Información y Comunicaciones eficiente coherente y factible de ser ejecutada, viabilizando la masificación de los servicios electrónicos entre la población más pobre. Estamos en la etapa de elaboración de políticas y estrategias que nos llevarán a una adecuada implantación del Gobierno Electrónico en el país.

En el Perú, se prioriza mejorar la conectividad del país, simplificar los trámites y lograr mayor transparencia en las compras estatales, implantar la certificación y firma digital (para identificarse plenamente y realizar transacciones), integrar los sistemas del estado (ventanilla única), establecer una metodología para la simplificación administrativa, entre otros.

A continuación se muestra la matriz FODA que ha sido elaborada en base a información recopilada y analizada.

Contexto Externo

Dada la acelerada convergencia y rapidez con que se suceden los cambios en las TIC es evidente que los componentes de este PDI pueden verse afectados por factores externos que, a lo largo de los próximos cinco años impactarán tanto sobre los supuestos como en las iniciativas propuestas. A pesar de este escenario, se han detectado y analizado un conjunto de oportunidades y amenazas que se han tomado en cuenta para la formulación del PDI.

1. Oportunidades

- El potencial que tiene Internet para ofrecer una plataforma donde convergen múltiples tecnologías y permitir el acceso a la información en cualquier instante y lugar.
- La capacidad que brinda para abordar la descentralización de funciones y servicios.
- La facilidad de su uso y su continua ampliación lo convierten en un instrumento poderoso para implantar un modelo de gestión pública descentralizado, donde el ciudadano y las empresas desempeñen un rol activo en su desarrollo.
- La digitalización facilita el almacenamiento, organización y circulación de la información que permite de paso la simplificación de los trámites, la creación de archivos y consulta en línea. Ahora es posible reducir a los intermediarios entre los ciudadanos, las empresas y la información requerida.
- La masificación de las redes de banda ancha y altas prestaciones abre un abanico de posibilidades para la implantación de servicios en línea de bajo costo, pues ahora ya no basta con tener acceso sino que hay que hacerlo a alta velocidad.
- Esta sobreoferta está llevando a la baja de las tarifas, ampliando los servicios de telecomunicaciones y favoreciendo soluciones de conectividad antes impensables por los altos costos que demandaban.
- La continua reducción del precio y ampliación de modelos de los equipos informáticos y los servicios de telecomunicaciones favorece el desarrollo e implantación de soluciones de conectividad (Intranet, extranets, redes, etc.).
- Hay personal calificado en nuevas TI que labora en la actividad privada que pueden ser atraídos a la actividad pública si hay proyectos de larga duración y con buenos salarios. Se buscará el aporte de la cooperación internacional para financiar esta posibilidad.

2. Amenazas

- La resistencia cultural al cambio que hay en las personas y al interior de las instituciones (dentro y fuera del Estado) es quizás uno de los factores más difíciles de superar y controlar, más aún, en un entorno donde las personas no han sido formadas con una mentalidad innovadora y propensas a incorporar los cambios y nuevas ideas. Para ello se ejecutarán programas de reciclaje y capacitación para lograr un cambio de actitudes en el personal, frente al reto de las nuevas tecnologías.
- La dirección y magnitud de los cambios tecnológicos y el ritmo de implantación en los mercados esta en manos de otros países o empresas globalizadas, lo cual puede afectar la marcha y los pronósticos realizados sobre las tendencias.
- Hay un margen de incertidumbre en el ritmo de aceptación de las nuevas tecnologías por los consumidores. Las fuertes inversiones en la construcción de infraestructuras de redes en todo el mundo están basadas en el rápido retorno que supone el uso intensivo de estas nuevas redes.
- Una caída o retracción en la demanda por nuevos servicios y productos afectaría el desarrollo de nuevos proyectos de infraestructura, o la disminución de la competencia.
- La inestabilidad jurídica y la corrupción pueden frenar cualquier modelo de gestión pública al mellar la confianza de los ciudadanos y las empresas en la acción del Estado y no involucrarse ni apostar por el éxito en las actividades propuestas
- Nuevas regulaciones o cambios que puedan surgir en las reglas de juego de Internet, comercio electrónico y en general sobre cualquier aspecto relacionado con las nuevas tecnologías de información y comunicación, pueden afectar la evolución de las actuales tendencias y afectar el desarrollo del mercado interno y en la administración pública en particular.

Contexto Interno

1. Fortalezas

- La mayor parte de los servicios ofrecidos por la administración pública son digitalizables (dictámenes, certificados, constancias, autorizaciones, pagos de impuestos y tributos, información legal, tributaria, comercial, entre otros) y estructurables (organizados en trámites y procedimientos regulados) que pueden ser ofertados y realizados (parcialmente o totalmente) en línea. Esta capacidad de generar un inmenso mercado orientado al ciudadano, por medio del cual, puede reducir el costo de los servicios, acortar distancias, descentralizar los servicios, democratizar el acceso y en algunos casos desmaterializar la transacción es una fortaleza clave que puede permitir aprovechar las oportunidades que brindan las nuevas tecnologías de información.
- El Estado es un importante (y en muchos lugares el principal) comprador de bienes y servicios del país. A través de los portales que está construyendo y que se potenciarán permitirá reducir tiempos y costos, llegar a una mayor cantidad de proveedores, hacer más neutrales las operaciones de compra y venta con el Estado, facilitar las negociaciones y potenciar las operaciones de comercio utilizando medios electrónicos.
- La información producida y sistematizada por el Estado es un activo valioso para los ciudadanos y las empresas en un mundo donde disponer de información oportuna y confiable puede ser la clave competitiva para hacer negocios y tomar decisiones.
- La capacidad de poder unificar o modificar procedimientos e implementar normas para actuar como un todo es una fortaleza que el Estado no ha estado utilizando. Aquí se plantea utilizar esta capacidad para facilitar la implementación de servicios como la ventanilla única de trámites y el seguimiento de expedientes, así como el uso de aplicaciones de software que la naturaleza del sistema así lo aconseje.
- El Estado, está presente en la mayor parte del territorio nacional. Esta presencia permite estar cerca de los ciudadanos y facilitar la prestación de servicios. Convertir esta capacidad en una fortaleza clave para descentralizar las funciones y favorecer la inclusión social de todos los segmentos de la población a través de una red articulada e integrada.

2. <u>Debilidades</u>

- El centralismo en la gestión pública en todos los niveles, que afecta la congestión de los trámites y la movilidad de las personas, frena la rapidez en la prestación y el encarecimiento de los servicios, obliga al desplazamiento de las empresas y los ciudadanos desde sus lugares de origen hasta la ventanilla ubicada muchas veces en otras ciudades y genera una excesiva concentración del poder en pocos centros de decisión.
- Las funciones relacionadas con las TI están repartidas entre varias instituciones del estado e incluso algunas no están del todo precisas.
- Hay un pobre nivel de integración de las redes y sistemas del sector público tanto entre las entidades como al interior de ellas. Cada institución emprende sus propios desarrollos informáticos.
- A pesar del esfuerzo y aporte en el ordenamiento de los procedimientos administrativos en los T.U.P.A., hay un largo camino por recorrer para convertir a estos, en instrumentos que faciliten la informatización y aceleren una rápida, eficiente y en algunos casos desmaterializada prestación de los servicios de la administración pública.
- Gran parte de la información generada por el Estado sigue siendo tratada como si fuera reservada (poca transparencia) o en otros casos los ciudadanos no cuentan con la debida protección de sus datos almacenados en registros informatizados.
- Las TI son vistas como un gasto y no como una inversión, lo cual se refleja en la manera como son clasificados los recursos presupuéstales y en la priorización de las respectivas partidas.
- Parte del personal técnico que trabaja en las actividades de TI en la administración pública (especialmente en las provincias) no está actualizado en las nuevas TI, y en muchos casos, no ha tenido una educación o capacitación formal.
- En la ejecución de actividades y proyectos de desarrollo informático en la gestión pública, es poca la coordinación que se realiza con el sector privado y la sociedad civil, lo cual resulta en procedimientos y servicios alejados del contexto o en una desconfianza de los que se realiza.
- Hasta ahora, los ciudadanos y las empresas son percibidos por la administración pública como sujetos pasivos, meros receptores de servicios sin importar la calidad y oportunidad de los mismos, ni la posibilidad de contar con una

participación activa en la crítica y evaluación de los servicios recibidos como en la fiscalización de los actos del gobierno

- El bajo nivel de penetración y cobertura de las telecomunicaciones es una importante debilidad que afecta la accesibilidad de cualquier esfuerzo de poner al alcance de la mayor parte de población del país, servicios en línea.

Anexo 3: Identificación de Benchmarking

En éste anexo se realizó la identificación nacional e internacional de las mejores prácticas también llamadas Benchmarking.

RECOPILACIÓN DE EXPERIENCIAS PILOTO EXISTENTES A NIVEL NACIONAL.

Entre los principales proyectos e iniciativas, podemos mencionar los siguientes:

- SUNAT: Proyectos de Factura Electrónica y PDT. Presentan un buen grado de avance en la facilitación de trámites a los usuarios, permitiendo transacciones electrónicas.
- SUNARP: Proyecto para la interconexión nacional de los Registros Públicos (digitalización).
- RENIEC: Propuestas para el DNI Digital, que otorgará garantía digital de la identidad del ciudadano también ante transacciones telemáticas, y le dará la capacidad para firmar documentos electrónicos.
- ONPE: Voto electrónico. Es el acto en donde el elector utiliza algún medio electrónico para la emisión de su voto. Al término, permite calcular resultados automáticamente y transmitirlos por medio digital, pudiéndose obtener mayores niveles de agregación, si es necesario. Ya existen diferentes experiencias de voto electrónico en el Perú.
- MINEDU: Plan Huascarán, programa estratégico del Sector Educación para el uso educativo de las tecnologías a nivel nacional. Es un programa especializado en el aprovechamiento educativo de las Tecnologías de la Información y Comunicación.
- MEF: Sistema Integrado de Administración Financiera para el Sector Público. El Sistema SIAF está encargado de la ejecución y control presupuestal y está integrado, con la SUNAT, par ala verificación de los proveedores y además, con el Banco de la Nación, para poder pagar a los proveedores.

- VARIOS: Existen además diferentes iniciativas tomadas por gobiernos locales, por ejemplo, los proyectos implementados por la Municipalidad de Miraflores; el proyecto "Ventana Pública" (implementación de un portal integrador de municipalidades locales de diferente ubicación, liderado por el CTT-PUCP), entre otros.

LAS MEJORES PRACTICAS INTERNACIONALES.

En los últimos años el tema e-government ha sido motivo de conferencias, foros, seminarios en casi todos los países del mundo, dando lugar a que algunos países inicien el desarrollo de esta nueva modalidad del quehacer gubernamental y de relación y atención a los ciudadanos. A su vez, otros países están en vías de comenzar el proceso o ven en éste una oportunidad para su desarrollo.

La experiencia internacional es variada en cuanto a los ámbitos de aplicación del Gobierno Electrónico, aunque, en su mayoría, los esfuerzos se han orientado principalmente a la provisión de información y servicios a los ciudadanos y empresas.

De acuerdo a los trabajos desarrollados por las Naciones Unidas (ONU, 2000; ONU, 2002), en su índice de Gobierno Electrónico, los países que más han avanzado en el desarrollo del Gobierno Electrónico son Estados Unidos, Australia, Nueva Zelanda, Singapur, Noruega, Canadá y el Reino Unido. Asimismo, destacan países que presentan situaciones similares entre sí, ya sea por sus condiciones de desarrollo, culturales o económicas, tales como México, Brasil, Chile, Sudáfrica, China y Egipto.

MEJORES PRÁCTICAS EN AMÉRICA LATINA.

Entre las mejores prácticas en América Latina destacan las siguientes:

- México y Colombia con sus agendas de más alto nivel.
- Costa Rica eliminando los aranceles a las computadoras y atrayendo grandes inversiones como la planta de microprocesadores de Intel.
- Brasil con su desarrollo temprano y ambicioso.
- Chile con sus propuestas modernas integrando al sector privado.

El gobierno electrónico pasa a desempeñar un rol fundamental en la modernización del Estado. En el caso de América Latina, los países que destacan por sus avances en materia de gobierno electrónico son Brasil y Chile.

De acuerdo con el informe de desempeño de Gobierno electrónico de Naciones Unidas, Brasil es el líder en Sudamérica en materia de gobierno electrónico. Chile, que últimamente ha logrado muy interesantes avances, es calificado por este reporte en muy buena posición, aunque los cambios más trascendentales se han dado recién durante el año 2002 (Naciones Unidas. *Benchmarking E-government: A Global Perspective*. 2002).

COMO ESTAMOS EN COMPARACION CON LOS DEMAS

Según el informe de la Unidad de Inteligencia de IBM el desempeño de un país es una medición del ambiente de e-business, un conjunto de factores que indican cuan atractivo es un mercado para oportunidades basadas en Internet. Los criterios analizados son:

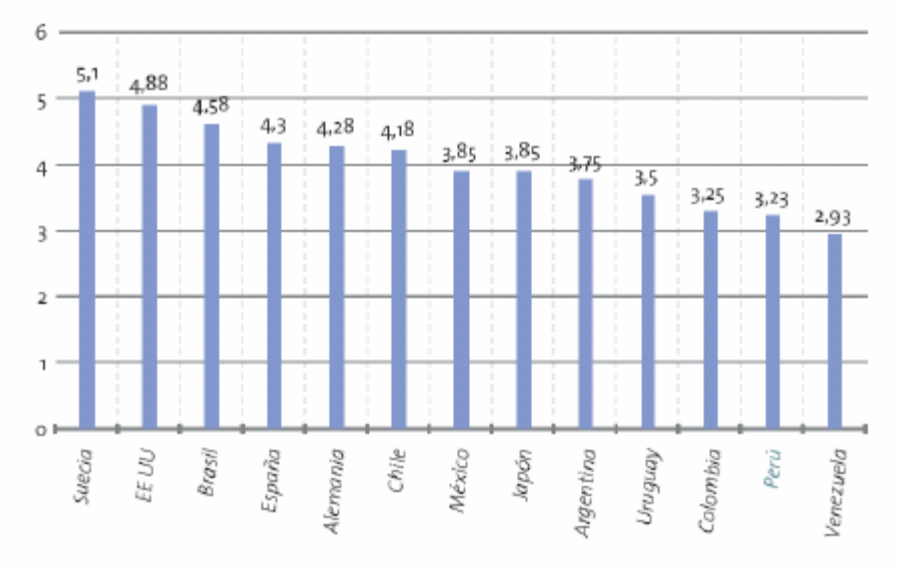
- La infraestructura tecnológica (conectividad).
- El ambiente general de los negocios.
- El grado de adopción del e-business por consumidores y compañías.
- El entorno legal y político.
- Las condiciones sociales y culturales que influencias en uso de Internet.
- La disponibilidad de servicios para soportar el e-business (Economist Intelligence Unit / IBM Institute for Business Value. e-readiness ranking 2004. 2005).

Cada criterio tiene un peso diferente, según su importancia.

En líneas generales, el Perú se encuentra en la posición 47 (de 64) a nivel mundial.

De otro lado, la Universidad de Harvard ha elaborado un índice indicativo del grado de desarrollo del gobierno electrónico en el seno de diferentes países. Tal y como se puede comprobar en la figura adjunta, el Perú presenta un índice realmente bajo, pues ocupa el puesto 50 entre las 75 naciones analizadas, por detrás incluso de varios países de su mismo entorno.

Índice de desarrollo de Gobierno Electrónico en el mundo

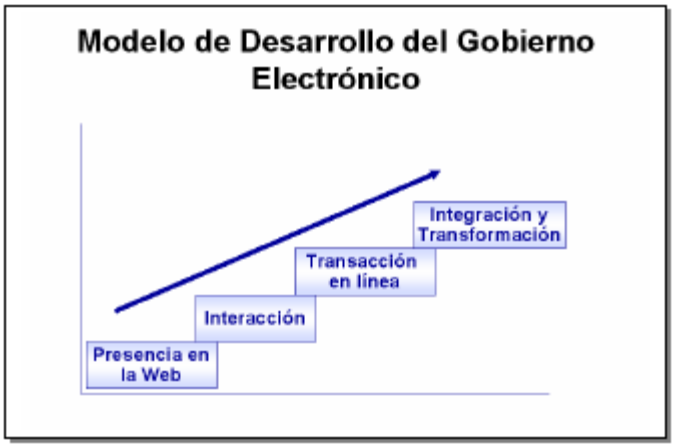


Fuente: Universidad de Harvard – 2001

En línea con lo anterior, la Organización de las Naciones Unidas publicó un informe con un índice de gobierno electrónico para 2001, en el que evaluó y clasificó a sus estados miembros en cuatro grupos según el grado de desarrollo: alto, medio, mínimo y deficiente. Si bien el Perú fue ubicado en el grupo de capacidad media, ocupaba el último lugar del mismo. En comparación con el resto de países sudamericanos, sólo se encontraba por delante de Paraguay (Naciones Unidas. *Benchmarking E-government: A Global Perspective*. 2002)

ELEMENTOS CLAVE PRELIMINARES PARA EL DESARROLLO DEL GOBIERNO ELECTRONICO

Es consenso en la comunidad internacional, que la implantación del gobierno electrónico pasa por cuatro fases:



- Presencia del Gobierno en la Web.
- Interacción del usuario con la Web a través de aplicaciones.
- Desarrollo de transacciones del usuario con la Web.
- Transformación total de los servicios del Estado hacia el usuario.

Las características de estas fases se detallan a continuación:

1ª Fase - Presencia en la Web

- Aprobación del público
- Flujo de procesos
- Costos de los procesos

2ª Fase – Interacción

- Búsqueda en bases de datos
- Respuesta del público por e-mail
- Administración del conocimiento
- Administración de contenidos
- Metadata
- Sincronización de datos
- Motor de búsqueda
- Sistema e-mail

3ª Fase – Transacción

- Confidencialidad/Privacidad

- Pago por transacción
- Autenticación
- Reingeniería de procesos del negocio
- Administración de relaciones con el ciudadano
- Proceso de interfase en línea
- Reglas de enlaces al sistema
- Seguridad
- Acceso a la información (Infraestructura para 24 horas x 7 días)

4ª Fase – Transformación

- Atención personalizada
- Agentes de identificación
- Navegador multifuncional y multiservicios
- Servicios integrados
- Cambios en la cadena de valor
- Nuevos procesos/servicios
- Cambios en la interacción entre: G2B, G2G, G2C y sus evoluciones
- Nuevas Aplicaciones
- Nueva estructura de datos

En el Perú, el Gobierno del Presidente Constitucional Dr. Alejandro Toledo Manrique, constituyó el Proyecto de Gobierno Electrónico, dependiente de la Presidencia del Consejo de Ministros, en junio del año 2002. A partir del mes de junio del 2003 y como consecuencia del Decreto Supremo Nº 066-2003-PCM, fusionó este proyecto de gobierno electrónico con la Sub Jefatura de Informática del INEI, constituyendo la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), con el fin de desarrollar el objetivo de poner "Un Estado al servicio de los ciudadanos".

Las acciones del Estado en el proceso de incorporación y uso de las nuevas tecnologías de información y comunicación, estarán enmarcadas por cuatro directrices:

- Servicios organizados en función del ciudadano.
- Accesibilidad sin exclusiones a los servicios y a la Administración.

- Acceso universal, irrestricto y seguro a la información.
- Transparencia.

El plan de acción preliminar constará de una seria de propuestas que sean acordes a estas directrices y que formen parte de una estrategia para el desarrollo del Gobierno Electrónico en el Perú (punto que se tratará más adelante).

Anexo 4: Dimensionamiento de equipamiento

Tabla A4.1

Dimensionamiento de equipamiento

Capacidad	Certificados	Requerimiento de almacenamiento	Nota
Tamaño BD CA	4,000,000 de certificados (4 KB) se agregan a la BD cada año	La BD de Certificados crecerá 16 GB cada año, 48 GB después de 3 años.	Permite conocer el tamaño del almacenamiento y el back UP, La capacidad total será : Tamaño BD CA+ Tamaño del Log de la BD CA + Tamaño BD CRL= 48 GB+ 130 MB+12 MB= 48.142 GB al año
Tamaño del log de la BD de la CA	RENIEC emitirá un promedio de 16,333 certificados al DIA consideremos un pico del 100% Pico	El log crecerá a un máximo de 130 MB GB en el peor caso de pico pero a 65 MB en situación normal	
Tamaño de CRL	400,000 certificados estarán en el CRL(30 B)	El total de CRL ocupara 12 MB (consideremos que se emitirá una vez a la semana) esto hace 2.4 MB diarias máximo.	El tiempo y la frecuencia de publicación son muy importantes sobre todo para clientes con líneas de baja velocidad. En la práctica esto se resuelve efectuando las transferencias a partir de las 00:00 Hras los fines de semana .Se contará con un Ancho de banda de 2 Mbps.
Trafico de replicación de directorio LDAP	En el peor caso la cantidad pico de certificados a emitir será de 33,332 Certificados en un dia de 8 horas.	Esto causara 33,332 x 1500 bits/3600 Seg=13,888 bps Aprox 14 Kbps	Considerando que el ancho de banda de Área Local es 100 Mbps no hay inconvenientes, tampoco por el enlace E1 WAN.
Memoria RAM	La cantidad de certificados tiene relación directa con la cantidad de Memoria del servidor donde alojaran los certificados y de acuerdo a los fabricantes de productos PKI es: 1 GB RAM=2 000 000 de Certificados	Para 4 000 000 se requiere 2 GB RAM	Todos los Servidores tendrán 2 Gb RAM .Todos los Servidores deben tener una configuración similar para cumplir con la regla de la redundancia.

(continúa)

(continuación)

Capacidad	Certificados	Requerimiento de almacenamiento	Nota
Tamaño BD CA	4,000,000 de certificados (4 KB) se agregan a la BD cada año	La BD de Certificados crecerá 16 GB cada año, 48 GB después de 3 años.	Permite conocer el tamaño del almacenamiento y el back UP, La capacidad total será : Tamaño BD CA+ Tamaño del Log de la BD CA + Tamaño BD CRL= 48 GB+ 130 MB+12 MB= 48.142 GB al año
Tamaño del log de la BD de la CA	RENIEC emitirá un promedio de 16,333 certificados al DIA consideremos un pico del 100% Pico	El log crecerá a un máximo de 130 MB GB en el peor caso de pico pero a 65 MB en situación normal	
Tamaño de CRL	400,000 certificados estarán en el CRL(30 B)	El total de CRL ocupara 12 MB (consideremos que se emitirá una vez a la semana) esto hace 2.4 MB diarias máximo.	El tiempo y la frecuencia de publicación es muy importante sobre todo para clientes con líneas de baja velocidad. En la práctica esto se resuelve efectuando las transferencias a partir de las 00:00 Hras los fines de semana .Se contará con un Ancho de banda de 2 Mbps.
Trafico de replicación de directorio LDAP	En el peor caso la cantidad pico de certificados a emitir será de 33,332 Certificados en un dia de 8 horas.	Esto causara 33,332 x 1500 bits/3600 Seg=13,888 bps Aprox 14 Kbps	Considerando que el ancho de banda de Área Local es 100 Mbps no hay inconvenientes, tampoco por el enlace E1 WAN.
Memoria RAM	La cantidad de certificados tiene relación directa con la cantidad de Memoria del servidor donde alojaran los certificados y de acuerdo a los fabricantes de productos PKI es: 1 GB RAM=2 000 000 de Certificados	Para 4 000 000 se requiere 2 GB RAM	Todos los Servidores tendrán 2 Gb RAM .Todos los Servidores deben tener una configuración similar para cumplir con la regla de la redundancia.

Elaboración propia

Anexo 5: Dimensionamiento de comunicaciones

El volumen de transacciones estimado por Internet para los 3 primeros años es de 56,000,000 de transacciones. Las transacciones consisten en peticiones del usuario para validar o verificar si un certificado está revocado utilizando el protocolo OCSP y se dirige al Servidor de directorio LDAP de la AERC. Estas peticiones tienen un tamaño promedio de 2 Kbytes el resultado del cálculo se muestra en el siguiente cuadro.

Tabla A5.1

Dimensionamiento del ancho de banda inicial

Oferta Inicial		
Capacidad Transaccional		
Ancho de Banda Efectivo	512	Mbps
Tamaño de transacción	16	Kbits
Transacciones por Segundo	32	
Transacciones por Hora	115,200	
Transacciones por Día (7 horas)	806,400	
Transacciones por mes (20 Días)	16,128,000	
Transacciones por año	193,536,000	
Capacidad de Emisión de Certificados Digitales		
Tiempo por Operación de Registro y Verificación	300	Seg
Tiempo por Operación de Emisión	15	Seg
Considerando 10 Emisores	1.5	Seg
Certificados Emitidos por Hora	2,400	
Certificados Emitidos por Día (7 horas)	16,800	
Certificados Emitidos por Mes (20 Días)	336,000	
Certificados Emitidos por año (12 meses)	4,032,000	
Conclusiones:		
1. A nivel transaccional la Demanda es Satisfecha ampliamente		
2. A nivel de Emisión de Certificados Digitales se presenta la Brecha del 40% con la Demanda proyectada		

Elaboración propia

Tabla A5.2

Dimensionamiento del ancho de banda de internet

Ancho de banda requerida para transacciones INTERNET		
No Transacciones Promedio anual para los primeros 3 años	56,000,000	
Transacciones X Mes	4,666,667	
Transacciones X día	233,333	
Transacciones X hora	33,333	
Transacciones X minuto	556	
Transacciones X Seg	9	
Tamaño de las Transacciones OCSP	2	kb
Trafico Kbps	148	
Considerando un pico de sobre carga de 300%	444	kbps
Ancho de banda normalizado	512	kbps

Elaboración propia

Anexo 6: Situación del Sector Privado

En este sector, el sector financiero es el que más rápidamente ha adoptado el uso de las tecnologías de información TIC.

En un mundo globalizado donde el Internet ha transformado la manera de hacer negocios, el sistema financiero no podía quedarse atrás. Se incorporan nuevas tecnologías de información en los servicios bancarios, que están alterando las definiciones tradicionales de producto, mercado y cliente, y que han cambiado la banca global, desarrollándose la banca por Internet, como un medio de comunicación entre los bancos y sus clientes ya sean personas naturales o jurídicas, para realizar transacciones en línea a un menor tiempo y costo para sus usuarios, optimizando mejor sus recursos.

En un principio cuando los bancos abrieron sus páginas web, con el fin de alinearse con las nuevas tecnologías, no estaban convencidos de la rentabilidad ni del potencial de este negocio. Es así que las primeras páginas tenían un diseño complicado, que impedía la navegación rápida y que sólo repetía los mismos mensajes publicitarios de las sucursales. Posteriormente, los bancos realizaron grandes inversiones en tecnologías y marketing, que les permiten hoy en día ofrecer una alta gama de servicios online gratuitos, desde consultas de saldos de cuentas de ahorros, transferencias entre cuentas, pago de servicios como luz, agua, teléfono, cable, inversiones en fondos mutuos, pago de impuestos, información de productos y servicios para la banca personal y empresarial, entre otros, a los cuales puede accederse desde la comodidad del hogar, la empresa o cualquier lugar. Asimismo, los bancos ya han desarrollado sofisticadas estructuras que garantizan la privacidad de las operaciones y ofrecen la máxima seguridad en la identificación de sus clientes a través del acceso vía Internet entre ellos tenemos:

Por otra parte, si bien en los inicios de la banca por Internet, los clientes no tenían confianza en este nuevo medio; la facilidad de su uso, la rapidez del servicio online y la reducción de costos que representa no tener que trasladarse a las oficinas de los Bancos ni realizar largas colas, son sus más significativas ventajas, y los factores que explican su importante crecimiento.

Los Bancos están realizando esfuerzos para fomentar la migración de sus clientes actuales hacia los medios electrónicos, ya que resultan más baratos que la sucursal; así como para atraer nuevos clientes virtuales a la banca por Internet. Si bien las estadísticas demuestran que el número de clientes que realizan operaciones a través de Internet no dejan de crecer; sin embargo se trata de un nuevo producto en maduración, y es preciso establecer una cultura de uso de esta tecnología fomentado la confianza y seguridad del usuario.

En la actualidad en el Perú los bancos ofrecen a sus clientes la posibilidad de realizar transacciones a través de los medios electrónicos, y vienen fomentando la migración de sus clientes hacia estos medios, debido a que son más baratos que la sucursal y mejoran la eficiencia. Por ejemplo, los bancos en el Perú cobran una comisión por pagar los servicios (teléfono, cable, agua, luz) en sus oficinas, mientras que si los pagos se efectúan por cajeros automáticos o por Internet no cobran ninguna comisión.

Según Business Perú, revista especializada del medio, el Banco de Crédito atiende en línea a unas 125 mil personas, que generan un movimiento anual de más de 450 millones de dólares. Las transacciones efectuadas por la red de redes constituyen alrededor del 15% del total de operaciones del banco.

En el BBVA Banco Continental la banca por Internet de personas naturales crece en 41% anual. En tanto que a nivel de empresas la expansión es más veloz aun y llega a 68%.

En Interbank la red ha jugado un papel importante en la modernización de la institución en este caso, el peso transaccional reside más o menos en un 60% en las personas y en un 40% en las empresas del total de transacciones, Internet representa el 19%, y también constituye el segundo canal en importancia

La realidad es similar en el Banco Wiese Sudameris esta realidad se traduce en eficiencia y costos no solamente para los usuarios, sino también al propio banco, sobre todo por el lado de los costos. Internacionalmente el costo transaccional por Internet es de 0.06 dólares por transacción, comparado con los 1.43 dólares a través de la ventanilla del banco.

La seguridad implementada por los bancos se basa en la tecnología criptográfica de 128 bits en combinación con el protocolo Sesiones Seguras SSL, en caso del Banco de Crédito e Interbank su zona segura está certificada por Verisign.

EMPRESAS DE CERTIFICACIÓN DIGITAL

En el Perú se han constituido como filiales de Autoridades Certificadoras internacionales las siguientes empresas:

- Telefónica Empresas:

Telefónica tiene un acuerdo con Verisign para suministrar soluciones de seguridad electrónica en Internet.

Según el acuerdo, Telefónica Empresas a través de su participada ACE (Agencia de Certificación Electrónica) ofrece al mercado Peruano servicios de Certificados y Firmas digitales.

Características de sus productos:

Los mismos se encuentran disponibles en tres categorías:

- CERTIFICADO DE USUARIO

  Utilizado para la firma digital de documentos y envío cifrado de información. Existen 2 tipos de certificados de usuario: Clase 1 y Clase 2

- CERTIFICADO DIGITAL CLASE 1

  Los Certificados Digitales de Clase 1 ofrecen el nivel más bajo de autenticación; por esta razón su principal uso es la codificación del correo electrónico y la autentificación de la identidad de la persona registrada. No se recomienda su uso para las aplicaciones comerciales en los casos en que se exija la prueba de la identidad.

- CERTIFICADO DIGITAL CLASE 2

  Certificado Digital de Clase 2 ofrece un nivel intermedio de autenticación; prueba razonablemente la identidad de la persona. Por esta razón su principal uso es la codificación del correo electrónico y la autentificación de la identidad de la persona registrada. Por lo tanto se recomienda su empleo en la realización de compras y transacciones "de bajo riesgo" efectuadas al interior de una organización o entre organizaciones.

Tabla A6.1

Certificados de usuarios

Certificado digital CLASE 1	Certificado digital CLASE 2	Validez
PRECIO	PRECIO	Un Año
Sin IGV:	Sin IGV:	
US$ 15.00	US$ 30.00	

Elaboración propia

- CERTIFICADO DE SERVIDOR

  Los Certificados de Servidor realizan comunicaciones seguras en línea a través de la tecnología Secure Sockets Layer (SSL). Se tiene en dos versiones

  Certificado de Servidor verisign secure site (40 bits)

  Certificado de Servidor verisign global secure site (128 bits)

- CERTIFICADO DE SERVIDOR VERISIGN SECURE SITE (40 BITS)

  Los certificados Secure Site usan certificados VeriSign Secure Site (formalmente llamados Server IDs), las compañías basadas en EE. UU. con servidores ubicados en EE. UU. pueden comunicarse a 128 bits dentro de los EE. UU. y a 40 bits fuera de los EE. UU. Servidores no basados en EE. UU., pueden comunicarse con 40 bits con sus clientes. Notar que la comunicación a 128 bits requiere software con capacidad para 128 bits tanto para el servidor como para el cliente.

- CERTIFICADO DE SERVIDOR VERISIGN GLOBAL SECURE SITE (128 BITS)

  Los Certificados Global Secure Site habilitan negociaciones de sesión SSL o TLS, usando el cifrado robusto de 128 bits RC2 o RC4.

Tabla A6.2

Certificados de Servidor

Descripción	Secure Server ID	Global Server ID	Validez
Venta	$374	$958	1 Año
Renovación	$374	$958	1 Año

Elaboración propia

- Servicios de CERTIFICADOS DIGITALES

Permite a una empresa establecer su propia infraestructura de llave pública sin incurrir en inversión de plataforma física. Lo que significa que una empresa podrá emitir a nombre propio sus certificados utilizando la infraestructura de TEmpresas y la validación de Verisign. Integración a múltiples aplicaciones: web browser, e-mail, Web Server, firewall entre otros. Estándar X.509.v3

Problema detectado

Cabe mencionar que los Certificados Digitales emitidos por telefónica tienen diferentes niveles de verificación, lo que les da diferentes aplicaciones y valores.

En el marco legal Peruano sólo existe sólo un nivel de verificación para los Certificados Digitales, que es el de verificación presencial (cara a cara) que se equipara al de mayor valor de los Certificados en Europa y Estados Unidos por ser el más confiable.

Telefónica ofrece un tipo de Certificado Digital con el nivel de verificación requerido por la legislación Peruana, sin embargo no tienen valor oficial al no haber pasado por el mecanismo de acreditación de la Autoridad Administrativa Competente.

Este proceso de acreditación, toma varios meses para verificar el cumplimiento de los requerimientos para emitir y administrar Certificados Digitales con los requerimientos de Seguridad utilizados a nivel internacional, así mismo implicará muy probablemente que se tenga que realizar una serie de modificaciones y ampliaciones de la inversión ya realizada por telefónica para poder lograr la acreditación.

- COSAPISOFT:

COSAPISOFT ha suscrito un acuerdo con DIGITAL SIGNATURE TRUST (DST). DST es un proveedor especializado de servicios de Autoridad Certificadora, para la emisión, validación y revocación de certificados digitales.

Gracias al patrocinio de la Autoridad Certificadora Digital Signature Trust (DST), COSAPISOFT, se ha constituido como Autoridad de Registro en el Perú, para proveer certificados digitales a nivel local, con expectativas de crecimiento en Latinoamérica. Además, asociado a la provisión de certificados digitales, COSAPISOFT a través de su unidad de negocios IDentID@Digital, provee una gama de soluciones, como firma digital, encriptación, correo electrónico seguro, certificados para servidor web, VPNs, servicio de time stamping, entre otros.

Los productos que ofrecen son los siguientes:

- **Certificados Digitales Personales**

Certificados que permiten asegurar y autenticar personas, garantizando la identidad de éstas y autenticidad de los negocios y transacciones que realizan on-line. El certificado digital LatinSignID, tiene el respaldo de la prestigiosa Autoridad Certificadora Digital Signature Trust (DST) – http://www.trustdst.com - cumple con los estándares x.509 v3 para certificados digitales.

El certificado digital LatinSignID, entre múltiples aplicaciones puede ser usado para firma de documentos, control de acceso, enviar correo electrónico seguro, intercambio seguro de información, entre otras que se pueden desarrollar de acuerdo a los requerimientos del usuario.

- **Certificados Digitales para Servidor**

Este tipo de certificados LatinSignWebID permite asegurar y autenticar un servidor Web o de red usando el protocolo Secure Socket Layer (SSL). El certificado digital para servidor, cumple con los estándares x.509 v3 SSL para certificados digitales; y son iguales en términos técnicos que los certificados digitales TrustID Server de DST, además cabe destacar que cumplen con las mismas exigencias en cuanto a políticas para su emisión.

Los navegadores que son capaces de soportar el uso de certificados digitales son:

- Netscape Navigator 3.0 y superior.
- Netscape Communicator 4.0 y superior.
- Microsoft Internet Explorer 3.0 y superior.

Problema detectado

COSAPISOFT al igual que las demás empresas que ofrecen Certificados Digitales, aún no han pasado por el mecanismo de acreditación de la Autoridad Administrativa Competente.

Cabe mencionar que los Certificados Digitales emitidos por COSAPISOFT al igual que los de su Entidad de Certificación Extranjera DST no cuentan con el nivel de verificación requerido por el marco legal Peruano.

Como se sabe en el marco legal Peruano sólo existe sólo un nivel de verificación para los Certificados Digitales, que es el de verificación presencial (cara a cara) que se equipara al de mayor valor de los Certificados en Europa y Estados Unidos por ser el más confiable.

Así mismo, CosapiSoft no ha pasado por el proceso de acreditación de la Autoridad Administrativa Competente, como se sabe este proceso de acreditación, toma varios meses para verificar el cumplimiento de los requerimientos para emitir y administrar Certificados Digitales con los requerimientos de Seguridad utilizados a nivel internacional, para el caso de CosapiSoft implicará que se tenga que realizar una serie de modificaciones y ampliaciones importantes de la inversión ya realizada para poder lograr la acreditación, lo que probablemente desanime a CosapiSoft a tomar esta opción.

- PERU SECURE E NET:

Empresa que tiene convenio con WISeKey - Autoridad de Certificación con sede en Suiza y que como las anteriores comercializara:

- Certificados Individuales
- Certificados de Servidor
- Certificados Empresariales

Esta empresa aun no ofrece servicios de Emisión de Certificados Digitales, pero habiendo observado la forma de trabajo de esta entidad en Suiza, y habiendo conversado con sus integrantes en el Perú, es de prever que estarán emitiendo Certificados Digitales con el nivel de verificación acorde a los requerimientos de la Ley Peruana.

Anexo 7: Conceptos técnicos

Resumen de mensajes

Aunque Alicia puede cifrar su mensaje para hacerlo privado, allí sigue existiendo una preocupación, que alguien puede modificar su mensaje original o sustituirlo con uno diferente, por ejemplo, para transferirse el dinero a sí mismos. Una forma de garantizar la integridad del mensaje de Alicia es crear un resumen sucinto de su mensaje y enviar también esto al Banco. Con la recepción del mensaje, el Banco crea su propio resumen y lo compara con el enviado por Alicia. Si son iguales entonces el mensaje fue recibido intacto.

Un resumen tal como este se llama es un resumen del mensaje, función de un sentido o función hash. Los resúmenes de mensajes crean representaciones cortas de tamaño fijo de mensajes más grandes y de longitud variable. Los algoritmos de resumen están diseñados para producir resúmenes únicos para diferentes mensajes.

Los resúmenes de mensaje hacen difícil determinar el mensaje desde su resumen, y hacen difícil encontrar dos mensajes diferentes que creen el mismo resumen, eliminando así la posibilidad de sustituir un mensaje por otro mientras se mantiene el mismo resumen.

Otro desafío que Alicia enfrenta es encontrar una manera de enviar el resumen al Banco con seguridad; cuando esto se alcanza, la integridad del mensaje asociado se asegura. Una forma para hacer esto es incluir el resumen en una firma digital.

Firma digital

Cuando Alicia envía un mensaje al Banco, éste necesita asegurarse que el mensaje sea realmente de ella, y no de un intruso que solicita una transacción que involucra su cuenta. Una firma digital, creada por Alicia e incluida con el mensaje, responde a este propósito.

Las Firmas Digitales son creadas mediante el cifrado del resumen del mensaje y otra información (tal como un número secuencial) con la llave privada del que origina el mensaje. Aunque cualquier persona puede descifrar la firma usando la llave pública, sólo

el firmante conoce la llave privada. Esto asegura que solamente el firmante lo haya firmado.

Incluyendo el resumen en la firma significa que la firma es solamente buena para ese mensaje; también asegura la integridad del mensaje puesto que nadie puede cambiar el resumen y además firmarlo.

Para protegerse contra la interceptación y la reutilización de la firma de un intruso en una fecha posterior, la firma contiene un número secuencial único. Esto protege al Banco contra un reclamo fraudulento de Alicia indicando que ella no envió el mensaje. Solamente ella pudo haberlo firmado (No Repudio).

Certificados digitales

Aunque Alicia hubiera podido enviar un mensaje privado al Banco, firmarlo y todavía asegurar la integridad del mismo, ella aún necesita estar segura que realmente se está comunicando con el Banco. Esto significa que ella necesita asegurarse que la llave pública que está utilizando corresponde a la llave privada del Banco. Igualmente, el Banco necesita también verificar que la firma del mensaje realmente corresponda a la firma de Alicia.

Si cada parte tuviera un certificado que valide la identidad de la otra parte, confirma su llave pública, y sea firmada por una tercera entidad de confianza, entonces ambos se asegurarían que se están comunicando con quién creen que se estaban comunicando. Cada parte utiliza la llave pública de la tercera entidad de confianza para verificar el certificado de la otra parte y para asegurar posteriormente la autenticidad de la llave pública del usuario.

Cabe indicar que los Certificados Digitales tienen tres aplicaciones, el de Autenticación, el de Firma y el de Encriptación.

Entidad de certificación (EC)

La tercera entidad de confianza que firma certificados con su llave privada y permite a otros verificar certificados por el uso de su llave pública correspondiente se llama Entidad de Certificación, o EC. Esta entidad de certificación también se la conoce como tercera parte de confianza, debido a este rol, no deben existir intereses comunes con ninguna de las dos partes.

Nota: Se cree que un Banco no debería ser una entidad de certificación y que sea a la vez una de las partes con las que usted hace transacciones económicas. La Razón para ello es que, como una entidad de Certificación, podría favorecerse, ya que es también parte interesada con la que Ud. hace negocios.

Importancia de la verificación

Uno de estos detalles que son importantes en la tecnología de Certificados Digitales es el factor de la verificación, un Certificado digital vale de acuerdo a la política de verificación que se utiliza. Si no se verifica nada el Certificado no tiene ningún valor, esto quiere decir que no hay una verificación previa para la emisión del certificado, por el contrario si por ejemplo se realiza una verificación presencial previamente, que es la que está contemplada por ejemplo en la Ley peruana, el certificado digital emitido es uno de los más valorados y dicho sea de paso es una de las metodologías de verificación más confiables a nivel internacional.

Lo que sucede es que normalmente en Europa y EE. UU. los Certificados Digitales tienen cuatro niveles, normalmente el 1 y el 2 no sirven para hacer ningún tipo de transacción, no proveen efecto legal ni económico, y el 3 y 4 tienen diferentes métodos de verificación, obteniendo mayor valor los que realizan una verificación más confiable, como la verificación presencial (cara a cara).

Necesidad de la autoridad reguladora

Es necesario que la Autoridad Reguladora entre en funcionamiento para primero acreditar que las Entidades de Certificación y las Entidades de Registro o Verificación cuenten con la infraestructura necesaria para emitir y administrar los Certificados Digitales, y que para ello sigan procedimientos estándares controlados y cuentan con los requisitos Administrativos, Técnicos y Físicos para dar un servicio seguro y confiable.

Así mismo se requiere que esta entidad reguladora supervise la operación de las Entidades Certificadora y las Entidades de Registro o Verificación y aplique acciones correctivas cuando sea necesario o adopte cambios en el Sistema debido a que toda esta tecnología tiene una dinámica muy alta y se requiere ínter operar con un ambiente internacional bajo reglas que también son dinámicas.

Forma de trabajo del certificado digital

Lo que hace esta tecnología es que al utilizarla, se va ha contar con una especie de "notario" en línea en todo momento, que va a dar fé que esta llave pública le pertenece a Alicia. Cuando ella usa la llave para firmar, la persona que recibe el mensaje, le pregunta a la entidad que firma el Certificado Digital, ¿Es ésta la llave de Alicia? Al hacerse la pregunta en forma electrónica, en ese instante, la Entidad Certificadora que ha firmado este certificado, responderá diciendo si el certificado es válido o no.

Llave privada, forma de trabajo

La llave privada no se lleva consigo, se instala en su máquina, y se queda dentro de su máquina, no se mueve, o se deja en un sitio de confianza como en un smartcard.

Participación de los privados

Tenemos que las entidades privadas también participarían del sistema porque la expectativa es que haya una demanda bastante grande y es muy posible que el Estado no tenga la capacidad suficiente para cubrir toda esta demanda, entonces, necesitamos también que los privados proporcionen parte de la oferta para poder satisfacer la demanda, y para mantener todo el sistema.

Por eso es que de acuerdo a Ley estas entidades privadas tienen que pasar por todo el proceso de certificación y acreditación a través de INEDCOPI la cual va a administrar el sistema de acreditación y supervisión de estas entidades.

Proceso de acreditación

El proceso de acreditación se realiza primero haciendo una revisión administrativa de los documentos presentados por la Entidad de Certificación solicitante donde se encuentra su declaración de prácticas describiendo sus procesos y su instalación implementada, esto se verifica que cumpla con los estándares aprobados y luego se hace una auditoria presencial que evalúa la funcionalidad y seguridad de la infraestructura, internacionalmente estas auditorías se delegan a terceras empresas que realizan la auditoria.

Estas terceras empresas realizan sus auditorías, previo paso de una acreditación donde se verifica que tenga personal capacitado certificados en CISSP (Certified Information Systems Security Professional) y que tenga conocimientos de la tecnología de Certificados Digitales.

Luego esta empresa realizará la auditoria tomando en cuenta el estándar de seguridad ISO-17799 o el de Common Criteria, ISO-15408.

Todo este proceso no debe tener una duración superior a los 120 días útiles de acuerdo a la ley vigente de Firmas y Certificados Digitales

Criterios para la autorización de una AERC

En el presente estudio se proponen los criterios para la autorización de la creación de una Entidad de Certificación del Estado (Autoridad de Emisión y Registro de Certificados AERC), el objetivo principal es que cubra las necesidades del estado, hay criterios de varios tipos, uno es el de cobertura es decir que si falta cobertura a nivel nacional para emisión de certificados necesitamos otras entidades que apoyen a asumir estas necesidades a nivel nacional; Otro es el criterio de confianza, esto es debido a que existen otras entidades dentro del estado que tienen unos requerimientos de seguridad y confianza mayor, como por ejemplo el sector Defensa, entonces ellos podrían tener sus propias Entidades de Certificación para uso interno.

Algoritmos criptográficos

La criptografía tiene varias diferencias de las matemáticas puras. Una de éstas es que la criptografía es más descriptiva en sus libros de textos. Mientras que un matemático puede utilizar A y B para explicar un algoritmo, un criptógrafo puede utilizar los nombres ficticios Alicia y Bob. Así, en las secciones siguientes, ya no se eligen los nombres Alicia y Bob aleatoriamente; y pueden ser encontrados en casi todos los libros de textos de la criptografía.

Supongamos que Alicia desea enviar un mensaje a su Banco para transferir dinero. Alicia quisiera que el mensaje fuera privado, puesto que incluye información tal como su número de cuenta y el monto de la transferencia. Una solución es utilizar un algoritmo criptográfico, una técnica que transformaría su mensaje en una forma cifrada, ilegible excepto para ésas personas a las que va dirigido. Cuando está cifrado, el mensaje se puede interpretar solamente con el uso de la llave secreta correspondiente. Sin la llave el mensaje es inútil. Los buenos algoritmos criptográficos hacen esta labor de descifrar el texto original tan difícil para los intrusos que no vale la pena hacer el esfuerzo.

Hay dos categorías de algoritmos criptográficos:

- Convencional

- Llave pública

La criptografía convencional, también conocida como criptografía simétrica, requiere que el remitente y el receptor compartan una llave, un pedazo de información secreta, que se utiliza para cifrar o para descifrar un mensaje. Si esta llave es secreta, entonces nadie con excepción del remitente o del receptor puede leer el mensaje.

Si Alicia y el Banco cada uno tienen una llave secreta, entonces pueden enviarse mensajes privados. Sin embargo, la tarea de elegir una llave privada antes de comunicarse, puede ser problemática.

La criptografía de llave pública, también conocida como criptografía asimétrica, soluciona el problema del intercambio de llaves, definiendo un algoritmo que utilice dos llaves, cada uno de las cuales se puede utilizar para cifrar un mensaje. Si una llave se utiliza para cifrar un mensaje, entonces la otra se debe utilizar para descifrarlo. Esto permite recibir mensajes seguros simplemente publicando una llave (la llave pública) y guardando la otra en secreto (la llave privada).

Cualquier persona puede cifrar un mensaje usando la llave pública, pero solamente el dueño de la llave privada puede leerla. De esta manera, Alicia puede enviar mensajes privados al dueño de un par de llaves (el Banco) cifrándolos con el uso de su llave pública. Solamente el Banco podrá descifrarlos.

Firmas electrónicas y certificados digitales

La tecnología de Certificados Digitales nació en los años 90. Alrededor del año 2000, muchos estados visualizaron su aplicación para aplicaciones estatales, sin embargo en ésta época a pesar que habían enfocado muy bien el tema de que el problema era identificar a la gente en forma electrónica, pero los estándares todavía no estaban tan maduros la tecnología no estaba tan estable y cuando empezaban a instalar algunos estados por ejemplo en EEUU empezaron a frustrarse con las implementaciones, entonces buscaron una forma de escaparse del sistema, para ello crearon un mecanismo que lo llamaron “el principio de neutralidad tecnológica”, entonces de acuerdo a este principio de neutralidad tecnológica, estabas obligado a aceptar otros tipos de tecnologías de identificación.

Esas otras tecnologías alternativas de autenticación, con el tiempo fracasaron y desaparecieron, mientras que la tecnología de Certificados Digitales siguió madurando,

se organizaron, crearon estándares que estabilizó la tecnología y se estabilizaron mucho más las cosas que se construían encima, actualmente se ha difundido a nivel mundial con infraestructuras con millones de Certificados y realizando transacciones por miles de millones de dólares al año.

En el Perú, dejaron esta huella vamos a decir el principio de neutralidad tecnológica que incluso fue incorporado en el marco legal Peruano, nuestra legislación. Así mismo, se encontró en la legislación la idea de que la firma electrónica podría ir por su lado, y se menciona en nuestra legislación aunque no se desarrollan sus atribuciones.

Tecnología del pin

Algo que se comenta últimamente es lo referente al PIN, son claves que utilizan los Bancos, los cuales no son certificados digitales, sino que están asociados a las firmas electrónicas.

Un pin es un secreto compartido que lo conocen el Banco y el cliente, tienen todo un estándar técnico para su funcionamiento (SET), se cuenta con un procedimiento para generar las llaves, una identificación que se tiene que mantener encriptada para guardar estos pines y una forma de entrega que es confidencial y segura (Vía transporte seguro a su domicilio). Por otro lado, cuando se realiza transacciones existen mecanismos de defensa, por ejemplo, se puede revisar una transacción y no autorizarla posteriormente, cosa que no se podría hacer con un certificado digital; otro mecanismo consiste en un control en su uso, se verifica si la tarjeta existe, si corresponde al titular y se pide una Cédula de Identidad al realizar la transacción.

Estas tecnologías de Firmas Electrónicas, requieren de otros elementos que deben ser incorporados para proveerles un nivel de seguridad y funcionalidad mínimos, a diferencia de la tecnología de Certificados Digitales, que provee sus propios elementos de seguridad y funcionalidad necesarios.

La firma electrónica

Es aquí donde se identifica a la Firma Electrónica como el Universo de todas las firmas. Técnicamente se la define como “cualquier símbolo basado en medios electrónicos, empleado por una persona natural o jurídica para expresar su voluntad y que cumple algunas o todas las funciones de una firma autógrafa”.

En nuestra legislación la firma electrónica es definida como: “Cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse, autenticar y garantizar la integridad de un documento electrónico o un mensaje de datos cumpliendo todas o algunas de las funciones características de una firma manuscrita” (Ley Nº 27269)

La firma electrónica como complemento

Existen Firmas Electrónicas que sirven de complemento a la firma digital en la medida que se soportan sobre los Certificados Digitales, el Certificado Digital autentica a una persona, pero lo que puede hacerse con la autenticación es solo una parte de toda la transacción, por ejemplo si se quiere realizar un pago en un Banco, no solo basta saber quién es la persona, se tiene que saber cuál es su número de cuenta, es decir saber otros datos, estos otros datos también son información electrónica, y de alguna forma pueden haber otras Firmas Electrónicas, como por ejemplo es posible que incluya su huella digital además de otros tipos de mecanismos para tener una mayor certeza.

Anexo 8: Procesos Principales

En función del perfil del usuario final del certificado y por tanto del uso que va a dar a este, La AERC tiene definidas las siguientes clases de certificados:

- Certificados personales
- Certificados para empresas
- Certificados para sitios o Servidores

Independientemente del tipo de certificado todos los certificados emitidos por la AERC son certificados X.509 v3.

La prestación de estos servicios de certificación involucra los siguientes procesos:

Proceso de Solicitud y Emisión de Certificados digitales

El proceso para la obtención de un certificado digital tendrá dos partes:

Una primera, que consiste en una pre-inscripción que el usuario realizará desde su domicilio o una cabina de Internet accediendo para ello a un portal WEB de la Entidad de Registro (ER).

La segunda será un acto presencial por única vez en las oficinas de la ER para probar su identidad después de la cual se le otorgará el certificado digital firmada por la AERC.

Requisitos:

- Ser ciudadano mayor de 18 años
- Poseer un cuenta de correo electrónico
- Documento de identidad DNI
- El representante de una empresa solicitante tiene autorización para realizar la petición además de poseer un certificado digital personal.
- Poseer al menos un diskette de 3.5

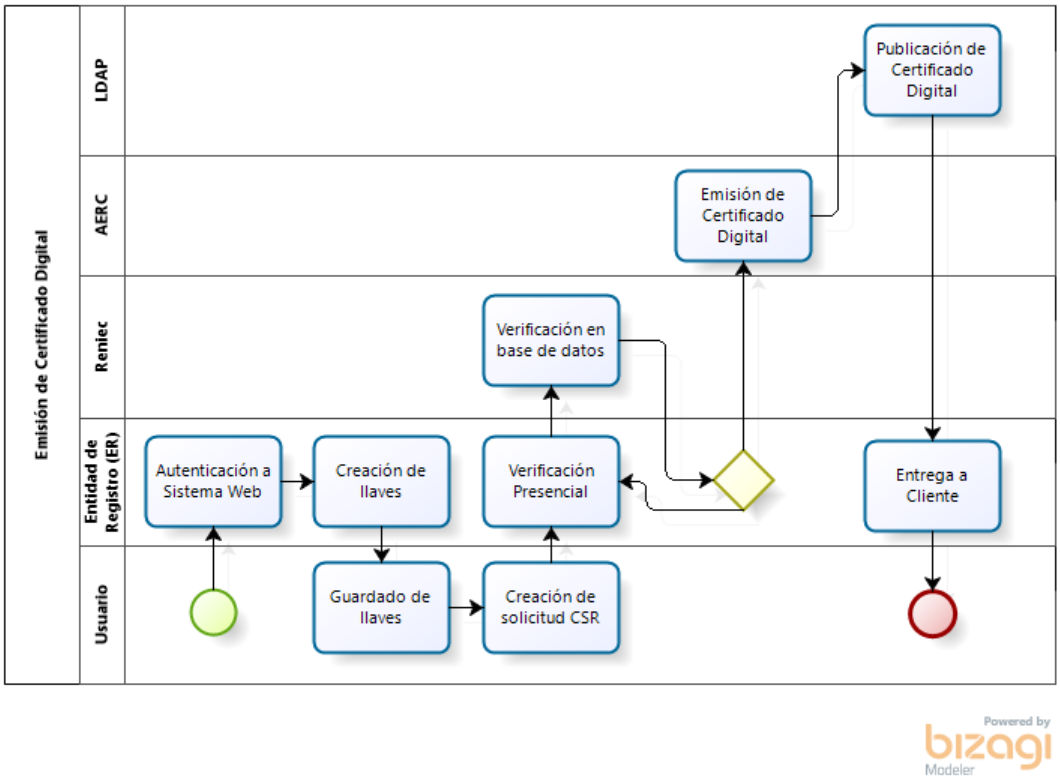
El procedimiento es como sigue:

- El usuario accede al portal de la ER a la página de solicitud de certificados digitales se identifica con su DNI.
- Genera el par de claves y graba el diskette
- Llena el formulario de pre-inscripción
- Solicita una cita en el mismo formulario
- La ER verifica el formulario de pre-inscripción con la BD de Reniec y si es correcta confirma la cita.
- El usuario se presenta a la Oficina de la ER portando sus documentos de identidad en la fecha y hora de la cita.
- La ER verifica, valida la identidad del solicitante, genera una solicitud, firma y envía a la AERC.
- La AERC genera el certificado y lo firma
- La AERC y publica el certificado en el directorio LDAP.
- La ER importa el certificado de la BD de la AERC y procede a la entrega del certificado en el diskette del usuario quien firma el cargo de recepción.

En la siguiente página se presenta el diagrama de flujo del proceso de obtención de un certificado digital:

Figura A8.1

Proceso de emisión de Certificado Digital



Elaboración propia

Proceso de uso de un Certificado Digital

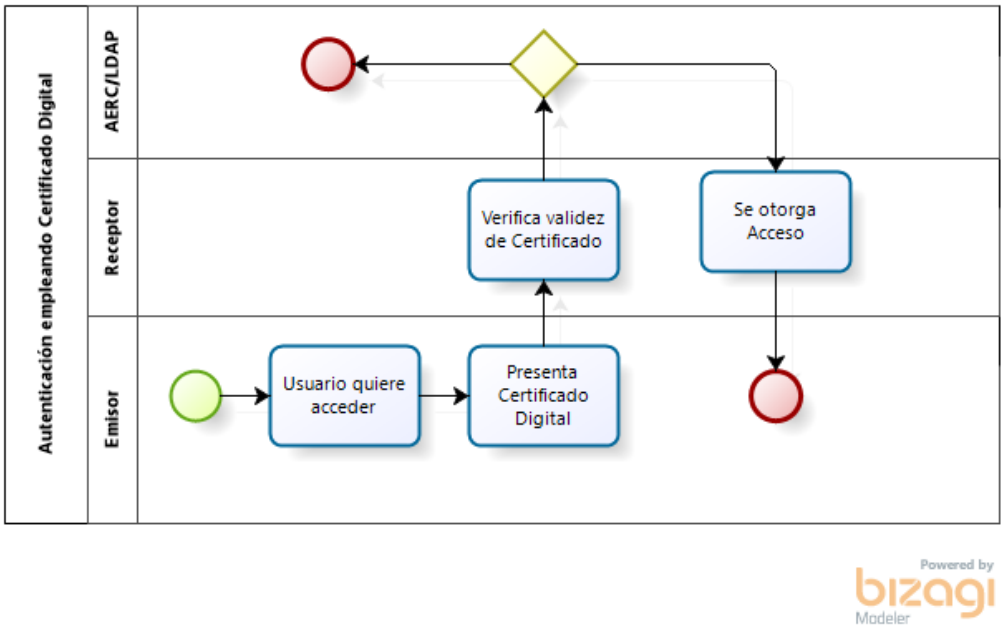
Una vez obtenido el certificado el propietario está habilitado para realizar las operaciones de autenticación, firmado y encriptación empleando certificados digitales, esto con total garantía debido al uso de las Entidades Certificadoras que permiten la verificación de todos los certificados digitales en tiempo real, el uso de las claves públicas y privadas permite la integridad, confidencialidad de sus comunicaciones y como consecuencia las operaciones que cumplen estas condiciones no pueden se repudiadas y se pueden emplear en los siguientes procedimientos:

Proceso de autenticación usando un Certificado Digital

- El usuario quiere acceder a una página web, a una aplicación o a una infraestructura física
- El usuario presenta su certificado digital
- El receptor verifica la validez del certificado empleando el protocolo OCSP con el servicio de publicación de la AERC
- Si el proceso de validación es exitoso, el acceso es concedido, sino es denegado.

Figura A8.2

Proceso de autenticación empleando certificado digital



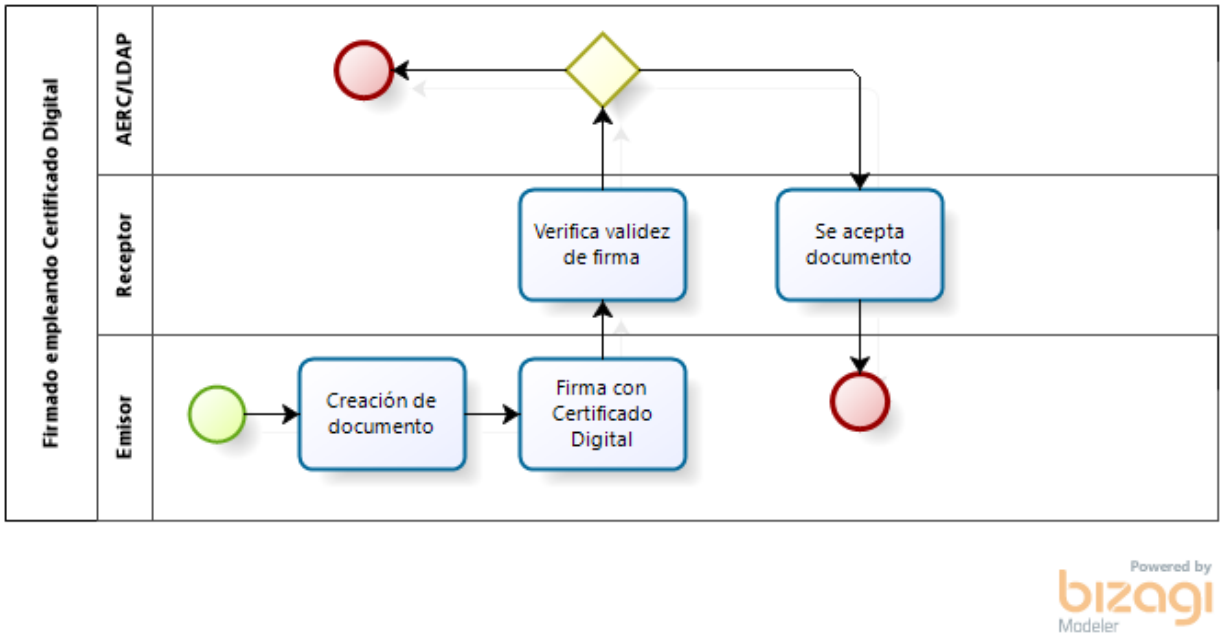
Elaboración propia

Proceso de Firmado usando un Certificado Digital

- El usuario Genera mensaje o archivo a ser transmitido usando cualquier aplicación de comunicación o de negocio
- El usuario firma el documento empleando su certificado digital
- El destinatario recibe el documento
- El destinatario verifica la firma y verifica la validez del certificado
- Si el proceso de verificación es exitoso, el documento es original y no ha sido alterado.

Figura A8.3

Proceso de firmado empleando certificado digital



Elaboración propia

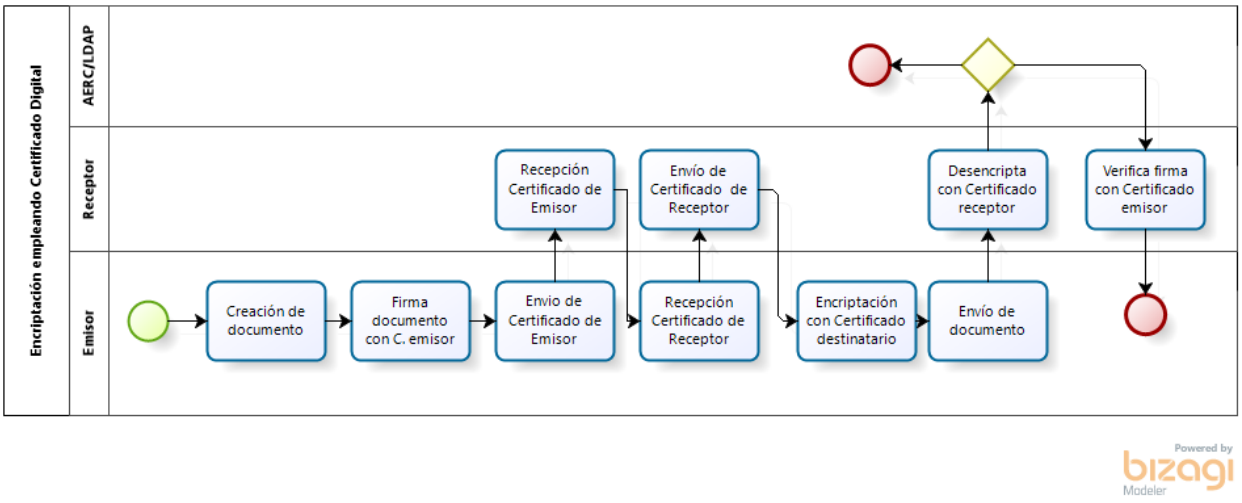
Proceso de encriptación usando un Certificado Digital

- El usuario Genera mensaje o archivo a ser transmitido usando cualquier aplicación de comunicación o de negocio
- El usuario Firma el mensaje o archivo con su Certificado Digital
- El usuario envía su Certificado Digital y solicita el Certificado Digital del Destinatario
- Destinatario recibe Certificado Digital del Emisor y envía su Certificado Digital
- El usuario Encripta el mensaje o archivo con Certificado Digital del Destinatario
- Usuario Envía el mensaje o archivo firmado y encriptado
- El destinatario recepciona el mensaje o archivo firmado y encriptado
- El destinatario verifica la firma de la Entidad de Certificación que firma Certificado del Usuario remitente contra el Servidor de directorios de la AERC.
- Desencriptación del mensaje o archivo empleando su llave privada

Todo este procedimiento es realizado en forma automática por el sistema de cómputo de la AERC utilizando el Protocolo de Estado de Certificado en línea OCSP.

Figura A8.4

Proceso de encriptación empleando certificado digital



Elaboración propia

Proceso de Revocación de un certificado digital

La revocación de un certificado se puede dar por:

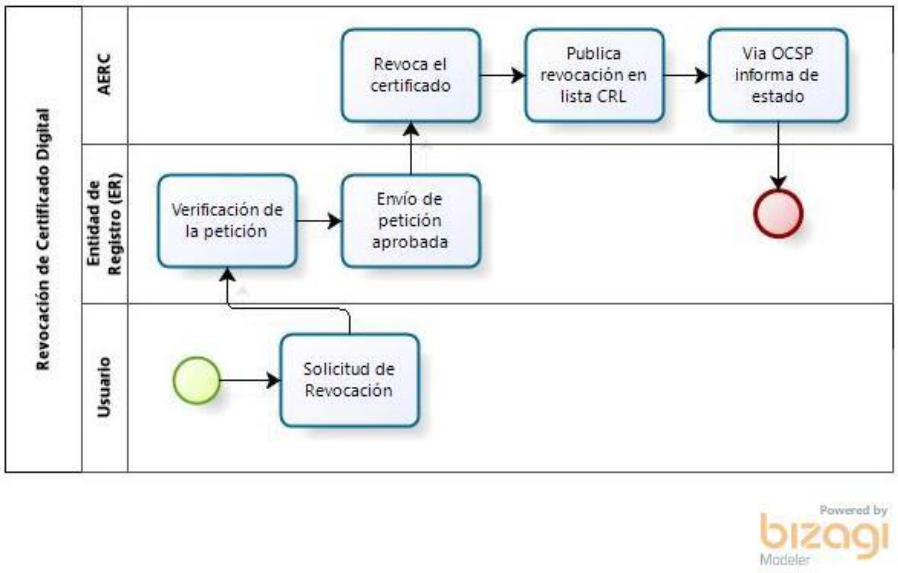
- La expiración del tiempo de validez del certificado,
- Cualquier cambio en la identidad del usuario
- El usuario sospecha que su clave privada ha sido comprometida.

El procedimiento es el siguiente:

- El usuario remite la Solicitud de anulación de Certificado Digital a la Entidad de Certificación a través de la ER utilizando el servicio de portal de la ER..
- La ER efectúa una segunda verificación de información sustentatoria
- La ER inicia la Generación y envío de solicitud de anulación de Certificado Digital a Entidad de Certificación en este caso a la AERC.
- La AERC Recibe la solicitud de anulación de Certificado Digital
- La AERC Ingresa el Certificado en la Lista publicada de Revocación de Certificados
- La AERC Actualización de Lista de Revocación consolidada del Estado y via OCSP informa del estado del Certificado Digital

Figura A8.5

Proceso de revocación de certificado digital



Elaboración propia