Universidad Nacional de Costa Rica
Programa de Gestión de Tecnologías de Información y Comunicación (ProGesTIC)
Maestría en Administración de Tecnologías de Información y comunicación con énfasis en la Administración de Proyectos
Proyecto Integrado II

PEDRO HUMBERTO LEIVA CERDAS (FIRMA)

Digitally signed by PEDRO HUMBERTO LEIVA CERDAS (FIRMA)
DN: CN = PEDRO HUMBERTO LEIVA CERDAS (FIRMA), SN = LEIVA CERDAS, G = PEDRO HUMBERTO, C = CR, O = PERSONA FISICA, OU = CIUDADANO
Reason: Documento firmado por Pedro Leiva.
Date: 2009.12.06 13:26:56 -06'00'

Conceptualización del marco metodológico para la implementación de la herramienta de firma digital, que le permita al Instituto Costarricense de Acueductos y Alcantarillados obtener una posición de vanguardia tecnológica, además de una mayor agilidad en sus procesos de negocio y las TIC.

Pedro Leiva Cerdas

Christian Vargas Araya

Heredia, Costa Rica. 01 de Diciembre, 2009

Dedicatorias

Agradezco a DIOS, por darme la vida, la salud y la sabiduría para hacer realidad un logró más en mi vida. Dedico este trabajo mi Madre que siempre me ha dado más que su apoyo, será una deuda nunca saldada, la amo con todo mi corazón, a mi Padre que desde el cielo me ha iluminado los últimos 18 años y a mis hermanos que siempre han creído en mí.

Agradezco a mis colegas de la MATI por sus innumerables consejos, trasferencia de conocimientos y apoyo durante estos dos maravillosos años. A José Rafael mi hermano mayor, por su apoyo en la lectura y observaciones al documento. Agradezco a Ma. Lorena Echandi, patrocinadora del proyecto, sus observaciones fueron un aporte de gran valor. También, mis más sinceras gracias a los compañeros de AyA que brindaron información importante y colaboraron para el éxito de este proyecto. A todos muchas gracias.

*_ Pedro Leiva Cerdas_*

Dedico el logro a Dios por darme la fortaleza y la perseverancia para afrontar y superar este reto. A mi padre y madre (+) por ser mi incondicional apoyo, luz y guía en la vida; les amo con todo mi corazón. A mis seres queridos y razones de vida Roberto, Graciela, Susan, la pequeña Brenda, y mi preciosa Lucy, a quienes les amo. A toda mi familia y amigos por su apoyo.

Agradezco a aquellos colegas que desinteresadamente nos compartieron su conocimiento. A Don Ismael Mora por su apoyo incondicional en este proceso; y a mi gran amigo y compañero Pedro, quien me acompañó desde el primer día hasta la fecha a vivir esta gran aventura.

_ Christian Vargas Araya _

Índice General

Índice de figuras

Índice de cuadros

Índice de fotografías

Resumen ejecutivo

En la actualidad se vive en la era del conocimiento y la tecnología, la cual ha mantenido al mundo en constante aceleración con logros y avances que, décadas atrás, no estaban presentes en la mente o imaginación del ser humano. La globalización ha cambiado la forma de hacer negocios, y por consiguiente, la visión de quienes aprovechan las nuevas oportunidades que a nivel comercial y tecnológico, el mundo nos brinda.

Costa Rica no escapa de ser partícipe de ese mundo globalizado y acelerado. El país ha tenido que modificar la manera de legislar y administrar sus tecnologías de información y comunicación; al punto de introducir el concepto de "Gobierno Digital", el cual pretende incursionar en nuevas técnicas para optimizar los procesos internos y, lograr así, una mejora en la entrega de productos y servicios a los costarricenses. Por esa necesidad de impulsar un gobierno más ágil tecnológicamente, es que nace la iniciativa de incentivar la creación e implementación de la herramienta de firma digital, como primer paso para digitalizar los productos y servicios del Estado.

La iniciativa de Gobierno Digital se hizo realidad cuando en mayo del 2006, la Asamblea Legislativa de Costa Rica declara de interés público la realización de esfuerzos para desarrollar el "Gobierno Digital" en las instituciones públicas costarricenses, mediante el Decreto N°33147-MP **[DEC33147]**. En diciembre del 2007, Costa Rica contó con su primera Ley de Certificados, Firmas Digitales y Documentos Electrónicos No 8454, redactada por el Ministerio de Ciencia y Tecnología (MICIT).

Por lo anterior expuesto crea una nueva necesidad tecnológica en el Instituto Costarricense de Acueductos y Alcantarillados, lo que dio vida a la conceptualización del marco metodológico para la implementación de la herramienta de firma digital; ─razón de este estudio─.

En las primeras páginas de este documento, se pretende explicar, de una forma fácil y amigable para cualquier lector, los diversos términos que involucra el concepto

de la herramienta “Firma Digital”. Entre los términos más destacados se redacta una definición sobre qué es firma digital, sus diversos componentes ─como la llave pública, la privada─, cómo se realiza en forma gráfica el proceso de firma digital y la definición de otros conceptos fundamentales para la implementación, entre ellos, la definición de la infraestructura de llave pública (PKI).

En las siguientes secciones, se presentan algunas recopilaciones sobre el conocimiento adquirido y mejores prácticas de implementación que han realizado varios profesionales expertos, partícipes de la ejecución de firma digital en sus respectivos países; como por ejemplo, en Argentina, México, Chile, Brasil y otros. Estas diversas perspectivas de desarrollo de nuevas tecnologías permitieron obtener información depurada y con varios años de implementación; así como, la mejor forma de realizar el proceso de firma digital en una empresa gubernamental costarricense.

Posteriormente, se comenta la historia de la firma digital y sus comienzos, desde que fue planteada como una iniciativa necesaria para lograr el concepto de Gobierno Digital en Costa Rica. Se logró detallar la creación y el funcionamiento de varias instancias fundamentales para que la firma digital pueda funcionar en Costa Rica como, por ejemplo, la infraestructura de llave pública (PKI), la autoridad certificadora dependiente del Sistema Nacional de Pagos Electrónicos (CA-SINPE), y el papel que juegan actualmente las entidades financieras públicas como el Banco Central de Costa Rica (BCCR), el Banco de Costa Rica (BCR) y el Banco Popular y de Desarrollo Comunal (BPDC).

Una vez aclarados los conceptos básicos y la historia de la herramienta de firma digital en Costa Rica, seguidamente, se plantea la situación actual, pendiente de resolver, en el Instituto Costarricense de Acueductos y Alcantarillados. Para este propósito, se esboza la razón de ser del marco de conceptualización, así como una solución detallada del problema planteado y un escenario meta que apunta a definir un plan para implementar la herramienta de firma digital en los procesos de negocio del AyA. También, pretende generar un valor agregado y agilización de los servicios para suplir servicios electrónicos seguros y rápidos.

También se presenta una sección con las diversas justificaciones que han respaldado el Proyecto de Firma Digital en Costa Rica, con experiencias aportadas por los profesionales involucrados, las iniciativas legales por impulsar la creación y desarrollo del concepto de Gobierno Digital en Costa Rica y los incipientes pasos que ha dado el proyecto, ya que es un proyecto muy reciente que aún no ha tenido mucho desarrollo. Se estima que el avance y perfeccionamiento de este proyecto llevará varios años.

Además, para complementar esas justificaciones, se plantea un análisis de costo beneficio. En este análisis, fueron considerados cuatro servicios que provee el Instituto Costarricense de Acueductos y Alcantarillados, divididos de la siguiente manera: dos servicios internos y dos externos. Este análisis expone los costos que tiene la implementación de cada uno de esos servicios y los requisitos necesarios para lograrlo, en cuanto a infraestructura, asesoría en seguridad, solicitud de certificados, entre otros. Así como los beneficios que esta reciente y segura herramienta de identificación de individuos le genera a la Institución y a los usuarios que la aprovechan, ─como por ejemplo, el ahorro de tiempos de traslado para el cliente o el fácil acceso por internet de los servicios que brinda la Institución sin tener que desplazarse a sus instalaciones─.

El análisis se complementa con una serie de criterios para gestionar los riesgos de este proyecto, así como el cambio cultural interno y externo que implica su implementación; además, de una estrategia futura que pretende esclarecer un eventual camino proyectado sobre la post implementación de la herramienta de firma digital.

Luego en este documento se desarrolla un prototipo funcional explicado gráficamente que pretende demostrar el potencial y la facilidad que implica la utilización de la firma digital en un eventual sistema *Web* de la Institución. Finalmente se definieron una serie de conclusiones, recomendaciones y análisis retrospectivo que reflejan la experiencia vivida en la implementación de este novedoso e innovador proyecto tecnológico. A continuación, el detalle del trabajo realizado.

Antecedentes

Introducción.

Antecedentes de la empresa.

El Instituto Costarricense de Acueductos y Alcantarillados (AyA) fue fundado mediante la a Ley Constitutiva No. 2726 del 14 de abril de 1961, y en su artículo primero reza *"Con el objeto de dirigir, fijar políticas, establecer y aplicar normas, realizar y promover el planeamiento, financiamiento y desarrollo y de resolver todo lo relacionado con el suministro de agua potable y recolección y evacuación de aguas negras y residuos industriales líquidos, lo mismo que el aspecto normativo de los sistemas de alcantarillado pluvial en áreas urbanas, para todo el territorio nacional se crea el Instituto Costarricense de Acueductos y Alcantarillados, como institución autónoma del Estado*" **[LEY2726]**.

> Cuya **misión** es: *"Normar y garantizar los servicios de agua potable, alcantarillado sanitario y tratamiento, según los requerimientos de la sociedad y nuestros clientes, contribuyendo al desarrollo económico, ambiental y social del país".*
>
> Y su **visión** dice así: *"Ser la Empresa Pública líder en agua potable y saneamiento comprometida con la excelencia en el servicio al cliente, para brindar calidad de vida a la sociedad costarricense en armonía con el ambiente.".*

Definición del problema.

Actualmente el Instituto Costarricense de Acueductos y Alcantarillados se ve en la necesidad de implementar la herramienta de firma digital, como parte de una iniciativa en materia de crecimiento y transparencia de la gestión pública, disminución de la brecha digital, además del desarrollo tecnológico del gobierno de Costa Rica, el

cual mediante el Decreto N°33147-MP **[DEC33147]**, declara de interés público los esfuerzos por desarrollar el Gobierno Digital en las instituciones públicas.

El proyecto encuentra viabilidad y sustento jurídico, para su aplicación en el Instituto Costarricense de Acueductos y Alcantarillados, en la *Ley de Certificados, Firmas Digitales y Documentos Electrónicos No. 8454* **[LEY8454]**. Esta aplicación se enmarca a toda clase de transacciones y actos jurídicos, públicos o privados, salvo disposición legal en contrario, o que la naturaleza o los requisitos particulares del acto o negocio concretos resulten incompatibles. Además, porque la misma norma en el artículo primero establece el ámbito de su competencia y faculta al Estado y a todas las entidades públicas para utilizar los certificados, las firmas digitales y los documentos electrónicos, dentro de sus respectivos ámbitos de competencia.

Asimismo, es importante destacar que en esta materia se deberán observar los siguientes principios:

a) Regulación legal mínima y desregulación de trámites.
b) Autonomía de la voluntad de los particulares para reglar sus relaciones.
c) Utilización, con las limitaciones legales de reglamentos autónomos por la Administración Pública para desarrollar la organización y el servicio interno o externo.
d) Igualdad de tratamiento para las tecnologías de generación, proceso o almacenamiento involucradas.

Dada esta condición de ley, se pretenden identificar una serie de factores externos e internos, tales como los siguientes:

- ✓ **Externos:** la centralización de trámites digitales, mejoras en los servicios y productos que se ofrecen y la coordinación e intercomunicación entre instituciones del Estado**.**

- ✓ **Internos:** como la mejora en la infraestructura tecnológica, adquisición o desarrollo de sistemas informáticos y de comunicación ─capaces de interactuar bajo el concepto de firma digital─, la definición de procedimientos del negocio para

funcionar con la herramienta, experiencia y especialización del personal para el buen funcionamiento y asesoría en el ámbito de firma digital. Todos en aras de promover la modernización, simplificación, reducción de costos y eficiencia de la prestación de servicios y trámites que ofrece la Institución.

Pertinencia de la situación.

El proyecto de implementación de la herramienta de firma digital adquiere gran importancia y apoyo en la función de la Secretaria Técnica de Gobierno Digital (STGD), como un proyecto de gestión y de políticas según lo expresa el Plan de Acción Gobierno Digital 2008-2010 en su punto "D" **[STGD-08]**. Generó un avance importante en el uso de tecnología, para circular por la vía del Gobierno Digital, una vez implementado el proyecto, y una adecuada promoción del uso de dicha herramienta. Esto propició una importante y significativa disminución en la brecha digital costarricense y sería un detonante significativo en una lista infinita de utilidades, para utilización de los funcionarios y clientes de las instituciones públicas.

Objetivos del proyecto.

Objetivo general.

Conceptualización del marco metodológico para la implementación de la herramienta de firma digital, que le permita al Instituto Costarricense de Acueductos y Alcantarillados obtener una posición de vanguardia tecnológica, además de una mayor agilidad en sus procesos de negocio y las TIC.

Objetivos específicos. (Etapa I)

1. Investigar mejores prácticas en al menos un caso de éxito donde se ha implantado firma digital a nivel nacional y/o internacional.
2. Realizar diagnósticos de situación actual en cuanto a procesos donde estaría involucrada la herramienta de firma digital en una empresa de gobierno (AyA), y otro diagnóstico respecto a la infraestructura tecnológica.
3. Identificar los diferentes servicios en una empresa de gobierno (AyA), que estarán involucrados dentro del concepto de la herramienta de firma digital.
4. Definir el marco metodológico de implementación para la herramienta de firma digital en empresas del sector público.
5. Formular propuestas preliminares de solución a través del uso de esta tecnología para el AyA.

Objetivos específicos. (Etapa II)

1. Elaborar un análisis de costo beneficio para la utilización de la herramienta de firma digital en el AyA.
2. Definir la estrategia para que funcionarios y clientes del AyA logren obtener un certificado de firma digital expendido por un CA autorizado *(Autoridad Certificadora Licenciada).*
3. Diseñar el plan de implementación de la herramienta de firma digital para el AyA, tomando en cuenta la metodología MIFID*
4. Diseñar un prototipo funcional de la herramienta de firma digital.

(*) **MIFID:** Metodológica de Implementación para Firma Digital, ver documentos primera etapa del proyecto, específicamente el producto No.3, sobre el desarrollo metodológico.

Marco teórico y conceptual

¿Qué es firma digital?

La Firma Digital es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, para crear la posibilidad de que éstos gocen de una característica e identidad que hasta ahora era exclusiva de los documentos en papel.

Una firma digital es un conjunto de datos asociados a un mensaje electrónico que permite garantizar la identidad del firmante y la integridad del mensaje.

Esta identificación no implica el aseguramiento de la confidencialidad del mensaje; un documento firmado digitalmente puede ser visualizado por otras personas, al igual que cuando se firma de puño y letra un documento basado en un soporte papel.

Adicionalmente el mensaje podría estar cifrado para que sólo pueda ser leído o interpretado por quien conozca la clave de cifrado.

La firma digital es también un instrumento con características técnicas y normativas propias.

Figura 1: Sistema de criptografía asimétrico mediante la utilización de un par de llaves.

Esto significa que existen mecanismos estándar que permiten la creación y verificación de la firma digital.

También es necesario darle el sustento legal para que pueda adecuadamente implementarse, para lo cual existen documentos normativos oficiales **[DEC-33018]**, que respaldan el valor legal quien le estable su alcance (Integridad, autenticación y no repudio).

La tecnología está disponible a nivel global, pero el marco legal que la regula depende de cada país. Hay ámbitos y situaciones donde la firma digital no tiene sentido ser aplicada si el marco legal no le da el sustento adecuado que la haga confiable.

¿Qué es clave privada y clave pública?

En la elaboración de una firma digital y en su correspondiente verificación se utilizan procedimientos matemáticos basados en criptografía asimétrica. *(fig.1)*

En un sistema criptográfico asimétrico, cada usuario posee un par de claves propio. Estas dos claves, llamadas clave privada y clave pública, poseen la característica que, si bien están fuertemente relacionadas entre sí por medio de una función matemática conocida, no es posible calcular o deducir la clave privada a partir de los datos de la clave pública, ni tampoco a partir de los documentos firmados con la clave privada. Justamente la clave *"pública"* y el documento firmado se suponen, a priori, *"públicos",* es decir que pueden ser accedidos o leídos sin restricciones; mientras que la clave "privada" debe ser resguardada por su propietario.

El sistema opera de tal modo que una información firmada con una clave privada, puede ser validada con la clave pública que se corresponda, pero sin poder deducir la clave privada. De este modo si un receptor verifica la información firmada con la clave pública del firmante, podrá validar el documento.

Cabe acotar que, para los efectos prácticos, la clave privada no requiere ser conocida por su titular sino que está almacenada en un medio seguro denominado dispositivo criptográfico. Estos dispositivos criptográficos deben cumplir con un estándar de seguridad que garantiza la imposibilidad práctica de mostrar, revelar o perder la clave privada que almacenan.

¿Cómo es el proceso de firma digital?

La firma digital utiliza un procedimiento matemático que relaciona un documento digital (que será firmado electrónicamente) con información propia de la persona que se hace responsable de dicho documento (denominada firmante), y permiten que los terceros usuarios puedan reconocer la identidad del firmante y asegurarse de que los contenidos del documento firmado no han sido modificados.

El mensaje electrónico puede ser de muy diversos tipos, tales como; un documento de texto, una factura, una transacción bancaria, una solicitud de servicios, una orden de pago, un reclamo, etcétera. Por un lado, el documento es sometido a una operación de generación de una huella digital (que es la generación de un código que se corresponde con el documento) que se envía adjunto al mensaje original. De esta manera, se agregará al documento una marca que es única para dicho documento y que sólo el firmante es capaz de producir. La acción de firmar digitalmente, que es un acto esencialmente voluntario de una persona, es llevada a cabo por el dispositivo criptográfico.

Para realizar la verificación del mensaje o la aplicación, el programa receptor del documento firmado verifica la firma digital del mensaje, para lo que utiliza la clave pública del firmante. Si la operación es exitosa, significa que no hubo alteración y que el firmante es quien dice serlo. Al igual que cuando se firma digitalmente, estas acciones son efectuadas automáticamente por medio de facilidades que deben estar previstas en las aplicaciones o programas, lo que permite indicar la validez de la operación o alertar al receptor alguna anormalidad.

La clave privada es entonces usada para firmar un documento electrónico mientras que la clave pública es utilizada por los destinatarios (o llamados también "terceros usuarios") de un documento firmado, para verificar la firma de los documentos o mensajes. Este proceso garantiza *integridad* y *autenticidad*, sin embargo no se garantiza el principio de *confidencialidad.*

Para los fines prácticos, algunos soportes de claves privadas seguros son del tamaño y operación similares a un dispositivo tipo memoria portátil o *"llave maya"*, (en inglés conocido como *Flash Memory*).

Dentro de ellos fue generada y permanece almacenada la clave privada y no puede extraerse o visualizarse. Una clave privada segura está formada por una sucesión de 128 caracteres o más, que puede llegar actualmente hasta los 2048 caracteres. El dispositivo debe estar siempre bajo control del firmante y se recomienda que esté protegido por una clave personal.

¿Qué es un certificado digital?

Un certificado digital es un documento digital que "da fe" de la vinculación entre una clave pública y su poseedor, y se almacena y resguarda en el sitio *web* del certificador que lo otorgó. De este modo, permite verificar que una clave pública específica pertenece, efectivamente, a un individuo determinado. Cuando un documento recibido está firmado digitalmente, tiene adjuntada su clave pública. Luego de realizar el procedimiento de verificación de firma, por medio del certificado se individualiza al firmante.

En su forma más simple, el certificado digital es un documento digital que contiene la clave pública y los datos personales de su titular (como nombre, apellido y número de documento), la fecha de vencimiento, el nombre de la Autoridad de Certificación (CA) que lo emitió, un número de serie y otros datos técnicos. Pero es fundamental destacar que el certificado propiamente dicho está firmado digitalmente por su emisor (la Autoridad de Certificación). A su vez, el certificado digital de la

Autoridad de Certificación está firmado digitalmente por la Autoridad de Certificación Raíz, primer eslabón de la cadena de confianza.

Su formato está definido por un estándar internacional respetado por toda la industria informática y de telecomunicaciones. De esta forma, puede ser leído o escrito por cualquier aplicación o sistema informático que cumpla con el estándar.

¿Cómo revisar un certificado de firma digital?

Cuando se recibe un archivo o una macro firmada digitalmente es aconsejable chequear el certificado con el cual fue firmado, a fin de comprobar su respectiva validez y a partir de aquí, confiar en el contenido del documento recibido.

Los certificados contienen mucha información que puede parecer muy complicada, sin embargo el procedimiento para verificar su validez del mismo es relativamente sencillo y debe ser siempre una sana costumbre de poner en práctica.

Cuando el certificado no es válido o es de un emisor del cual no se puede confiar muestra una “x” de color rojo (en una esquina), además un aviso de precaución de su invalidez, como se detalla en la siguiente figura. *(fig.2)*

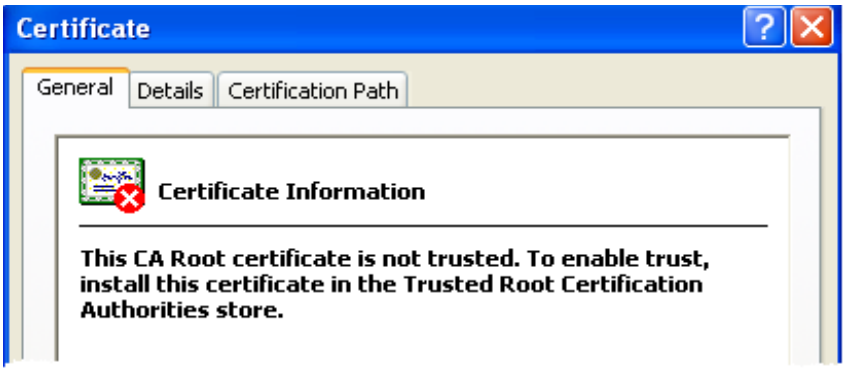

Figura 2: Certificado no válido.

Para asegurar la confianza en un certificado de firma digital se deberán de verificar como mínimo los siguiente datos; *(fig.3)*

1. Que cumpla los propósitos para lo que se utilizo la firma. *(purpose:)*
2. Que sea emitido a nombre de la persona quien firmo el documento *(issue to:)*
3. Que lo haya emitido una organización de confianza. *(Issue by:)*
4. Si se utilice mientras tenida validez. *(Valid from)*

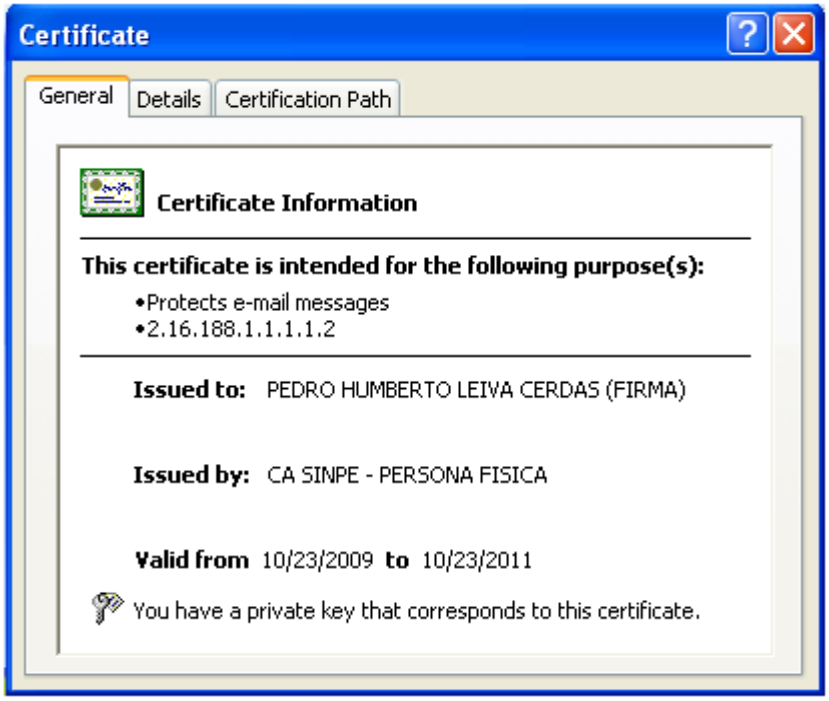

Figura 3: Certificado válido.

Alcance de la ley de Firma Digital.

La Ley de Firma Digital actual costarricense **[LEY8454]** asegura los principios de *Integridad, Autenticación y no repudio*. *(fig.4)*

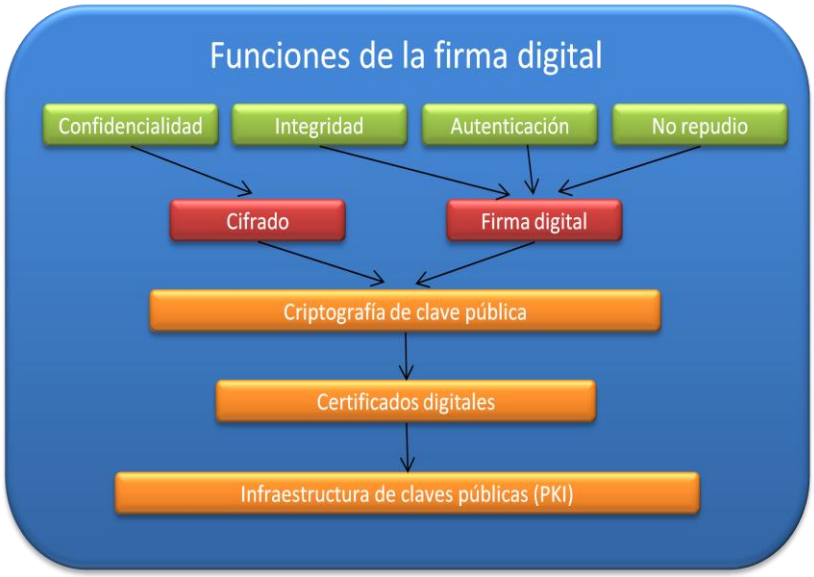

Figura 4: Funciones de la Firma Digital, según alcance de la Ley 8454.

Valor equivalente: La ley establece claramente su valor equivalente con respecto a los documentos firmados en manuscrito, en su Artículo Noveno reza *"Los documentos y las comunicaciones suscritos mediante firma digital, tendrán el **mismo valor** y la eficacia probatoria de su equivalente firmado en manuscrito"*.

Presunción de autoría y responsabilidad: Expresado en su Artículo Décimo, *"Todo documento, mensaje electrónico o archivo digital asociado a una firma certificada se presumirá, salvo prueba en contrario, de la autoría y responsabilidad del titular del correspondiente certificado digital […]"*

¿Qué es infraestructura de firma digital?

En Costa Rica se denomina *"Infraestructura de Firma Digital"* al conjunto de leyes, normativas legales, hardware, software, estándares tecnológicos, procesos de seguridad y personas que utilizan tecnología de firma digital para proveer una asociación verificable entre una llave pública y un suscriptor específico quien posee la llave privada correspondiente. Este concepto es conocido mundialmente como PKI (por sus siglas en inglés *Public Key Infraestructure*) ó Infraestructura de Clave Pública.

Diagnóstico

Con el objeto de centrarse en el problema por resolver y validar la totalidad y magnitud del proyecto, se debe conceptualizar como desarrollar la implementación de firma digital para el AyA. Dicha conceptualización parte de una serie de ideas discutidas ampliamente, logrando definir su ejecución en dos etapas muy puntuales. *(fig.5)*

Figura 5: Esquema general solución.

La *primera etapa* se abocó al logró de la metodología de implementación para la herramienta de firma digital en empresas del sector gubernamental. Se obtuvo mediante el análisis de casos de éxito documentados y las diversas metodologías estándar en el mercado de la informática y las comunicaciones como son COBIT, CMMI, ITIL, y otras, **[RODRIGUEZ]**.

Se definieron cinco objetivos que fueron desarrollados en doce semanas de trabajo (*fig.6 - Esquema parte izquierda)* y se obtuvo, entre otros, un sistema metodológico que se denominó *"Metodología de Implementación para la Firma Digital" (MIFID)".* **[MIFID-09]**, el detalle de este documento podrá ser consultado en los anexos.

Figura 6: Esquema general de la solución para la implementación de la Herramienta de Firma Digital en el AyA.

Países con experiencia en firma digital y las mejores prácticas para implementación.

Diversos países de la región latinoamericana cuentan con la tecnología de firma digital, tal como es el caso de Colombia en 1998, México y Perú durante el año 2000, Venezuela y Brasil en 2001, seguidos por Chile en 2002. Otros países Europeos con mucho más experiencia, tal como España que implementó esta tecnología en año 1995, con algunas frustraciones encontradas en el camino hacia la implementación, hasta que se publicó la Ley de Firma Digital en el 2003. Igualmente existen muchas iniciativas en otros para la utilización de esta novedosa tecnología.

En Argentina el marco normativo se dio en el año 2001, luego se crearon los reglamentos y en el 2004 se formó la comisión para la Infraestructura de firma digital. Sin embargo, ya habían realizado esfuerzos en 1998, pero esa primera iniciativa fue muy restrictiva, faltó liderazgo y seguimiento por parte del gobierno.

En diciembre del 2008 la AFIP (Administración Federal de Ingresos Públicos de la República de Argentina *www.afip.gov.ar*), obtiene licenciamiento y crea una de las primeras autoridades certificadoras, presentado en este documento como el *"Caso de estudio"* **[ROLANDO-09]**. La AFIP es un ente gubernamental, cuya función es fiscalizar la actividad económica federal, encargado de recaudar las contribuciones a nivel nacional para administrar más de 7 millones de personas del padrón de contribuyentes de Argentina. Los certificados emitidos serán utilizados para los contratos internacionales de comercialización de granos (exportación de cereales). **[PRO1-09].**

Para la implementación utilizaron herramientas como TRAC (sistema para la administración de proyectos) y realizaron un estudio de las herramientas existentes en el mercado de cuyo análisis concluyeron que no era necesario tercerizar el proyecto y tomaron la decisión de desarrollarlo con recursos internos del departamento de Seguridad Informática, con personal altamente capacitado en redes, seguridad, criptografía, desarrollo de software y normativa técnica. Sin embargo, el tiempo para el proyecto no fue muy bien manejado.

Otro de los operadores argentinos licenciados a la fecha es el ANSES (Administración Nacional de Seguridad Social), organización gubernamental orientada a la seguridad social, aunque con un alcance de la herramienta de firma digital mucho más limitado, puesto que han utilizado los certificados únicamente para los usuarios internos; sin embargo, están preparados o tienen intención de ampliar su uso. **[PRO1-09]**

Implementación de firma digital en Costa Rica.

Todo inicia con un proyecto de Ley incentivado por el Poder Ejecutivo en la Asamblea Legislativa en febrero del 2002, tramitado con el expediente número 14276.

Luego de varios años de conversaciones sobre el tema se culmina con la aprobación de la Ley de Certificados Digitales, Firmas Digitales y Documentos Electrónicos No. 8454, aprobado en 2005, y publicada en la Gaceta número 197.

Implementación del PKI Costa Rica.

En Costa Rica la firma digital da sus primero pasos y los esfuerzos por implementar esta novedosa tecnología inician con la aprobación de la Ley 8485 en agosto 2005.

Para el año 2006, por medio del convenio MICIT-BCCR (2006), se logra una serie de procesos de investigación, planeación, definición de modelos y estándares a seguir que culminaron con la implementación de la CA Raíz Costa Rica, operada a nivel técnico por el Banco Central de Costa Rica (BCCR).

Implementación del CA-SINPE.

En julio del 2009 el Banco Central de Costa Rica (BCCR), utilizó la plataforma ya instalada del SINPE (Sistema Nacional de Pagos Electrónicos), y es autorizado como la primera autoridad certificadora costarricense, bajo el nombre de *"CA-SINPE"* dentro de la infraestructura del Sistema Nacional de Certificación Digital.

En agosto del 2009, el Ministro de la Presidencia, Señor Rodrigo Arias Sánchez recibió la primera firma digital, en calidad de ciudadano costarricense. Así fue como se inauguró oficialmente el *Sistema Nacional de Certificación Digital* **[NACION-12/09]**. A partir de ese momento se inicia el proceso de emisión de certificados. Sin embargo, los primeros clientes a certificarse, serán los usuarios del servicio de Central Directo del BCCR.

Por ser Costa Rica un país relativamente pequeño, se estima que la demanda de certificados digitales será suficientemente atendida con una sola CA. Es de esperar que no exista una proliferación de estos entes certificantes **[SOLIS-09]**. Sin embargo, está

contemplado, tanto en la legislación vigente como en los estándares utilizados, que exista interoperabilidad técnica entre varias CA.

Implementación del PKI interno del Ministerio de Hacienda.

En Junio del 2003 por Decreto No.32457-H se oficializa la creación del la Autoridad Certificadora del Ministerio de Hacienda **[ROJAS-8/09]**.

En el 2004 se da inicio al proyecto a fin de desarrollar el PKI, y se iniciaron actividades para lograr los componentes, normas, procedimientos y la gestión de los certificados digitales requeridos.

Dicha tecnología se utilizó para ser implementada como modo de autenticación en su sitio *web* de forma segura, ingresando a los sistemas TICA (Tecnología de Información para el Control Aduanero ─con 3000 usuarios que incluyen auxiliares de la Función Pública Aduanera, entidades que otorgan notas técnicas como MAG, Ministerio de Salud y COMEX)─ y COMPRARED ─que incluía proveedurías de 22 ministerios y otras instituciones del estado costarricense─

En el 2009 y debido a la entrada en operación del *"CA-SINPE"*, los certificados por el CA de Hacienda pierden validez jurídica; por tanto, se ven obligados a alinearse al Sistema de la Jerarquía Nacional de Certificación Digital, y a realizar los cambios en los dos sistemas mencionados anteriormente.

Implementación de la RA del Banco Popular y de Desarrollo Comunal (BPDC).

En el 2006, el BPDC realiza esfuerzos por mejorar la seguridad en sus sistemas, motivado por el inicio de los fraudes electrónicos en los servicios *web* de las entidades financieras del país. Inician sus primeros pasos en el desarrollo de un PKI interno e

implementan el servicio de correo electrónico interno con firma digital **[CASTRO&PICADO-09].**

En el 2007, por el aumento en los fraudes electrónicos **[NACION-3/09]**, la gerencia del BPDC ordena la implementación de los certificados de firma digital en su plataforma *web*, momento que inician con el servicio denominado *e-token* **[E-TOKEN]**, dispositivo o medio físico que resguarda y permite la verificación de la identidad digital del propietario representado por un Certificado Digital, donde el formato físico es similar al de una memoria portátil.

Para setiembre del 2009, con la apertura del *Sistema Nacional de Certificación Digital* y la primera CA licenciada del país (CA-SINPE), el BPDC inicia operaciones con firma digital dentro de la jerarquía nacional, convirtiéndose en la primera RA del país **[NACION-18/09].** Al utilizar firma digital a lo interno, utilizaron estándares internacionales, y el pase con los certificados de la jerarquía nacional fue rápidamente adaptado. A la fecha utilizan el PKI interno para el servicio de correo electrónico.

Futuras implementaciones.

Según Carlos Melegatti, subgerente del Banco Central de Costa Rica, la estrategia implementada para el despliegue de esta novedosa tecnología les permitirá en un futuro construir unas mil sucursales encargadas de emitir y distribuir estos certificados distribuidos en varias entidades de registro **[NACION-18/09].**

Se espera que antes que finalice el año 2009, se realice la apertura de las RA del Banco Nacional de Costa Rica, Banco de Costa Rica, Mutual Alajuela y el BAC San José, este último muy adelantado en el proceso.

Procesos, servicios y la infraestructura tecnológica del AyA.

El AyA es una Institución relativamente grande con instalaciones físicas distribuidas por todo el territorio nacional. Actualmente cuenta con 3,333 funcionarios aproximadamente, y desempeña una gran cantidad de procesos y servicios a clientes y público en general.

A nivel interno, la herramienta de firma digital puede llegar a ser de mucha utilidad para validar los trámites administrativos realizados electrónicamente, tales como el envío de documentos, mensajes e informes, optimización de tiempo y recursos, mejora de la gestión documental, ahorro en costos incurridos por la compra de papel y tintas, costos de envío de los documentos, entre otros. Los costos de almacenaje son también un rubro importante a considerar para la implementación de esta tecnología **[PRO2-09].**

En lo particular se identifican una serie de procesos sujetos para aplicar dicha tecnología.

Servicios externos identificados tales como;

- ✓ *Trámites para nuevos servicios*
- ✓ *Arreglos de pago y ordenes de servicio*
- ✓ *Envío de carteles, Certificaciones y recepción de ofertas a proveedores*
- ✓ *Envío de cartas a otras instituciones*
- ✓ *Resultados de exámenes de laboratorio*
- ✓ *Certificaciones e historial para empleados*

Servicios Internos tales como;

- ✓ *Envío y recepción de estudios técnicos y legales*
- ✓ *Correspondencia y/o informes*
- ✓ *Resultado de exámenes de laboratorio*
- ✓ *Constancias, certificaciones y colillas e pago de salario*
- ✓ *Registro de firmas de autorización*
- ✓ *Autorizaciones de pago de viáticos y otros trámites administrativos*
- ✓ *Visado de planos*

Solución detallada del problema

(Segunda etapa del proyecto)

Escenario meta.

En esta *segunda etapa,* se busca obtener el plan adecuado con el fin de aportar soluciones al problema planteado inicialmente y para que el AyA implemente la herramienta de firma digital en sus procesos de negocios, y pueda generar valor agregado importante al asegurar una gestión ágil en los servicios y un ambiente altamente seguro, para que ahora los costarricenses realicen sus trámites desde una plataforma de servicios digital.

Es así como se han definido cuatro objetivos puntuales, mencionados al inicio de este documento. El esquema general de solución se muestra en la figura 6 del diagnostico.

De tal manera, el escenario meta esperado, (como producto del desarrollo del proyecto) será un esquema de firma digital que le permita al AyA brindar, entre otras cosas;

- ✓ Transparencia en la gestión pública.
- ✓ Centralización de trámites digitales.
- ✓ Disminución de la brecha digital.
- ✓ Mejoramiento de la infraestructura tecnológica.
- ✓ Desarrollo de un Gobierno Digital en cumplimiento al Decreto No. 33147-MP.

El Instituto Costarricense de Acueductos y Alcantarillados podrá ofrecer a sus clientes una mejora considerable en los servicios y productos, y podrá aprovechar las bondades que las tecnologías de información y comunicación le brindan, específicamente en el ámbito de la digitalización, mantenimiento, seguridad y resguardo de la misma.

Justificación de la solución planteada.

En marco de solución de este proyecto, se ha logrado determinar la implementación de firma digital como la solución para lograr el escenario meta propuesto.

Esta solución se fundamenta mediante una serie de razones que se mencionan a continuación:

- ✓ Los alcances y logros obtenidos en el apartado de diagnóstico de la situación actual del AyA.

- ✓ Las experiencias, conclusiones y lineamientos aportados por profesionales expertos en el tema de firma digital, específicamente en el Ministerio de Hacienda **[ROJAS-8/09]**, el MICIT **[SOLIS-09]** y el Banco Popular **[CASTRO&PICADO-09]**.

- ✓ La no conveniencia aventurarse en realizar una implementación masiva, justificada en un sentido claramente positivo. En Costa Rica esta tecnología y la plataforma de servicios de firma digital nacional está en etapa de prueba.

- ✓ Un requerimiento de ley como parte del esfuerzo de alinear a las instituciones gubernamentales al concepto de Gobierno Digital, además de que la proliferación de la tecnología apunta a nuevos esquemas de autentificación y certificación de información digital y, por otro lado, representa un medio seguro y tecnológicamente avanzado que cuenta con el respaldo legal del Gobierno de Costa Rica.

Análisis de costo vs. beneficio para el AyA.

Costos: Implementación para 4 servicios.

El costo de la solución planteada incluye, en su mayoría, recursos humanos y tecnológicos ya existentes; excepto dos ítemes que se detallan a continuación;

- ✓ una **consultoría** en aspectos de seguridad informática.

  Se requiere 40 horas de consultoría a un costo de $55 la hora.

- ✓ la **adquisición de los paquetes** con los certificados de firma digital *(tarjetas inteligentes).*

  Cada tarjeta inteligente incluye un certificado de firma y otro de autenticación (ambos son certificados de persona física) que deberá adquirir el AyA para cada uno de los funcionarios que requieran utilizar esta tecnología.

  Para la implementación de los cuatro servicios seleccionados, se estima que se requieren 25 tarjetas inteligentes, a fin de cumplir con la *Fase.1:"Apertura",* según el siguiente detalle: *(Cuadro No.1)*

Cuadro No. 1: Inventario estimado de tarjetas inteligentes requeridas para la Fase 1

Inventario de tarjetas inteligentes requeridas			
Fase I: Apertura			
Servicios Externos			
	Depto. Comercial	**Dpto. Proveeduría**	**Total**
Solicitud de nuevos servicios	1 jefatura 2 encargados		1 2
Registro de proveedores		1 jefatura 1 encargado	1 1
Servicios Internos			
Autentificación en Sistemas (WAS*) y Firma de documentos internos	Sub Gerencia de Gestión de Sistemas Periféricos		5
	Sub Gerencia Administrativa y Financiera		5
	Dirección de Planificación		3
	Dirección Jurídica		2
	Laboratorio Nacional de Aguas AyA		5
Total			25
Costo unitario por tarjeta:			**$35**
Costo total			**$875**

(*) WAS: Web Application Security.

En este momento el Instituto cuenta con 4 tarjetas inteligentes listas para realizar las pruebas correspondientes, lo que es una ventaja importante en cuanto a tiempo de adquisición. El siguiente cuadro detalla los roles de pruebas para los cuales se utilizaran las tarjetas recién adquiridas. *(Cuadro No.2)*

Cuadro No. 2: Inventario actual de tarjetas inteligentes adquiridas para pruebas

Inventario de tarjetas inteligentes adquiridas		
Dependencia	**Rol de pruebas**	**Cant. Tarjetas**
Ingeniería en Tecnologías	***-Infraestructura Tecnológica-*** Pruebas de conectividad, de seguridad y verificación del desempeño del prototipo en los equipos y red institucionales.	1
Gestión de proyectos	***-Director del Proyecto-*** Pruebas en prototipo para aprobación funcional del modelo planteado.	1
Gestión de proyectos	***-Construcción y Desarrollo-*** Diseño, construcción del código en ambiente WEB y aseguramiento en la aplicación de estándares.	1
Gestión de proyectos	***-Coordinador del proyecto-*** Responsable de asegurar los requerimientos del alcance, verificación de la funcionabilidad del prototipo propuesto, y aprobación de las pruebas.	1
Total		**4**

El siguiente cuadro muestra el costo total del proyecto para los 4 servicios seleccionados. *(Cuadro No.3)*

Cuadro No. 3: Costo estimado total para la fase 1

Costo Fase 1 *(4 servicios)*		
Ítem	**Costo Unitario**	**Costo Total**
Mano de obra -costo de administrador de proyecto, desarrollador en .net, otros-		$15,160
Consultor Senior en seguridad Informática	$55 p/hora	$2,200
Compra de tarjetas inteligentes- Certificado de Persona Física -25 paquetes* que incluye: tarjeta inteligente, lector de tarjeta y los respectivos drivers-	$35 p/paquete	$875
COSTO TOTAL		**$18,235**

(*): Cada tarjeta inteligente, tiene una validez de dos años, (tiempo de uso, según Ley 8454).

De lo anterior se deduce que el Instituto deberá presupuestar $3,075 para iniciar la *Fase 1*, el resto del costo corresponde a recurso ya existentes.

Estrategia para gestionar las tarjetas inteligentes.

En definitiva, para poder implementar esta tecnología se requiere, entre otras cosas, que cada funcionario que interactué con algún proceso y/o servicio implementado mediante firma digital, posea el dispositivo físico (tarjeta inteligente) asignado a su nombre, como parte de sus herramientas de oficina.

De tal manera que el Instituto deberá de asumir el costo de adquisición de dichas tarjetas. Se habla de un costo relativamente bajo, comparado con la utilidad y versatilidad que recibirá con esta nueva tecnología, además de mejorar sus procesos rutinarios, logrando así generar un valor agregado importante.

Para gestionar las tarjetas inteligentes ante una entidad registro autorizada, AyA podría utilizar el servicio denominado ─estándar electrónico─ (ver detalles en CD anexos).

En el caso de los clientes de AyA, estos deberán de gestionarlo a por sus propios medios, sin embargo el AyA podría eventualmente referenciar a los CA respectivos.

Beneficios esperados a corto plazo.

Es difícil determinar los beneficios de forma cualitativa del uso de esta tecnología en razón a que cada elemento asociado a dicho beneficiado podría ser muy amplio. Seguidamente se detallan los beneficios en forma cualitativa.

Para el Instituto Costarricense de Acueductos y Alcantarillados.

- ✓ Tener la tecnología para firmar documentos sin la posibilidad de repudio.
- ✓ Ahorro en tiempos de gestión y procesamiento de documentos.
- ✓ Ahorros significativos en costos de impresión y envío (papel, tintas, utensilios para papel, etcétera).
- ✓ Automatización estandarizada de procesos.

- ✓ Integridad y confidencialidad en el almacenamiento y tratamiento de documentos por medios digitales.
- ✓ Modernización tecnológica del AyA por utilizar tecnologías de vanguardia.
- ✓ Evidencia del mejoramiento en la imagen como Institución modernizada.
- ✓ Uso de estándares mundiales normalizados de última tecnología para el mejoramiento en el ámbito de seguridad de las tecnologías de la información y comunicación.
- ✓ Ser participe directo en el impacto positivo que el concepto de Gobierno Digital aportara al país.

Para los clientes de AyA.

- ✓ Ahorro en tiempos y costos para el ciudadano al gestionar tramites sin desplazarse de su casa u oficina.
- ✓ Recibir atención inmediata sin hacer fila.
- ✓ Posibilidad de utilizar la misma tarjeta inteligente, para diversos trámites en distintas instituciones.
- ✓ Utilización de tecnología de punta en sus gestiones personales.
- ✓ Disponibilidad de servicios en horario 24x7/365.

Para el Gobierno Digital.

- ✓ Disminución importante en la brecha digital.
- ✓ Proporciona al ciudadano un mecanismo de autenticación única para interactuar con los servicios de Gobierno Digital.
- ✓ Estandarizar el esquema de seguridad del Gobierno.
- ✓ Ahorro en costos por economías de escala.
- ✓ Brindar el servicio de autenticación a entidades estatales.

Gestión del riesgo del proyecto.

Para esta gestión se utilizará el procedimiento de definición y análisis de riesgos que el AyA provee por medio del Departamento de Gestión de Proyectos.

Se estable el siguiente cuadro que indica: categoría, probabilidad, impacto y magnitud, así como el plan de acciones a realizar en caso de su materialización. **[GUIA]**

Cuadro No. 4: Plan de riesgos para el desarrollo de la propuesta

Categoría Riesgo	Descripción del riesgo (Condición)	Probabilidad (P)	Impacto (I)	Magnitud (P*I)	Estrategia (*)	Cod. Color Magnitud	Acciones de mitigación y/o contingencia
1.1	Cambios en el alcance y los requerimientos por parte del cliente.	4 (Casi Cierta)	4 (Crítico)	16	Evitar		Realizar un análisis exhaustivo de los requerimientos, diseñar talleres con los usuarios expertos y diseño de prototipos con base a los requerimientos durante la etapa de análisis.
1.3	Fondos insuficientes para capacitación (previa o pos).	2 (Poco probable)	4 (Crítico)	8	Mitigar		Negociar con el patrocinador para gestionar y destinar fondos presupuestarios para mitigar este riesgo.
2.2	Mala estimación en las actividades o tareas del cronograma.	3 (Probable)	2 (Moderado)	6	Mitigar		Identificar las actividades atrasadas y aplicar técnicas de reducción de tiempos para lograr el tiempo estimado.
3.1	Problemas con tecnologías no controladas / problemas para entender complejidad de nuevas tecnologías requeridas por el Patrocinador.	4 (Casi Cierta)	4 (Crítico)	16	Evitar		Mediante capacitaciones previas a la adquisición o asimilación de nuevas tecnologías para con los usuarios expertos.

3.2	Usar herramientas mal adaptadas o implementadas.	3 (Probable)	3 (Alto)	9	Mitigar		Identificar los procesos o procedimientos inadecuados que suscitaron esta situación, para la raíz de los problemas y erradicarla mediante la re definición de procesos o procedimientos.
3.4	Problemas de hardware/software.	3 (Probable)	3 (Alto)	9	Mitigar		Identificar los daños de los equipos y gestionar el soporte adecuado con departamentos de Gestión de Servicios e Ingeniería Tecnológica.
3.5	Dependencia externa (terceros).	3 (Probable)	2 (Moderado)	6	Mitigar		Generar los respectivos contratos con terceros para sentar responsabilidades y recurrir a las multas en caso de fallos o incumplimientos, y subsanar así los daños causados.
6.1	Cantidad, experiencia, habilidades, integración, disponibilidad de los expertos.	3 (Probable)	3 (Alto)	9	Mitigar		Realizar las respectivas convocatoria y cronograma de actividades e involucramiento en el proyecto para evitar la no disposición de algún miembro importante.
6.2	Disponibilidad de los usuarios / No tener la combinación adecuada de habilidades en el equipo / No hay un nivel de compromiso en algunos de los miembros, o del patrocinador.	2 (Poco Probable)	2 (Moderado)	4	Mitigar		Que el patrocinador así como los miembros involucrados en el equipo de trabajo se comprometan de antemano hasta concluir el proyecto.
7.1	Problemas de integración de las diferentes partes o componentes del proyecto desarrolladas en paralelo.	**2 (Poco Probable)**	**3 (Alto)**	6	Evitar		Seleccionar los equipos de trabajo el cual mantiene de antemano el compromiso y las buenas relaciones entre sus miembros.

(*) Estrategia de administración (Evitar el riesgo, mitigar el riesgo, aceptar el riesgo).

Gestión del cambio cultural en el AyA.

Conocido el impacto que tienen los proyectos que cuentan con componentes tecnológicos novedosos tal como lo es la firma digital, es de esperar que exista algún grado de resistencia en razón al cambio de paradigma requerido, en las personas quienes utilizarán dicha tecnología.

Anticipándose a situaciones como éstas, es que se considera incluir una metodología de implementación (Anexo No.1), que contenga actividades de sensibilización y formación en las cuales se fomente el cambio cultural en la organización del AyA, con el fin de no sólo informar la tecnología que se desea implementar, sino promover la disposición para su uso, tanto a funcionarios como los clientes de la Institución.

Es importante acotar que el apoyo gerencial, realizar jornadas de difusión y talleres de formación y capacitación al personal es un factor que no debe de estar ausente antes, durante y después del desarrollo del proyecto.

En este particular se realizó una actividad el día 30 de noviembre de 2009, para la cual se invitó al Lic. Oscar Solís Solís de la Dirección de Certificación de Firma Digital del MICIT, la cual se efectuó con mucho éxito participando funcionarios de diversas áreas de la Institución. También fue transmitida vía videoconferencia a 4 regiones del país (Pacifico Central, Huetar Atlántica, Brunca y la Chorotega). Esto como parte de las recomendaciones indicadas dentro de la Metodología de Implementación de Firma Digital (MIFID). *(Fotografía 1)*

Fotografía 1: Charla del Lic. Oscar Solís Solís, titulada; "Sistema Nacional de Certificación Digital", 30 de noviembre 2009. Auditorio Central AyA-Pavas.

Desarrollo de la alternativa seleccionada.

Se propone desarrollar la implementación de la herramienta de firma digital por fases, que son explicadas más adelante.

En una primera fase denominada; “fase de Apertura”, se incluyen, dos servicios internos y dos servicios externos. *(fig.7)*

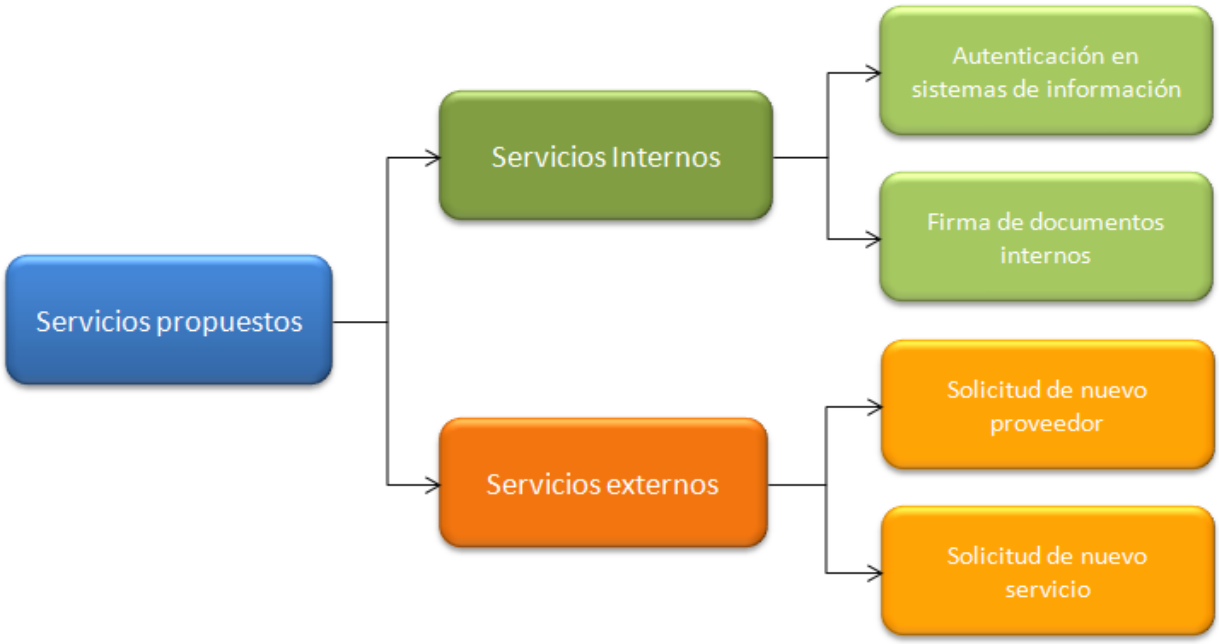

Figura 7: Servicios propuestos para ser implementados como una primera fase.

Se propone un cronograma de implementación con un tiempo estimado para desarrollo de 120 días, que da inicio el 15 de enero y finaliza el 7 de julio del 2010. Las etapas propuestas están definidas según el ciclo de vida del proyecto, donde se definen para ello cuatro etapas puntuales; (*fig.8*)

Etapa I: Aspectos de preparación del ambiente.

En esta etapa, se deberán de realizar tareas tales como el estudio de la metodología MIFID, la creación de un catálogo de servicios debido a la ausencia del

mismo en la Institución, asimismo la preparación del servidor o repositorio de seguridad de los archivos que se firmarán digitalmente.

Por último, es requerida la contratación de un consultor en materia de seguridad informática, según se expuso anteriormente.

Etapa II: Implementación Servicios Internos.

Servicios de autenticación.

Históricamente, el modo de autenticación se realizaba con la introducción de un usuario y una contraseña. Originalmente, estos modos de autenticación se daban de la terminal hacia un computador central, dentro de una Intranet; por lo tanto, el riesgo de transmitir la contraseña en texto plano no era un problema. Hoy en día las redes locales están conectadas entre sí y ellas están conectadas a Internet. Los usuarios se autentican en cualquier parte del mundo, donde se pone en riesgo la seguridad de las tramas que llevan las contraseñas. Actualmente el AyA cuenta con una gama de sistemas en ambiente *web* que requieren una mejora en el proceso de autenticación.

Existe un sistema denominado WAS, en inglés (*Web Application Security*), que requiere de este tipo de tecnología, por esta razón uno de los servicios seleccionados corresponde a la autenticación de los sistemas de información.

Servicio con la finalidad de firmar digitalmente un documento.

El segundo servicio interno corresponde a la firma de documentos, aprovechando las ventajas de la firma digital, y evitar la impresión o presencia física de quien envía el documento.

Etapa III: Implementación Servicios Externos.

Se propone elegir dos servicios importantes para el AyA. Actualmente, el cliente externo debe presentarse personalmente a las oficinas del Instituto. Al utilizar esta

novedosa tecnología, podrían hacer uso de esos servicios desde la comodidad de su casa u oficina y utilizar la plataforma propuesta para firmar digitalmente los documentos. Posteriormente, los documentos serían recibidos por funcionarios del Instituto, que luego de comprobar que la firma es válida, le darían el trámite correspondiente, agilizaría significativamente el servicio.

Los servicios seleccionados son: "Solicitud de nuevos servicios" y "el Registro de Proveedor".

Etapa IV: Adquisición y Capacitación.

En esta etapa se pretende gestionar los certificados ante una entidad de registro que pertenezca a la Jerarquía Nacional de Firma Digital en Costa Rica. Para lo cual, se recomienda utilizar el servicio denominado estándar electrónico, con el formato de archivo para pago del servicio, según lo definido por el SINPE.

Es importante acotar que está previsto iniciar el proyecto de implementación a partir del 15 de enero del 2010, por lo que fue necesario adquirir las tarjetas inteligentes, a fin ganar tiempo durante la ejecución del plan de implementación propuesto, además para realizar las pruebas al prototipo funcional y asegurar el éxito del mismo.

El siguiente cuadro detalla las fechas y actividades a realizar durante la primera fase: Apertura. *(cuadro. 5)*

Cuadro No. 5: Propuesta del cronograma de implementación

	Task Name	Duration	Start	Finish	Resource Names
1	**Implementar la Herramienta de Firma Digital en AyA**	**120 days**	**Fri 1/15/10**	**Thu 7/1/10**	
2	**Inicio**	**1 day**	**Fri 1/15/10**	**Fri 1/15/10**	
3	Project Charter	1 day	Fri 1/15/10	Fri 1/15/10	Patrocinador
4	**Plan de proyecto**	**10 days**	**Mon 1/18/10**	**Fri 1/29/10**	
5	Desarrollo del plan de proyecto	5 days	Mon 1/18/10	Fri 1/22/10	Administrador de proyecto[30%]
6	Aprobación plan de proyecto	5 days	Mon 1/25/10	Fri 1/29/10	Patrocinador
7	**Ejecución**	**111 days**	**Fri 1/15/10**	**Fri 6/18/10**	
8	Gestionar expectativas con los Stakeholders	0 days	Mon 2/1/10	Mon 2/1/10	Administrador de proyecto
9	**ETAPA I: Aspectos de preparación del ambiente**	**26 days**	**Fri 1/15/10**	**Fri 2/19/10**	
10	Estudio y revision de la metodología MIFID	5 days	Mon 2/1/10	Fri 2/5/10	Desarrollador .NET[20%],Administrador de proyecto[20%]
11	Ivestigación de estándares de desarrollo	10 days	Mon 2/8/10	Fri 2/19/10	Desarrollador .NET[50%]
12	Crear catalogo de servicios	0 days	Fri 1/15/10	Fri 1/15/10	
13	Servidor p/repositorio de archivos firmados	3 days	Mon 2/1/10	Wed 2/3/10	Ingenieria en Tecnología
14	Consultaría con: Consultor Senior en seguridad Informática	5 days	Thu 2/4/10	Wed 2/10/10	Outsourcing
15	**ETAPA II: Implementar Servicios Internos**	**35 days**	**Mon 2/22/10**	**Fri 4/9/10**	
16	Desarrollo código requerido según el estándar para N Capas	15 days	Mon 2/22/10	Fri 3/12/10	Desarrollador .NET
17	SI No.1- Autenticación en los sistemas de información	5 days	Mon 3/15/10	Fri 3/19/10	Admin. Pág. WEB
18	SI No.2- Firma de documentos internos	5 days	Mon 3/22/10	Fri 3/26/10	Admin. Pág. WEB
19	Pruebas de los servicios	10 days	Mon 3/29/10	Fri 4/9/10	Administrador de proyecto[20%],Desarrollador .NET[20%],Admin.
20	**ETAPA II: Implementar Servicios Externos**	**35 days**	**Mon 4/12/10**	**Fri 5/28/10**	
21	Desarrollo código requerido según el estándar de la página WEB	15 days	Mon 4/12/10	Fri 4/30/10	Desarrollador .NET
22	SE No.1- Solicitud de nuevos servicios	5 days	Mon 5/3/10	Fri 5/7/10	Admin. Pág. WEB
23	SE No.2- Registro de proveedores	5 days	Mon 5/10/10	Fri 5/14/10	Admin. Pág. WEB
24	Pruebas de los servicios	10 days	Mon 5/17/10	Fri 5/28/10	Administrador de proyecto[20%],Desarrollador .NET[50%],Admin.
25	**ETAPA IV: Adquisición y Capacitación**	**15 days**	**Fri 5/28/10**	**Fri 6/18/10**	
26	Adqusición de 25 SmartCard	0 days	Fri 5/28/10	Fri 5/28/10	Proveeduría
27	Documentación	5 days	Mon 5/31/10	Fri 6/4/10	Desarrollador .NET
28	Definir lineamientos para los servicios implementados	5 days	Mon 6/7/10	Fri 6/11/10	Administrador de proyecto[10%],Grupo usuarios expertos[10%]
29	Capacitación al personal (servicios liberados)	5 days	Mon 6/14/10	Fri 6/18/10	Gestión de Proyectos
30	**Seguimiento y Control**	**5 days**	**Fri 1/15/10**	**Thu 1/21/10**	
31	Control y aseguramiento de la calidad	5 days	Fri 1/15/10	Thu 1/21/10	Gestión de Proyectos,Grupo usuarios expertos
32	Detalle de tareas de control y seguimiento	5 days	Fri 1/15/10	Thu 1/21/10	Administrador de proyecto[50%]
33	**Cierre**	**9 days**	**Mon 6/21/10**	**Thu 7/1/10**	
34	Reporte Final	3 days	Mon 6/21/10	Wed 6/23/10	Administrador de proyecto
35	Acta de recepción y aceptación del proyecto	2 days	Thu 6/24/10	Fri 6/25/10	Patrocinador
36	Liberación de los servicios implementadados	4 days	Mon 6/28/10	Thu 7/1/10	Admin. Pág. WEB[10%]

Las fechas correspondientes a cada una de las etapas del cronograma propuesto de implementación se detallan en la siguiente figura. *(fig.8)*

Figura 8: Etapas del ciclo de vida del proyecto de implementación.

Estrategia para el desarrollo futuro del proyecto.

Si bien es cierto que los primeros estándares de la criptografía datan de los años 70, el concepto como tal de "firma digital" tiene mayor importancia en los últimos 10 años, desde el año 2000 a la fecha. En nuestro país, el proceso de legalidad inició en el 2005 y la disponibilidad de los certificados en mano de los costarricenses,

aparece en agosto del 2009, cuando se hace realidad la apertura del Centro Nacional de Certificación Digital; a partir de este momento los costarricenses pueden tener acceso al servicio de firma digital.

Según palabras del Director de Certificadores de Firma Digital del MICIT, Lic. Oscar Solís, *"...ya está definida la autopista para que transiten los servicios, falta ahora que el gobierno, empresas e individuos diseñen los servicios que utilizarán ese medio para transitar…".*

De tal forma, es de esperar que esta tecnología tome un tiempo prudencial para que los productos y usos que se diseñen para ser utilizados mediante la firma digital, inicien su desarrollo y liberación; y los próximos años estén a disposición de todos los costarricenses.

Para representar gráficamente (en forma general) el desarrollo futuro de la implementación de la herramienta de firma digital, se definieron una serie de fases en las cuales se espera ocurra una masificación del uso de la herramienta de firma digital en un plazo aproximado de cuatro años; esta proyección se detalla en la siguiente figura. (*fig. 9*)

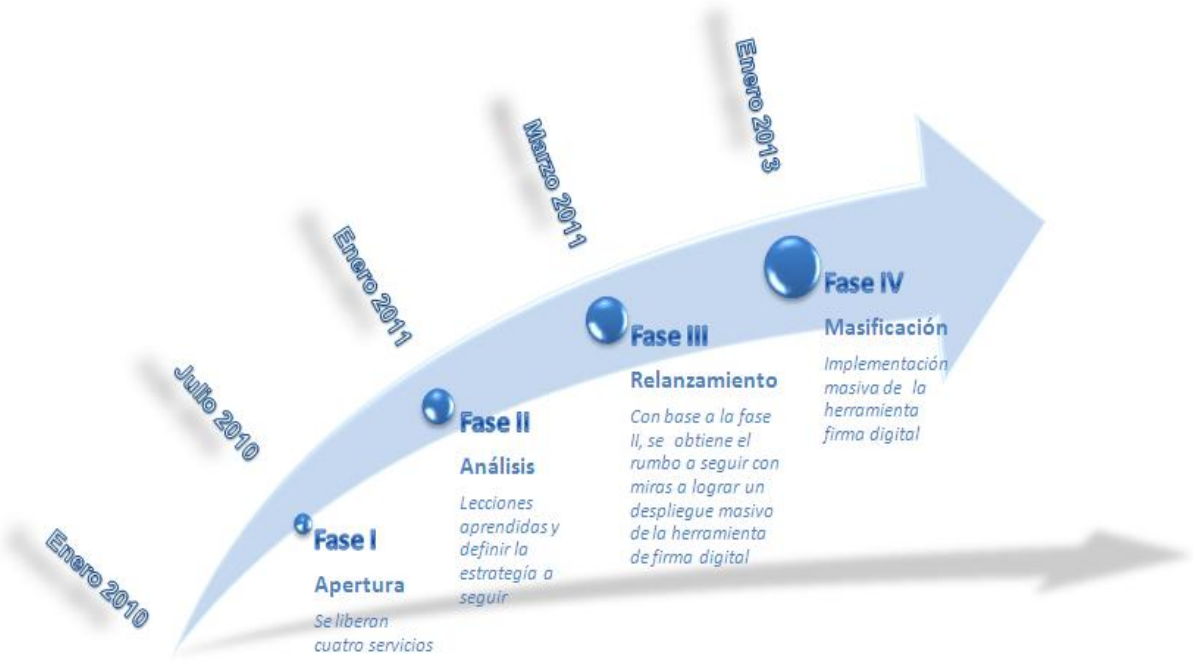

Figura 9: Diseño por fases a mediano y largo plazo (proyectado 2010-2013), propuesta para dar sostenibilidad del proyecto de Firma Digital en el AyA.

El detalle de actividades de cada fase se describe a continuación:

FASE I (Apertura):

Esta fase da inicio cuando los primeros cuatro servicios se liberán y comienzan a funcionar paralelamente con los servicios tradicionales. Se espera que esta liberación suceda a partir de julio del 2010 a enero del 2011, mediante el cronograma propuesto de implementación en la sección anterior, el cual será la guía de ejecución de las tareas de implementación en esta fase.

FASE II (Análisis):

Luego de puestos en marcha los cuatro servicios seleccionados, será de gran importancia el considerar un análisis detallado, 6 meses después de puesta en marcha la fase de apertura, visto como el *"hacer un alto en el camino",* donde se pretende documentar las lecciones aprendidas, y con base en éstas, poder generar mediciones en cuanto a los tiempos de desarrollo, de implementación y recursos necesarios para las próximas fases; se define así, la estrategia futura basada en las mediciones

obtenidas para lograr resultados acertados. Tal es la importancia de esta fase de análisis, que deberá considerarse como un método fundamental y básico para este proceso organizacional de implementación. Se pretende que esta etapa inicie en enero del 2011.

FASE III (Relanzamiento**):**

Con base en las lecciones aprendidas y resultados obtenidos en la fase anterior, además de la aceptación de esta tecnología por los usuarios internos (funcionarios) y externos (clientes) de la Institución, se deberá diseñar la estrategia siguiente, con la finalidad de definir los procesos adecuados para lograr el siguiente paso que implica la masificación de la herramienta de firma digital en el Instituto Costarricense de Acueductos y Alcantarillados.

Adicionalmente, será importante realizar las consideraciones de seguridad, legislación y actualización tecnológica en materia de firma digital, además de fortalecer los procesos de mejora continua que intervienen en la metodología MIFID. Se espera que esta etapa inicie en marzo del 2011.

FASE IV (Masificación**):**

Esta fase representa el desafio más importante, ya que se espera, para entonces, que esta tecnología no sea ajena a la gestión normal de productos y servicios en la Institución, donde existe una apertura total y la cultura necesaria para utilizarla. Así quedarían atrás los contratiempos del cambio cultural y las barreras que éste genera, además de haber creado la confianza necesaria para lograr que la herramienta de firma digital sea un dispositivo más, para facilitar la vida cotidiana de los costarricenses.

Se proyecta el inicio de esta fase para enero del 2013.

Aplicación de la metodología MIFID.

La implementación de firma digital es un ejercicio extenso, involucra una serie de actividades y procesos, sin olvidar el cambio cultural ideal que se espera, posean los usuarios de esta tecnología.

Todo esto requiere —y debe— considerar un tiempo para su desarrollo, de modo que cualquier deseo de implementación deber de poseer algunos ingredientes necesarios a fin de lograr con éxito la utilización adecuada de dicha tecnología.

Por esta razón, se trabajó fuertemente en diseñar *(primera etapa)* un modelo metodológico denominado MIFID *(ver anexo 1),* con el fin de contar con una guía de procesos y principios adecuados para lograr la correcta gestión de cualquier plan o planes de implementación necesarios para lograr con éxito el cometido inicial. Adicionalmente, generar métricas que sean capaces de indicar su avance *(modelo de madurez)*, y que vienen incluidas en dicha metodología.

La figura 10 explica cómo madura el proceso de implementación dentro del modelo MIFID.

En nivel 1 (Dominio: Planear y Organizar); porque logra crear un ambiente (de apertura) para definir procedimientos, estudiar y comunicar la legislación vigente, lograr un apoyo gerencial, realizar análisis de riesgos y crear un ambiente de cultura tanto a nivel interno como externo del AyA.

En nivel 2 (Dominio: Adquirir e Implementar); acreditar con tarjetas inteligentes de firma digital a funcionarios, poner a prueba algunos procesos o servicios, crear soluciones basadas en la nueva tecnología y adquirir los recursos que dicha tecnología demanda. *(fig.10)*

Figura 10: Sostenibilidad proyectada al 2013 y su proceso de madurez aplicando MIFID.

En los niveles posteriores (3 y 4), se espera que ocurra lo siguiente;

En nivel 3 (Dominio: Entregar y dar Soporte); en este nivel se espera que ocurran ocho procesos de los 26 en total que posee la metodología MIFID, generar actividades para garantizar la calidad de los servicios, capacitar a los usuarios, generar un portafolio de esos servicios y administrar las operaciones del proceso.

Se espera que esto ocurra entre fase I y fase III o sea del año 2010 al 2011. *(fig.10)*

En nivel 4 (Dominio: Monitorear y Evaluar); en este nivel se espera realizar actividades para monitorear el buen desempeño de la herramienta, garantizar el cumplimiento de la legislación y mejorar los procesos que utilizan la herramienta de firma digital. Se espera que esto ocurra en la fase IV, según lo planeado para enero del 2013.

De esta forma continuar con ese proceso de implementación, y muy importante, mantenerse alineado a la metodología MIFID.

Es importante indicar que la metodología MIFID es una herramienta invaluable en todo el proceso de implementación a corto y largo plazo, por lo que será importante seguir los 4 pasos indicados en ella (*ver anexo 1*), así como, será de valor agregado la práctica del estudio y la mejora continua que se pueda aplicar a dicha metodología, Se debe de recordar una vieja frase que dice: *"esta metodología no está escrita en piedra".*

Desarrollo del prototipo.

Uno de los requisitos de este documento se ha enfocado en llevar a la práctica las capacidades y funcionalidades básicas de uso de la herramienta de firma digital en una organización estatal, todo esto en tiempo real. Mediante el análisis y desarrollo de una solución de carácter representativo como lo es un prototipo, se pretende demostrar el impacto positivo que aporta la firma digital a cualquier organización que aprovecha su potencial, donde resaltan características como:

- ✓ El alto nivel de seguridad que la herramienta de firma digital provee al utilizar los mejores estándares internacionales conocidos a la fecha.

- ✓ La versatilidad que tiene la herramienta de firma digital para operar paralelamente con servicios tradicionales, lo que logrará igualar o mejorar los tiempos de respuesta, mientras traduce esto en crecimiento y mejor atención de parte de la organización hacia sus clientes internos y externos.

- ✓ La disminución de costos por concepto de papelería, utensilios de oficina, creación y mantenimiento de grandes áreas que son exclusivas para el almacenamiento y resguardo de documentos.

- ✓ El impacto en cuanto a la disminución de tiempo que requiere un usuario en realizar solicitud de productos o servicios a la organización.

- ✓ La disminución del tiempo de respuesta que la organización le brinda a sus clientes, de una forma ordenada y sistemática.

- ✓ La orientación tecnológica positiva que le depara a la organización involucrarse y funcionar activamente con este tipo de tecnologías de punta.

De ahí que, para representar en forma gráfica las características anteriormente descritas, se ha desarrollado el siguiente esquema de prototipo: *(fig.11)*

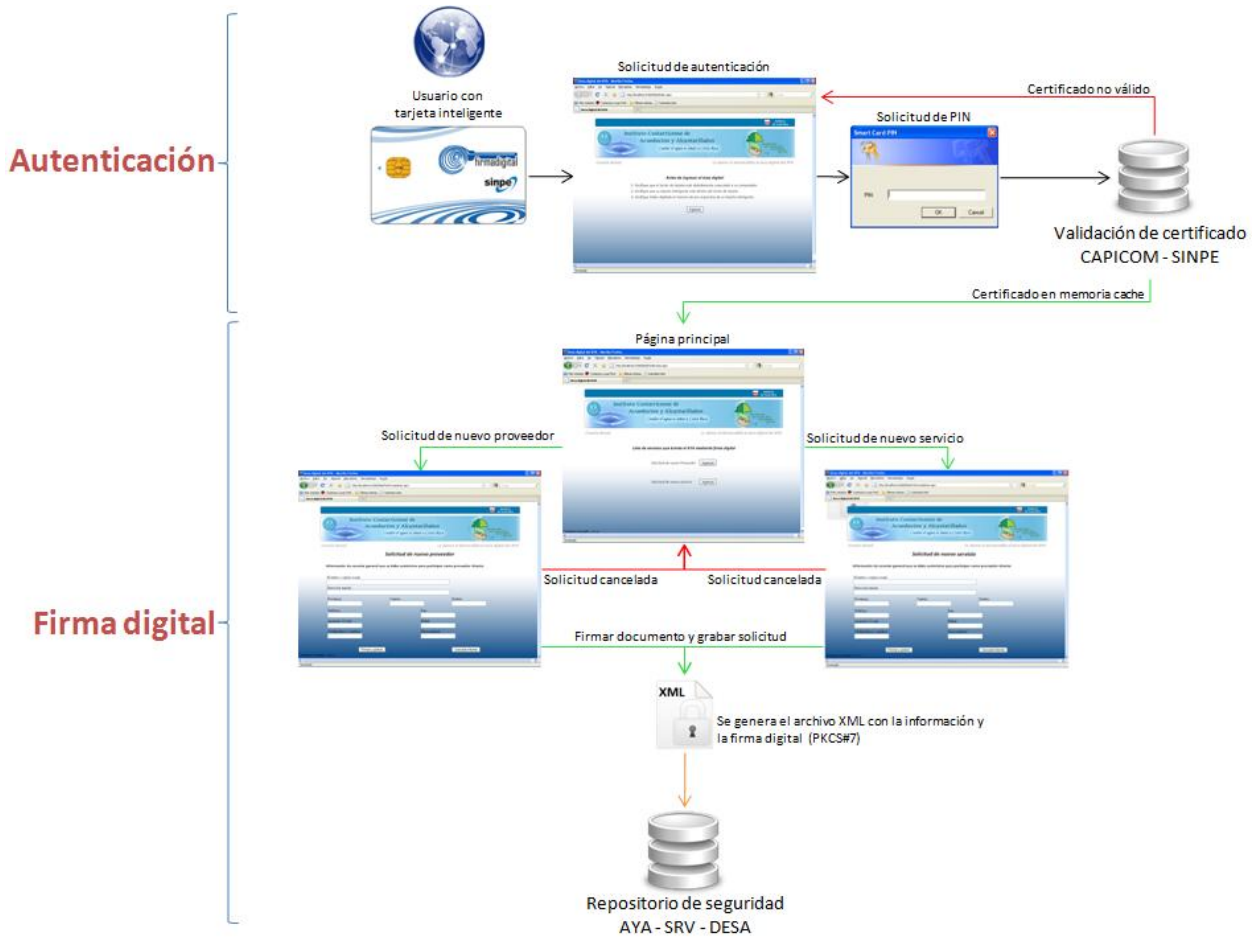

Figura 11: Esquema gráfico del prototipo para demostrar el funcionamiento de la firma digital en el AyA.

Este prototipo intenta representar de una forma general el uso y aplicación de la firma digital en una Institución pública costarricense, cuenta con varios componentes, divididos en dos fases:

Fase de autenticación: En esta fase se experimenta la facilidad con la que el usuario interactúa con una aplicación *web* destinada a funcionar mediante certificados digitales. En esta fase se inserta la tarjeta inteligente en el respectivo lector, y mediante la librería *CAPICOM* (de Microsoft) se generan una serie de algoritmos encargados de realizar la lectura del *chip* de datos, donde extrae su contenido y coloca en la memoria cache del computador que lo accede, después de haber solicitado el pin respectivo, el cual funciona bajo el mismo concepto de las tarjetas de crédito. Si el usuario final digita un código de pin erróneo, la librería *CAPICOM* inmediatamente evita que el certificado se almacene en memoria, y no se podrá acceder a su contenido.

En este proceso de autenticación o verificación de usuario, la librería se comunica con el respectivo servicio de CA-SINPE para verificar si el certificado es válido o no mediante el formato OID, donde se utilizan los protocolos de validación CRL/OCSP, y utiliza la política para certificados de autenticación 2.16.188.1.1.1.1.3. El detalle de esta información se encuentra contenido en la respectiva ley de certificados, firmas digitales y documentos electrónicos No 8454, lo que permite regular los certificados de persona física.

Fase de firma digital: Una vez almacenado el certificado de autenticación y el de firma digital en la memoria caché del computador, se puede ingresar a la página principal, la cual contiene los diversos servicios digitales que la Institución ofrece a los clientes externos. Al seleccionar uno de esos servicios, se ingresa a la respectiva página de formulario, donde se capturan los datos requeridos y se habilitan las opciones de firmar y guardar, o cancelar la solicitud. Si el usuario selecciona la opción de firmar y guardar, la solución informática automáticamente genera un archivo de formato *XML*, donde se almacena la información digitada por el usuario, y se genera el respectivo digesto que contiene la encriptación de datos mediante la firma digital en la memoria *cache*, esto para validar futuras alteraciones o modificaciones al archivo generado.

Este archivo una vez creado, será almacenado en una plataforma de base de datos, la cual será resguardada bajo la mayor seguridad y con la mínima cantidad de usuarios de acceso. El formato de almacenamiento de los archivos *XML*, es el *PKCS#7*, estándar internacional de seguridad para encriptación de archivos de datos privados.

Si se cancela la solicitud, se vuelve al menú principal de servicios disponibles.

Conclusiones

- ✓ Una de las particularidades más reconocida de esta nueva tecnología, es poder interactuar en el medio virtual con un alto nivel de seguridad tecnológica mediante complejos algoritmos matemáticos. Al desarrollar este proyecto se ha comprobado esa efectividad y ese alto nivel de seguridad que la firma digital proporciona para poder usarla.

- ✓ Existen algunos elementos que podrían dar una pista de los beneficios directos que reciben los usuarios, tales como parámetros de horarios, traslados físicos a una ofician, costos de trasporte, papelería, etcétera.

- ✓ Una vez desarrolladas las utilidades básicas de la firma digital, es fácil determinar el gran potencial que esta conlleva, al poder utilizar una misma tarjeta inteligente en todas las instituciones públicas o privadas que funcionen bajo las políticas del sistema nacional de certificación.

- ✓ El sistema financiero costarricense se ha caracterizado por ser pionero en el uso del internet como medio de gestión de transacciones electrónicas. La gran aceptación de esta nueva forma de gestión del dinero, ha provocado satisfacción de los usuarios, pero también lamentables hechos de estafadores cibernéticos que han provocado pérdidas nunca antes vistas en bancos estatales de miles de millones de colones por concepto de estafas electrónicas. Por todas estas razones, se ha determinado que la firma digital es actualmente el medio más seguro ya que contiene además de certificados encriptados, una serie de medidas de seguridad en caso de extravío de la tarjeta inteligente.

- ✓ Como cualquier otra innovación tecnológica que hayan adoptado los costarricenses en el pasado, la firma digital no escapa actualmente de un ambiente de incertidumbre y desconfianza, debido al desconocimiento de su funcionamiento y potencial. Por ello, es necesaria la adaptación y

culturización de los usuarios, además de dar un tiempo prudencial para su crecimiento y adopción por parte de las instituciones públicas y privadas.

- ✓ También, sin salirse del ámbito interno del Instituto Costarricense de Acueductos y Alcantarillados, se ha determinado que por varios factores no es factible implementar una masificación de la firma digital en todos los servicios del AyA. Esto está fundamentado en razón a que se deben realizar una serie de actividades a priori que garanticen la creación de un catálogo corporativo de servicios de la Institución.

- ✓ Otro consideración es que este proyecto no ha necesitado de planes de financiamiento ni inversión para poder desarrollarse, ya que depende plenamente de una partida presupuestaria exclusiva para su desarrollo, siendo un proyecto financiado con fondos propios del AyA.

- ✓ En cuanto a los diversos beneficios generados por la adopción de esta tecnología, se ha determinado que la imagen de Institución tecnológica avanzada es uno de los puntos importantes, lo que conlleva la agilización ordenada y reducción de tiempos de respuesta de los mecanismos y gestiones que ofrece el AyA en sus servicios.

- ✓ AyA cuenta con una infraestructura tecnológica importante, por esta razón el costo del plan de implementación propuesto es relativamente bajo.

Recomendaciones

- ✓ En todo momento que se utilicen tecnologías de información y comunicación será de vital importancia la protección y reserva de la información almacenada de los clientes, y en este caso particular de todos los firmantes. Por ello será necesario desarrollar técnicas y soluciones de software que mantengan la integridad y confiabilidad de la información privada, además de la debida infraestructura destinada para ello. Es de entender que se debe conocer e incentivar el uso y aplicación de estándares internacionales de seguridad, protocolos de gestión y resguardo de información y comunicaciones para evitar al máximo la intercepción y mala manipulación de esta nueva tecnología.

- ✓ La firma digital es utilizada en gran medida sobre tecnologías y plataformas *web*, por lo cual será necesario mantener la infraestructura, equipos y recursos humanos en constante actualización, para aplicar técnicas seguras y modernizadas en vías de evitar la falsificación de identidades, copias de certificados y cualquier otra amenaza que ponga en riesgo el buen desempeño y la confianza de la firma digital como una herramienta segura.

- ✓ La firma digital debe ser considerada como una herramienta para agilizar los procesos tradicionales de una organización, sin que esto implique que deban desaparecer. Parte de la culturización de la firma digital es capacitar a los usuarios a trabajar paralelamente de ambas formas; sin que afecte el buen rendimiento o la buena gestión de ambos.

- ✓ Para lograr la masificación de la firma digital en el Instituto Costarricense de Acueductos y Alcantarillados, es necesario contar con un portafolio de servicios bien definido, claro y que haga referencia a aquellos servicios que pueden funcionar bajo la filosofía de firma digital. Este se deberá desarrollar, paulatinamente según el avance del proceso de implementación.

- ✓ Debido a la implementación de esta nueva tecnología en el Instituto Costarricense de Acueductos y Alcantarillados, definitivamente habrá mucho camino por recorrer y lecciones por aprender. Por tal motivo, será fundamental

el evitar la masificación de la firma digital en el AyA hasta que el uso en los primeros servicios se haya garantizado (utilidad, conveniencia para usuarios, desarrollo de habilidades y confianza), y con ello adquirir experiencia tanto técnica como administrativa, en el uso de dicha tecnología.

- ✓ En toda adquisición de nueva tecnología siempre será importante promover el adecuado uso de los recursos y alcances que ésta provee a los funcionarios y usuarios finales. Por tanto, será necesario crear consciencia con respecto a la forma adecuada de utilizar la tecnología de firma digital, en la cual, la buena manipulación iniciará en manos de quienes la hacen parte de su vida cotidiana. El uso correcto de los diversos dispositivos como el lector de tarjeta inteligente, la tarjeta inteligente, controladores del computador y demás utilidades que involucren firma digital serán siempre responsabilidad de sus portadores y usuarios.

- ✓ Una de las características constantes en cuanto a esta nueva innovación tecnológica será el actuar de la mano con la legislación nacional destinada para éstos fines **[LEY8454]**, debido a que en la actualidad la firma digital ya interactúa con servicios comerciales, gubernamentales y financieros, y en los años venideros será incluida para interactuar con servicios civiles y legales.

Análisis retrospectivo del proyecto

La aplicación adecuada y oportuna de los cinco grupos de procesos y las nueve aéreas de conocimiento, aplicadas a la gestión de proyectos y en éste caso en particular, comprobaron ser una guía indispensable en el desarrollo y cumplimiento del proyecto; se logra así asegurar los objetivos planteados y cumplirlos dentro del tiempo y alcance planeados.

Sin embargo definir, delimitar y orientar los objetivos de la primera y segunda etapa del proyecto (proyectos integrados I y II) no fue tarea sencilla, en razón al alto grado de incertidumbre que se presenta en las etapas tempranas de cualquier proyecto y este no fue la excepción.

Un elemento clave en el cumplimiento de las actividades, lo aportaron la guía y asesoría de los profesores Ismael Mora y José Arrieta, cuyos comentarios y consejos, representaron una excelente guía y orientaron para lograr con éxito la consecución del objetivo principal del proyecto.

Durante el desarrollo de la investigación teórica en los conceptos de firma digital, y gracias a las acertadas y valiosas reuniones que se lograron concretar con los expertos en el tema *(Lic. Oscar Solís, Ing. Mario Álvarez-MICIT, Lic. Jairo Rojas-HACIENDA, Lic. Noe Castro, Gabriel Picado-Banco Popular, Ing. Daniel Rolando, Ing. Ricardo Gorosito-AFIP Republica de Argentina)*, quienes aportaron una guía invaluable al hilo conductor del proyecto, las dudas y la incertidumbre del proyecto fueron disminuyendo gradualmente, hasta lograr la ejecución exitosa de objetivos y las actividades que, para este fin se planearon, en el siguiente cuadro se detallan los objetivos y su adecuada gestión durante el proyecto; *(Cuadro No.6)*

Cuadro No. 6: Gestión de objetivos específicos

OBJETIVO	ACTIVIDADES EN CRONOGRAMA	¿SE ENTREGO?
Elaborar un análisis de costo beneficio para la utilización de la herramienta de firma digital en el AyA.	Producto No. 1 *(8 actividades)*	Sí
Definir estrategia para que funcionarios y clientes del AyA logren obtener un certificado de firma digital expendido por un CA autorizado *(Autoridad Certificadora Licenciada)*.	Producto No. 2 *(3 actividades)*	Sí
Diseñar el plan de implementación de la herramienta de firma digital para el AyA, tomando en cuenta la metodología MIFID	Producto No. 3 *(1 actividades)*	Sí
Diseñar un prototipo funcional de la herramienta de firma digital.	Producto No. 4 *(9 actividades)*	Sí

El primer objetivo se logró sin ningún problema ya que en la etapa anterior *(proyecto integrado I)* se había trabajado con algunos funcionarios del AyA, para definir los servicios candidatos, a los cuales se podría implementar firma digital. Es con esa lista que se priorizaron cuatro servicios que figuran en el cronograma propuesto de implementación; adicionalmente a esto se obtuvo el cálculo estimado para el costo unitario por servicio implementado.

El segundo objetivo es quizás uno de los más complejos a desarrollar; hay que recordar que el Instituto es un usuario de la tecnología únicamente y como tal, se convierte en un consumidor del servicio de una autoridad certificante, de modo que la estrategia a seguir será únicamente adquirir los certificados

Seguidamente se tiene el tercer objetivo gestionado por medio de un *WBS* y un cronograma propuesto de implementación, definido para un periodo de seis meses plazo y una visión de futuro proyectada hasta el 2013 donde se hablaría de una masificación de los servicios en el Instituto Costarricense de Acueductos y Alcantarillados.

Como último objetivo, se preparó un prototipo funcional para tomar en cuenta cuatro servicios. Este ejercicio fue de gran relevancia técnica para la gestión del proyecto, ya que fortaleció al plan de implementación propuesto; gracias a esto se mejoró la conceptualización de actividades, especialmente en la necesidad de adicionar un consultor en el tema de la seguridad, se mejoró la estimación en la asignación de tiempos, además de adquirir gran relevancia para demostrar de forma sencilla la utilidad del concepto de firma digital, y las virtudes que ofrecerá al AyA en un tiempo relativamente corto.

Para finalizar, se resalta la importancia que ha tomado este proyecto en la Institución, por lo que se le ha asignado el código No. 015, para que sea parte del portafolio oficial de proyectos del Departamento de Gestión de Proyectos de la Dirección de Sistemas de Información del AyA.

Carta de aceptación

INSTITUTO COSTARRICENSE DE ACUEDUCTOS Y ALCANTARILLADOS
San José, Costa Rica
Apartado 1097-1200 - Teléfono 2242-5401 - lechandi@aya.go.cr
GG-SUG-AF-DSI-842-2009

CARTA DE ACEPTACIÓN DEL PROYECTO

Conceptualización del marco metodológico para la implementación de la herramienta de firma digital, que le permita al Instituto Costarricense de Acueductos y Alcantarillados obtener una posición de vanguardia tecnológica, además de una mayor agilidad en sus procesos de negocio y las TIC

Mediante oficio SUB-GG-DSI-2009-238 del 23 de marzo del 2009, este Instituto, dio por aceptado el Proyecto denominado "Propuesta de implementación de la herramienta de firma digital en el Instituto Costarricense de Acueductos y Alcantarillados", formulado por los estudiantes Pedro Leiva Cerdas y Christian Vargas Araya, candidatos al grado de Magister en Administración de la Tecnologías de Información de la Universidad Nacional.

Una vez ejecutado el proyecto en sus dos etapas, de conformidad a lo establecido en la planeación original, y en cumplimiento con los objetivos del Plan estratégico de TI y las Normas Técnicas de TI de la Contraloría General de la República, se manifiesta su **ACEPTACIÓN,** como aporte fundamental para la gestión de las TIC's en AyA.

Este proyecto, incorporado dentro del portafolio de proyectos de TI, será parte de las estrategias institucionales para una mejora continua en la administración y seguridad de la información y de los servicios que se brindan a los clientes.

Se hace un reconocimiento especial a los señores Leiva y Vargas, por el empeño en la investigación del tema, y el esfuerzo realizado para plasmar cada una de las etapas y fases del trabajo.

Se extiende la presente a los treinta días del mes de noviembre del dos mil nueve.

María Lorena Echandi Echeverría
Directora de Tecnologías de Información
cc. Archivo

Glosario

Certificado Digital	Un certificado digital es un documento electrónico que contiene la identidad, la llave pública y la información personal del suscriptor. Es creado y firmado digitalmente por una persona jurídica prestadora del servicio de creación, emisión y operación de certificados digitales, conocida como Autoridad Certificadora.
Firma Digital	Es un método que asocia la identidad de una persona o equipo, con un mensaje o documento electrónico, para asegurar la autoría y la integridad del mismo. La firma digital del documento es el resultado de aplicar algoritmos matemáticos, (denominados función *hash*), a su contenido y así generan una firma digital del documento.
Infraestructura de clave pública - PKI	Combinación de hardware, software, políticas y procedimientos de seguridad que permiten la ejecución de operaciones de firma digital seguras. Esta definición es conocida mundialmente bajo las siglas PKI que significa *Public Key Infraestructure*.
Integridad	Es la información contenida en el mensaje o transacción electrónica que no ha sido modificada luego de su firma.
Autenticación	La información del documento y su firma se corresponden indubitablemente con la persona que ha firmado.
No repudio	Es la capacidad de afirmar la autoría de un mensaje o información del que un tercero es autor. De este modo el autor no puede negar su propia autoría. Bajo la figura del “no repudio”, una determinada comunicación o mensaje electrónico adquiere fuerza vinculante o efectos jurídicos, ante el posible rechazo o reclamación de su no-existencia por parte de su autor.
Token	Dispositivo o medio físico que resguarda y permite la verificación de la identidad digital del propietario representado por un Certificado Digital.
Prototipo	Modelo o ejemplar que permite testear algo antes de que entre a producción, detectarle errores, o presentar la idea general que por la cual fue construido.
XML	Lenguaje de etiquetas extendido, o por sus siglas en inglés *Extensible Markup Language*.
FIPS 140-2 nivel 2	Estándar para los dispositivos criptográficos (FIPS por sus siglas en inglés Federal Información Processing Standard).

Nomenclatura utilizada

AFIP	Administración Federal de Ingresos Públicos (República de Argentina)
AyA	Instituto Costarricense de Acueductos y Alcantarillados
ANSES	Administración Nacional de Seguridad Social (República de Argentina)
TRAC	Sistema para la administración de proyectos (Metodología)
AyA	Instituto Costarricense de Acueductos y Alcantarillados
BCCR	Banco Central de Costa Rica
CA	AC, o CA por sus siglas en inglés *Certificate Authority*, es una entidad de confianza del emisor y del receptor de una comunicación. Esta confianza de ambos en una 'tercera parte confiable' (*trusted third party*) permite que cualquiera de los dos confíe a su vez en los documentos firmados por la Autoridad Certificadora, en particular, en los certificados que identifican ambos extremos. En Costa Rica autorizada o registrada ante la Dirección de Certificadores de Firma Digital (DCFD)
RA	Autoridad de Registro, es la entidad responsable por la comunicación entre el suscriptor y la autoridad certificadora (CA). Está vinculada a una CA y tiene por objetivo recibir, validar, verificar y gestionar las solicitudes de emisión o revocación de certificados digitales, cumpliendo con lo establecido en la política de certificación nacional y en concordancia con las políticas y procedimientos definidos por la CA correspondiente.
CMMI	Capability Maturity Model Integration
COBIT	Objetivos de Control para la Información y la Tecnología relacionada
ECA	Ente Costarricense de Acreditación
DCFD	Se refiere a la "Dirección de Certificadores de Firma Digital", es la dependencia del Ministerio de Ciencia y Tecnología, encargada de la administración y supervisión del sistema de certificación digital.
FODA	Fortalezas, oportunidades, debilidades y amenazas
HFD	Herramienta de Firma Digital
INTE/ISO/IEC	Instituto de Normas Técnicas de Costa Rica / International Organization for Standardization / international Electrotechnical Commission
ITIL	Information Technology Infrastructure Library
MICIT	Ministerio de Ciencia y Tecnología
MIFID	Metodología de implementación para Firma Digital
PMBOK	Project Management Body of Knowledge
RE	Entidad Registro
SINPE	Sistema Nacional de Pagos Electrónicos
STGD	Secretaria Técnica de Gobierno Digital
BPDC	Banco Popular y de Desarrollo Comunal

COMEX	Comercio Exterior
TICA	Tecnología de Información para el Control Aduanero: Es un sistema que permite a los usuarios hacer sus trámites en forma electrónica, lo que evita presentarse a las ventanillas de oficinas públicas y llevar papeles físicos.
COMPRARED	Compras Electrónicas del Estado
MAG	Ministerio de Agricultura y Ganadería
STGD	Secretaría Técnica de Gobierno Digital
BPDC	Banco Popular y de Desarrollo Comunal
CAPICOM	Serie de componentes de *"Microsoft"* para utilizar plataformas telemáticas. i.e. tarjetas inteligentes
ACUERDO DE SUSCRIPTOR	Se refiere al "Acuerdo de Suscriptor para Suscriptores de Certificados de Firma Digital y de Autenticación de Persona Física Emitidos por la Autoridad Certificadora CA" en el cual, entre otros aspectos, se establecen los deberes y responsabilidades entre la CA y el suscriptor.

Anexos

Anexos en DVD.

1	**Documentos Oficiales utilizados para elaborar Etapas: Anteproyecto, Proyecto Integrado I y Proyecto Integrado II.**
2	**Documentos del Anteproyecto, carta autorización para iniciar proyecto.**
3	**Información General de Soporte a la Investigación.**
4	**Proyecto Integrado I.** (entregables)
	WBS - Cronograma - Anexos Varios.
	Carta constitutiva - Plan de proyecto, Documentos de productos 1,2,3,4 - Documentos de cierre - entrevistas y archivos en audio - Paper - Presentación de defensa Proyecto Integrado I.
5	**Proyecto Integrado II.** (entregables)
	WBS - Cronograma, Anexos Varios - documentos charla Auditorio AyA.
	Carta constitutiva - Plan de proyecto - Documentos de productos 1,2,3,4 - Documentos de cierre, entrevistas y archivos en audio - Carta Aceptación - Tesina y Presentación de defensa Proyecto Integrado II.

Anexos en este documento.

Anexo No. 1 – Metodología MIFID.

Introducción

Actualmente el mundo vive la era de la digitalización y las diversas formas de gestionar la información y las comunicaciones. Costa Rica no escapa a esta realidad, donde se hace lo propio para circular por la vía del desarrollo tecnológico y sus nuevas tendencias, como es el caso del concepto de Gobierno Digital, el cual pretende digitalizar ya no sólo los datos organizacionales, sino también a quienes son responsables de ellos.

Nuestro país ha iniciado los primeros pasos para introducirse en ese gran concepto, mediante la definición e implementación de legislación pertinente para regular la firma digital y sus aspectos legales. Desde octubre del 2005, en la gaceta número 197, la Asamblea Legislativa de la República de Costa Rica decreta la ley de certificados digitales, firmas digitales y documentos electrónicos. Basado en este marco legal vigente hasta la fecha, además del análisis de casos de éxito documentados y las diversas metodologías estándar en el mercado de la informática y las comunicaciones como los son *COBIT, CMMI, ITIL*, y otras, se ha desarrollado esta guía de diseño, administración e implementación, se busca como finalidad la descripción de una serie de buenas prácticas, un modelo de madurez, plantillas y esquemas para poder implementar la herramienta de firma digital en instituciones gubernamentales.

Este documento intenta de una forma ordenada y estructurada identificar las fortalezas y debilidades de una Institución estatal para poder utilizar paralelamente la herramienta de firma digital junto con sus procesos tradicionales, se intento que ambas formas convivan libremente sin colisionar o provocar conflictos entre estos, se busca agilizar y/o mejorar los productos y servicios que se ofrecen. A continuación se detalla la Metodología de Implementación de Firma Digital (MIFID).

Metodología de Implementación para Firma Digital (MIFID).

El desarrollo de este modelo metodológico de implementación progresiva, está orientado inicialmente para adaptar el concepto de firma digital a los procesos y servicios de empresas en el sector público.

En sus primeras actividades pretende realizar una ambientación adecuada; tanto a nivel técnico, administrativo y procedimental como a nivel de aceptación cultural, se entiende este último como uno de los aspectos más relevantes para el éxito del proyecto, especialmente porque se habla de un cambio cultural que involucra componentes tecnológicos novedosos, donde se requiere que los funcionarios involucrados posean un perfil donde estén acostumbrados al hábito del acceso a internet, el uso de correo electrónico, la creación y modificación archivos digitales, etcétera.

Además, se deberá realizar el esfuerzo de involucrar a la alta gerencia a participar activamente en el desarrollo, implementación y puesta en marcha de este proyecto, donde se fortalezca la identificación del proyecto con todas las áreas involucradas, y se incentiva a considerar desde el inicio la importancia de la seguridad que amerita este tipo de soluciones tecnológicas.

En sus procesos medios, pretende impulsar a la organización para que se inicie en el mundo de la Herramienta de Firma Digital, mediante la asignación de certificados digitales a los miembros involucrados, la adquisición de los recursos necesarios para lograr la puesta en marcha, su respectivo mantenimiento, e inicia una ordenada administración y gestión de información, de los cambios en el proyecto y se fortalezca aun más, el concepto de seguridad.

En sus procesos finales, pretende garantizar productos y/o servicios eficientes y confiables, mediante el mejoramiento continuo y el buen desempeño de las herramientas implementadas, además de reiteradas mediciones y

verificaciones de esas herramientas, y la actualización constante de quienes interactúan con esta solución tecnológica.

Análisis descriptivo del proceso utilizado para construir MIFID

El desarrollo de este modelo se ha basado en tres componentes como parámetros de entrada.

El primer componente son los marcos metodológicos mundialmente reconocidos tales como CMMI (*Capability Maturity Model Integration*)[1] COBIT(Objetivos de Control para la Información y la Tecnología relacionada)[2], la metodología de gestión de proyectos cuyos conceptos están reunidos en el PMBOK (*Project Management Body of Knowledge*)[3], vistos como un cuerpo de conocimientos reconocidos y mejores prácticas, que apuntan a una gran gama de procesos organizacionales que para efectos de la metodología buscada serán definidos en políticas concretas, sin dejar de lado sus conceptos originales.

El segundo componente a tomar en cuenta serán los casos de estudio de algunas implementaciones exitosas tal como en el caso de México, Chile y Brasil (Información bibliográfica y apuntes de personas que visitaron estos países, quienes fueron los encargados del proyecto para la implementación del CA Raíz para Costa Rica); además se contó con el caso de éxito de la Administración Federal de Ingresos Públicos (AFIP), una organización gubernamental de la República de Argentina, para este caso se contó con la participación de dos de los integrantes que participaron activamente en el equipo de implementación de la firma digital en dicha organización.[4]

[1] Capabilty Maturity Model® Integration (CMMISM), Version 1.1, CMMISM for Systems engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing (CMMI-SE/SW/IPPD/SS, V1.1), Marzo del 2002.
[2] Documento COBIT 4.0, IT Gobernance Institute, 2005.
[3] Guía de los Fundamentos de la Dirección de Proyectos, Tercera Edición, ANSI/PMI 99-001-2004.
[4] Documento Producto No. 3: Metodología de implementación de HFD, Junio del 2009.

El tercero y último componente a tomar en cuenta lo conforman los lineamientos, políticas y reglamentos contenidos en la **"LEY DE CERTIFICADOS, FIRMAS DIGITALES Y DOCUMENTOS ELECTRONICOS No. 8454"** publicada el 13 de octubre del año 2005 en la Gaceta Oficial numero 197. Una vez obtenido el análisis de estos componentes se tiene la metodología definida y denominada MIFID -Metodología de implementación para Firma Digital, cuya aplicación será orientada al sector público costarricense. *(fig.1a)*

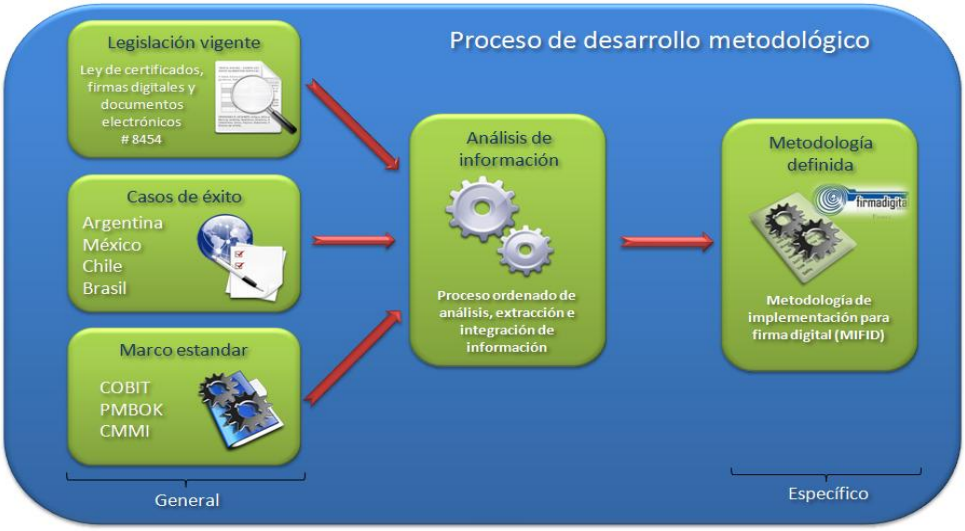

Figura No. 1a: Integración de elementos dentro del proceso de desarrollo metodológico MIFID.

Modelo de madurez para MIFID

Basado en el marco estándar metodológico de COBIT, este modelo de madurez establece un conjunto de prácticas que deben de ser evidenciadas e identificadas en cada nivel del modelo, se logró convertirlo en una excelente herramienta como indicador del estado actual y futuro de la organización en cuanto al tema de firma digital se refiere.

Importante es indicar que esta escalada por niveles también es de gran ayuda al generar metas específicas para cada nivel, traduciéndolo como un plan de implementación para la herramienta de firma digital. Lograrlo con éxito no es una tarea fácil, no por su significado a nivel técnico, sino más bien la dificultad

intrínseca que existe en el ser humano y los inconvenientes para adaptarse rápidamente a los cambios tecnológicos, que ahora más que nunca, son cada vez más acelerados.

Cada nivel debe se deberá superar secuencialmente y sobre todo deberá de existir un compromiso en la gestión organizacional, en sentido de que lo logrado deberá mantenerse y de ser posible mejorarse, a fin de escalar en cada uno de los niveles siguientes. Si al menos un requisito no se cumple, no será posible avanzar al siguiente nivel. Esto se logra mediante el diagnóstico, que es el que identifica en qué nivel de implementación se encuentra la organización. *(fig.2a)*

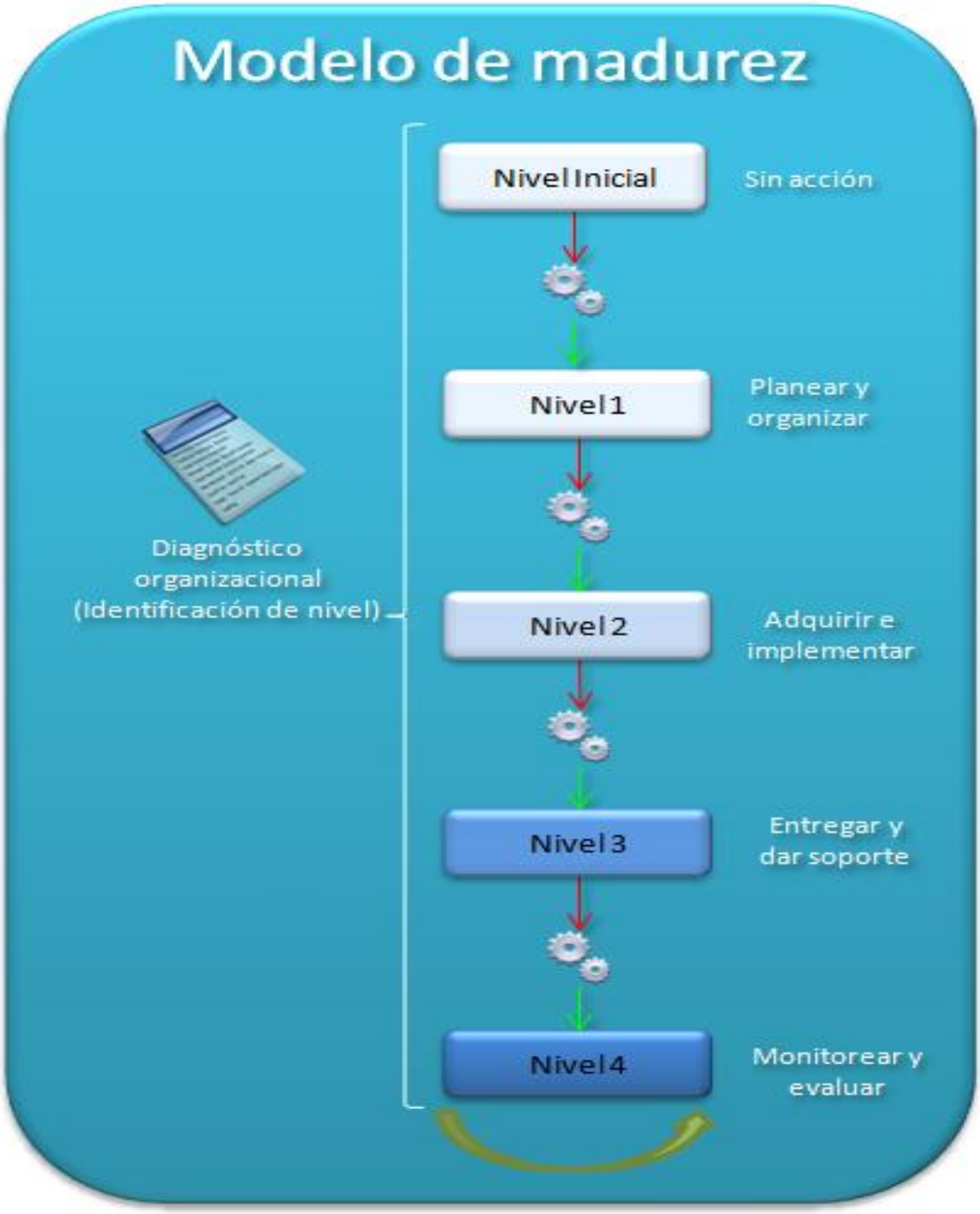

Figura No. 2a: Escala del modelo de madurez MIFID de 4 niveles.

Algunas preguntas que responden este modelo son:

- ✓ *Un indicador del desempeño real de la organización, que responde a* ***¿Dónde se encuentra la organización hoy?***
- ✓ *Un indicador del desempeño con respecto a otras organizaciones,* ***bien en comparación con quien.*** *(Benchmarking).*
- ✓ *Permite alinearse con los objetivos (misión y visión),* ***¿Dónde se desea estar?***

El siguiente cuadro detalla los requerimientos que evidencia el nivel de madurez donde se encuentra la organización y hacia donde puede dirigirse; se puede ver también como la respuesta a las preguntas; ¿Qué tenemos?, ¿Dónde estamos?, pero sobre todo la respuesta a la pregunta ¿Qué debemos hacer para llegar al siguiente nivel?, se convierte en una herramienta ideal para orientar la gestión de la organización en el sentido que se pretende.

Modelo de Madurez		
Nivel 4	**Optimizado**	La organización en este nivel evidencia controles y optimizaciones constantes de sus operaciones, infraestructura, recursos humanos, nuevos requerimientos de mercado. Mide el rendimiento y desempeño de la herramienta de firma digital y la mantiene en constante depuración y mejora, así como también los controles internos que son responsables de su buen desempeño. Controla el cumplimiento estricto y riguroso de los estatutos de legislación vigente y se mantiene en constante mejora continua.
Nivel 3	**Administrado**	La organización en este nivel evidencia una garantía del desempeño y calidad de sus recursos para funcionar con la herramienta de firma digital, se garantizará también la calidad de sus servicios y la seguridad imperante, especializa a su personal respecto al concepto de la firma digital, se preocupa por considerar las expectativas y observaciones de los usuarios finales o clientes, administra y gestiona los problemas actuales, el ambiente de infraestructura tecnológica y las operaciones.
Nivel 2	**Definido**	La organización en este nivel evidencia una preparación formal para introducirse de lleno en el concepto de implementación de la herramienta de firma digital, realiza certificaciones de su personal, identifica necesidades para adquirir nuevas tecnologías informáticas y soluciones de software, formaliza y documenta el camino a seguir como autoridad certificadora(CA), autoridad de registro(RA) y/o suscriptor, implementa la documentación pertinente para usuarios internos y finales, se preocupa por definir ordenadamente la administración de cambios que pueden surgir en la implementación de la herramienta, además de iniciar controles para obtener los resultados esperados de la implementación.
Nivel 1	**Preliminar**	La organización en este nivel evidencia un ambiente de adaptación para lograr procedimientos definidos, estudiar y comunicar la legislación vigente sobre certificados, firmas digitales y documentos electrónicos. Además cuenta con apoyo gerencial para la implementación de firma digital en la organización. Se tiene documentado y formalizado un plan estratégico, se realizan evaluaciones y administración de riesgos, se ha modificado la cultura organizacional para convivir con la herramienta de firma digital además de identificar si se implementa el CA.
Nivel Inicial	**Inicial**	La organización en este nivel no evidencia procesos definidos, no se conoce la legislación vigente, ni existe comunicación con la alta gerencia sobre el proyecto de implementación, ni existen procesos ni procedimientos de medición, ni metas establecidas.

Beneficios de utilizar el marco metodológico y un modelo de madurez

En definitiva, la utilización de las metodologías son de gran ayuda para la ejecución de proyectos; se identifican los siguientes beneficios asociados:

- ✓ *Administrar este tipo de proyectos tecnológicos que utilicen una guía ordenada y objetiva que logre todos los objetivos planificados. Este tipo de documentación estandarizada, la cual utiliza plantillas, modelo de madurez, además de estándares de planificación y control de requerimientos, pretende determinar el alcance y la buena gestión de esos requerimientos, así lograr un cumplimiento total de éstos, con la mejor calidad posible, en el tiempo previamente planificado.*

- ✓ *Identificar los requerimientos, procesos y recursos. Mediante una serie de pautas definidas en la metodología, se pretenden identificar todos aquellos aspectos (culturales, operativos y administrativos), procesos y recursos que se verán afectados o tendrán que convivir paralelamente con la herramienta de firma digital, con la finalidad de ofrecer productos y/o servicios tradicionales de la mano con las nuevas tecnologías digitales, sin descuidar en ningún momento los conceptos de calidad y seguridad.*

- ✓ *Identificar y administrar los riesgos presentes de una implementación de la herramienta de firma digital. Este tipo de estándar pretende evitar pasar por alto los riesgos en una eventual implementación de la herramienta de firma digital y un eventual impacto negativo en ésa, además de definir una serie de buenas prácticas para su administración, medición, control y tratamiento.*

- ✓ *Controlar ordenadamente el crecimiento y avance que obtiene la organización a través de tiempo respecto a un modelo de madurez. Este tipo de herramienta de medición y control pretende controlar y medir que se cumpla las métricas y metas organizacionales establecidas, además de garantizar el mejoramiento continuo cuando se ha llegado al máximo nivel, se asegura con esto que siempre se esté en constante renovación o mejora continua de los productos y/o servicios ofrecidos.*

- ✓ *Gestionar en forma oportuna los cambios al darse la implementación de la herramienta de firma digital. Mediante una estrategia establecida y aprobada se podrán asistir los procesos de transformación que tienen como objetivo específico la potenciación de la flexibilidad de la organización y su capacidad de respuesta rápida a situaciones nuevas.*

Marco general de la metodología

La metodología MIFID es un concepto básico y de aplicación sencilla, que busca asegurar un proceso de implementación ordenado y sistemático para la herramienta de firma digital.

Las características que identifican el alcance para cada nivel de madurez delimitan y definen los procesos en los que se debe desarrollar, además de identificar la madurez que la organización posee en el proceso de implementación de la firma digital. *(fig.3a)*

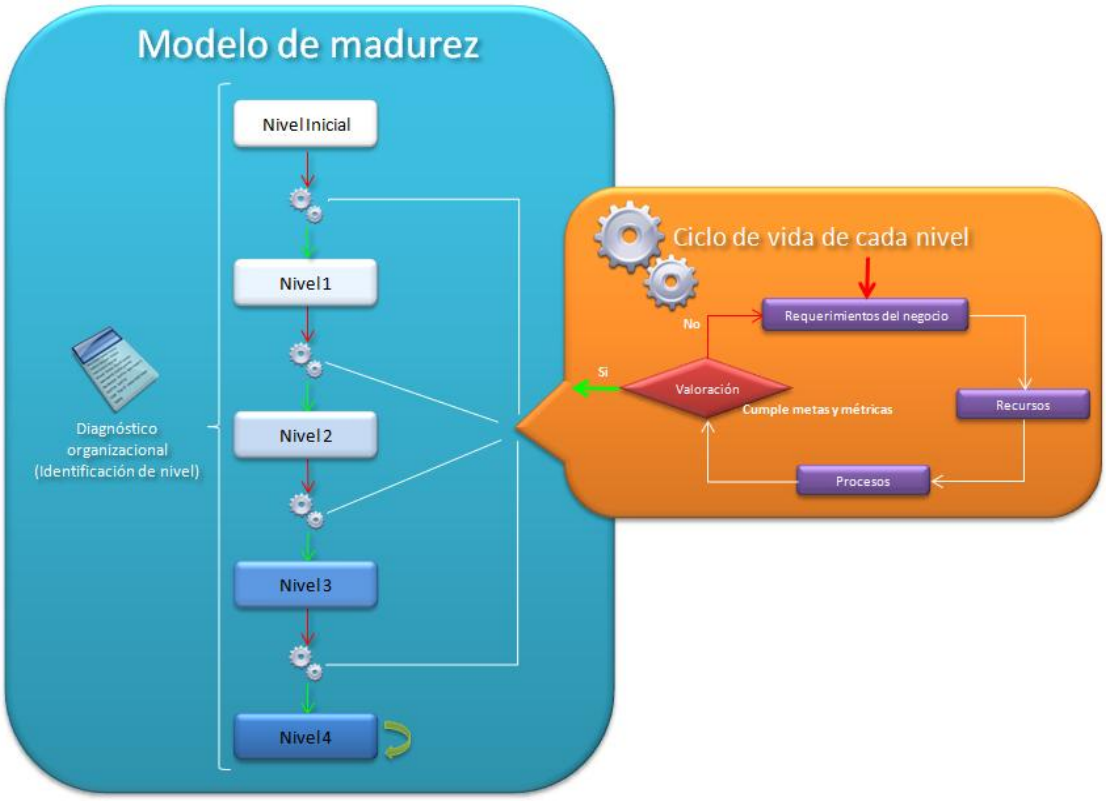

Figura No. 3a: Modelo de madurez y el ciclo de vida de cada nivel.

PASO No.1

El diagnóstico organizacional, va a definir la madurez inicial en el momento del abordaje del proceso de implementación, por ejemplo si la organización no evidencia ningún requisito del nivel de madurez 1, se puede decir que esta en un nivel inicial. (en este punto, la organización no posee ningún grado de madurez)

Es así como una vez identificado el nivel (según diagnóstico organizacional), se debe de trabajar en desarrollar los procesos del siguiente nivel.

PASO No.2

Los procesos identificados entran en varios ciclos denominados "ciclos de vida de cada nivel", donde se transforman las acciones (PROCESOS) en hechos medibles y verificables, originados por una necesidad (REQUERIMIENTOS DEL NEGOCIO), que evidencia la existencia y aplicación de la herramienta de firma digital dentro de la organización.

El siguiente subproceso describe con más detalle el paso número dos: *(fig.4a)*

- ***a-*** *Se identifican los requerimientos del negocio.*
- ***b-*** *Se identifican los recursos necesarios para realizar dichos requerimientos.*
- ***c-*** *Se ejecutan los procesos que satisfacen esos requerimientos.*
- **d-** *Por último, esos procesos son valorados y verificados. (cumple metas y métricas)*

Figura No. 4a: Ciclo de vida de cada nivel.

PASO No.3

Al determinar, mediante la acción de valoración, que todas las metas se han completado, se deberá escalar al siguiente nivel.

Pero, en caso de obtenerse una valoración de métricas "no aceptable", o dicho en otras palabras, no se cumple alguna de ellas, se repite el paso No.2 hasta completar todas las metas (procesos) definidos según el nivel que se desea superar.

Dominios para la metodología MIFID

El avance de implementación de la herramienta de firma digital dentro de la organización, es un recorrido por cuadro dominios básicos (PO, AI, ES y ME) en los cuales los PROCESOS son ubicados (agrupados) según corresponda el nivel de madurez que se quiere alcanzar. *(fig.5a)*

Figura No. 5a: Dominios de la metodología.

Cada dominio, representa un nivel de madurez y una cantidad de procesos que los identifican, los cuales son resumidos en la matriz de dominios. *(fig.6a)*

Nombre del Dominio	Alias	Nivel de madurez	Cantidad procesos
Planear y Organizar	PO	1	7
Adquirir e Implantar	AI	2	7
Entregar y dar Soporte	ES	3	8
Monitorear y Evaluar	ME	4	4
TOTAL		**Niveles: 4**	**Procesos: 26**

Figura No. 6a: Matriz de dominios MIFID.

La cantidad de procesos para cada dominio, puede variar, según sea ajustado el proceso de implementación, esto dependerá de los requerimientos de la organización.

1. Detalle de PROCESOS para cada nivel

Nivel 1: **Planear y organizar**

La siguiente matriz detalla los procesos para este nivel.

ID	NOMBRE DEL PROCESO	DETALLE DE TAREAS A REALIZAR
PO1	Solicitar apoyo gerencial y comunicar logros organizacionales	Formalizar el apoyo de parte de la gerencia general y patrocinadores del proyecto, creando a la vez conciencia de la importancia del éxito del proyecto para la organización. Además, asegurar la comunicación efectiva y eficaz entre las figuras anteriormente descritas y el departamento de TI. La información comunicada debe abarcar una misión claramente definida, los objetivos que la componen, un análisis de la seguridad organizacional actual, una descripción de los controles internos actuales, un análisis del nivel de calidad según los objetivos planteados, el código de ética y conducta, políticas y procedimientos, etcétera. Toda la anterior información debe ser incluida dentro de un programa de comunicación continua debidamente documentado, todo esto apoyado por la alta gerencia. La dirección del proyecto debe dar especial atención a comunicar la conciencia sobre las consideraciones de la seguridad y el mensaje de que el tema de la seguridad es responsabilidad de todos.
PO2	Estudiar y comunicar legislación vigente	Se deberá crear un grupo de trabajo interdisciplinario, coordinado por la gerencia, que analice e intérprete los temas técnicos y legales de la legislación vigente en el momento. Formular un documento que abarque los artículos legislados así como todas las disposiciones indicadas por el DCFD y el ECA, que por alguna razón no favorezcan o entorpezcan los procesos cotidianos de la organización, o no fomenten su crecimiento y/o la mejora de tiempos de respuesta sobre los productos o servicios. Generar un manual de procedimientos internos que conviva libremente con la legislación vigente, a fin de evitar cualquier acción que implique sanciones legales para la organización. Es de especial atención de parte de la dirección de proyectos comunicar a la alta gerencia el resultado del análisis legal y el manual interno de procedimientos.

ID	NOMBRE DEL PROCESO	DETALLE DE TAREAS A REALIZAR
PO3	Definir plan estratégico de implementación	Crear un plan estratégico que defina, en cooperación con los interesados, cómo la firma digital contribuirá a los objetivos estratégicos o metas de la organización, así como los costos y riesgos relacionados. Define cómo se cumplirán y medirán los objetivos y recibirá una autorización formal de los interesados. El plan estratégico debe incluir el presupuesto operativo de la inversión, las fuentes de financiamiento, la estrategia de adquisición, los requerimientos legales y regulatorios, etcétera. El plan estratégico debe ser lo suficientemente detallado para permitir la definición transparente de la implementación de la firma digital.
PO4	Fomentar el cambio cultural en la organización	una serie de actividades, programas, eventos publicitarios, informativos y comunicativos, etcétera., sobre la nueva tecnología a implantar en la organización. Considerar a todos los involucrados, llámese patrocinadores, gerentes, directores, técnicos, jefaturas, proveedores, recursos humanos, usuarios de aplicaciones, usuarios finales, etcétera.
PO5	Determinar la implementación de la autoridad certificadora	Realizar un estudio de viabilidad técnica, legal y administrativa, así como un análisis de costo beneficio al implementar un CA. Esta información deberá ser conocida y debidamente procesada por la alta gerencia, patrocinadores y demás entidades encargadas de valorar la responsabilidad civil que conlleva la creación de la oficina de autoridad certificadora.
PO6	Definir los procesos de la organización	Definir un marco de trabajo para la implementación de firma digital. Este marco incluye estructura y relaciones de procesos a modificar para que convivan mediante la utilización de los métodos tradicionales junto con la firma digital (así administra brechas y superposiciones de procesos), propiedad, medición del desempeño, mejoras, cumplimiento, metas de calidad y planes para alcanzarlas. Proporciona integración entre los procesos normales y los que son específicos de firma digital, procesos de negocio y procesos de cambio del negocio. El marco de trabajo de implementación debe estar integrado en un sistema de administración de calidad y en un marco de trabajo de control interno.
PO7	Evaluar y administrar riesgos	Crear y mantener un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de la implementación, estrategias de mitigación y riesgos acordados. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de

ID	NOMBRE DEL PROCESO	DETALLE DE TAREAS A REALIZAR
		riesgos para minimizar los riesgos a un nivel aceptable. El resultado de la evaluación debe ser entendible para los participantes y se debe expresar en términos financieros, para permitir a los participantes alinear los riesgos a un nivel aceptable de tolerancia. Esta documentación debe ser conocida por los patrocinadores del proyecto para su debida aprobación formal.

Nivel 2: **Adquirir e implementar**

La siguiente matriz detalla los procesos para este nivel.

	Acreditar a los respectivos miembros con un certificado de subscriptor	Definir el proceso de acreditación a cada miembro de la organización que se verá involucrado en la aplicación de la metodología de implementación y que inicialmente requiera hacerlo. Se pretende que en caso de demostraciones técnicas o aplicativas los miembros puedan participar activamente en el impulso del concepto de firma digital dentro de la organización
AI	Identificar soluciones automatizadas	Identificar mediante un informe técnico la necesidad de adquirir una serie de soluciones de software mediante adquisición de compra o por medio de desarrollos, que puedan satisfacer la utilización de la firma digital tanto en el seno interno como para que los usuarios finales interactúen con los servicios que ofrece la organización, para garantizar que los requisitos del negocio se satisfacen con un enfoque efectivo y eficiente. Este proceso cubre la definición de las necesidades, considera las fuentes alternativas, realiza una revisión de la factibilidad tecnológica y económica, ejecuta un análisis de riesgo y de costo-beneficio, además de concluir con una decisión final de desarrollar o comprar.
AI	Adquirir los recursos para lograr la implementación de la HFD	Realizar un estudio técnico de viabilidad sobre la adquisición mediante compra o desarrollo de software especial y/o especializado para utilizar la herramienta de firma digital en procesos o servicios sumamente específicos, si existen en la organización.

AI	Implementar un CA, RA y/o ente de registro	Crear un documento formal para describir detalladamente el proceso de implementación de firma digital que va a implementar la organización, tanto si se va a crear la CA, como para desarrollar los procedimientos de seguridad acordes a la infraestructura, estándares y procesos internos de la organización, además del plan de arquitectura tecnológica, tanto para la CA como la RA. El documento generado deberá apegarse estrictamente a la legislación vigente del momento, donde se cumple con requerimientos y documentación ahí expresos, se pueden identificar el nombre de la razón social, número de cédula de persona jurídica, domicilio, página web, dirección de correo electrónico, responsables administrativos y técnicos, etcétera.
AI	Facilitar la operación y el uso	Identificar y compartir el conocimiento sobre los nuevos sistemas, el cual debe estar disponible para todos los involucrados. Este proceso requiere la generación de documentación y manuales para usuarios técnicos, administrativos y finales, y proporciona entrenamiento para garantizar el correcto uso y la efectiva operación de las aplicaciones y la infraestructura.
	Administrar cambios	Todos los cambios, incluidos los mantenimientos preventivos y correctivos relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formal y controladamente. Los cambios (incluye procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar, medir y autorizar previo a la implementación. Se deben revisar contra los resultados planeados después de la implementación. Esto garantiza la reducción de riesgos que impacta negativamente la estabilidad o integridad del ambiente de producción.
AI	Instalar y acreditar soluciones y cambios	Se pretende lograr que los nuevos sistemas sean funcionales una vez que su desarrollo se completa. Esto requiere pruebas adecuadas en un ambiente dedicado, con datos de prueba relevantes, además de definir la transición e instrucciones de migración, la planificación de la liberación y la transición al ambiente de producción, y revisar la post-implementación. Esto garantiza que los sistemas operacionales estén en línea con las expectativas convenidas y con los resultados.

Nivel 3: **Entregar y dar soporte**

La siguiente matriz detalla los procesos para este nivel.

ES1	Administrar desempeño y capacidad de recursos de HFD	La necesidad de administrar el desempeño y la capacidad de los recursos de la herramienta de firma digital requiere de un proceso para revisar periódicamente el desempeño actual y la capacidad de esos recursos que la componen. Este proceso incluye el pronóstico de las necesidades futuras, basadas en los requerimientos de carga de trabajo, almacenamiento y contingencias. Este proceso brinda la seguridad para que los recursos de información que soportan los requerimientos del negocio estén disponibles de manera continua.
ES2	Garantizar la calidad de servicios con HFD	La necesidad de brindar continuidad en los servicios que consideran la herramienta de firma digital requiere desarrollar, mantener y probar planes de continuidad, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad. Un proceso efectivo de continuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios mencionados, sobre funciones y procesos claves del negocio.
ES3	Garantizar la seguridad de los servicios de HFD	La necesidad de mantener la integridad de la información y de proteger los activos organizacionales, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos que resguarden esa integridad. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de la organización para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad.
ES4	Educar y entrenar a los usuarios en el uso de HFD	Para una educación efectiva de todos los usuarios de la herramienta de firma digital, (se incluye aquellos dentro de la organización), se requieren identificar las necesidades de entrenamiento de cada grupo de usuarios. Además de identificar las necesidades, este proceso incluye la definición y ejecución de una estrategia para efectuar un entrenamiento efectivo y para medir los resultados. Un programa efectivo de entrenamiento incrementa el uso efectivo de la tecnología al disminuir los errores, se incrementa la productividad y el cumplimiento de los controles clave tales como las medidas de seguridad de los usuarios.

ES5	Administrar la mesa de servicio y los incidentes	Este proceso pretende responder de manera oportuna y efectiva a las consultas y problemas de los usuarios internos y finales de la herramienta de firma digital mediante un espacio físico en la organización. Se requiere de una mesa de servicio bien diseñada, ejecutada, y de un proceso de administración de incidentes. Este proceso incluye la creación de una función de mesa de servicio con registro, escalamiento de incidentes, análisis de tendencia, análisis causa-raíz y resolución. Los beneficios del negocio incluyen el incremento en la productividad gracias a la resolución rápida de consultas. Además, el negocio puede identificar la causa raíz (tales como un pobre entrenamiento a los usuarios) a través de un proceso de reporte efectivo.
ES6	Administrar los problemas	Una efectiva administración de problemas requiere la identificación y clasificación de problemas, el análisis de las causas desde su raíz, y la resolución de problemas. El proceso de administración de problemas también incluye la identificación de recomendaciones para la mejora, el mantenimiento de registros de problemas y la revisión del estatus de las acciones correctivas. Un efectivo proceso de administración de problemas mejora los niveles de servicio, reduce costos y mejora la conveniencia y satisfacción del usuario.
ES7	Administrar el ambiente físico del CA y RA	La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos (site), la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.
ES8	Administrar las operaciones	Un procesamiento de información completo y apropiado requiere de una efectiva administración del procesamiento de datos y del mantenimiento del hardware. Este proceso incluye la definición de políticas y procedimientos de operación para una administración efectiva del procesamiento programado, protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimiento preventivo de hardware. Una efectiva administración de operaciones ayuda a mantener la integridad de los datos y reduce los retrasos en el trabajo y los costos operativos.

Nivel 4: **Monitorear y evaluar**

La siguiente matriz detalla los procesos para este nivel.

ME	Monitorear y evaluar el desempeño de HFD	Una efectiva administración del desempeño de la herramienta de firma digital requiere un proceso de monitoreo. El proceso incluye la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan desviaciones. El monitoreo se requiere para garantizar que las cosas correctas se continúen haciendo y que estén de acuerdo con el conjunto de directrices y políticas.
	Monitorear y evaluar el control interno	Establecer un programa de control interno efectivo requiere un proceso bien definido de monitoreo. Este proceso incluye el monitoreo y el reporte de las excepciones de control, resultados de las auto-evaluaciones y revisiones por parte de terceros. Un beneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables de la organización.
ME	Garantizar el cumplimiento regulatorio	Crear y verificar el catálogo de requerimientos legales y regulatorios relacionados con la herramienta de firma digital y su legislación vigente.
ME	Mejoras al marco de procesos	Revisar y verificar constantemente las mejoras al marco de procesos donde se promueve el mejoramiento continuo y constante.

Referencias

[DEC33147] Decreto Ejecutivo N° 33147-MP que Crea la Comisión Intersectorial de Gobierno Digital y la Secretaría Técnica de Gobierno, Publicado el 6 de marzo del 2008.

[LEY2726] Ley Constitutiva Instituto Costarricense Acueductos y Alcantarillados, No. 2726, Publicada el 14 de Abril de 1961.

[DEC33147] Decreto Ejecutivo N° 33147-MP que Crea la Comisión Intersectorial de Gobierno Digital y la Secretaría Técnica de Gobierno, Publicado el 6 de marzo del 2008.

[LEY8454] Ley de Certificados, Firmas Digitales y Documentos Electrónicos, No. 8454, Publicada el 30 de agosto del 2005.

[STGD-08] Secretaría Técnica de Gobierno Digital (STGD), (2008, Enero). *Plan de Acción Gobierno Digital 2008-2010*.

[DEC-33018] Decreto Nº 33018 –MICIT, El Presidente de la República y el Ministro del Ciencia y Tecnología. Publicado el 20 de marzo del 2006.

[RODRIGUEZ] Rodríguez Cervera, Lucas, Nevant, (n.d.). *Cree su Propia Metodología basado en un Marco Estándar*, info@nevant.com, (Parte I, II y II).

[MIFID-09] Etapa I de este Proyecto, (2009, Agosto 14). Documento *Metodología Integrada para la Firma Digital*, mismos autores.

[ROLANDO-09] Rolando Daniel, (2009, Abril). *Firma Digital en la República Argentina, Un modelo para su desarrollo, Trabajo Integrador del Curso de Posgrado "Especialista en Gestión de las Telecomunicaciones 2007-2008*", drolando@afip.gov.ar. Instituto Tecnológico de Buenos Aires, Argentina.

[PRO1-09] Etapa I de este Proyecto, (2009, Agosto 14). *Documento Producto No. 1: Informe de un caso de éxito de la HFD,* mismos autores.

[NACION-12/09] Fonseca, Pablo. (2009, Agosto 12). "Rodrigo Arias ya tiene su firma digital", *Periódico La Nación*, Sección Aldea Global, página 21A.

[SOLIS-09] Solís, Oscar, (2009, Julio). Responsable de la Dirección de Certificadores de Firma Digital del MICIT, osolis@micit.go.cr. Entrevista personal.

[ROJAS-8/09] Rojas, Jairo, (2009, Agosto 20). *Experiencia del Ministerio de Hacienda en la Adaptación de sus Sistemas para Usar Firma Digital Certificada*, Conferencia dictada por Lic. Jairo Rojas, rojascja@hacienda.go.cr funcionario del Ministerio de Hacienda, quien participo en el proyecto de implementación de firma digital, Auditorio MICIT, San José, Costa Rica.

[CASTRO &PICADO-09] Castro, Noe noecastro@bp.fi.cr y Picado, Gabriel gabrielpicado@bp.fi.cr, (2009, Octubre 6). Funcionarios del Departamento de TI del Banco Popular, participantes del proyecto fe implementación de firma digital. Entrevista personal.

[NACION-3/09] Feigenblatt, Hazel. (2008, Marzo 20), "BCR podría ir a arbitraje por fraudes electrónicos", *Periódico La Nación,* Sección "El país"

[E-TOKEN] BPDC, (2009). *El BPDC implementa en su plataforma web el dispositivo "e-token"* tttps://www.popularenlinea.fi.cr/Bpop/Menu/Personas /e_Token/

[NACION-18/09] Mayorga, Gabriela. (2009, Setiembre 18), "Banco Popular inicia entrega de tarjetas de firma digital", *Periódico La Nación,* Sección Economía.

[PRO2-09] Etapa I de este Proyecto, (2009, Agosto 14). Documento *Producto No. 2: Diagnósticos de la situación actual de infraestructura y procesos*, mismos autores.

[GUIA] Departamento de Gestión de Proyectos TI-AyA, (2009). **"***Procedimiento para la Gestión del Riesgo",* Gestión de Proyectos AyA, versión 2.

Nota: las referencias a links de Internet a lo largo de todo el documento, son válidas al momento de la presentación del mismo, y podrían dejar de serlo en el futuro. Los autores no se hace responsables de su actualización de dichos sitios.