

1 MARCO INTRODUCTORIO

1.1 INTRODUCCIÓN

La gran necesidad de los gobiernos de agilizar, optimizar, flexibilizar, transparentar y abaratar procesos y/o actividades del sistema público, ha motivado a utilizar en forma acelerada y sustancial las tecnologías de información y comunicación para el desarrollo de aplicaciones, diseñadas para trabajar de la manera más óptima, integrando sistemas, utilizando las mejores herramientas de gestión y desarrollando modelos adecuados a las necesidades de los gobiernos.

En el ámbito de este cambio surge el concepto de gobierno electrónico¹, el cual se refiere a la transformación de todo el gobierno como un cambio de ejemplo en la gestión gubernamental, es un concepto de gestión que fusiona la utilización intensiva de las tecnologías de información y comunicación , con modalidades de gestión, planificación y administración, como una nueva forma de gobierno.

Para lograr esta transformación un punto fundamental es el uso de firmas digitales que en términos legales es el equivalente a las firmas manuscritas, cumpliendo de esta formas las funciones principales de las firmas manuscritas como ser: la autenticación de la identidad del firmante, la integridad de la información del documento, la confidencialidad de los datos en casos de ser necesarios y el no repudio de la información.

Bolivia ha empezado a adoptar estas legislaciones con la ley Nro. 164² vigente desde el año 2011 el cual promueve y otorga validez al uso de firmas digitales, tanto en las entidades publicas como privadas, con la finalidad de favorecer la accesibilidad, la transparencia y un mejor control de las actividades de estas entidades.

El Ministerio de Obras Públicas, Servicios y Vivienda siendo uno de los Ministerios mas

1 Consiste en el uso de las tecnologías de la información y el conocimiento en los procesos internos de gobierno, así como en la entrega de los productos y servicios del Estado tanto a los ciudadanos como a la industria.

2 Ley general de telecomunicaciones, Tecnologías de Información y Comunicación.

importantes del estado y coordinador para la implementación tanto de gobierno electrónico, plan de software libre y firma digital, se ve en la necesidad de ser el pionero en la utilización y desarrollo de estas tecnologías.

1.2 ANTECEDENTES

1.2.1 Antecedentes institucionales

El ministerio de Obras Públicas, Servicios y Vivienda es una institución pública del estado que maneja alrededor de un mil setecientos millones de dolares anuales de inversión pública, en esta institución se encuentran el viceministerio de vivienda y urbanismo, viceministerio de transporte y viceministerio de telecomunicaciones, así también se encuentran las siguientes entidades importantes bajo tuición.

Actualmente el Ministerio es coordinador del plan de Gobierno electrónico³ y según la ley Nro. 164⁴ y decreto supremo 1793⁵ el ministerio de Obras Públicas, Servicios y Vivienda también es coordinador para el plan de software libre⁶ y firma digital.

1.2.1.1 Misión

Promover y gestionar el acceso universal y equitativo de la población boliviana a obras y servicios de calidad, en telecomunicaciones, transportes y vivienda, en armonía con la naturaleza.

1.2.1.2 Visión

Somos una entidad que con calidad y transparencia, satisface las necesidades de transportes, telecomunicaciones y vivienda de la población boliviana.

3 El nivel central del Estado promueve la incorporación del Gobierno Electrónico a los procedimientos gubernamentales, a la prestación de sus servicios y a la difusión de información, mediante una estrategia enfocada al servicio de la población. (Cap. 2, Artículo 75, ley Nro 164).

4 Ley general de telecomunicaciones, tecnologías de información y comunicación(8 de agosto de 2011)

5 Aprobación reglamento a la ley Nro. 164

6 Los Órganos Ejecutivo, Legislativo, Judicial y Electoral en todos sus niveles, promoverán y priorizarán la utilización del software libre y estándares abiertos, en el marco de la soberanía y seguridad nacional. (Cap. 2, Artículo 77, ley Nro. 164).

1.2.1.3 Principios

Satisfacción compartida de las necesidades humanas que incluye la afectividad y el reconocimiento, en armonía con la naturaleza y en comunidad con los seres humanos.

- **Calidez.-** Trato amable, cortés y respetuoso entre los servidores y servidoras públicos del MOPSV y con la población que usa los servicios de la entidad.
- **Ética.-** Compromiso efectivo del servidor y servidora pública con valores y principios establecidos en la CPE, que lo conducen a un correcto desempeño personal y laboral.
- **Legitimidad.-** Reconocimiento pleno del Soberano a los actos de la administración pública, cuando éstos sean justos y respondan a sus necesidades.
- **Legalidad.-** Actuar en el marco de las disposiciones legales vigentes en el país que responden a la voluntad soberana del pueblo.
- **Igualdad.-** Reconocimiento pleno del derecho de ejercer la función pública, sin ningún tipo de discriminación, otorgando un trato equitativo sin distinción de ninguna naturaleza a toda la población.
- **Descolonización.-** Compromiso para que las políticas públicas estén diseñadas en base a los valores, principios, conocimientos y prácticas del pueblo boliviano; por lo que las acciones de las servidoras y servidores públicos deben estar orientadas a preservar, desarrollar, proteger y difundir la diversidad cultural con diálogo intracultural, intercultural y plurilingüe.

1.2.1.4 Objetivos

Objetivo estratégico institucional

Contar con una Institución Moderna, Sólida y Transparente, que apoye eficazmente al logro de los objetivos y resultados.

Objetivo estratégico telecomunicaciones

Promover el acceso universal de la población boliviana a los servicios de Telecomunicaciones, Tecnologías de la Información y Comunicación en condiciones de calidad y asequibilidad

Objetivo estratégico transporte

Vertebrar internamente e integrar externamente el país, a través de un sistema multimodal que promueva y garantice los servicios de transporte con accesibilidad universal, contribuyendo al desarrollo socio económico del país

Objetivo estratégico vivienda

Contribuir a la reducción progresiva del déficit habitacional a través de políticas, normas, programas y proyectos integrales basados en la participación, auto gestión, concurrencia, ayuda mutua, responsabilidad compartida y solidaridad social.

1.2.1.5 Fortalecimiento

Fortalecer la gestión de la Administración Central, para el cumplimiento de los objetivos del MOPSV, de manera eficaz y transparente en la planificación, ejecución, control y evaluación de los planes, programas, proyectos a cargo de los Viceministerios.

1.2.1.6 Sistemas en producción del ministerio

El Ministerio de Obras Públicas, Servicios y Vivienda hasta la fecha tiene desarrollado mas de 30 sistemas en producción para diferentes actividades que se llevan a cabo dentro del Ministerio. Los sistemas mas importantes son:

- Sistema de correspondencia
- Sistema de POA
- Sistema de pasajes y viáticos
- Sistema de RRHH

1.2.1.7 Organigrama

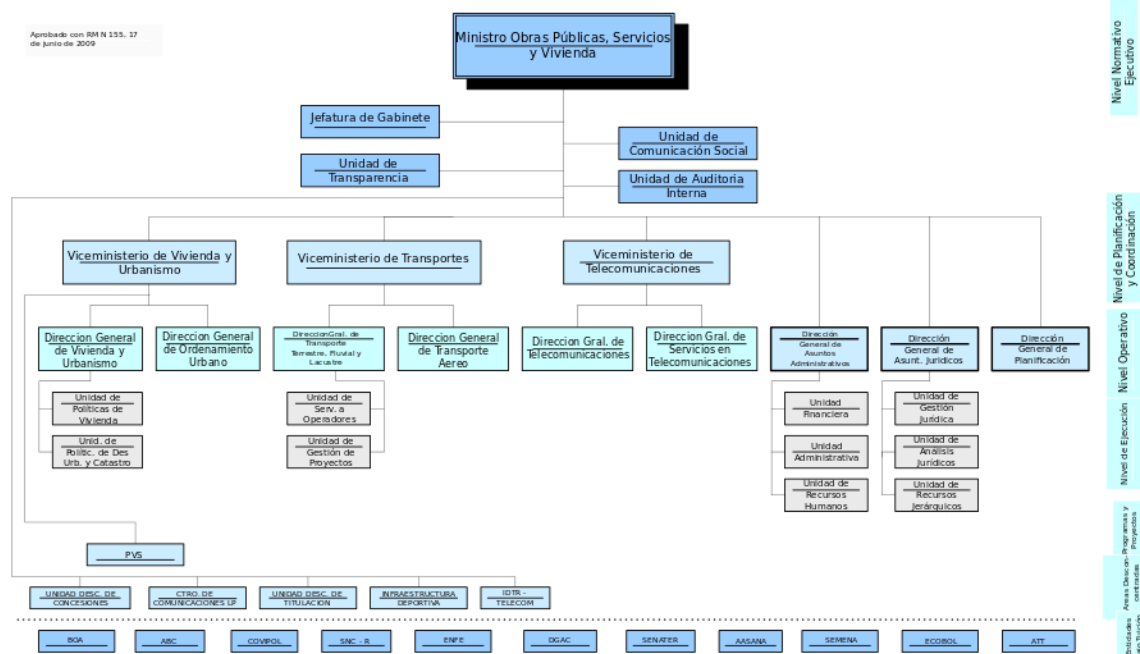


Figura 1.1 Organigrama M.O.P.S.V.

Fuente: Elaboración propia

1.2.2 Antecedentes de proyectos similares

Varias instituciones gubernamentales internacionales hacen uso de las nuevas tecnologías de información para agilizar procesos y abaratar costos, por esta razón, tanto instituciones como empresas han empezado a crear normas y métodos para adoptar nuevas alternativas a la firma manuscrita, siendo una alternativa eficiente y segura la firma digital.

El Ministerio no es la excepción, por esta razón quiere adoptar la firma digital para sus diferentes sistemas en producción para desburocratizar y agilizar el acceso a tramites, ya sea para servidores públicos o personas que se relacionan con el Ministerio. Algunos de proyectos similares encontrados son los siguientes:

- PDFCreator, pdfforge, 2012, es una herramienta desarrollada en lenguaje visual basic que permite crear archivos PDF a partir de otros tipos de documentos, impresiones de aplicaciones, imágenes, paginas webs. Tiene una sección donde se

puede la clave privada de tu firma digital y configurar ciertos parámetros de la firma.

- DigiSigner, DigiSigner Software, 2013, es una herramienta para visualizar y firma digital de documentos PDF, soporta y gestiona los certificados X.509⁷, esta desarrollada en tecnología java.
- Sinadura, Sinadura, 2008, es una aplicación de escritorio multiplataforma líder en su mercado para la firma digital de cualquier tipo de archivo. El software garantiza la integridad, identidad y el no repudio en cualquier archivo, como pueden ser nóminas, contratos, facturas o certificaciones en archivos de texto, canciones en archivos de sonido o archivos de vídeo.
- JsignPdf, Josef Cacek, 2012, es una aplicación Java que añade firmas digitales a documentos PDF. Se puede utilizar como una aplicación independiente o como un add-on en OpenOffice. La aplicación utiliza la biblioteca-JSignPdf itxt para manipulaciones PDF, es un software de código abierto y se puede utilizar libremente en los sectores privado y de negocios.
- XolidoSign, Xolido, 2010, es software propietario que tiene una interfaz bien amigable para nuevos usuarios, permite firmar archivos de cualquier tipo, considerado uno de los programas mas completos en cuanto al formato de la firma digital.

En la siguiente tabla se muestran las ventajas y desventajas de los proyectos.

PROYECTOS SIMILARES	VENTAJAS	DESVENTAJAS
PDFCreator	<ul style="list-style-type: none"> • Permite el sellado de tiempo. • Permite la marca de agua en documentos PDF. • Visor de documentos PDF. 	<ul style="list-style-type: none"> • No es una herramienta multiplataforma. • No permite firmar documentos por lotes.
DigiSigner	<ul style="list-style-type: none"> • Multiplataforma. 	<ul style="list-style-type: none"> • Es de licencia propietaria.

7 **X.509:** Estándar UIT-T para infraestructuras de claves públicas.

	<ul style="list-style-type: none"> • Visor de documentos PDF. • Permite la marca de agua en documentos PDF. • Permite el sellado de tiempo. • Permite firmar documentos por lotes. 	<ul style="list-style-type: none"> • No permite poner la marca de agua en diferente posición • No permite multifirma • La herramienta es de pago.
Sinadura	<ul style="list-style-type: none"> • Multiplataforma. • Firmado de documentos por lotes. • Permite el sellado de tiempo. • Permite ver estado de certificados. 	<ul style="list-style-type: none"> • No permite colocar marca de agua en documentos. • No permite multifirma.
JSigndf	<ul style="list-style-type: none"> • Permite la marca de agua en los documentos firmados. • Permite el almacenamiento de claves. • Permite el sellado de tiempo. • Permite la validación de certificados. • Multiplataforma. • Plugin para OpenOffice. 	<ul style="list-style-type: none"> • No permite la verificación de la firma digital. • La herramienta es de pago.
XolidoSign	<ul style="list-style-type: none"> • Permite varios formatos de estándares de criptografía de clave publica. • Permite la verificación de los documentos firmados. • Permite el sellado de tiempo. 	<ul style="list-style-type: none"> • Es de licencia propietaria.

Tabla 1.1 Proyectos similares

Fuente: Elaboración propia

1.3 PLANTEAMIENTO DEL PROBLEMA

1.3.1 Problema central

La firma manuscrita es utilizada para relacionar un documento con una persona en particular de manera legal, siendo la forma mas difundida en la vida cotidiana. Sin embargo, este método puede causar demoras y deficiencias con los diferentes procedimientos que requieren la firma manuscrita ya que es un requisito la presencia física de la persona para realizar dicha actividad. En caso que una parte interesada se encuentre en

un lugar distante y tenga que hacer el envío del documento físico o tenga que desplazarse hasta un punto de encuentro, ocasiona perdida de tiempo y de un presupuesto económico. Otro problema es la desconfianza de la firma manuscrita, debido a que una persona carece de los conocimientos grafotécnicos⁸ para identificar la veracidad de una firma manuscrita en un documento en particular, incluso esto puede sucederle al titular de la firma que no advierte sus propias particularidades en su firma.

El Ministerio de Obras Públicas, Servicios y Vivienda no es la excepción, maneja mucha información tanto física como digital e interactúa con muchas personas, empresas y/o jurídicas y maneja un presupuesto considerable, lo cual conlleva una gran responsabilidad para con sus usuarios.

Actualmente, el Ministerio de Obras Públicas, Servicios y Vivienda cuenta con más de 400 usuarios donde el mayor flujo de trabajo es el procedimiento manuscrito como ser: hojas de ruta, inventarios y otros trámites que burocratizan y retardan el trabajo institucional, ocasionando pérdidas de tiempo y dinero.

Según datos de la gestión 2014 el Ministerio de Obras Públicas Servicios y Vivienda elaboró solo más de 46.000 hojas de ruta y hasta la fecha ha generado más de 133.000 hojas de ruta, esta cantidad de trámites es considerable y altamente peligroso por lo cual la firma manuscrita se está convirtiendo en un problema de control. A causa de estos problemas surge la siguiente interrogante:

¿De qué manera se puede agilizar, transparentar y simplificar los procedimientos administrativos de la gestión pública del Ministerio de Obras Públicas, Servicios y Vivienda?

1.3.2 Problemas secundarios

Partiendo del problema principal surgen los siguientes problemas secundarios:

⁸ **Grafotécnica:** disciplina de las ciencias periciales o forenses, que tiene como finalidad el estudio y análisis de documentos desde el punto de vista material para determinar autoría del contenido de documentos, como también determinar la naturaleza o constitución del material utilizado para su confección.

- Hay incremento de la documentación física, debido a que todos los informes, notas internas, circulares y otros documentos de apoyo necesitan la firma manuscrita del servidor público, dificultando el acceso a la documentación física de forma precisa y oportuna.
- Varios documentos necesitan ser firmados por diferentes personas, es decir, que en un documento se pueden necesitar la firma manuscrita de varias personas. Esto se dificulta si uno de los servidores públicos esta ausente, dando lugar a retrasos a la hora de aprobación de documentos.
- La firma manuscrita es propensa a sufrir alteraciones y/o suplantaciones, causando desconfianza de un documento físico.
- El envío de documentación física es morosa y propensa a perdida en el transcurso del envío, ocasionando retrasos y perdidas económicas, tanto a la institución como al servidor público.
- Los servidores públicos se encuentran en procesos burocráticos largos y morosos, ocasionando disgusto y un bajo desempeño a la hora de realizar sus actividades.

1.4 DEFINICIÓN DE OBJETIVOS

1.4.1 Objetivo general

Desarrollar e implementar un sistema de firma digital para el Ministerio de Obras Públicas, Servicios y Vivienda que permita agilizar, transparentar y simplificar las procedimientos administrativos de la gestión pública.

1.4.2 Objetivos específicos

- Diseñar el modelo uso de la firma digital para documentos en formato PDF realizados por los servidores públicos o generados por los diferentes sistemas con los que cuenta el Ministerio.
- Incorporar varias firmas digitales dentro de un documento en formato PDF. Esto

permitirá que varias personas puedan firmar un documento en la que es necesaria su firma.

- Mostrar la información de una persona, como ser nombre completo, carnet de identidad y cargo institucional en una marca de agua dentro de un documento en formato PDF firmado.
- Incluir un sello de tiempo que consistirá un mecanismo de consulta que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante en específico en el tiempo. Esto permitirá mantener la validez de documentos en formato PDF que necesiten ser firmados.
- Comprobar y autenticar firmas digitales de los servidores públicos en documentos en formato PDF dentro de los sistemas en producción del Ministerio que requieran interactuar con la firma digital.
- Verificar y validar el estado de un certificado proporcionado por la entidad certificadora para verificar si dicho certificado se encuentra aun vigente o fue vulnerado.

1.5 JUSTIFICACIÓN

1.5.1 Justificación económica

Los tramites y actividades que realiza el Ministerio son registrados en documentos como hojas de ruta, resoluciones, informes, ordenes administrativas, circulares y demás documentos de apoyo. Un alto porcentaje de estos documentos tienen como soporte físico el papel desde su creación o recibo, sin olvidar que generalmente se exigen copias adicionales de los mismos para distribuirlos entre las dependencias que así lo requieran.

Cuando un documento se alista para su versión final, es frecuente que se impriman hasta dos y tres borradores para su revisión. En la mayoría de estos casos solo se utiliza una cara de la hoja, este mismo hecho conlleva a que la institución tenga que adquirir inmuebles, materiales de impresión y ampliar el espacio para el almacenamiento de documentación

física, lo que ocasiona una gran cantidad de gastos asociados a la administración del papel dentro del Ministerio.

El flujo efectivo de la información en la institución se reduce al manejo del papel, los problemas y pérdidas económicas surgen cuando la información debe llegar a los usuarios y no llega o sencillamente tarda debido a las distancias que este debe recorrer o a incidentes que este pueda tener en el transcurso de su transporte.

La firma digital incrementa la productividad porque ayuda a centralizar la información y a utilizar documentos electrónicos que hacen fluir la información rápidamente. Incrementa la eficiencia de los procesos de trabajo, lo cual permite ahorrar tiempo y medir la productividad, además se reducen los costos adicionales asociados al transporte de la documentación física, al uso de papel y a los materiales de impresión.

1.5.2 Justificación social

Para las diferentes actividades como ser tramites, seguimiento de hojas de ruta, entrega de informes y otros, realizadas en el Ministerio se requiere la presencia física de la persona interesada para realizar el seguimiento, entrega o recepción de las mismas lo cual conlleva a pérdida de tiempo en casos que el servidor público encargado no se encuentre presente, que la cantidad de servidores públicos que necesiten ser atendidos sea alta y se tenga que proceder a hacer fila o la distancia que tenga que recorrer el servidor publico sea larga. Debido a estas situaciones se genera malestar tanto en los servidores públicos como en los usuarios externos que tengan que interactuar con los sistemas en producción del Ministerio.

El uso de la firma digital facilitara:

- El acceso a la información de los sistemas que brinda el Ministerio serán más rápidos, de esta forma se vera la satisfacción por parte de los servidores públicos.
- Se mejorara la calidad y rapidez de los sistemas del Ministerio al reducir los tiempos de respuesta ya que no se necesitara hacer el envío de documentación física.

- Los tiempos de espera y atención se irán decrementando gracias a que la documentación sera digital.
- Se evitara el traslado a los puntos de atención presencial, permitiendo ahorrar tiempo en tramites.

Todo esto mejorara la relación entre los sistemas en producción del Ministerio y servidores públicos.

1.5.3 Justificación técnica o tecnológica

El estándar usado para el certificado otorgado por una empresa o institución certificadora sera la RFC 5280⁹, usando la ISO ITU X.509¹⁰ v2, tanto para el formato, codificación contenidos e interpretación. De esta forma, los certificados pueden ser leídos o escritos por cualquier aplicación que cumpla con el mencionado estándar.

Por otra parte la firma digital consta de un par de claves criptográficas¹¹, una publica y una privada, creadas con el algoritmo matemático RSA¹². Todos estos estándares y especificaciones técnicas se mencionan en la resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015 de Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transporte.

1.6 ALCANCES Y LIMITES

1.6.1 Alcances

Para cumplir con los requerimientos y propósitos del Ministerio, el sistema de firmas digitales para el ministerio, desde su análisis, diseño, desarrollo e implementación se realizaran los siguientes módulos:

- Módulo para visualizar un documento en formato PDF.

9 **RFC 5280:** Estándar para la infraestructura X.509 clave publica para su uso en Internet.

10 **X.509:** Estándar para infraestructura de claves publicas, especifica, entre otras cosas, formatos para certificados de claves publicas y un algoritmo de validación de la ruta de certificación.

11 **Criptografía:** Estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican.

12 **RSA:** Algoritmo asimétrico, asimétrico significa que hay dos claves diferentes utilizados para cifrar y descifrar mensajes.

- Módulo que permita usar la firma digital de un servidor público almacenada en un token para firmar documentos en formato PDF.
- Módulo que permita firmar documentos en formato PDF.
- Módulo de validación y verificación de firmas digitales en documentos con formato PDF.
- Módulo de validación y comprobación de estado del certificado otorgado por la entidad certificadora para tener una constancia del estado del certificado.
- Módulo para incluir la marca de agua con la información del servidor publico.
- Módulo para incluir sello de tiempo de la entidad certificadora para los documentos firmados en formato PDF.
- Módulo para el almacenamiento del historial de firmas realizadas por los servidores públicos.
- Módulo para almacenamiento de documentos firmados realizadas por los signatarios y generación QR con URL de acceso al documento pdf firmado.

1.6.2 Limites

Los limites de la implementación del modelo aplicable de firmas digitales son los siguientes:

- No se puede asegurar la seguridad de mantener bajo su exclusivo control los datos de creación de la firma digital por parte de los funcionarios públicos.
- El uso inadecuado por parte de los servidores públicos de las firmas digitales pueden causar problemas y costos a la institución.
- No se puede garantizar que las firmas digitales sean concebidas para perdurar en el tiempo, ya que el software puede quedar obsoleto en el tiempo, debido a fallas u otros problemas relacionados con la evolución tecnológica.

- Por los estándares que se usaran en Bolivia el sistema de firma digital no puede ser desarrollada en un entorno cliente servidor.
- El modelo de uso de firma digital sera utilizada unidamente en Ministerio de Obras Públicas, Servicios y Vivienda, su publicación a otras instancias deberá ser aprobada por la máxima autoridad ejecutiva.
- El sistema de firma digital no puede ser certificada por una institución certificadora nacional debido a que aun no se encuentra en funcionamiento.

1.7 APORTES

1.7.1 Aporte práctico

La implementación del modelo aplicable de la firma digital para el Ministerio ofrecerá los siguientes aportes:

- Las transacciones con los diferentes sistemas con los que cuenta el Ministerio serán mas eficientes y ágiles, brindando una mayor seguridad en la validez de los documentos emitidos.
- La presencia fisica del servidor publico no sera necesaria para firmar un documento ya que podrá realizarse desde cualquier lugar.
- Se reducirá considerablemente el sudo del papel ahorrando dinero al Ministerio; así mismo esto colaborará con el medio ambiente (Madre Tierra).
- Se tendrá mas seguridad de los documentos firmados por algún funcionario publico, ya que la firma digital es considerada mas segura que una firma manuscrita.
- Varios de los sistemas con los que cuenta el Ministerio se convertirán en servicios totalmente a distancia, aportando a un Ministerio hacia el gobierno electrónico.
- La integridad de los documentos firmados no sera vulnerada gracias a la detección de cambios realizados en dicho documento.
- El modelo de firma digital sera el primero en realizarse a nivel institucional

logrando una replica en otras instituciones.

1.7.2 Aporte teórico

El sistema de firma digital es desarrollado con la metodología ágil eXtreme Programming (XP), es el más destacado de los procesos ágiles de desarrollo de software, se diferencia de las metodologías tradicionales principalmente en que pone más énfasis en la adaptabilidad que en la previsibilidad. La programación extrema adopta las mejores metodologías de desarrollo de acuerdo a lo que se pretende llevar a cabo con el proyecto, y aplicarlo de manera dinámica durante el ciclo de vida del software. En la XP se consideran que los cambios de requisitos sobre la marcha son un aspecto natural, inevitable e incluso deseable del desarrollo de proyectos. Creen que ser capaz de adaptarse a los cambios de requisitos en cualquier punto de la vida del proyecto es una aproximación mejor y más realista que intentar definir todos los requisitos al comienzo del proyecto e invertir esfuerzos después en controlar los cambios en los requisitos.

1.8 METODOLOGÍA

1.8.1 Metodología de investigación

La metodología que se emplea para este proyecto de grado es el método científico, con el tipo descriptivo que se utiliza para recoger, organizar, resumir, presentar, analizar y generalizar los resultados de las observaciones. Este método implica la recopilación y presentación sistemática de datos para dar una idea clara de una determinada situación. Esta metodología es fácil, de corto tiempo y económica. El método empleado para hacer el desarrollo del sistema de firma digital será el método ágil XP.