ÍNDICE

[1 INTRODUCCIÓN 1](#__RefHeading___Toc22746_2089674402)

[2 ANTECEDENTES 1](#__RefHeading___Toc22748_2089674402)

[2.1 ANTECEDENTES INSTITUCIONALES 1](#__RefHeading___Toc22750_2089674402)

[2.1.1 MISIÓN 1](#__RefHeading___Toc22752_2089674402)

[2.1.2 VISIÓN 1](#__RefHeading___Toc22754_2089674402)

[2.1.3 PRINCIPIOS 2](#__RefHeading___Toc22756_2089674402)

[2.1.4 OBJETIVOS 2](#__RefHeading___Toc22758_2089674402)

[2.1.4.1 OBJETIVO ESTRATÉGICO INSTITUCIONAL 2](#__RefHeading___Toc22760_2089674402)

[2.1.4.2 OBJETIVO ESTRATÉGICO TELECOMUNICACIONES 3](#__RefHeading___Toc22762_2089674402)

[2.1.4.3 OBJETIVO ESTRATÉGICO TRANSPORTE 3](#__RefHeading___Toc22764_2089674402)

[2.1.4.4 OBJETIVO ESTRATÉGICO VIVIENDA 3](#__RefHeading___Toc22766_2089674402)

[2.1.5 FORTALECIMIENTO 3](#__RefHeading___Toc22768_2089674402)

[2.1.6 SISTEMAS EN PRODUCCIÓN DEL MINISTERIO 3](#__RefHeading___Toc23572_2089674402)

[2.1.7 ORGANIGRAMA 4](#__RefHeading___Toc22770_2089674402)

[2.2 ANTECEDENTES DE PROYECTOS SIMILARES 4](#__RefHeading___Toc22772_2089674402)

[3 PLANTEAMIENTO DEL PROBLEMA 6](#__RefHeading___Toc22774_2089674402)

[3.1 PROBLEMA CENTRAL 6](#__RefHeading___Toc22776_2089674402)

[3.2 PROBLEMAS SECUNDARIOS 8](#__RefHeading___Toc22778_2089674402)

[4 DEFINICIÓN DE OBJETIVOS 8](#__RefHeading___Toc22780_2089674402)

[4.1 OBJETIVO GENERAL 8](#__RefHeading___Toc22782_2089674402)

[4.2 OBJETIVOS ESPECÍFICOS 8](#__RefHeading___Toc22784_2089674402)

[5 JUSTIFICACIÓN 9](#__RefHeading___Toc22786_2089674402)

[5.1 JUSTIFICACIÓN ECONÓMICA 9](#__RefHeading___Toc22788_2089674402)

[5.2 JUSTIFICACIÓN SOCIAL 10](#__RefHeading___Toc22790_2089674402)

[5.3 JUSTIFICACIÓN TÉCNICA O TECNOLÓGICA 11](#__RefHeading___Toc22792_2089674402)

[6 ALCANCES Y LIMITES 12](#__RefHeading___Toc22794_2089674402)

[6.1 ALCANCES 12](#__RefHeading___Toc22796_2089674402)

[6.2 LIMITES 13](#__RefHeading___Toc22798_2089674402)

[7 APORTES 13](#__RefHeading___Toc22800_2089674402)

[7.1 APORTE PRÁCTICO 13](#__RefHeading___Toc22802_2089674402)

[7.2 APORTE TEÓRICO 14](#__RefHeading___Toc22804_2089674402)

[8 METODOLOGÍA 15](#__RefHeading___Toc22806_2089674402)

[8.1 METODOLOGÍA DE INVESTIGACIÓN 15](#__RefHeading___Toc22808_2089674402)

[8.1.1 HERRAMIENTA DE DESARROLLO 15](#__RefHeading___Toc22810_2089674402)

[9 MARCO TEÓRICO 15](#__RefHeading___Toc22812_2089674402)

[9.1 CRIPTOGRAFÍA 15](#__RefHeading___Toc22814_2089674402)

[9.1.1 TIPOS DE CRIPTOGRAFÍA 16](#__RefHeading___Toc22816_2089674402)

[9.1.2 CRIPTOGRAFÍA SIMÉTRICA 17](#__RefHeading___Toc22818_2089674402)

[9.1.3 CRIPTOGRAFÍA ASIMÉTRICA 17](#__RefHeading___Toc22820_2089674402)

[9.1.4 CRIPTOGRAFÍA HÍBRIDA 18](#__RefHeading___Toc22822_2089674402)

[9.2 CERTIFICADOS 18](#__RefHeading___Toc22824_2089674402)

[9.2.1 CERTIFICADO DIGITAL 18](#__RefHeading___Toc22826_2089674402)

[9.2.2 AUTORIDAD DE CERTIFICACIÓN 18](#__RefHeading___Toc22828_2089674402)

[9.2.2.1 CACERT 19](#__RefHeading___Toc22830_2089674402)

[9.2.3 PROCESO PARA OBTENCIÓN DE DE UN CERTIFICADO DIGITAL 20](#__RefHeading___Toc22832_2089674402)

[9.3 FIRMA DIGITAL 20](#__RefHeading___Toc22834_2089674402)

[9.3.1 INFRAESTRUCTURA DE CLAVE PUBLICA 20](#__RefHeading___Toc22836_2089674402)

[9.3.2 SELLADO DE TIEMPO 20](#__RefHeading___Toc22838_2089674402)

[9.3.3 FUNCIÓN HASH 20](#__RefHeading___Toc22840_2089674402)

[10 INDICE TENTATIVO 21](#__RefHeading___Toc22842_2089674402)

[11 CRONOGRAMA DE AVANCE 24](#__RefHeading___Toc22844_2089674402)

[12 BIBLIOGRAFÍA 25](#__RefHeading___Toc22846_2089674402)

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 electrónico[[1]](#footnote-1), 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 firmas manuscritas y debe cumplir las mismas funciones principales como ser: la autentificación 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. 164[[2]](#footnote-2) vigente desde el año 2011 el cual promueve y otorga validez al uso de firmas digitales, tanto en las entidades públicas 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 más 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. ANTECEDENTES
   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 dólares 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 electrónico[[3]](#footnote-3) y según la ley Nro. 164[[4]](#footnote-4) y decreto supremo 1793[[5]](#footnote-5) el ministerio de Obras Públicas, Servicios y Vivienda también es coordinador para el plan de software libre[[6]](#footnote-6) y firma digital.

* + 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. VISIÓN

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

* + 1. 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.

Ama Qhilla, Ama Llulla, Ama Suwa.- No seas flojo, no seas mentiroso ni seas ladrón.

**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. OBJETIVOS
       1. OBJETIVO ESTRATÉGICO INSTITUCIONAL

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

* + - 1. 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

* + - 1. 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

* + - 1. 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.

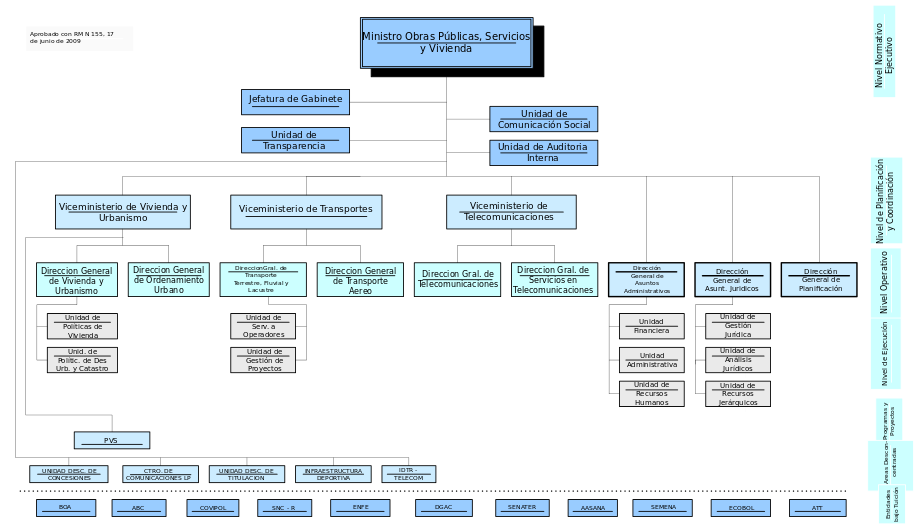
* + 1. FORTALECIMIENTO

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. 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. ORGANIGRAMA
  1. ANTECEDENTES DE PROYECTOS SIMILARES

Ilustración 1: Organigrama MOPSV

Fuente: MOPSV

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.509[[7]](#footnote-7), 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 | * Permite el sellado de tiempo. * Permite la marca de agua en documentos PDF. * Visor de documentos PDF. | * No es una herramienta multiplataforma. * No permite firmar documentos por lotes. |
| DigiSigner | * Multiplataforma. * Visor de documentos PDF. * Permite la marca de agua en documentos PDF. | * Es de licencia propietaria. * No permite poner la marca de agua en diferente posición |
| Sinadura | * Multiplataforma. * Firmado de documentos por lotes. * Permite el sellado de tiempo | * No permite colocar marca de agua en documentos. * No permite multifirma. |
| JSignPdf | * Permite la marca de agua en los documentos firmados. * Permite el almacenamiento de claves. | * No permite la verificación de la firma digital. * La herramienta es de pago. |
| XolidoSign | * Permite varios formatos de estándares de criptografía de clave publica. * Permite la verificación de los documentos firmados. * Permite el sellado de tiempo. | * Es de licencia propietaria. |

Tabla 1: Ventajas y desventajas de programas similares

Fuente: elaboración propia

1. PLANTEAMIENTO DEL PROBLEMA
   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 envió 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 grafotécnicos[[8]](#footnote-8) para identificar la veracidad de un 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 interactua 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 mas 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 elaboro solo más de 46.000 hojas de ruta y hasta la fecha ha generado más de 133.000 hojas de ruta, esta cantidad de tramites 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. PROBLEMAS SECUNDARIOS

Partiendo del problema principal surgen los siguientes problemas secundarios:

* 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 está 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 envió de documentación física es morosa y propensa a perdida en el transcurso del envió, 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. DEFINICIÓN DE OBJETIVOS
   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. 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 firmas 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 autentificar 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.
* Corroborar y validar el estado de un certificado proporcionado por la entidad certificadora para verificar si dicho certificado se encuentra aún vigente o fue vulnerado.

1. JUSTIFICACIÓN
   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 distribuirlas 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 perdidas 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. 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 público 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 verá 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 él envió de documentación física.
* Los tiempos de espera y atención se irán decrementando gracias a que la documentación será digital.
* Se evitara el traslado a los puntos de atención presencial, permitiendo ahorrar tiempo en trámites.

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

* 1. JUSTIFICACIÓN TÉCNICA O TECNOLÓGICA

El estándar usado para el certificado otorgado por una empresa o institución certificadora será la RFC 5280[[9]](#footnote-9), usando la ISO ITU X.509[[10]](#footnote-10) 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 criptográficas[[11]](#footnote-11), una publica y una privada, creadas con el algoritmo matemático RSA[[12]](#footnote-12). 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. ALCANCES Y LIMITES
   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 generar un certificado público y privado, siguiendo los estándares y formatos propuestos por la ATT.
* Módulo para visualizar un documento en formato PDF.
* Módulo que permita usar la firma digital de un servidor público para firmar documentos en formato PDF.
* Módulo que permita firmar documentos en formato PDF por lotes, permitiendo firmar varios varios documentos a la vez.
* 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 público y sello de tiempo para los documentos firmados en formato PDF.
* Módulo para el almacenamiento del historial de firmas realizadas.
* Módulo para la validación de un documento impreso, mediante un código QR que permitirá hacer una consulta de verificación de contenido de un documento impreso y el documento digital firmado.
  1. LIMITES

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

* No se pude 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 será utilizada únicamente 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 aún no se encuentra en funcionamiento.

1. APORTES
   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 más eficientes y ágiles, brindando una mayor seguridad en la validez de los documentos emitidos.
* La presencia física del servidor público no será 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 más seguridad de los documentos firmados por algún funcionario público, ya que la firma digital es considerada más 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 será vulnerada gracias a la detección de cambios realizados en dicho documento.
* El modelo de firma digital será el primero en realizarse a nivel institucional logrando una réplica en otras instituciones.
  1. 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. METODOLOGÍA
   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 par a 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.

* + 1. HERRAMIENTA DE DESARROLLO

Para el desarrollo del sistema se emplea Maven, que es una herramienta de software para la gestión y construcción de proyectos Java, tiene un modelo de configuración de construcción más simple, basado en un formato XML. Maven utiliza un Project Object Model (POM) para describir el proyecto de software a construir, sus dependencias de otros módulos y componentes externos, y el orden de construcción de los elementos. Viene con objetivos predefinidos para realizar ciertas tareas claramente definidas, como la compilación del código y su empaquetado.

También haremos uso de MySQL que es un sistema de gestión de bases de datos relacional, multihilo y multiusuario.

1. MARCO TEÓRICO
   1. CRIPTOGRAFÍA

La criptografía es la creación de técnicas para el cifrado de datos. Teniendo como objetivo conseguir la confidencialidad de los mensajes. Si la criptografía es la creación de mecanismos para cifrar datos, el criptoanálisis son los métodos para “romper” estos mecanismos y obtener la información.

Una vez que nuestros datos han pasado un proceso criptográfico decimos que la información se encuentra cifrada.

La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etc.) y, en segundo lugar, asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito.

La criptografía cuenta con tres usos: Cifrar, autenticar y firmar.

* Cifrar: Como ya hemos dicho, siempre hay cierta información que no queremos que sea conocida más que por las personas que nosotros queramos. En esto nos ayuda el cifrado. Cifrando un mensaje hacemos que este no pueda ser leído por terceras personas consiguiendo así la tan deseada privacidad.
* Autenticación: Otra de las necesidades que surgen con la aparición de Internet es la necesidad de demostrar que somos nosotros y que el emisor es quien dice ser. Un método de autenticación puede ser el propio cifrado. Si ciframos un mensaje con una clave solo conocida por nosotros, demostrando que somos quien decimos ser, el receptor podrá constatar nuestra identidad descifrándolo. Esto se puede conseguir mediante clave simétrica (el receptor tiene que estar en posesión de la clave empleada) o usando clave asimétrica en su modo de autenticación.
* Firmar: Dados los trámites que podemos realizar hoy en día a través de Internet se hace necesaria la aparición de la firma digital. Igual que firmamos un documento, la firma digital nos ofrece la posibilidad de asociar una identidad a un mensaje.
  + 1. TIPOS DE CRIPTOGRAFÍA

Se pueden distinguir tres tipos de criptografía: simétrica, asimétrica e híbrida.

* + 1. CRIPTOGRAFÍA SIMÉTRICA

La criptografía Simétrica es un método criptográfico monoclave, esto quiere decir que se usa la misma clave para cifrar y descifrar. Esto supone un grave problema a la hora de realizar el intercambio entre el emisor y el receptor, dado que si una tercera persona estuviese escuchando el canal podría capturar la clave, siendo inútil el cifrado.

Es importante que la clave sea difícil de adivinar y el método de cifrado empleado sea adecuado. Hoy en día, con la capacidad computacional disponible, si se emplean los algoritmos adecuados, dependiendo del método de cifrado empleado se puede obtener una clave en cuestión de tiempo reducida. Algunos ejemplos de algoritmos simétricos son 3DES, AES, Blowfish e IDEA.

* + 1. CRIPTOGRAFÍA ASIMÉTRICA

La criptografía asimétrica, también conocida como de clave pública es un sistema que emplea una pareja de claves. Esta pareja de claves pertenecen a la misma persona. Una es de dominio público y cualquiera puede tenerla y la otra es privada. El funcionamiento de este sistema es el siguiente: El remitente usa la clave pública del destinatario y sólo con la clave privada se podrá descifrar el mensaje. De esta forma se consigue que sólo el destinatario pueda acceder a la información.

De la misma forma si el propietario usa su clave privada para cifrar un mensaje sólo se podrá descifrar con la clave pública. La mayor ventaja de este sistema es que la distribución de claves es más fácil y segura que usando clave simétrica. Algunos ejemplos de algoritmos asimétricos son: Diffie-Hellman, RSA, DSA, ElGamal, Criptografía de curva elíptica.

El más extendido de los sistemas de clave pública es el RSA, que fue desarrollado por Rivest, Shamir y Adleman, este algoritmo se basa en escoger dos números primos grandes elegidos de forma aleatoria y mantenidos en secreto. La principal ventaja de este algoritmo desde el punto de vista de seguridad radica en la dificultad a la hora de factorizar números grandes. RSA es reversible, es decir, además de permitir cifrar con la clave pública y descifrar con la privada, permite cifrar con la clave privada y descifrar con la clave pública.

En Bolivia se usa este tipo de criptografía, siendo el algoritmo RSA usado preferentemente para la generación de la clave pública como privada. Esto está regulado por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y transporte (ATT).

* + 1. CRIPTOGRAFÍA HÍBRIDA

Este tipo de criptografía utiliza tanto el cifrado simétrico como el asimétrico. Emplea el cifrado de clave pública para compartir una clave para el cifrado simétrico. El mensaje que se envía en el momento, se cifra usando la clave única (cifrado asimétrico) y se envía al destinatario. Tanto PGP como GnuPG usan sistemas de cifrado híbridos.

* 1. CERTIFICADOS
     1. CERTIFICADO DIGITAL

Es un documento electrónico que contiene información de una persona en particular, garantizando la vinculación entre la identidad de la misma con su clave pública, este certificado es emitido por una entidad o empresa denominada Autoridad de certificación. En el caso de Bolivia la entidad certificadora sera la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB).

* + 1. AUTORIDAD DE CERTIFICACIÓN

Una autoridad de certificación (AC o CA por sus siglas en inglés Certification Authority) o entidad de certificación, es una persona jurídica que presta servicios de emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.

Las CAs disponen de sus propios certificados públicos, cuyas claves privadas asociadas son empleadas por las CAs para firmar los certificados que emiten. Un certificado de CA puede estar auto-firmado cuando no hay ninguna CA de rango superior que lo firme. Este es el caso de los certificados de CA raíz (autoridad de certificación raíz), el elemento inicial de cualquier jerarquía de certificación.

Una jerarquía de certificación consiste en una estructura jerárquica de CAs en la que se parte de una CA auto-firmada, y en cada nivel, existe una o más CAs que pueden firmar certificados de entidades finales (personas, aplicación de software, etc) o bien certificados de otras CAs subordinadas, plenamente identificadas y cuya Política de Certificación sea compatible con la CA de rango superior.

En el caso de Bolivia la entidad certificadora raíz es la Autoridad de Regulación y Fiscalización de Transportes y Telecomunicaciones (ATT).

* + - 1. CACERT

CAcert.org es una Autoridad de certificación administrada por la comunidad que otorga gratuitamente certificados de clave pública. Estos certificados pueden ser usados para firmar y cifrar correo electrónico, identificar y autorizar usuarios conectados a sitios web y transmisión segura de datos en Internet. Cualquier aplicación que soporte Secure Socket Layer (SSL) puede usar certificados firmados por CAcert, tal como lo puede hacer cualquier aplicación que use certificados X.509, por ejemplo para cifrar o firmar documentos digitalmente.

El procedimiento de expedición de certificados es muy riguroso en cuanto a la comprobación de documentos de identidad, y exige personación ante más de un agente de verificación de identidad que tiene funciones de Autoridad de Registro.

* + 1. PROCESO PARA OBTENCIÓN DE DE UN CERTIFICADO DIGITAL
  1. FIRMA DIGITAL

Según la ley Nro. 164, la firma digital es la firma electrónica que identifica únicamente a su titular, creada por métodos que se encuentren bajo el absoluto y exclusivo control de su titular, susceptible de verificación y está vinculada a los datos del documento digital de modo tal que cualquier modificación de los mismos ponga en evidencia su alteración.

* + 1. INFRAESTRUCTURA DE CLAVE PUBLICA

Es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución segura de operaciones criptográficas (como el cifrado, la firma digital, el no repudio de transacciones electrónicas).

* + 1. SELLADO DE TIEMPO

El sellado de tiempo es un método para probar que un conjunto de datos existió antes de un momento dado y que ninguno de estos datos ha sido modificado desde entonces. El sellado de tiempo proporciona un valor añadido a la utilización de firma digital ya que ésta por sí sola no proporciona ninguna información acerca del momento de creación de la firma, y en el caso de que el firmante la incluyese, ésta habría sido proporcionada por una de las partes, cuando lo recomendable es que la marca de tiempo sea proporcionada por una tercera parte de confianza.

* + 1. FUNCIÓN HASH

Las funciones criptográficas hash juegan un papel fundamental en la criptografía moderna. Hay muchas funciones hash, comúnmente usadas en aplicaciones no criptográficas. Nosotros nos referiremos siempre a las que admiten el adjetivo de criptográficas, y las llamaremos habitualmente simplemente funciones hash.

Una función hash, o función resumen, toma un mensaje como entrada y produce una salida que llamamos código hash, o resultado hash, o valor hash, o simplemente hash. La idea básica de las funciones criptográficas hash es que los valores hash obtenidos con ellas sirven como una imagen representativa y compactada de una cadena de entrada, y pueden usarse como un posible identificador único de esa cadena de entrada: ese valor hash obtenido del mensaje de entrada suele llamarse resumen del mensaje o huella digital del mensaje.

Las funciones hash se emplean en criptografía junto con los criptosistemas de firma digital para otorgar integridad a los datos. A la hora de firmar digitalmente un documento o mensaje, es práctica habitual hacer la firma sobre la huella digital del mensaje y no sobre la totalidad del mensaje a firmar.

1. INDICE TENTATIVO

CAPÍTULO I MARCO INTRODUCTORIO

* 1. INTRODUCCIÓN
  2. ANTECEDENTES
     1. ANTECEDENTES INSTITUCIONALES
     2. ANTECEDENTES DE PROYECTOS SIMILARES
  3. PLANTEAMIENTO DEL PROBLEMA
     1. PROBLEMA CENTRAL
     2. PROBLEMAS SECUNDARIOS
  4. DEFINICIÓN DE OBJETIVOS
     1. OBJETIVO GENERAL
     2. OBJETIVOS ESPECÍFICOS
  5. JUSTIFICACIÓN
     1. JUSTIFICACIÓN ECONÓMICA
     2. JUSTIFICACIÓN SOCIAL
     3. JUSTIFICACIÓN TECNOLÓGICA
  6. ALCANCES Y LÍMITES
     1. LÍMITES
     2. ALCANCES
  7. APORTES
     1. APORTE TEÓRICO
     2. APORTE PRÁCTICO

CAPÍTULO II MARCO TEÓRICO

* 1. CRIPTOGRAFÍA
     1. TIPOS DE CRIPTOGRAFÍA
  2. CERTIFICADOS
     1. CERTIFICADO DIGITAL
     2. AUTORIDAD CERTIFICADORA
        1. CACERT
     3. PROCESO DE OBTENCIÓN DE CERTIFICADO
  3. FIRMA DIGITAL
     1. TIPOS DE FIRMA DIGITAL
     2. FORMATOS DE FIRMA DIGITAL
  4. SELLADO DE TIEMPO
  5. FUNCION HASH
  6. CÓDIGOS DE BARRA USADOS: CÓDIGO QR
  7. INGENIERÍA DE SOFTWARE
  8. METODOLOGÍAS DE DESARROLLO DE SOFTWARE
  9. METODOLOGÍA ÁGIL PROGRAMACIÓN EXTREMA (XP)
     1. TEORÍA DE XP
     2. ELEMENTOS DE XP
     3. FASES DE XP
  10. HERRAMIENTAS DE DESARROLLO
      1. MAVEN
      2. GESTOR DE BASE DE DATOS MYSQL

CAPÍTULO III MARCO APLICATIVO

* 1. INTRODUCCIÓN
  2. IDENTIFICACIÓN DE ROLES Y TAREAS
  3. DESCRIPCIÓN DE LOS ESCENARIOS
  4. MODELO DE CASOS DE USO
  5. FASE I: EXPLORACIÓN
     1. HISTORIAS DE USUARIO
     2. DETALLE DE LAS HISTORIAS DE USUARIO
     3. PLATAFORMA DE DESARROLLO
  6. FASE II: PLANIFICACIÓN DE LA ENTREGA
     1. ESTIMACIÓN DE ESFUERZO
     2. PLANIFICACIÓN
  7. FASE III: ITERACIONES
     1. PRIMERA ITERACIÓN
     2. SEGUNDA ITERACIÓN
     3. TERCERA ITERACIÓN
     4. CUARTA ITERACIÓN
     5. POLÍTICAS DE SEGURIDAD
     6. POLÍTICAS DE MANTENIMIENTO
        1. PLAN DE CAPACITACIÓN
        2. MANTENIMIENTO PREVENTIVO
        3. MANTENIMIENTO CORRECTIVO
     7. DIAGRAMA DE CLASES
     8. ARQUITECTURA DEL SISTEMA

CAPITULO IV EVALUACIÓN DE FIRMA DIGITAL

* 1. FUNCIONALIDAD
  2. CONFIABILIDAD
  3. CERTIFICACIÓN

CAPITULO V ANÁLISIS COSTO BENEFICIO

* 1. COCOMO
     1. COSTO DE LA ELABORACIÓN DEL PROYECTO
     2. COSTOS DEL SOFTWARE DESARROLLADO
     3. COSTOS DE LA IMPLEMENTACIÓN DEL SISTEMA

CAPITULO VI CONCLUSIONES Y RECOMENDACIONES

* 1. CONCLUSIONES
  2. RECOMENDACIONES

BIBLIOGRAFÍA

ANEXOS

1. CRONOGRAMA DE AVANCE

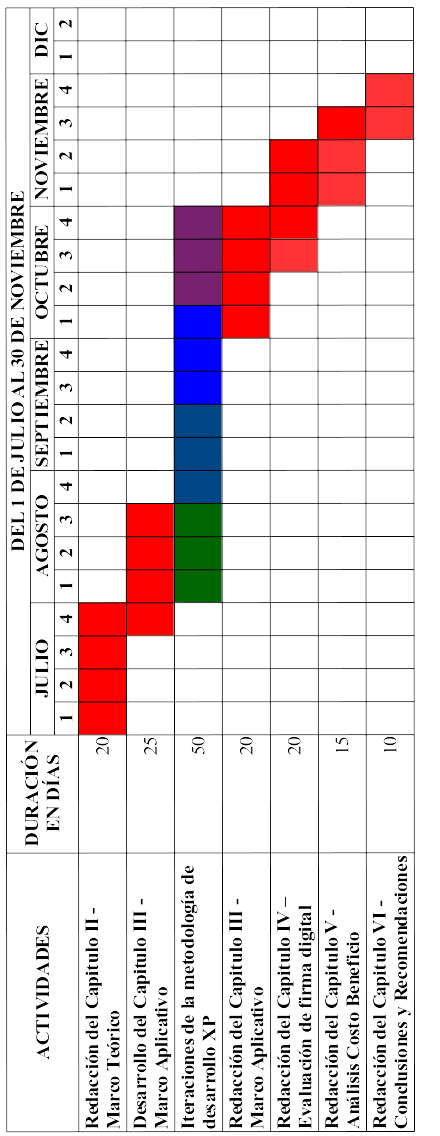
**

Ilustración 3 Cronograma de avance  
Fuente Elaboración propia

1. BIBLIOGRAFÍA

**REFERENCIAS BIBLIOGRÁFICAS**

1. BOLIVIA. Ministerio de Obras Públicas, Servicios y Vivienda. 2012. Ley 164: Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, agosto 2012. 15 p.
2. VIEGA, R. M. J. y RODRIGUEZ, A. B. 2005. Documento electrónico. En: Documento electrónico y firma digital. Uruguay, pp. 26-41.
3. VIEGA, R. M. J. y RODRIGUEZ, A. B. 2005. Firma electrónica y digital. En: Documento electrónico y firma digital. Uruguay, pp. 83-94.
4. CARVAJAL, A. 2007. PKI\* y firmas digitales: aplicaciones reales. Inventum. 3:13-26.
5. GARCIA R., W. A. 2008. Implementación de firma digital en una plataforma de comercio electrónico. Ingeniero informático. Perú, Universidad Católica del Perú, Facultad de Ciencias e Ingeniería. 102 p.
6. ATT. 2015. Resolución Administrativa Regulatoria ATT-DJ-RA TL LP 32/2015 En: REUNION Estandares Técnicos y Otros Lineamientos Establecidos para el Funcionamiento de la Entidades Certificadoras y sus diez Anexos. La Paz, Bolivia, ATT. pp. 34 p.

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. [↑](#footnote-ref-1)
2. Ley general de telecomunicaciones, Tecnologías de Información y Comunicación. [↑](#footnote-ref-2)
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, Articulo 75, ley Nro 164). [↑](#footnote-ref-3)
4. Ley general de telecomunicaciones, tecnologías de información y comunicación(8 de agosto de 2011) [↑](#footnote-ref-4)
5. Aprobación reglamento a la ley Nro. 164 [↑](#footnote-ref-5)
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, Articulo 77, ley Nro. 164). [↑](#footnote-ref-6)
7. **X.509:** Estándar UIT-T para infraestructuras de claves públicas. [↑](#footnote-ref-7)
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. [↑](#footnote-ref-8)
9. **RFC 5280:** Estándar para la infraestructura X.509 clave pública para su uso en Internet. [↑](#footnote-ref-9)
10. **X.509:** Estándar para infraestructura de claves públicas, especifica, entre otras cosas, formatos para certificados de claves públicas y un algoritmo de validación de la ruta de certificación. [↑](#footnote-ref-10)
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. [↑](#footnote-ref-11)
12. **RSA:** Algoritmo asimétrico, asimétrico significa que hay dos claves diferentes utilizados para cifrar y descifrar mensajes. [↑](#footnote-ref-12)