UNIVERSIDAD MAYOR DE SAN ANDRES
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMATICA

TESIS DE GRADO

SEGURIDAD DE FIRMA Y CONTRATOS DIGITALES EN BOLIVIA

PARA OPTAR AL TITULO DE LICENCIATURA EN INFORMATICA

MENCION: INGENIERIA DE SISTEMAS INFORMATICOS

TESISTA: Univ. ERICK FELIPE TABOADA ZAMBRANA.

TUTOR: Lic. MARIO LOAYZA MOLINA.

REVISOR: Lic. GROVER ALEX RODRIGUEZ RAMIREZ

ASESOR : Dr. VICTOR UZEDA CHAVARRIA

LA PAZ – BOLIVIA

2009

DEDICATORIA

Quiero dedicar mi trabajo a Dios, por haberme acogido como un hijo, sabiendo El de lo que necesitaba en todo tiempo, en todo lugar, y que en el plan divino de su creación, sabía que el esfuerzo y la entrega darían su fruto. Además deseo dedicarlo a mi padre a quien estoy seguro le hubiera gustado ver el logro de su hijo. A mi madre por la ayuda brindada en todo este tiempo. Finalmente a mi familia que soportaron la carga que conllevó el esfuerzo a través de los años de estudio y culminación en el presente trabajo de investigación, el cual tomo una gran cantidad de esfuerzo y tiempo pero al final se desenvolvió como una obra maestra.

AGRADECIMIENTOS

En primer lugar y como debe ser a Dios, por darme la fuerza y la entrega, y porque el es siempre tan bueno.

A mi familia, a mi madre, por luchar por mi hermano y por mi y sacarnos adelante sin dejarse vencer por las circunstancias, a mi hermano por darme la mano desinteresadamente cuando así lo necesite, a José María Ortiz, María José Ortiz.

Al Lic. Mario Loayza Molina, por su guía en cuanto a presentar un trabajo impecable. Lic. Alex G. Rodríguez por darle una estructura y sentido claro al trabajo de investigación. A ambos por mostrar una calidez como personas, profesionales y amigos.

Al Dr. Victor Uzeda Chavarria, por aceptar el desafío de guiar una tesis desde el punto de vista técnico, y llevarla a una conclusión legal.

A Geila Uzeda por haberme impulsado a seguir adelante en todos los aspectos, tanto del trabajo de investigación, como en las demás áreas.

A mi persona por haber aprendido a sobrellevar las adversidades con un criterio independiente y no rendirse aun cuando la vida te lo implora. Por poner la mirada en el objetivo y alcanzarlo.

RESUMEN

La economía de los países desarrollados se mantiene gracias a la innovación de sus empresarios a través de mecanismos de la época, al principio fueron las herramientas manuales de trabajo, después las grandes maquinas operadas por el ser humano, en nuestros días la tecnología a través de computadoras donde el trabajo es reducido al control.

En un mundo donde la tecnología ha tenido un crecimiento exponencial, es de vital importancia hacer de la tecnología una herramienta útil para el individuo, lo que nos lleva a que debe haber control social sobre ella.

La globalización fue posible gracias a la comunicación sin fronteras entre ciudadanos de todas partes del mundo haciendo del Internet el nuevo mercado mundial. La rapidez del crecimiento dejo un vacío en muchas áreas que todavía intentan acomodarse a la nueva forma de hacer negocios, como el derecho. La regulación legal de transacciones, intercambio de servicios a través de la Web en Bolivia es nula, ahí es donde nace el tema de CONTRATOS ELECTRONICOS SEGUROS. Según sondeos realizados en la facultad de derecho, el profesional en derecho es escéptico de los procesos informáticos y de su seguridad ya que hasta ahora se prefiere todavía en el campo legal la firma manuscrita y el papel sellado. Para el universo de profesionales del ámbito legal es difícil de creer en la seguridad de la firma digital y sus procesos es por eso que en el trabajo de investigación se propone probar la seguridad de los contratos digitales autenticados bajo una firma digital de clave publica y clave privada, además de proponer un modelo de aplicación de contratos electrónicos con su respectiva propuesta de ley. Tocando aspectos técnicos y sociales de interés para la población en general

La informática y el derecho, la tecnología y el control legal de ella tiene que tornarse en un pilar fundamental para el desarrollo de Bolivia, tanto en lo económico como en lo social. El desarrollo de la investigación en un ámbito netamente técnico y la guía del Dr. Uzeda le dan a la tesis una visión completa de lo que debe aplicarse en cuanto al derecho informático en Bolivia.

ABSTRACT

The economy of developed countries thanks to the innovation of entrepreneurs through mechanisms of the time, at the begining were the tools of manual labor, then the big machines operated by humans, today the technology through computers where the work is reduced to the control.

In a world where technology has grown exponentially, it is vital to make technology a useful tool for people, which leads us to the need for social control over it.

Globalization was made possible by the communication lines between people from all over the world making the Internet the new global market. The quick growth left a vacuum in many areas still trying to accommodate the new way of doing business, such as the right. The legal regulation of trade, exchange of services through the Web in Bolivia is zero, that is where the issue arises of ELECTRONIC CONTRACTS INSURANCE. According to surveys carried out in the law faculty, professional in law is skeptical of the processes, and security, so far still prefer the legal field and the handwritten signature stamped paper. For the universe of legal professionals in the field is hard to believe the security of digital signatures and their processes that is why in the research aims to test the security of contracts under an authenticated digital signatures and public-key private-key, in addition to proposing a model for implementation of electronic contracts with their proposed law. Playing technical and social aspects of interest to the general population

Computer science and law, technology and legal control of it has to turn into a pillar for the development of Bolivia, both in economic and in social terms. The development of research in a purely technical level, and the guidance of Dr. Uzeda, the thesis gives a comprehensive view of what should apply in terms of computer law in Bolivia.

INDICE

1.1 INTRODUCCION

La seguridad ha sido es y será una parte muy importante dentro de la sociedad y de la vida personal de cada individuo. La expresión "globalización mundial" hizo posible, gracias a la explosión de la tecnología lo que hace años se denominaba, "la revolución electrónica". Según la Economía Moderna el mercado más grande es el mercado virtual aquel que reside en el ciberespacio, entonces para este tipo de transacciones se necesitan procedimientos que se adecuen al entorno, en cuanto a la contratación de servicios vía Internet ha sido muy cuestionada su seguridad. Gracias a la poca incursión de investigaciones en el campo de la seguridad informática, derecho informático en Bolivia, se desconoce que es un contrato electrónico o a que se refiere una firma digital a profundidad.

Al caer las fronteras de la comunicación, países como Bolivia ahora tienen acceso a tecnología y conocimiento, lo que antes era muy difícil tener en países subdesarrollados. Las transacciones o intercambio de servicios a nivel mundial ya no es un dominio de algunos. Ahora las leyes limitan a Bolivia de gozar de un desarrollo pleno. Si bien ahora se cuenta con comunicación con el mundo hace falta la regulación legal.

En la sociedad boliviana existe una vaga idea de regulación y uso de los documentos digitales en general, obviamente que es de la misma forma para contratos electrónicos. Contratación electrónica, el concepto en si es conocido por muy poca gente, además del cuestionamiento de su seguridad (integridad, confidencialidad, autenticidad). Sin embargo los contratos electrónicos son más seguros, incluso que los contratos firmados manualmente.

La presente tesis expondrá las principales fortalezas de la seguridad en cuanto a contratos digitalizados, además de brindar una fuerte explicación de la seguridad que ofrece la criptografía a los datos digitales, introducción a los algoritmos de encriptación hashing su funcionamiento y su aplicación y de la seguridad que brinda en contraste con la forma tradicional de hacerlo. Se mostrará la elaboración de un contrato electrónico seguro en sus dos partes; documento digital y firma digital utilizando las herramientas anteriormente citadas.

1.2 ANTECEDENTES

Hoy por hoy el tema de la legalidad de contratos electrónicos en países desarrollados es algo muy común. La primera escritura firmada en forma electrónica se realizo en Virginia, Estados Unidos, en septiembre del 2000.

Desde entonces, varios países en todo el mundo han promulgado leyes, decretos que apoyan el uso de la firma digital para todo tipo de trámites. Entre ellos Francia, Portugal, Perú, India, Dinamarca, Irlanda, Finlandia, Japón, Chile, Venezuela, Alemania, España, Pakistán, Italia, Canadá y Brasil. Recientemente, el gobierno danés autorizó la presentación de declaraciones juradas impositivas a través de la Red usando la firma digital. También los Consejos Generales de abogados y escribanos españoles formaron sus autoridades certificantes para proveer de firmas digitales a sus miembros y reducir el tiempo que toma un trámite.

En los últimos 7 años el movimiento económico del mundo en su mayoría ha sido estimulado por medios electrónicos, así como por ejemplo tenemos compra, venta e intercambio de información y servicios. Por otra parte los contratos realizados por Internet gracias a firmas digitales han producido un crecimiento económico en los países, los cuales implementaron una forma de contrato digital mediante firmas electrónicas y no solo incremento la economía como país si no también disminuyeron el índice de desempleo. Es por eso que el siguiente trabajo pretende introducir la idea de manejo de firma digital para contratos digitales mediante la autenticación.

Italia, fue el primer país de Europa en dictar reglamentación sobre firma digital y lo hizo con el "Regolamento contenente modalitá di applicazione dell ' artícolo 15,comma 2,della lege 15 marzo 1997,n ° 59,in formazione, archivazione e trasmissione di documenti con strumenti informatici e telematici ".[2]
Este reglamento da diversos conceptos en su art.1 °, como por ejemplo: firma digital, par de claves asimétricas, clave privada y certificado.
En el art.2 ° se establece la validez y eficacia del documento electrónico.
Este reglamento no regula a las Autoridades Certificantes, las define como sujetos públicos o privados que certifican y guardan las claves públicas de firma por 10 o más años.

Alemania, la Ley del 13 de junio de 1997 posee un cuerpo breve y conciso de 16 artículos. En el art.1 ° se encarga de definir los objetivos de la ley, tal como la creación de condiciones generales para el uso seguro de la firma digital.

El art.2 ° define la firma digital como un sello creado con una clave privada, que permite mediante el uso de la clave pública asociada la verificación del propietario de la clave y el carácter de auténtica de la información.

La directiva de la Unión Europea, el 24 de mayo de 1999, se dictó la Directiva Europea sobre un Sistema Común para Firmas Electrónicas. Señala que la firma electrónica adjuntada a un documento electrónico, tiene exactamente el mismo valor legal que la firma manuscrita adjuntada a un documento escrito en soporte papel. Por ello la admite como medio de prueba y reconoce su valor probatorio.

Además, establece un sistema voluntario de acreditación de los prestadores de servicios de certificación, basado en condiciones objetivas, transparentes, proporcionadas y no discriminatorias y cuyo objetivo es proveer un grado de confianza y seguridad superior.

Portugal, Decreto Ley N ° 290-D/99 del 2 de agosto de 1999 regula la validez, eficacia y valor probatorio de los documentos electrónicos y de la firma digital, sin prejuicio de otras formas de firma electrónica que posean exigencias de seguridad como las de la firma digital.

España, decreto-ley N ° 14/1999 del 17 de septiembre de 1999.Esta normativa distingue entre: firma electrónica y firma electrónica avanzada, permitiendo en este último caso la identificación del signatario y que ha sido creada por medios que este mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos.

La ley federal norteamericana, en Estados Unidos se aprobó la Electronic signatures in global and National Comerce Act. Establece una regla de validez para todos los actos y transacciones celebrados por medios electrónicos. Lo que significa que ninguna ley, reglamento o norma podrá negar valor legal a un acto o contrato por el sólo hecho que su firma está en forma electrónica.

Incluye, además un capítulo sobre derechos básicos que deben tener los consumidores que van a realizar transacciones por medios electrónicos.

Perú, el Decreto Legislativo N ° 681 del 14 de octubre de 1991 y la Ley N ° 26.612 del 21 de mayo de 1996 son normas que van a cimentar las bases de la contratación electrónica. Las Leyes N ° 27269 del 26 de mayo del 2000 y la N ° 27291 del 24 de junio del mismo año regulan de manera directa la seguridad en la

Contratación Electrónica. La primera de ellas Ley de Firmas y Certificados Digitales establece el concepto de firma y certificados digitales y garantiza en forma universal la autenticidad, integridad, confidencialidad y el no repudio de las transacciones electrónicas.

Ley de Japón En el mes de mayo del año 2000, Japón ha aprobado la Ley sobre

Firmas Electrónicas y Servicios de Certificación que entro en vigor en el mes de abril del 2001.

Argentina, la resolución 45/97 de la Secretaría de la Función Pública, incorpora la tecnología de la firma digital a los procesos de información del sector público, adoptando las conclusiones el 30 de septiembre de 1996 del Subcomité de criptografía y Firma digital del Comité de Usuarios de Procesamientos e Imágenes (CUPI)autorizando la tecnología sugerida en el ámbito de la Administración Pública "para la promoción y difusión del documento y firma digitales en los términos y con los alcances allí definidos ", según el artículo 2 °.

El Decreto 427/1998 publicado en el Boletín Oficial del 21 de abril de 1998, el Poder Ejecutivo dispuso promover el uso de la firma digital en toda la Administración Pública Nacional, estableciendo que el documento electrónico cumple con la condición de no repudio, lo que posibilita la prueba inequívoca de que una persona firmó efectivamente un documento digital, y que tal documento no sufrió alteración alguna desde el momento de la firma.

Existen en Argentina dos proyectos de ley que se encuentran en discusión.

Chile, en junio de 1999 se dictó el Decreto Supremo N ° 81, regulador del uso de firmas digitales y documentos electrónicos al interior de la Administración del

Estado. Este Decreto obedece a uno de los compromisos adoptados por una Comisión Presidencial de Nuevas Tecnologías que sesionó durante 1998,en orden a dotar a los órganos estatales del marco legal que permita el uso de la informática y de las telecomunicaciones en reemplazo de sus procedimientos manuales, específicamente relacionado con el uso de firmas y documentos digitales o electrónicos, pero solo al interior de la Administración del Estado y no de las relaciones con los administrados.

Bolivia, cualquier tipo de contratación de servicios de toda índole tiene que realizarse con firma manuscrita ya que la legislación boliviana carece de regulaciones legales en cuanto al tema. Haciéndose ilegales las transacciones como compra, venta, contratación de servicios, etc. vía Internet. Las personas en el área de derecho desconocen la forma de construcción y la seguridad de los contratos electrónicos, eso impide su confianza en ellos.

Con la apertura del mercado a nivel mundial, la globalización, además del avance de la tecnología, las transacciones digitales son una necesidad que debe cubrirse en la sociedad. Hasta ahora ha sido muy difícil para países que cuentan con legislación acerca de contratos electrónicos interactuar con Bolivia en cuanto a transacciones digitales. Por otra parte para profesionales que apostaron por el mercado establecido en el Internet, se les dificulta las transacciones ya que la legalidad de ellos no existe en el territorio.

Plagio de firmas manuscritas

Jorge Bazo
December 26, 2005

Según un informe del diario El Comercio, desde el 19 de junio del 2004 hasta el 14 de septiembre del 2005, la Oficina Nacional de Procesos Electorales (ONPE) ha denunciado diversos casos de falsificación de firmas ante las distintas fiscalías penales. Hasta el momento han sido denunciadas 17 agrupaciones inscritas, o en proceso de inscripción, ante el Jurado Nacional de Elecciones (JNE), presentando un total de 120,541 firmas falsas, la mayoría realizadas con el mismo puño.

Agrupaciones políticas unidas por el mismo error

Durante año y medio, la ONPE investigó y denunció casi sistemáticamente a los partidos cuyas firmas de adherentes fueron realizadas con el mismo puño. La investigación busca descartar la responsabilidad de las agrupaciones.

Demandado	Firmas falsas	Fecha de denuncia	Oficio	Instancia	Situación
Y se Llama Perú *Líder: Ricardo Wong*	4,950	19 de junio (2004)	570-2004-SG	5° JP *	Inscrito
	30	22 de octubre (2004)	956-2004-SG	25° FPPL	Inscrito
Partido Reformista del Perú	254	19 de junio (2004)	570-2004-SG	5° JP **	En proceso
Líder: *Víctor Echegaray* (Primera entrega)	550	28 de junio (2005)	193-2005-SG	9° FPPL	En proceso
	103	12 de octubre (2004)	919-2004-SG	23° FPPL	En proceso
Partido Democrático Descentralista *Líder: Javier Díez Canseco*	58,413	19 de agosto (2004)	736-2004-SG	17° FPPL	Inscrito
Proyecto País *Líder: Marco Antonio Arrunátegui*	1,679	26 de agosto (2004)	761-2004-SG	17° FPPL	En proceso
Coordinadora Nacional de Independientes	1,345	15 de setiembre (2004)	822-2004-SG	19° FPPL	Inscrito
Líder: *Drago Kisic* (Tercera entrega)	91	4 de octubre (2004)	894-2004-SG	23° FPPL	Inscrito
(Cuarta entrega)	26	14 de octubre (2004)	933-2004-SG	24° FPPL	Inscrito
(Quinta entrega)	6	23 de noviembre (2004)	1022-2004-SG	31° FPPL	Inscrito
Trabajo y Dignidad *Líder: Martín del Pomar*	72	22 de setiembre (2004)	850-2004-SG	20° FPPL	En proceso
República Solidaria *Líder: Jorge Luis Bustamante Chávez*	4,884	25 de setiembre (2004)	867-2004-SG	21° FPPL	En proceso
Partido por la Democracia Social-Compromiso Perú	3,288	6 de octubre (2004)	911-2004-SG	23° FPPL	En proceso
Líder: Susana Villarán	5,654	30 de mayo (2005)	147-2005-SG	4° FPPL	En proceso
Renovación Nacional (Primera entrega) *Líder: Rafael Rey*	121	23 de noviembre (2004)	999-2004-SG	31° FPPL	Inscrito
Nueva Generación (Primera entrega) *Líder: Pedro Koechlin Von Stein*	8,807	-	-	23° FPPL	En proceso
Empecemos Perú (Primera entrega) *Líder: Juan Vera Caro*	1,099	3 de diciembre (2004)	1028-2004-SG	32° FPPL	En proceso
Restauración Nacional *Líder: Humberto Lay Sun*	1,150	19 de mayo (2005)	137-2005-SG	4° FPPL	En proceso
Insurgencia Renovadora *Líder: José Cardo Guarderas*	2,180	30 de mayo (2005)	146-2005-SG	4° FPPL	En proceso
Partido Político Nacional Adelante *Líder: Rafael Belaunde*	1,450	17 de junio (2005)	184-2005-SG	7° FPPL	En proceso
Despertar Nacional *Líder: Ricardo Noriega Salaverry*	20,325	1 de agosto (2005)	237-2005-SG	13° FPPL	En proceso
Movimiento Humanista Peruano *Líder: Yehude Simon*	2,064	14 de setiembre (2005)	287-2005-SG	20° FPPL	Inscrito
Partido Nacionalista Peruano *Líder: Ollanta Humala*	2,000	-	-	33° FPPL	En proceso
TOTAL	**120,541**	**JP: Juzgado Penal de Lima **FPPL: Fiscalía Provincial Penal de Lima*			

Fuente: ONPE — EL COMERCIO

Fuente: weblogs.elearning.ubc.ca/.../2005_12.php

Casos concretos de falsificación de firmas alrededor del mundo han sido denunciados, tratándose de contratos firmados manualmente. Contrariamente, existen denuncias del rompimiento de la seguridad de los algoritmos básicos de la firma digital, claro que ninguno de ellos ha sido probado satisfactoriamente. En los países donde se instauraron la tecnología de firma digital, la falsificación de firmas tuvo un decrecimiento favorable para las transacciones hechas en esta forma

1.3 PLANTEAMIENTO DEL PROBLEMA

Las transacciones realizadas en base a contratos electrónicos y afirma digital son poco conocidos en la sociedad, es así que se necesita urgentemente una investigación que engrane un trabajo entre la informática y el derecho

Están estrechamente ligadas al objeto de estudio las siguientes disciplinas:

- Informática
- Derecho

El derecho informático en Bolivia esta naciendo pero la tecnología a crecido a pasos agigantados es por eso que en los últimos años las leyes con respecto a derecho informático es un problema de orden general. La poca incursión e ínteractuación de Abogados e Informáticos en este campo deja vacíos legales a lo largo del derecho informático. Uno de los grandes problemas de los profesionales en el área del derecho es que no confían del todo en los procedimientos digitales. Por otra parte los contratos electrónicos han estado sustituyendo, en otros países, muchos trámites de contratación pudiendo utilizarse no solo a nivel local sino nacional e internacional. Para palear el problema Bolivia debe contar con regulación legal para documentos digitales.

Una firma digital es creada después de pasar el texto de un mensaje a través de un algoritmo de "hashing" lo cual genera un mensaje comprimido. El mensaje comprimido es luego encriptado empleando la Clave Privada del individuo que está generando el mensaje, transformándolo en una firma digital. La firma digital sólo puede ser desencriptada empleando la Clave Pública del individuo. El receptor del mensaje desencripta la firma digital y recalcula entonces el mensaje comprimido. El valor calculado del nuevo mensaje comprimido se compara con el valor del mensaje

comprimido hallado en la firma. Si los dos cálculos son iguales, significa que el mensaje no ha sido alterado. Desde el momento en que la Clave Pública del emisor fue usada para verificar la firma, el texto tiene que haber sido firmado con la Clave Privada, conocida exclusivamente por el emisor. El proceso de autenticación será incorporado en toda aquélla aplicación que exija seguridad en las comunicaciones.

No es factible encontrar un mensaje que posea una determinada numeración, o encontrar dos mensajes que posean una numeración idéntica. Si los supuestos mencionados anteriormente fueran posibles, un intruso podría adjuntar un mensaje falso.

La firma digital es un sistema para encriptar un documento; es decir, para codificarlo de tal manera que su contenido sólo pueda volverse inteligible con una contraseña particular.

Si alguien quiere enviarle información confidencial a un interlocutor, invierte el uso de claves: encripta los datos con la clave pública del receptor. Se hace así porque es, en teoría, el único que tiene la clave privada complementaria y, por lo tanto, sólo él puede desencriptar los datos.

Lo bueno del proceso es que quien se encarga del trabajo duro es el software de la computadora; lo único que tiene que hacer el usuario es conseguir un par de claves, el software correspondiente y dejar que la máquina haga el resto.

El cambio del modo de hacer transacciones seguramente asusta a algunos sectores de la sociedad ya que es un cambio de lo tradicional a lo contemporáneo en un tiempo corto, lo cual significa, a la velocidad de la tecnología, siendo los beneficios mayores que los miedos, por tanto no existe razón alguna para temerle al cambio. Además las nuevas generaciones, las que nacen en la era de la tecnología, no concebirán un mundo con tanta burocracia en cuanto a tramites teniendo la automatización al alcance de sus manos, siendo que la legalidad de contratos electrónicos, agilizara la forma de intercambio de servicios y nos hará a todos la vida un poco mas fácil.

Las transacciones digitales hoy en día se han convertido de ser un pasatiempo a ser algo necesario ya sea este de orden económico, de servicios, o cualquier otro tipo de contacto vía Internet de intercambio de información.

La falta de seguridad de los contratos electrónicos y firmas digitales es la excusa que se maneja para no hacer posible la legalidad de los documentos digitales, además de la falta de información o mecanismos de funcionamiento. Los contratos electrónicos ampliarían en gran manera el mercado de trabajo. Por otra parte la elaboración de un documento que acredite la seguridad no solo de contratos sino de documentos electrónicos en general seria de gran ayuda a la sociedad. Los contratos electrónicos basados en los algoritmos de hashing proporcionan un grado mayor de seguridad que los contratos usados manualmente hoy en día en Bolivia. La firma digital basada en algoritmos hashing es más fácil de autenticar y validar que la firma hecha a mano. Entonces los contratos electrónicos y firma digital no es mas una opción en el movimiento económico de un país si no que ahora se convierte en una necesidad.

El contrato electrónico tiene dos partes:

Documento digital, es el documento en el cual se estipulan los puntos de intercambio deservicios que se utilizara entre las partes, el documento es redactado y diseñado como los contratos tradicionales. Dichos contratos deben ser hechos en forma digital, luego pasaran por un algoritmo que dará la seguridad en el aspecto de integridad que se refiere a que el documento llega a su destino tal y como fue diseñado originalmente así el documento pasara por la autopista de la información, el destinatario podrá saber si el documento es el original o si fue alterado

Firma digital, es la parte del contrato electrónico que da la seguridad de autenticidad. La firma digital certifica que el documento enviado y recibido por el receptor es realmente del emisor que aparece en la firma del documento.

¿Qué es necesario realizar para impulsar la legalidad del documento digital y firma digital en la sociedad boliviana?

1.4 OBJETIVO

1.4.1 OBJETIVO GENERAL

Establecer la seguridad de contratos y firma digital en Boliva mediante la aplicación de autenticación.

1.4.2 OBJETIVOS ESPECIFICOS

- Introducir el concepto general de los contratos electrónicos y su elaboración.
- Establecer la seguridad del contrato digital propiamente dicho.
- Demostrar la seguridad del contrato digital propiamente dicho
- Constituir la seguridad de la firma digital
- Demostrar la seguridad de la firma digital.
- Elaborar una propuesta de ley basada en el enfoque técnico de la seguridad en contratos electrónicos.

1.5 HIPOTESIS

Los contratos electrónicos (documento digital y firma digital) tienen un alto nivel de seguridad para remplazar la tradicional forma de hacer transacciones bajo una autenticación.

1.6 JUSTIFICACION

Alrededor del mundo la mayoría de los negocios y transacciones se hacen vía Internet lo cual nos obliga a desarrollar seguridad en cuanto a documentación mediante Internet. Los contratos digitales se han convertido últimamente en una herramienta imprescindible en el campo de transacciones digitales. Por lo tanto, la seguridad en cuanto a integridad, autenticidad de documentos es vital. En Bolivia todavía no se implementa la idea no solamente en el campo de negocios sino también en el campo del derecho. Entonces se carece de la legalidad de lo que es contratos electrónicos y firma digital lo que perjudica enormemente al desarrollo del país y de ciudadanos comunes que podrían acceder a trabajos fuera del país. La legalidad de los

documentes es importante para la sociedad ya que se necesita estar en contacto con el desarrollo electrónico y madures económica alrededor del mundo.

1.6.1 JUSTIFICACION CIENTIFICA

Según la ISO-17000 los documentos digitales en cuanto a la seguridad de la información deben cumplir con, integridad, disponibilidad, autenticidad, no repudio. Solamente así se considera un documento digital seguro. Por otra parte las leyes están basadas en argumentos sólidos, en al caso de contratos electrónicos la seguridad para otorgar legalidad. Los algoritmos hashing permiten salvaguardar dichas características en un contrato electrónico, como se puede ver los documentos realizados digitalmente tienen una gran ventaja, sobre los documentación realizada en forma tradicional ya que en el caso digital se puede verificar la autenticidad, integridad, disponibilidad, mediante dispositivos de red a nivel mundial de una manera rápida y eficiente

1.6.2 JUSTIFICACION ECONOMICA

Bolivia no se encuentra entre los países que tienen un gran movimiento económico a través de la Web. Tema que da mucho que pensar acerca del movimiento transaccional de Bolivia hacia el mundo y viceversa.
En estos días donde, la tecnología es la base de la economía, el Internet la base de intercambio de servicios a nivel internacional. Para medir la perdida económica de un país el cual no cuenta con una legislación de legalidad de dichas transacciones seria medir desde el pasaje que gasta un individuo al llevar declaraciones juradas hasta contratos millonarios perdidos por la falta regulación jurídica. Sin hablar del tiempo y del espacio que simplifica una transacción digital.

1.6.3 JUSTIFICACION SOCIAL

En el día a día todas las personas buscan un futuro mejor, la utilidad de los contratos electrónicos es una herramienta que acorta distancias en cuanto el sentido de contratar personal o servicios. Por ejemplo si una persona que radica en La Paz estuviera buscando un trabajo en Santa Cruz necesariamente tiene que viajar, presentar su

documentación para ser un postulante al cargo. Los contratos digitales acortarían espacio y tiempo haciendo el trámite mucho más fácil, además que pasaría si no accede al puesto. Peor aun si el ejemplo se desarrollaría fuera del país como en España, seria toda una odisea solo acceder a la visa pero con un contrato electrónico legal esa persona podría acceder a su visa de manera inmediata solo a la presentación de este contrato. Así es como los contratos están remplazando a contratos en papeles y firmados a mano a nivel mundial.

1.7 METODOLOGIA Y HERRAMIENTAS

En el trabajo de investigación utilizaremos dos tipos de metodología, el deductivo y el inductivo ya que la naturaleza de la investigación así lo requiere.

El método inductivo es un proceso mental que consiste en inferir de casos particulares observados a deducciones generales así como su nombre es a través de la inducción que intuimos algo general partiendo de lo particular. Descifrando un documento "contrato" y su respectiva firma digital en cuanto a su seguridad.

El método deductivo lo realizaremos al ver el comportamiento de la sociedad con respecto a la contratación legal como su nombre lo indica de lo general deducimos algo particular. La necesidad de contratos digitales parte de de una revolución electrónica general

Para el desarrollo de las aplicaciones se usara la técnica de algoritmos hashing para firma digital y contratos electrónicos.

Para entender la seguridad en el comercio electrónico es necesario conocer y entender los siguientes conceptos básicos:

La Criptología (del griego criptos = oculto y logos = tratado, ciencia) es el nombre genérico con el que se designan dos disciplinas opuestas y a la vez complementarias:

- Criptografía
- Criptoanálisis

La Criptografía se ocupa del diseño de procedimientos para cifrar, es decir, para enmascarar una determinada información de carácter confidencial. El Criptoanálisis, por su parte, se ocupa de romper esos procedimientos de cifrado para así recuperar la información original.

Ambas disciplinas siempre se han desarrollado de forma paralela, pues cualquier método de cifrado lleva siempre emparejado su Criptoanálisis correspondiente.

La Criptografía como medio de proteger la información personal es un arte tan antiguo como la propia escritura. Como tal, permaneció durante siglos vinculada muy estrechamente a los círculos militares diplomáticos, puesto que eran los únicos que en principio tenían auténtica necesidad de ella.

1.8 ALCANCES Y APORTES

1.8.1 LIMITES Y ALCANCES.

El estudio para desarrollar en la tesis se avocara a la ciudad de la paz localizada en Bolivia. Se hará un estudio de contratos electrónicos y su contexto para dar a conocer la utilidad, además del alto grado de seguridad que ofrecen.

En cuanto a los alcances de la tesis se evocara a; probar la autenticidad del documento digital mediante algoritmos hashing, probar la seguridad de las firmas digitales, y con el apoyo del derecho informático promover un proyecto de ley para la legalidad de contratos electrónicos.

1.8.2 APORTES

El aporte del proyecto es de magnitudes inconmensurables porque al hacer realidad el objetivo en el proyecto, además de introducir la idea de contratos electrónicos seguros y promover un proyecto de ley, el crecimiento económico en nuestro país con especto a este punto será real. Otro punto importante de aporte es la apertura del mercado laboral de Bolivia hacia el mundo y viceversa de una manera formal.

En cuanto a la introducción de la idea de la seguridad de contratos electrónicos, cambiará el modo tradicional de hacer contratos, declaraciones juradas, todo tipo de documentos los cuales necesitan de una autenticación con firma de puño y letra, haciendo notar a la población en su conjunto que dichos documentos son más seguros que los tradicionales.

En cuanto a promover la legalidad de contratos electrónicos, es un avance y también sirve para alcanzar el nivel de países desarrollados en materia de derecho informático. La legalidad propuesta permitiría acceder a trabajos fuera del país además de reemplazar la firma tradicional así todos los documentos dependientes de una autenticación o firma a mano, ahora haciéndolo mediante firma digital sin tener que estar presente en algún lugar en particular sino con solo contar con una conexión a Internet.

El aporte hacia la sociedad boliviana es, a cada persona que necesita hacer algún tipo de contrato, intercambio de servicios, podrá ser hecho desde la posición donde se encuentra tan solo con acceder a Internet sin olvidar la accesibilidad a transacciones digitales por medio de la telefonía celular

1.9 MARCO TEORICO

Para cumplir con el objetivo en cuanto a la seguridad de contratos electrónicos, se debe pensar en las propiedades de un contrato electrónico digital seguro y además legal.

Legalmente un contrato de cualquier índole debe cumplir con la Ley Nº 11, libro II, parte II, titulo I y titulo II de la republica de Bolivia.

En Bolivia no se cuanta con regulaciones digitales, internacionalmente contamos con la ISO-17000 que pone bases sobre la seguridad de documentación digital.

La confidencialidad es la propiedad de la seguridad que permite mantener en secreto la información y solo los usuarios autorizados pueden manipular dicha información. Un

servicio de confidencialidad es designado para evitar la disponibilidad del tráfico de un mensaje a entidades o usuarios no autorizados. Los usuarios pueden ser una persona, un proceso, un programa, etc.

Esta característica de la información debe asegurar que ninguna entidad no autorizada entienda la información. Para lograrlo se utilizan las técnicas de encriptación o codificación de datos, mediante las cuales se codifica un mensaje de tal forma que no pueda ser entendido por el ser humano o descifrado por un equipo computacional.

El nivel o grado de confidencialidad debe estar en relación con la importancia de la información. Debe existir un balance entre el esfuerzo requerido para obtener la información decodificada y la ganancia que se obtendría con ello.

La confidencialidad debe incluir el tiempo de diseminación de la información por ejemplo, el presupuesto anual de una empresa tendría una vigencia de un año.

La integridad de la información corresponde a lograr que la información transmitida entre dos entidades no sea modificada por un tercero y esto se logra mediante la utilización de firmas digitales.

Las firmas digitales codifican un mensaje de tal forma que mediante una función hash (la cual es similar a un *Checksum*) calcula un resumen único (*message digest*) del mensaje original. Esta función solo es de una vía, esto es que no existe reversión del procedimiento de cálculo, con lo cual no es posible determinar el mensaje original a partir del *digest*. Una buena función hash debe detectar el más mínimo cambio en el mensaje original.

La validación de la integridad del mensaje se da al aplicar al mensaje original la misma función hash y comparar el resultado con el resumen recibido.

El objetivo de verificar la integridad es debido a la preocupación para mantener la información sin modificación por usuarios no autorizados.

Los servicios de no-repudiación ofrecen una prueba al emisor de que la información fue entregada además es una prueba para el receptor del origen de la información.

Esta característica garantiza que la persona o entidad que envía un mensaje no pueda rechazar el envío o recepción de un mensaje. Es necesario este mecanismo debido al proceso de comercio electrónico de envío y recepción de información para garantizar la realización de las transacciones para ambas entidades participantes.

Existen dos lados de la no-repudiación, un lado es relevante para el emisor, conocido como no-repudiación de origen, para asegurar que el emisor no pueda negar el envío del mensaje. El otro lado es del receptor, conocido como no-repudiación del receptor, para asegurar que el receptor no pueda negar la recepción del mensaje.

Mediante las técnicas de autentificación se garantiza la no-repudiación debido a la utilización de la llave privada de cada entidad.

La seguridad de la información se logra implementando un conjunto adecuado de controles, que abarca políticas, practica, procedimientos, estructuras organizacionales y funciones de software.

Los contratos electrónicos debido a su diseño y control digital mediante los algoritmos de hashing ofrecen, la confidencialidad sumando el no repudio a este punto primero que el documento viene de la persona o empresa que realmente firma y que la misma no puede negar que fue enviada por ella misma, la integridad del documento a través de dos autenticaciones del documento y de la firma mediante la encriptación, la disponibilidad del contrato que se realiza mediante la red a nivel mundial, en general un alto grado de seguridad mucho más que el método tradicional.

2.1 PRINCIPALES PROBLEMAS

A lo largo de la investigación se identifico los siguientes problemas:
Los documentos electrónicos han sido tomados como un intercambio de correspondencia nada muy privado, ya que no se avanzo al paso de la tecnología, tratando de confiar en lo que ya se conoce de las empresas que manejan el mercado (yahoo, hotmail, gmail, etc.). Entonces es fácil saber que no se ha llegado a una conciencia de lo que son los contratos electrónicos menos de su seguridad.
Además la legislación boliviana carece de aspectos relacionados con el tema, siendo el punto neurálgico del tema la seguridad de los contratos electrónicos.

2.2 LEGISLACION BOLIVIANA

La legislación boliviana tiene muy poco contenido acerca del tema, LA LEY DE TELECOMUNICACIONES Nº 1632 del 5 de julio 1995 no contempla la legalidad de los contratos electrónicos (ANEXO A).
La modificación de los artículos 2º, 4º, 11º, 21º, titulo VII y 28 de la ley 1632 en LA LEY Nº 2342 del 25 de abril de 2002 tampoco introduce un concepto de contratos electrónicos a las leyes bolivianas (ANEXO A).

Como se puede ver en el anexo A la ley 1632 tiene 2 artículos que tratan acerca de contratos, los cuales no tocan el aspecto digital ni los mecanismos de seguridad. La ley 2342, que es una modificación a la ley 1632, no toma en cuenta los artículos 7 y 8 así que los cambios o reformas realizadas no incumben los contratos, manteniendo la posición de la ley frente a los contratos como al principio.

2.3 CRIPTOTOLOGIA

2.3.1 CRIPTOGRAFIA

La criptografía se origina del griego *κρύπτω krypto*, «oculto», y *γράφω graphos*, «escribir», literalmente «escritura oculta», es el arte o ciencia de cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura que sólo puedan ser leídos por las personas a quienes van dirigidos.

Con más precisión, cuando se habla del área de conocimiento como ciencia se debería hablar de criptología, que engloba tanto las técnicas de cifrado, la criptografía propiamente dicha, como sus técnicas complementarias: el criptoanálisis, que estudia los métodos que se utilizan para romper textos cifrados con objeto de recuperar la información original en ausencia de las claves.

2.3.1.1 FINALIDAD

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.
Otro método utilizado para ocultar el contenido de un mensaje es ocultar el propio mensaje en un canal de información, pero en puridad, esta técnica no se considera criptografía, sino esteganografía. Por ejemplo, mediante la esteganografía se puede ocultar un mensaje en un canal de sonido, una imagen o incluso en reparto de los espacios en blanco usados para justificar un texto. La esteganografía no tiene porqué ser un método alternativo a la criptografía, siendo común que ambos métodos se utilicen de forma simultánea para dificultar aún más la labor del criptoanalista.

En la actualidad, la criptografía se utiliza para comunicar información de forma segura ocultando su contenido a posibles fisgones. Una de las ramas de la criptografía que más ha revolucionado el panorama actual de las tecnologías informáticas es el de la firma digital: tecnología que busca asociar al emisor de un mensaje con su contenido de forma que aquel no pueda posteriormente repudiarlo.

2.3.1.2 CONCEPTOS

En la Jerga de la criptografía, la información original que debe protegerse se denomina texto en claro. El cifrado es el proceso de convertir el texto plano en un galimatías ilegible, denominado texto cifrado o criptograma. Por lo general, la aplicación concreta del algoritmo de cifrado (también llamado cifra) se basa en la existencia de una clave:

información secreta que adapta el algoritmo de cifrado para cada uso distinto. Cifra es una antigua palabra arábiga para designar el número cero; en la antigüedad cuando Europa empezaba a cambiar del sistema de numeración romano al arábigo, se desconocía el cero por lo que este resultaba misterioso, de ahí probablemente que cifrado signifique misterioso.

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

El descifrado es el proceso inverso que recupera el texto plano a partir del criptograma y la clave. El protocolo criptográfico especifica los detalles de cómo se utilizan los algoritmos y las claves (y otras operaciones primitivas) para conseguir el efecto deseado. El conjunto de protocolos, algoritmos de cifrado, procesos de gestión de claves y actuaciones de los usuarios, en conjunto es lo que constituyen un criptosistema, que es con lo que el usuario final trabaja e interactúa.

Existen dos grandes grupos de cifras: los algoritmos que utilizan una única clave tanto en el proceso de cifrado como en el de descifrado, y los que utilizan una clave para cifrar mensajes y una clave distinta para descifrarlos. Los primeros se denominan cifras simétricas, de clave simétrica o de clave privada y son la base de los algoritmos de cifrado clásico. Los segundos se denominan cifras asimétricas, de clave asimétrica o de clave pública y forman el núcleo de las técnicas de cifrado modernas.

En el lenguaje cotidiano, la palabra código se usa de forma indistinta con cifra. En la jerga de la criptografía, sin embargo, el término tiene un uso técnico especializado: los códigos son un método de criptografía clásica que consiste en sustituir unidades textuales más o menos largas o complejas, habitualmente palabras o frases, para ocultar el mensaje; por ejemplo, "cielo azul" podría significar "atacar al amanecer". Por el contrario, las cifras clásicas normalmente sustituyen o reordenan los elementos básicos del mensaje letras, dígitos o símbolos, en el ejemplo anterior, "rcnm arcteeaal

aaa" sería un criptograma obtenido por transposición. Cuando se usa una técnica de códigos, la información secreta suele recopilarse en un libro de códigos.

Con frecuencia los procesos de cifrado y descifrado se encuentran en la literatura como encriptado y desencriptado, aunque ambos son neologismos anglicismos de los términos ingleses encrypt y decrypt, todavía sin reconocimiento académico. Hay quien hace distinción entre cifrado/descifrado y encriptado/desencriptado según estén hablando de criptografía simétrica o asimétrica, pero la realidad es que la mayoría de los expertos hispanohablantes prefieren evitar ambos neologismos hasta el punto de que el uso de los mismos llega incluso a discernir a los aficionados y novatos en la materia de aquellos que han adquirido mas experiencia y profundidad en la misma.

2.3.1.3 HISTORIA DE LA CRIPTOGRAFIA

La historia de la criptografía es larga y abunda en anécdotas. Ya las primeras civilizaciones desarrollaron técnicas para enviar mensajes durante las campañas militares de forma que si el mensajero era interceptado la información que portaba no corriera el peligro de caer en manos del enemigo. Posiblemente, el primer criptosistema que se conoce fuera documentado por el historiador griego Polibio: un sistema de sustitución basado en la posición de las letras en una tabla. También los romanos utilizaron sistemas de sustitución, siendo el método actualmente conocido como César, porque supuestamente Julio César lo utilizó en sus campañas, uno de los más conocidos en la literatura (según algunos autores, en realidad Julio César no utilizaba este sistema de sustitución, pero la atribución tiene tanto arraigo que el nombre de éste método de sustitución ha quedado para los anales de la historia). Otro de los métodos criptográficos utilizados por los griegos fue la escitala espartana, un método de trasposición basado en un cilindro que servía como clave en el que se enrollaba el mensaje para poder cifrar y descifrar.

En 1465 el italiano Leon Battista Alberti inventó un nuevo sistema de sustitución polialfabética que supuso un gran avance de la época. Otro de los criptógrafos más importantes del siglo XVI fue el francés Blaise de Vigenere que escribió un importante tratado sobre "la escritura secreta" y que diseñó una cifra que ha llegado a nuestros días asociada a su nombre. A Selenus se le debe la obra criptográfica

"*Cryptomenytices et Cryptographiae*" (Lüneburg, 1624). Durante los siglos XVII, XVIII y XIX, el interés de los monarcas por la criptografía fue notable. Las huestes de Felipe II utilizaron durante mucho tiempo una cifra con un alfabeto de más de 500 símbolos que los matemáticos del rey consideraban inexpugnable. Cuando el matemático francés François Viète consiguió criptoanalizar aquel sistema para el rey de Francia, a la sazón Enrique IV, el conocimiento mostrado por el rey francés impulsó una queja de la corte española ante del papa Pío V acusando a Enrique IV de utilizar magia negra para vencer a sus ejércitos. Por su parte, la reina María Estuardo, reina de los Escoceses, fue ejecutada por su prima Isabel I de Inglaterra al descubrirse un complot de aquella tras un criptoanálisis exitoso por parte de los matemáticos de Isabel.

La máquina Enigma utilizada por los alemanes durante la II Guerra Mundial
Desde el siglo XIX y hasta la Segunda Guerra Mundial las figuras más importantes fueron la del holandés Auguste Kerckhoffs y la del prusiano Friedrich Kasiski. Pero es en el siglo XX cuando la historia de la criptografía vuelve a presentar importantes avances. En especial durante las dos contiendas bélicas que marcaron al siglo: la Gran Guerra y la Segunda Guerra Mundial. A partir del siglo XX, la criptografía usa una nueva herramienta que permitirá conseguir mejores y más seguras cifras: las máquinas de cálculo. La más conocida de las máquinas de cifrado, posiblemente sea la máquina alemana Enigma: una máquina que automatizaba considerablemente los cálculos que era necesario realizar para las operaciones de cifrado y descifrado de mensajes. Para vencer al ingenio alemán, fue necesario el concurso de los mejores matemáticos de la época y un gran esfuerzo computacional. No en vano, los mayores avances tanto en el campo de la criptografía como en el del criptoanálisis no empezaron hasta entonces.

Tras la conclusión de la Segunda Guerra Mundial, la criptografía tiene un desarrollo teórico importante; siendo Claude Shannon y sus investigaciones sobre teoría de la información esenciales hitos en dicho desarrollo. Además, los avances en computación automática suponen tanto una amenaza para los sistemas existentes como una oportunidad para el desarrollo de nuevos sistemas. A mediados de los años 70 el Departamento de Normas y Estándares norteamericano publica el primer diseño lógico de un cifrador que estaría llamado a ser el principal sistema criptográfico de finales de siglo: el Estándar de Cifrado de Datos o DES. En esas mismas fechas ya se empezaba a gestar lo que sería la, hasta ahora, última revolución de la criptografía teórica y

práctica: los sistemas asimétricos. Estos sistemas supusieron un salto cualitativo importante ya que permitieron introducir la criptografía en otros campos que hoy día son esenciales, como el de la firma digital.

2.3.2 CRIPTOGRAFIA SIMETRICA

La criptografía simétrica es el método criptográfico que usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y el destinatario lo descifra con la misma.

2.3.2.1 SEGURIDAD

Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo. En otras palabras, no debería ser de ninguna ayuda para un atacante conocer el algoritmo que se está usando. Sólo si el atacante obtuviera la clave, le serviría conocer el algoritmo. Los algoritmos de cifrado usados, por ejemplo, en el sistema GNU, GnuPG tienen estas propiedades.

Dado que toda la seguridad está en la clave, es importante que sea muy difícil adivinar el tipo de clave. Esto quiere decir que el abanico de claves posibles, o sea, el espacio de posibilidades de claves, debe ser amplio. Richard Feynman fue famoso en Los Álamos por su habilidad para abrir cajas de seguridad; para alimentar la leyenda que había en torno a él, llevaba encima un juego de herramientas que incluían un estetoscopio. En realidad, utilizaba una gran variedad de trucos para reducir a un pequeño número la cantidad de combinaciones que debía probar, y a partir de ahí simplemente probaba hasta que adivinaba la combinación correcta. En otras palabras, reducía el tamaño de posibilidades de claves.

Actualmente, los ordenadores pueden descifrar claves con extrema rapidez, y ésta es la razón por la cual el tamaño de la clave es importante en los criptosistemas modernos. El algoritmo de cifrado DES usa una clave de 56 bits, lo que significa que hay 2 elevado a 56 claves posibles (72.057.594.037.927.936 claves). Esto representa

un número muy alto de claves, pero una máquina computadora de uso general puede comprobar el conjunto posible de claves en cuestión de días. Una máquina especializada puede hacerlo en horas. Algoritmos de cifrado de diseño más reciente como 3DES, Blowfish e IDEA usan claves de 128 bits, lo que significa que existen 2 elevado a 128 claves posibles. Esto equivale a muchísimas más claves, y aun en el caso de que todas las máquinas del planeta estuvieran cooperando, tardarían más tiempo en encontrar la clave que la edad del universo.

Como ejemplo de sistema simétrico está Enigma. Éste fue un sistema empleado por Alemania durante la Segunda Guerra Mundial, en el que las claves se distribuían a diario en forma de libros de códigos. Cada día, un operador de radio, receptor o transmisor, consultaba su copia del libro de códigos para encontrar la clave del día. Todo el tráfico enviado por ondas de radio durante aquel día era cifrado y descifrado usando las claves del día.

Inglaterra usó máquinas para descifrar las claves durante aquella guerra y aunque el citado sistema alemán, Enigma, estaba provisto de un amplio abanico de claves, los ingleses diseñaron máquinas de cómputo especializado, los Bombes, para comprobar las claves de modo mecánico hasta que la clave del día era encontrada. Esto significaba que algunas veces encontraban la clave del día pocas horas después de que ésta fuera puesta en uso, pero también que otros días no podían encontrar la clave correcta. Los Bombes no fueron máquinas de cómputo general, sino las precursoras de los ordenadores (computadoras) actuales. Algunos ejemplos de algoritmos simétricos son 3DES, AES, Blowfish e IDEA.

2.3.2.2 INCONVENIENTES

El principal problema con los sistemas de cifrado simétrico no está ligado a su seguridad, sino al intercambio de claves. Una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad, pero ¿qué canal de comunicación que sea seguro han usado para transmitirse las claves? Sería mucho más fácil para un atacante intentar interceptar una clave que probar las posibles combinaciones del espacio de claves.

Otro problema es el número de claves que se necesitan. Si tenemos un número n de personas que necesitan comunicarse entre sí, se necesitan n/2 claves para cada pareja de personas que tengan que comunicarse de modo privado. Esto puede funcionar con un grupo reducido de personas, pero sería imposible llevarlo a cabo con grupos más grandes.

2.3.3 CRIPTOGRAFIA ASIMETRICA

La criptografía asimétrica es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. El remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje.

Los sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos. Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario. Por tanto, se necesitarán sólo n pares de claves por cada n personas que deseen comunicarse entre sí.

2.3.3.1 BASES

Los sistemas de cifrado de clave pública se basan en funciones-trampa de un solo sentido que aprovechan propiedades particulares, por ejemplo de los números primos. Una función de un solo sentido es aquella cuya computación es fácil, mientras que su inversión resulta extremadamente difícil. Por ejemplo, es fácil multiplicar dos números primos juntos para obtener uno compuesto, pero es difícil factorizar uno compuesto en sus componentes primos. Una función-trampa de un sentido es algo parecido, pero tiene una "trampa". Esto quiere decir que si se conociera alguna pieza de la

información, sería fácil computar el inverso. Por ejemplo, si tenemos un número compuesto por dos factores primos y conocemos uno de los factores, es fácil computar el segundo.

Dado un cifrado de clave pública basado en factorización de números primos, la clave pública contiene un número compuesto de dos factores primos grandes, y el algoritmo de cifrado usa ese compuesto para cifrar el mensaje. El algoritmo para descifrar el mensaje requiere el conocimiento de los factores primos, para que el descifrado sea fácil si poseemos la clave privada que contiene uno de los factores, pero extremadamente difícil en caso contrario.

2.3.3.2 SEGURIDAD

Como con los sistemas de cifrado simétricos buenos, con un buen sistema de cifrado de clave pública toda la seguridad descansa en la clave y no en el algoritmo. Por lo tanto el tamaño de la clave es una medida de la seguridad del sistema, pero no se puede comparar el tamaño del cifrado simétrico con el del cifrado de clave pública para medir la seguridad. En un ataque de fuerza bruta sobre un cifrado simétrico con una clave de un tamaño de 80 bits, el atacante debe probar hasta 281-1 claves para encontrar la clave correcta. En un ataque de fuerza bruta sobre un cifrado de clave pública con un clave de un tamaño de 512 bits, el atacante debe factorizar un número compuesto codificado en 512 bits (hasta 155 dígitos decimales). La cantidad de trabajo para el atacante será diferente dependiendo del cifrado que esté atacando. Mientras 128 bits son suficientes para cifrados simétricos, dada la tecnología de factorización de hoy en día, se recomienda el uso de claves públicas de 1024 bits para la mayoría de los casos.

2.3.3.3 DESVENTAJAS RESPECTO AL CIFRADO SIMETRICO

La mayor ventaja de la criptografía asimétrica es que se puede cifrar con una clave y descifrar con la otra, pero este sistema tiene bastantes desventajas:
Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.

- Las claves deben ser de mayor tamaño que las simétricas.
- El mensaje cifrado ocupa más espacio que el original.

- El sistema de criptografía de curva elíptica representa una alternativa menos costosa para este tipo de problemas.

Herramientas como PGP, SSH o la capa de seguridad SSL para la jerarquía de protocolos TCP/IP utilizan un híbrido formado por la criptografía asimétrica para intercambiar claves de criptografía simétrica, y la criptografía simétrica para la transmisión de la información.

2.3.3.4 ALGORITMOS

Algunos algoritmos de técnicas de clave asimétrica son:
Diffie-Hellman, RSA, DSA, ElGamal, Criptografía de curva elíptica

Otros algoritmos de clave asimétrica con menor grado de seguridad son:
Merkle-Hellman, algoritmos "Knapsack".

2.3.4 CRIPTOGRAFIA HIBRIDA

Método criptográfico que usa tanto un cifrado simétrico como uno asimétrico. Emplea el cifrado de clave pública para compartir una clave para el cifrado simétrico. El mensaje que se esté enviando en el momento, se cifra usando la clave y enviándolo al destinatario. Ya que compartir una clave simétrica no es seguro, la clave usada es diferente para cada sesión.

Un ejemplo, tanto PGP como GnuPG usan sistemas de cifrado híbridos. La clave de sesión es cifrada con la clave pública, y el mensaje saliente es cifrado con la clave simétrica, todo combinado automáticamente en un sólo paquete. El destinatario usa su clave privada para descifrar la clave de sesión y acto seguido usa la clave de sesión para descifrar el mensaje.

Un sistema de cifrado híbrido no es más fuerte que el de cifrado asimétrico o el de cifrado simétrico de los que hace uso, independientemente de cuál sea más débil. En PGP y GnuPG el sistema de clave pública es probablemente la parte más débil de la combinación. Sin embargo, si un atacante pudiera descifrar una clave de sesión, sólo sería útil para poder leer un mensaje, el cifrado con esa clave de sesión. El atacante

tendría que volver a empezar y descifrar otra clave de sesión para poder leer cualquier otro mensaje.

2.3.5 ENCRIPTACION

Cifrado, proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros. Pueden ser contraseñas, números de tarjetas de crédito, conversaciones privadas, etc.

Para encriptar información se utilizan complejas fórmulas matemáticas y para desencriptar, se debe usar una clave como parámetro para esas fórmulas. El texto plano que está encriptado o cifrado se llama criptograma.

Las organizaciones de poder, a lo largo de la historia, han hecho del secreto de sus comunicaciones un principio fundamental de su actividad. Dicho secreto se intentó proteger mediante la encriptación, es decir, la codificación del lenguaje mediante una clave secreta sólo conocida por la organización emisora del mensaje y el destinatario del mensaje determinado por dicha organización. El anecdotario histórico abunda con ejemplos de batallas e, incluso, guerras supuestamente perdidas o ganadas mediante la interceptación y desencriptación de mensajes decisivos entre los centros de poder. El origen de la informática contemporánea durante la Segunda Guerra Mundial parece estar relacionado con los esfuerzos de matemáticos extraordinarios, como el inglés Turing, para desarrollar algoritmos capaces de descifrar los códigos del enemigo.

Por tanto, en cierto modo, no es de extrañar en la era de la información, basada en la comunicación de todo tipo de mensajes, que el poder (y, por tanto, la libertad) tenga una relación cada vez más estrecha con la capacidad de encriptar y descifrar. Hete aquí que lo que era una arcana tecnología matemática relegada a los dispositivos secretos de los servicios de inteligencia de los Estados se haya convertido, en el espacio de dos décadas, en la tecnología clave para el desarrollo del comercio electrónico, para la protección de la privacidad, para el ejercicio de la libertad en la red

y, también, paradójicamente, para nuevas formas de control en la red. La encriptación es el principal campo de batalla tecnológico-social para la preservación de la libertad en Internet.

2.4 CONTRATO ELECTRONICO

Es importante resaltar la importancia que día a día significan los contratos en el comercio globalizado. Las convenciones consentidas a través de instrumentos electrónicos conforman hoy una porción importante dentro del conjunto de relaciones que conforman y dan vida al mercado. Sin embargo es alarmante la falta de legislación al respecto, demostrándose una negación de los legisladores a viabilizar este tipo de contrataciones, así como también no se legisla sobre otras cuestiones que son paradigmas del avance científico y tecnológico actual, como la fertilización invitro y toda la cuestión de la manipulación de embriones.

El derecho como toda ciencia social tiene la obligación natural de acompañar el desarrollo del hombre en los aspectos científicos, tecnológicos y por ende sociales. Necesita para sobrevivir una innovación constante a la par de las otras ciencias, de lo contrario corre el riesgo de convertirse en una ciencia obsoleta, no idónea para regular y mantener los estados de derecho, estructura sobre la que se basamenta la civilización del hombre.

Con el surgimiento de Internet, se dieron lugar innumerables cuestiones acerca del cambio que representaría en las interrelaciones sociológicas, las cuales se verían afectadas hasta en la característica más elemental, como sostener una conversación con otra persona la cual se desarrollaría sin escucharse, sin mirarse, y utilizando como único medio de comunicación un teclado, todo ello por el precio de una llamada reducida de teléfono. El Chat o videoconferencia da lugar junto con el e-mail a un nuevo mundo de las comunicaciones, y por consiguiente a un sin fin de oportunidades de establecer negocios.

Las "nuevas realidades negociales" se forjaron sin ningún control, salvo el de los principios generales que regulan los contratos, que en muchos casos no alcanzan dada la peculiaridad y complejidad que las caracteriza. Dada esta condición es necesaria

una legislación especial, que regule las contrataciones electrónicas, para así evitar las frecuentes lagunas irreparables con las leyes actuales que se dispone.

Se Intentara, a través de la investigación, simplificar la realidad actual de los contratos digitales, y porque no, imponer ciertas bases que pueden fundamentar una futura y necesaria reforma.

Hay aspectos que no se pueden cubrir con los principios generales, sino que hay que normativizar ciertas cuestiones que afectan a las contrataciones virtuales con mas fuerza que a otros, por ejemplo: el perfeccionamiento de los contratos informáticos para que alcancen la validez deseada para producir efectos jurídicos, comenzando la primer problemática con la firma de las partes, para seguir luego con las formalidades tales como el doble ejemplar, en su caso los testigos, etc. Haciendo de la seguridad digital la piedra fundamental para incentivar el empate de la sociedad con la legislación tecnológica, una legislación que permita al individuo navegar por la tecnología sin fronteras legalmente.

Es claramente visible que el Código Civil Boliviano no esta a la altura de las implementaciones tecnológicas que tocan a la humanidad toda y obviamente al derecho, ya que es claramente inadecuada para regular apropiadamente la realidad negocial de los tiempos actuales. La problemática reside en el vacío de garantías a las que están sujetos los contratantes, situación encabezada por la inseguridad que significa la no existencia de una firma escrita para el perfeccionamiento del contrato. Sin embargo estas dos problemáticas están suplidas por los avances tecnológicos que signaron la aparición de estas contrataciones como lo es la firma digital.

2.4.1 DOCUMENTO DIGITAL

El documento digital es el contrato propiamente dicho el cual tiene que seguir las normas establecidas en el lugar o lugares donde el contrato es realizado. En Bolivia la Ley que pone reglamentos sobre este tipo de acciones es la ley 11, libro III, parte II, titulo I.

Un contrato, en términos generales, es definido como un acuerdo privado, digital, oral o escrito, entre partes que se obligan sobre materia o cosa determinada, y a cuyo cumplimiento pueden ser compelidas. Es un acuerdo de voluntades que genera derechos y obligaciones para las partes. Por ello se señala que habrá contrato cuando varias partes se ponen de acuerdo sobre una manifestación de voluntad destinada a reglar sus derechos.

Doctrinariamente, ha sido definido como un negocio jurídico bilateral o multilateral, porque intervienen dos o más personas (a diferencia de los actos jurídicos unilaterales en que interviene una sola persona), y que tiene por finalidad crear derechos y obligaciones (a diferencia de otros actos jurídicos que están destinados a modificar o extinguir derechos y obligaciones, como las convenciones). También se denomina contrato el documento que recoge las condiciones de dicho acto jurídico.

En el Derecho romano clásico, a su vez, el contrato se refiere a la concreta situación de estar ligadas las partes por un vínculo jurídico que crea derechos y obligaciones. No se refiere al acto jurídico mediante el cual las partes contraen dichos derechos, sino a lo contratado (*contractus*, lo contraído), la relación jurídica que ha quedado indisolublemente constituida mediante la convención generadora.

Las partes en un contrato son personas físicas o jurídicas. En un contrato hay dos polos o extremos de la relación jurídica obligacional, cada polo puede estar constituido por más de una persona revistiendo la calidad de parte.

El contrato, en general, tiene una connotación patrimonial, y forma parte de la categoría más amplia de los negocios jurídicos. La función del contrato es originar efectos jurídicos.

2.4.1.1 CONCEPTO LEGAL DE DOCUMENTO DIGITAL (CONTRATO)

La mayoría de los Códigos civiles contienen una definición de "contrato". Muchos de ellos, siguen los lineamientos del Código civil francés, cuyo artículo 1101 expresa que "El contrato es la convención por la cual una o más personas se obligan, con otra u otras, a dar, hacer, o no hacer alguna cosa".

El Código civil alemán prescribe que "para la formación de un negocio obligacional por actos jurídicos, como para toda modificación del contenido de un negocio obligacional se exige un contrato celebrado entre las partes, salvo que la ley disponga de otro modo". Mientras el Código civil suizo señala que "hay contrato si las partes manifiestan de una manera concordante su voluntad recíproca; esta manifestación puede ser expresa o tácita".

El Código Civil soviético solo expresaba que "Los actos jurídicos, esto es, los actos que tienden a establecer, modificar o extinguir relaciones de Derecho Civil, pueden ser unilaterales o bilaterales (contratos)".

2.4.2 FIRMA DIGITAL

El concepto de firma digital nació como una oferta tecnológica para acercar la operatoria social usual de la firma ológrafa (manuscrita) al marco de lo que se ha dado en llamar el ciberespacio o el trabajo en redes.

Consiste en la transformación de un mensaje utilizando un sistema de cifrado asimétrico de manera que la persona que posee el mensaje original y la clave pública del firmante, pueda establecer de forma segura, que dicha transformación se efectuó utilizando la clave privada correspondiente a la pública del firmante, y si el mensaje es el original o fue alterado desde su concepción.

El fin, de la firma digital, es el mismo de la firma ológrafa: dar asentimiento y compromiso con el documento firmado; y es por eso que a través de la legislación, se intenta acercarla, exigiéndose ciertos requisitos de validez.

2.4.2.1 FUNCIÓN DE UNA FIRMA DIGITAL

Primero se produce un resumen del mensaje, luego se encripta este resumen. Si se esta usando criptografía asimétrica se encripta el resumen con la clave privada.

De tal forma la única persona que conozca la clave privada será capaz de firmar digitalmente en nuestro nombre.

2.4.2.1.1 COMO COMPROBAR UNA FIRMA DIGITAL

- Se desencripta la firma digital, usando la clave publica si han utilizado un método asimétrico. Obtenemos el resumen del mensaje original.
- Hacemos un hash sobre el mensaje original.
- Comprobamos nuestro resumen con el obtenido al desencriptar y si coinciden la firma digital es valida.

2.4.2.2 VENTAJAS OFRECIDAS POR LA FIRMA DIGITAL

Gracias a la firma digital, los ciudadanos podrán realizar transacciones de comercio electrónico seguras y relacionarse con la Administración con la máxima eficacia jurídica, abriéndose por fin las puertas a la posibilidad de obtener documentos como la cédula de identidad, carnet de conducir, pasaporte, certificados de nacimiento, o votar en los próximos comicios cómodamente desde su casa.

Ahora bien, en un contexto electrónico, en el que no existe contacto directo entre las partes, ¿resulta posible que los usuarios de un servicio puedan presentar un documento digital que ofrezca las mismas funcionalidades que los documentos físicos, pero sin perder la seguridad y confianza de que estos últimos están dotados? La respuesta, por fortuna, es afirmativa, ya que el uso de la firma digital va a satisfacer los siguientes aspectos de seguridad:

- Integridad de la información: la integridad del documento es una protección contra la modificación de los datos en forma intencional o accidental. El emisor protege el documento, incorporándole a ese un valor de control de integridad, que corresponde a un valor único, calculado a partir del contenido del mensaje al momento de su creación. El receptor deberá efectuar el mismo cálculo sobre el documento recibido y comparar el valor calculado con el enviado por el emisor. De coincidir, se concluye que el documento no ha sido modificado durante la transferencia.

- Autenticidad del origen del mensaje: este aspecto de seguridad protege al receptor del documento, garantizándole que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo alguna otra entidad suplantar a un usuario del sistema. Esto se logra mediante la inclusión en el documento transmitido de un valor de autenticación (MAC, *Message autentication code*). El valor depende tanto del contenido del documento como de la clave secreta en poder del emisor.
- No repudio del origen: el no repudio de origen protege al receptor del documento de la negación del emisor de haberlo enviado. Este aspecto de seguridad es más fuerte que los anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje, transformándose en un medio de prueba inequívoco respecto de la responsabilidad del usuario del sistema.
- Imposibilidad de suplantación: el hecho de que la firma haya sido creada por el signatario mediante medios que mantiene bajo su propio control (su clave privada protegida, por ejemplo, por una contraseña, una tarjeta inteligente, etc.) asegura, además, la imposibilidad de su suplantación por otro individuo.
- Auditabilidad: permite identificar y rastrear las operaciones llevadas a cabo por el usuario dentro de un sistema informático cuyo acceso se realiza mediante la presentación de certificados,
- El acuerdo de claves secretas: garantiza la confidencialidad de la información intercambiada ente las partes, esté firmada o no, como por ejemplo en las transacciones seguras realizadas a través de SSL.

2.4.2.3 ASPECTOS TECNICOS Y LEGALES

Pensemos en aquellos programas de software que se realizaron en los años 80 con los dos primeros dígitos del campo fecha fijos ¿Cómo iba a saber el desarrollador de software que iba a dar los problemas que actualmente está dando el famoso año 2000? Entonces un ordenador no tenía ni mucho menos la potencia que las computadoras de ahora, siendo por tanto imprescindible aprovechar el mayor espacio posible tanto de memoria como de disco. Efectivamente, no habían previsto el cambio brutal que se iba a experimentar y optaron por una solución que en su tiempo evitó muchos quebraderos de cabeza. Sin embargo, en la actualidad la empresa que no

haya solucionado el problema del año 2000 tendrá problemas graves para poder continuar con su actividad empresarial, pues cuando sus sistemas informáticos se bloqueen será muy difícil encontrar a un programador que en pocos días solucione el problema, por no decir, que casi todos serán requeridos para la solución de dicho problema al mismo tiempo. Si a ello unimos la introducción del euro y la liberalización de las telecomunicaciones nos vemos ante un reto muy importante. Hay que subirse al tren por muy rápido que sea. Quizá las nuevas generaciones de abogados tengan más ventaja que otros que ya han visto pasar por sus ojos varias décadas. No obstante, es necesario por parte de todos hacer un esfuerzo por adaptarse lo mejor posible a la nueva sociedad de la tecnología.

En el contexto de nueva sociedad de la información se necesita de muchas regulaciones puesto que todo lo que esta saliendo es tan innovador que no existe siquiera una referencia legislativa. Difícil será entrar en dicha sociedad si todavía no se ha podido encontrar la forma de proteger la información. Y es aquí donde la informática y el derecho se deben unificar para consensuar entre toda la región boliviana una política legislativa común. Países como Alemania, Italia, Reino Unido, etc., vienen desarrollando sus propias legislaciones sobre firma digital, siendo por tanto imprescindible establecer una política común que nos sirviese a todos los bolivianos.

La firma digital es justificable desde el momento en que los contratos, las transacciones económicas, las compras, etc. se realizan *on-line*, es decir sin la presencia física de las partes. Surge de las tecnologías utilizadas para conseguir la confidencialidad en las comunicaciones, ante la proliferación de software que consigue pinchar las comunicaciones obteniendo la información deseada. Tal es el caso de un programa denominado satán, el cual puede recoger todo correo electrónico que lleve determinados contenidos (por ejemplo el número de una tarjeta de crédito) o determinado nombre (usuario@servidor.es). Esto quiere decir que nuestras comunicaciones por Internet están en peligro, siendo por tanto necesario realizar previsiones de seguridad lo suficientemente buenas para evitar que un ciberdelincuente haga con nuestro número de tarjeta las compras que quiera.

2.5 ALGORITMOS Y FUNCIONES HASHING

En esta parte se explicara las funciones Hash. La mayoría de la gente ha oído hablar de ellas, pero pocos tendrán claro lo que son realmente y como funcionan. Se empezará desde cero e irá aumentando su nivel progresivamente hasta lograr una descripción total de este tipo de funciones.

En informática, una función hash o algoritmo hash es una función para sumarizar o identificar probabilísticamente un gran conjunto de información, dando como resultado un conjunto imagen finito generalmente menor en tamaño que el original.

Una función hash es un algoritmo matemático que nos da un resultado B al aplicarlo a un valor inicial A. Es como cualquier función matemática, por ejemplo la función raíz cuadrada nos daría como resultado 2 si se la aplicamos al número 4. Igual que cualquier función matemática tiene que actuar de tal forma y tiene que cumplir con ciertos criterios. No nos puede devolver cualquier cosa, lo que nos devuelva requiere que tenga ciertas propiedades para que podamos usarlo.

Sea cual sea la longitud del texto base A, la longitud de su hash resultante B siempre va a ser la misma. Por ejemplo, si la longitud de la salida B esta definida en 128 bits, si aplicamos una función hash a un A de 5 bits nos dará un B de 128 bits, y si se la aplicamos a un A de 380 millones de bits, nos dará un B de 128 bits igualmente.

Para cada entrada A, la función generará una salida B única. O lo que es lo mismo, es imposible que dos textos bases A y A' tengan un mismo hash B.

Según estas dos primeras propiedades, nos damos cuenta enseguida de la utilidad de las funciones de hash.

La más inmediata es usarla para generar un resumen de algo. De hecho, estas funciones se conocen también como funciones resumen. Un ejemplo real puede ser el del típico repositorio de documentos. Si alguien quiere almacenar digamos "Las_Aventuras_Del_Ingenioso.doc" cuyo contenido es El Quijote de la mancha completo, el sistema lo primero que tiene que hacer es revisar que no está previamente ya almacenado con el mismo o con otro nombre, por ejemplo "ElQuijote.doc". El sistema puede comparar letra a letra el documento de entrada con todos los .doc de su BBDD para comprobar que no está, o puede comparar el resumen del documento de

entrada con los resúmenes de los documentos de la BBDD, opción mucho más manejable y rápida.

Además, como la salida B es única para cada A, se puede usar también para verificar la integridad de A. Podemos ver que muchos programas incluyen su hash junto con su descarga, de esta forma, podemos verificar que el programa no ha sido modificado ni le han introducido un virus o ha sido troyanizado. Si a los bytes de una aplicación A les calculo el hash B y lo adjunto, cuando alguien modifique la aplicación A, al calcular de nuevo su hash su valor habrá cambiado y será distinto de B.

Dado un texto base, es fácil y rápido (para un ordenador) calcular su número resumen.

Es imposible reconstruir el texto base a partir del número resumen.

Esto es lo que se conoce como *One-Way hash functions*. A partir del hash es imposible reconstruir el texto base.

Este es un punto que hay que aclarar. A partir del hash B es imposible sacar el texto A, quiere decir no existe forma o es computacionalmente imposible, que mediante operaciones matemáticas inversas o no a las del algoritmo de hash, se llegue desde B al texto base.

No tiene nada que ver. Con fuerza bruta le aplicamos la función de hash a diferentes textos hasta que obtenemos un hash similar al hash del texto que buscamos, con lo que por consecuencia tendremos el texto buscado.

Ejemplo de función hash.

Esto no podría tomarse como una función hash fiable porque es demasiado débil a ataques, pero sirve como ejemplo gráfico por si no ha quedado del todo claro.

Esta función hash de nuestro ejemplo lo que hace es traducir cada caracter del texto A de entrada en su equivalente código ASCII, los agrupa de 3 en 3 y les aplica la función matemática (1 - 2) * 3

E	n		u	n		l	u	g	a	r		d	e		
69	110	32	117	110	32	108	117	103	97	114	32	100	101	32	
-1312			224			-927			-544			-32			-2591
l	a		M	a	n	c	h	a		d	e		c	u	
108	97	32	77	97	110	99	104	97	32	100	101	32	99	117	
352			-2200			-485			-6868			-7839			-17040
															-19631

Fuente: Elaboración propia

Como vemos, el valor de nuestra función hash aplicada al texto base A "En un lugar de la Mancha de cu" es -19631.

Cumple la propiedad 1, con un poco más de desarrollo se puede hacer que el tamaño del hash devuelto sea siempre el mismo.

Cumple con la 2, el valor del hash es único para cada texto. Si modificamos lo más mínimo la frase, el valor cambia.

Cumple con la 3 ya que es inmediato sacar el resultado y con la 4, ya que a partir del -19631 no se puede llegar al texto.

2.5.1 SIN COLISIONES

Según la primera característica que hemos visto de las funciones hash, que nos dice que el tamaño del hash B resultante de A es siempre el mismo, deducimos que no puede cumplirse la segunda característica, que dice que el hash B tiene que ser único para cada A.

Por ejemplo, la función MD5 nos devuelve un hash de 128 bits. Para que cada hash equivalga a un único texto base, tendría que existir solamente un texto por cada combinación del hash devuelto, o sea, tendría que haber solamente 2^128 textos distintos, lo cual no es cierto. Como textos distintos hay infinitos, podemos decir que hay infinitas posibilidades de que dos textos tengan el mismo hash. Lo cual es conocido como colisiones.

La fortaleza de una función hash requiere que estas colisiones sean las mínimas posibles y que encontrarlas sea lo más difícil posible.

2.5.2 PROPIEDADES DE UNA FUNCION HASH CON RESPECTO A LAS COLISIONES

Las propiedades que deben de tener las primitivas hash son:

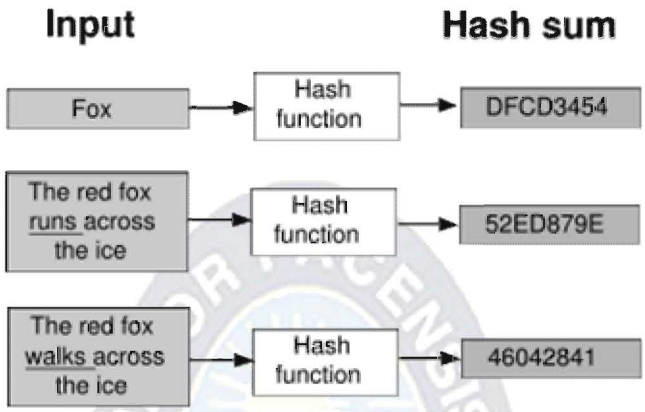
a) Resistencia a la preimagen: One *Way Hash Function*. Como hemos dicho antes, significa que dada cualquier imagen, es computacionalmente imposible encontrar un mensaje x tal que h(x)=y. Otra forma como se conoce esta propiedad es que h sea de un solo sentido.
b) Resistencia a segunda preimagen: OWHF: Weak One Way Hash Function. Significa que dado x, es computacionalmente imposible encontrar una x' tal que h(x)=h(x'). Otra forma de conocer esta propiedad es que h sea resistente a una colisión suave.
c) Resistencia a colisión: CRHF: Strong One Way Hash Function. Significa que es computacionalmente imposible encontrar dos diferentes mensajes x, x' tal que h (x)=h (x'). Esta propiedad también se conoce como resistencia a colisión fuerte. Tomando en cuenta un escenario de firma digital.
Un documento X se adjunta con su firma, que consiste en calcular el hash de X, h(X), y en cifrarlo, C(h(X)) con la clave privada del remitente o propietario.
Para verificar la integridad de X, el destinatario o la persona correspondiente descifra con la clave pública del propietario el C(h(X)) para obtener el h(X) inicial, calcula de nuevo el h(X) del documento y los compara. Si el h(X) inicial es igual al h(X) nuevo es que ese documento no ha sido modificado y que pertenece al firmante.

Si esa función de hash no tiene resistencia a una 2ª preimagen, un atacante C que podría encontrar un mensaje X' tal que h(X') = h(X), y reclamar que el documento firmado no es X sino X'.

Sea que C tiene que presentar para firmar por un tercero un documento X, y a la vez redacta otro documento Y. Si la función hash no tiene resistencia a las colisiones, C puede añadir información basura a X e Y (X' e Y') de forma que h(X+X') = h(Y+Y'). Entonces el que firme X también está firmando Y.

Por último si (e,n) es la clave pública RSA de A, C puede elegir aleatoriamente un y, y

calcular z = ye mod n, y reclamar que y es la firma de z, si C puede encontrar una preimagen x tal que z = h(x), donde x es importante para A. Esto es evitable si h es resistente a preimagen.



Fuente: Elaboración propia

Una función de hash en funcionamiento.

3.1 INTRODUCCION

La encriptación es la única forma eficiente de transmitir información confidencial por Internet. El objetivo de la encriptación es garantizar la confidencialidad, integridad e irrefutabilidad de la información. El objetivo es desarrollar y aplicar mecanismos de encriptación que no puedan detectarse ni piratearse teóricamente. Estos métodos se llaman "métodos de encriptación de alto nivel".

La operación de cifrado consiste en algoritmos matemáticos complejos en los que la clave es una cifra larga. La fuerza de la encriptación depende de la longitud de la clave, es decir, el número de bits que tiene el número. Es imposible piratear un código mediante métodos técnicos si la clave utilizada es lo suficientemente larga.

La mayoría de algoritmos de encriptación son públicos, pero no pueden utilizarse para descubrir la clave utilizada para codificar un mensaje. El hecho de que los algoritmos sean públicos no significa que puedan utilizarse gratis. La mayoría de algoritmos de encriptación están patentados y hay que pagar una tarifa para poder utilizarlos. Los algoritmos se utilizan también como base para otras aplicaciones, aparte de las de encriptación.

Los algoritmos públicos han pasado por un riguroso proceso de comprobación cuando se han intentado descifrar. Un algoritmo puede considerarse seguro si nadie ha podido descifrarlo en un período de unos cuantos años. Es por esta razón que los algoritmos públicos se consideran más seguros que los algoritmos secretos y no sometidos a comprobación.

3.2 ALGORITMO MD-5 (Algoritmo de Resumen del Mensaje 5)

3.2.1 HISTORIA

MD5 es uno de los algoritmos de reducción criptográficos diseñados por el profesor Ronald Rivest del MIT (*Massachusetts Institute of Technology*, Instituto Tecnológico de Massachusetts). Fue desarrollado en 1991 como reemplazo del algoritmo MD4 después de que Hans Dobbertin descubriese su debilidad.

A pesar de su amplia difusión actual, la sucesión de problemas de seguridad detectados desde que, en 1996, Hans Dobbertin anunciase una colisión de hash plantea una serie de dudas acerca de su uso futuro.

3.2.2 CODIFICACION

La codificación del MD5 de 128 bits es representada típicamente como un número de 32 dígitos hexadecimal. El siguiente código de 28 bytes ASCII será tratado con MD5 y veremos su correspondiente hash de salida:

MD5 ("Esto sí es una prueba de MD5") = e99008846853ff3b725c27315e469fbc

Un simple cambio en el mensaje nos da un cambio total en la codificación hash, en este caso cambiamos dos letras, el «sí» por un «no».

MD5 ("Esto no es una prueba de MD5") = dd21d99a468f3bb52a136ef5beef5034

Otro ejemplo sería la codificación de un campo vacío:

MD5 ("") = d41d8cd98f00b204e9800998ecf8427e

3.2.3 ALGORITMO

- Terminologías y notaciones

En este documento "palabra" es una entidad de 32 bits y byte es una entidad de 8 bits. Una secuencia de bits puede ser interpretada de manera natural como una secuencia de bytes, donde cada grupo consecutivo de ocho bits se interpreta como un byte con el bit más significativo al principio. Similarmente, una secuencia de bytes puede ser interpretada como una secuencia de 32 bits (palabra), donde cada grupo consecutivo de cuatro bytes se interpreta como una palabra en la que el byte menos significativo está al principio.

El símbolo "+" significa suma de palabras.
X <<< s se interpreta por un desplazamiento a la izquierda 's' posiciones
Not (x) se entiende como el complemento de x

- Descripción del algoritmo md5

Para empezar se supone que se tiene un mensaje de 'b' bits de entrada, y se desea encontrar su resumen. Aquí 'b' es un valor arbitrario entero no negativo, pero puede ser cero, no tiene por qué ser múltiplo de ocho, y puede ser muy largo. Imaginemos los bits del mensaje escritos así:

m0 m1... m {b-1}

Los siguientes cinco pasos son efectuados para calcular el resumen del mensaje.

Paso 1. Añadiendo bits

El mensaje será extendido hasta que su longitud en bits sea congruente con 448, módulo 512. Esto es, si se le resta 448 a la longitud del mensaje tras este paso, se obtiene un múltiplo de 512. Esta extensión se realiza siempre, incluso si la longitud del mensaje es ya congruente con 448, módulo 512.

La extensión se realiza como sigue: un sólo bit "1" se añade al mensaje, y después bits "0" se añaden hasta que la longitud en bits del mensaje extendido se haga congruente con 448, módulo 512. En todos los mensajes se añade al menos un bit y como máximo 512.

Paso 2. Longitud del mensaje

Un entero de 64 bits que represente la longitud 'b' del mensaje (longitud antes de añadir los bits) se concatena al resultado del paso anterior. En el supuesto no deseado de que 'b' sea mayor que 2^64, entonces sólo los 64 bits de menor peso de 'b' se usarán.

En este punto el mensaje resultante (después de rellenar con los bits y con 'b') se tiene una longitud que es un múltiplo exacto de 512 bits. A su vez, la longitud del mensaje es múltiplo de 16 palabras (32 bits por palabra). Con M[0 ... N-1] denotaremos las palabras del mensaje resultante, donde N es múltiplo de 16.

Paso 3. Inicializar el búfer MD

Un búfer de cuatro palabras (A, B, C, D) se usa para calcular el resumen del mensaje. Aquí cada una de las letras A, B, C, D representa un registro de 32 bits. Estos registros se inicializan con los siguientes valores hexadecimales, los bits de menor peso primero:

palabra A: 01 23 45 67
palabra B: 89 ab cd ef
palabra C: fe dc ba 98
palabra D: 76 54 32 10

Paso 4. Procesado del mensaje en bloques de 16 palabras

Primero definimos cuatro funciones auxiliares que toman como entrada tres palabras de 32 bits y su salida es una palabra de 32 bits.

$$F(X,Y,Z) = (X \wedge Y) \vee (\neg X \wedge Z)$$
$$G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge \neg Z)$$
$$H(X,Y,Z) = X \oplus Y \oplus Z$$
$$I(X,Y,Z) = Y \oplus (X \vee \neg Z)$$

Los operadores $\oplus, \wedge, \vee, \neg$ son las funciones XOR, AND, OR y NOT respectivamente.

En cada posición de cada bit F actúa como un condicional: si X, entonces Y sino Z. La función F podría haber sido definida usando + en lugar de v ya que XY y not(x) Z nunca tendrán unos ('1') en la misma posición de bit. Es interesante resaltar que si los bits de X, Y y Z son independientes y no sesgados, cada uno de los bits de F(X,Y,Z) será independiente y no sesgado.

Las funciones G, H e I son similares a la función F, ya que actúan "bit a bit en paralelo" para producir sus salidas de los bits de X, Y y Z, en la medida que si cada bit correspondiente de X, Y y Z son independientes y no sesgados, entonces cada bit de G(X,Y,Z), H(X,Y,Z) e I(X,Y,Z) serán independientes y no sesgados. Nótese que la función H es la comparación bit a bit "xor" o función "paridad" de sus entradas.

Este paso usa una tabla de 64 elementos T[1 ... 64] construida con la función Seno. Denotaremos por T[i] el elemento i-ésimo de esta tabla, que será igual a la parte entera del valor absoluto del seno de 'i' 4294967296 veces, donde 'i' está en radianes.

Código del MD5:

```
 /* Procesar cada bloque de 16 palabras. */
para i = 0 hasta N/16-1 hacer

  /* Copiar el bloque 'i' en X. */
  para j = 0 hasta 15 hacer
    hacer X[j] de M[i*16+j].
  fin para /* del bucle 'j' */

/* Guardar A como AA, B como BB, C como CC, y D como DD. */
AA = A
BB = B
CC = C
DD = D

/* Ronda 1. */
/* [abcd k s i] denotarán la operación
     a = b + ((a + F(b, c, d) + X[k] + T[i]) <<< s). */
/* Hacer las siguientes 16 operaciones. */
[ABCD  0  7  1] [DABC  1 12  2] [CDAB  2 17  3] [BCDA  3 22  4]
[ABCD  4  7  5] [DABC  5 12  6] [CDAB  6 17  7] [BCDA  7 22  8]
[ABCD  8  7  9] [DABC  9 12 10] [CDAB 10 17 11] [BCDA 11 22 12]
[ABCD 12  7 13] [DABC 13 12 14] [CDAB 14 17 15] [BCDA 15 22 16]

/* Ronda 2. */
/* [abcd k s i] denotarán la operación
    a = b + ((a + G(b, c, d) + X[k] + T[i]) <<< s). */
/* Hacer las siguientes 16 operaciones. */
[ABCD  1  5 17] [DABC  6  9 18] [CDAB 11 14 19] [BCDA  0 20 20]
[ABCD  5  5 21] [DABC 10  9 22] [CDAB 15 14 23] [BCDA  4 20 24]
```

[ABCD 9 5 25] [DABC 14 9 26] [CDAB 3 14 27] [BCDA 8 20 28]
[ABCD 13 5 29] [DABC 2 9 30] [CDAB 7 14 31] [BCDA 12 20 32]

/* Ronda 3. */
/* [abcd k s t] denotarán la operación
a = b + ((a + H(b, c, d) + X[k] + T[i]) <<< s). */
/* Hacer las siguientes 16 operaciones. */
[ABCD 5 4 33] [DABC 8 11 34] [CDAB 11 16 35] [BCDA 14 23 36]
[ABCD 1 4 37] [DABC 4 11 38] [CDAB 7 16 39] [BCDA 10 23 40]
[ABCD 13 4 41] [DABC 0 11 42] [CDAB 3 16 43] [BCDA 6 23 44]
[ABCD 9 4 45] [DABC 12 11 46] [CDAB 15 16 47] [BCDA 2 23 48]

/* Ronda 4. */
/* [abcd k s t] denotarán la operación
a = b + ((a + I(b, c, d) + X[k] + T[i]) <<< s). */
/* Hacer las siguientes 16 operaciones. */
[ABCD 0 6 49] [DABC 7 10 50] [CDAB 14 15 51] [BCDA 5 21 52]
[ABCD 12 6 53] [DABC 3 10 54] [CDAB 10 15 55] [BCDA 1 21 56]
[ABCD 8 6 57] [DABC 15 10 58] [CDAB 6 15 59] [BCDA 13 21 60]
[ABCD 4 6 61] [DABC 11 10 62] [CDAB 2 15 63] [BCDA 9 21 64]

/* Ahora realizar las siguientes sumas. (Este es el incremento de cada
uno de los cuatro registros por el valor que tenían antes de que
este bloque fuera inicializado.) */

A = A + AA
B = B + BB
C = C + CC
D = D + DD
fin para /* del bucle en 'i' */

Paso 5. Salida

El resumen del mensaje es la salida producida por A, B, C y D. Esto es, se comienza el byte de menor peso de A y se acaba con el byte de mayor peso de D.

3.2.4 Seguridad

A pesar de haber sido considerado criptográficamente seguro en un principio, ciertas investigaciones han revelado vulnerabilidades que hacen cuestionable el uso futuro del MD5. En agosto del 2004, Xiaoyun Wang, Dengguo Feng, Xuejia Lai y Hongbo Yu anunciaron el descubrimiento de colisiones de hash para MD5. Su ataque se consumó en una hora de cálculo con un clúster IBM P690.

Aunque dicho ataque era analítico, el tamaño del hash (128 bits) es lo suficientemente pequeño como para que resulte vulnerable frente a ataques de 'fuerza bruta' tipo 'cumpleaños' (Ataque de cumpleaños). El proyecto de computación distribuida MD5CRK arrancó en marzo del 2004 con el propósito de demostrar que MD5 es inseguro frente a uno de tales ataques, aunque acabó poco después del aviso de la publicación de la vulnerabilidad del equipo de Wang.

Debido al descubrimiento de métodos sencillos para generar colisiones de hash, muchos investigadores recomiendan su sustitución por algoritmos alternativos tales como SHA-1 o RIPEMD-160.

3.3.5 APLICACIONES

Los resúmenes MD5 se utilizan extensamente en el mundo del software para proporcionar la seguridad de que un archivo descargado de Internet no se ha alterado. Comparando una suma MD5 publicada con la suma de comprobación del archivo descargado, un usuario puede tener la confianza suficiente de que el archivo es igual que el publicado por los desarrolladores. Esto protege al usuario contra los 'Caballos de Troya' o 'Troyanos' y virus que algún otro usuario malicioso pudiera incluir en el software. La comprobación de un archivo descargado contra su suma MD5 no detecta solamente los archivos alterados de una manera maliciosa, también reconoce una descarga corrupta o incompleta.

Para comprobar la integridad de un archivo descargado de Internet se puede utilizar una herramienta MD5 para comparar la suma MD5 de dicho archivo con un archivo MD5SUM con el resumen MD5 del primer archivo. En los sistemas UNIX, el comando de md5sum es un ejemplo de tal herramienta. Además, también está implementado en el lenguaje de scripting PHP como MD5("") entre otros.

En sistemas UNIX y GNU/Linux se utiliza el algoritmo MD5 para cifrar las claves de los usuarios. En el disco se guarda el resultado del MD5 de la clave que se introduce al dar de alta un usuario, y cuando éste quiere entrar en el sistema se compara la entrada con la que hay guardada en el disco duro, si coinciden, es la misma clave y el usuario será autenticado. He ahí el problema de encontrar y generar colisiones de hash a voluntad.

El MD5 también se puede usar para comprobar que los correos electrónicos no han sido alterados usando claves públicas y privadas.

3.3 ALGORITMO SHA-1 (Algoritmo de Hash Seguro)

SHA-1 ha sido examinado muy de cerca por la comunidad criptográfica pública, y no se ha encontrado ningún ataque efectivo. No obstante, en el año 2004, un número de ataques significativos fueron divulgados sobre funciones criptográficas de hash con una estructura similar a SHA-1; lo que ha planteado dudas sobre la seguridad a largo plazo de SHA-1.

SHA-0 y SHA-1 producen una salida resumen de 160 bits de un mensaje que puede tener un tamaño máximo de 2^{64} bits, y se basa en principios similares a los usados por el profesor Ronald L. Rivest del MIT en el diseño de los algoritmos de resumen de mensaje MD4 y MD5.

La codificación hash vacía para SHA-1 corresponde a:

SHA1("") = da39a3ee5e6b4b0d3255bfef95601890afd80709

3.3.1 ATAQUES CONTRA SHA-1

La resistencia del algoritmo SHA-1 se ha visto comprometida a lo largo del año 2005. Después de que MD5, entre otros, quedara seriamente comprometido en el 2004 por parte de un equipo de investigadores chinos, el tiempo de vida de SHA-1 quedó visto para sentencia.

El mismo equipo de investigadores chinos, compuesto por Xiaoyun Wang, Yiqun Lisa Yin y Hongbo Yu (principalmente de la Shandong University en China), ha demostrado

que son capaces de romper el SHA-1 en al menos 2^{69} operaciones, unas 2000 veces más rápido que un ataque de fuerza bruta (que requeriría 2^{80} operaciones). Los últimos ataques contra SHA-1 han logrado debilitarlo hasta 2^{63}.

Este ataque es de particular importancia para las aplicaciones que usan firmas digitales tales como marcas de tiempo y notarías. Sin embargo, muchas aplicaciones que usan firmas digitales incluyen información sobre el contexto que hacen este ataque difícil de llevar a cabo en la práctica.

A pesar de que 2^{63} suponen aún un número alto de operaciones, se encuentra dentro de los límites de las capacidades actuales de cálculos, y es previsible que con el paso del tiempo romper esta función sea trivial, al aumentar las capacidades de cálculo y al ser más serios los ataques contra SHA-1.

La importancia de la rotura de una función hash se debe comprender de la siguiente manera: Un hash permite crear una huella digital, en teoría única, de un archivo. Si un hash fuese roto podría haber otro documento con la misma huella. La inicial similitud propuesta con la equivalencia a que hubiese personas que compartiesen las mismas huellas digitales, o peor aún, el mismo ADN no es adecuado pues, aunque fuera trivial encontrar dos ficheros con el mismo resumen criptográfico ello no implicaría que los ficheros fueran congruentes en el contexto adecuado. Siguiendo con la hipótesis de la similitud biométrica de dos personas, sería el equivalente a necesitar modificar el número de brazos en una persona para que su impresión dactilar fuera igual a la de otra.

A pesar de que el NIST contempla funciones de SHA de mayor tamaño (por ejemplo, el SHA-512, de 512 bits de longitud), expertos de la talla de Bruce Schneier abogan por, sin llamar a alarmismos, buscar una nueva función hash estandarizada que permita sustituir a SHA-1. Los nombres que se mencionan al respecto son Tiger, de los creadores de Serpent, y WHIRLPOOL, de los creadores de AES.

3.4 DEMOSTRACION DE LA SEGURIDAD HASHING

En primer lugar, se abordara forma sencilla este concepto para hacerlo entendible. Un HASH no es más que un número resumen. De hecho, en muchos sitios Web se puede

encontrar expresiones como "*checksum MD5*", lo que literalmente se traduce por "suma de comprobación". Así, el concepto no es complicado, pero sí su implementación. Pongamos un ejemplo: supongamos que tenemos un fichero cualquiera. Pues bien, si consideramos dicho fichero como un flujo de bits y le aplicamos un algoritmo de HASH lo que obtenemos es otro conjunto de bits (de longitud fija y que depende del número de bits de salida del algoritmo o función que utilicemos) que depende bit a bit del contenido del flujo original de bits que sirvió como entrada al algoritmo.

Además, cumplen las siguientes propiedades:

- Todos los HASH generados con una función de hash tienen el mismo tamaño, sea cual sea el mensaje utilizado como entrada.
- Dado un mensaje, es fácil y rápido mediante un ordenador calcular su HASH.
- Es imposible reconstruir el mensaje original a partir de su HASH.
- Es imposible generar un mensaje con un HASH determinado.

Es decir, un algoritmo de HASH no es un algoritmo de encriptación, aunque sí se utiliza en esquemas de cifrado, como algoritmos de cifrado asimétrico (por ejemplo en el RSA).

Ahora bien, tener una función de con dichas características puede tener muchas aplicaciones. Algunas de ellas pueden ser las siguientes:

- Comprobación de integridad de ficheros: Supongamos que queremos transmitir un fichero a un amigo. Si antes de realizar este envío calculamos la función HASH del fichero, para nuestro amigo del otro extremo es posible verificar la integridad del fichero aplicando el mismo algoritmo al archivo que recibe. Si ambos coinciden, podemos asegurar que el envío ha sido satisfactorio. Ésta es una aplicación real que se utiliza, por ejemplo, para comprobar la integridad de muchos paquetes que se descargan en distribuciones del sistema operativo GNU/Linux.

- Seguridad en procesos de identificación en sistemas: Los procesos de identificación *(Login+Password)* se ven reforzados por estos algoritmos. Se utilizan de la siguiente forma: cuando un usuario accede a su computadora debe introducir su nombre de usuario y su *password*. Pues bien, si el sistema operativo no registra estos datos como "texto claro", si no que registra el resultado de aplicarles una función HASH, en el caso de que un usuario malicioso logre acceder a nuestro archivo de registros no conseguirá (a menos que el algoritmo utilizado sea malo o disponga de una supercomputadora) revertir el contenido de dicho registro, y por tanto no puede acceder a nuestro sistema. Esta misma idea se aplica en identificación de usuarios en muchas webs, con la diferencia de que para que el esquema sea seguro debe incluir información adicional y "aleatoria", como marcas de tiempo y redundancias.

- Firma digital: los algoritmos hashing se utilizan en esquemas de firma digital para verificar la integridad de la información enviada por el canal de comunicaciones. Algoritmos de cifrado asimétrico, como RSA por ejemplo, realizan lo siguiente: calculan la función HASH del contenido del mensaje que se va a enviar y luego se firma dicho *checksum* con la clave privada del emisor. Así se asegura la integridad de la información y el "no repudio".

SHA-1 (*Secure Hash Algorithm 1 o* Algoritmo de Hash Seguro 1): El SHA-1 toma como entrada un mensaje de longitud máxima 2^{64} bits (más de dos mil millones de *Gigabytes*) y produce como salida un resumen de 160 bits. Este número es mayor que el que se utilizaba en el algoritmo SHA original, 128 bits. Ya existen nuevas versiones de SHA que trabajan con resúmenes de 224, 256,384 e incluso 512 bits.

En realidad, lo seguros o inseguros que los algoritmos sean no depende de los conocimientos informáticos o telemáticos que uno tenga, sino de sus conocimientos matemáticos. El objetivo de la investigación es demostrar por dónde cojean los algoritmos de HASH, la dificultad computacional que presentan, y qué soluciones se dan a los posibles ataques que puedan sufrir.

Desde el año 2004 aproximadamente, cuando saltaron las primeras noticias escandalosas sobre la ruptura de MD5, la seguridad que ofrecen los algoritmos de HASH a nuestros esquemas de cifrado ha sido una cuestión que se ha puesto en

entredicho. ¿Qué seguridad ofrecen estos algoritmos? ¿Resulta computacionalmente complejo romper uno de estos algoritmos? ¿Qué solución se debe adoptar? se demostrara la seguridad de hash para responder este tipo de cuestionamientos intentando resolver los cuestionamientos.

Ahora una descripción algo más matemática de lo que es una función HASH. Supongamos que tenemos un mensaje a, al que aplicamos una función resumen a la que llamaremos h. Decimos entonces que el resultado de esta operación, al que llamaremos b es el HASH de a. Es decir:

$$b = h(a)$$

Esta función debe ser sencilla de realizar para un computador, pero debe ser computacionalmente imposible realizar la operación inversa, al menos para usuarios normales.

Además, esta función tiene otra característica: el tamaño de la entrada no es de longitud fija, puede ser de longitud variable. Esto tiene la siguiente consecuencia, que no se demostrará matemáticamente, pero que asumiremos por razonado. Es posible que dos mensajes de entrada a produzcan el mismo mensaje de salida b. Es decir, es posible encontrar un mensaje c, tal que:

$$b = h(c)$$

Sin embargo, encontrar ese mensaje debe ser, al igual que la particularidad antes mencionada, muy complejo desde el punto de vista computacional. Para los algoritmos de HASH esto es lo que se conoce como colisión: que dos mensajes de entrada produzcan el mismo mensaje de salida.

Así, a priori, se puede establecer dos posibles vulnerabilidades de las funciones HASH:

- Que sea posible realizar la operación:

$$A = h^{-1}(b)$$

  Habitualmente, a la operación de invertir la función HASH comprobando todas las posibilidades para los bits de salida se le llama ataque de fuerza bruta. Esto

es lo que debe ser computacionalmente impracticable. Supondría aplicar la función HASH 2^n veces hasta encontrar la coincidencia (n es el número de bits de salida de la función).

- Que se hallen colisiones:

$$b = h(a) \text{ y } b = h(c), \text{ a distinto de c}$$

Lo que antes hemos denominado colisión.

Estas dos posibles debilidades dan lugar a cuatro tipos de ataques:

- Ataque Tipo 1: El atacante es capaz de encontrar dos mensajes al azar que colisionan pero es incapaz de hacerlo de forma sistemática. Si es capaz de dar sólo con dos mensajes que provocan colisión, esta no es razón suficiente para tildar el algoritmo de ineficiente. Índice de peligrosidad: *

- Ataque Tipo 2: El atacante es capaz de generar dos mensajes distintos de forma que sus HASH colisionen, pero sin saber a priori qué hash resultará. Es decir, el atacante no podría generar "queriendo" el HASH que necesite para fines maliciosos. Índice de peligrosidad: **

- Ataque Tipo 3: El atacante es capaz de construir un mensaje sin sentido de forma que su HASH colisione con el de un mensaje con sentido. Si éste es el caso, el agente malicioso puede atacar algoritmos de encriptación asimétricos con firma digital, haciendo que se firmen mensajes sin sentido, y que el destinatario los acepte como fidedignos. Índice de peligrosidad: ***

- Ataque Tipo 4: El atacante es capaz de crear un segundo mensaje falso que tiene sentido y cuyo hash colisiona con el del mensaje verdadero. En este caso, el atacante puede actuar con total impunidad, puede falsificar certificados, firmar mensajes etc. El resultado sería desastroso. Índice de peligrosidad: ****.

El problema entonces es el siguiente: ¿cómo de difícil es encontrar una solución? ¿Qué ataques reales son practicables? ¿Qué se gana incrementando el número de bits de salida del algoritmo?

En primer lugar, responderemos a la última pregunta. Si aumentamos el número de bits de salida del algoritmo, el ataque de fuerza bruta será más impracticable y también lo será encontrar los mensajes que colisionen, pues teóricamente se cumple que para confiar en que podemos encontrar dos mensajes que colisionen no hay que realizar 2^n operaciones, si no sólo $2^{n/2}$.

Realicemos algunos cálculos para realizar ataques de fuerza bruta:

- Para una clave de 12 dígitos, escrita con un teclado con 97 caracteres (base 97), habría que realizar (esto no tiene nada que ver con los algoritmos de HASH):

$$97^{12} = 693.842.360.995.438.000.295.041 \text{ comprobaciones.}$$

- Para MD5, la salida es de 128 bits, sería necesario realizar:

$$2^{128}=3'402823669 * 10^{38} \text{ operaciones.}$$

Trabajemos ahora con los ataques basados en búsqueda de colisiones:

- Para MD5, la salida es de 128 bits, luego hay que operar sobre la mitad de bits, y sería necesario realizar:

$$2^{64}=18.446.744.073.709.551.616 \text{ operaciones.}$$

- Para el algoritmo SHA 1, cuya salida es de 160 bits:

$$2^{80}=1.208.925.819.614.629.174.706.176 \text{ operaciones.}$$

  Curiosidad: 1.000.000 de ordenadores capaces de procesar en 1 µs cada operación tardarían más de 38.000 años en las 2^{80} operaciones.

Y para los más desconfiados e incluso paranoicos: ¿qué hay de las supercomputadoras y de la gente que sí dispone de los medios necesarios? Cuando saltaron las primeras alarmas sobre estos algoritmos, hace unos dos años, las cifras eran las siguientes:

- Para romper el SHA-0 completo se ha requerido un supercomputador de BULL de 256 procesadores durante unos 9 años de proceso, pero al supercomputador que está instalando IBM en la UPC (Barcelona) sólo le costaría del orden de 1 año.

- Los investigadores, Wang, Feng, Lai, y Yu han reportado haberlo conseguido con una complejidad aproximadamente 2000 veces menor (240 en vez de 251). Esta reducción equivaldría a una necesidad de cálculo de algo menos de 1 día, si la relación fuese lineal, pero los mismos investigadores han reportado necesitar sólo 1 día con un IBM P690 en cluster, para romper el MD5, que tiene una complejidad equivalente.

Lo habitual es que este tipo de usuarios realicen ataques basados en diccionarios, como la aplicación para Ñu/Linux John the Ripper. Este tipo de aplicaciones tiene una base de datos con claves comunes, que prueban sobre los sistemas a los que queremos acceder (por ejemplo Sistemas basados en UNIX donde se almacenan los resúmenes HASH del nombre de usuario y su clave para autenticar).

La otra forma es encontrar una colisión, suponiendo que así fuera que, con un computador se hallaría una colisión. En otras palabras un mensaje A genera una clave C, y un mensaje B genera la misma clave C, la debilidad en tal caso "inseguridad de los códigos" seria de orden lógico ya que el mensaje A y B no se parecerían en nada. Si de alguna manera se quisiera utilizar colisiones para realizar actos delictivos seria inútil ya que mientras mas se parezcan los mensajes la probabilidad de colisión es mas baja. De que serviría haber encontrado la manera de generar mensajes que produzcan las mismas claves si en un orden lógico seria simple de detectarlo. Los datos, si bien son información, ordenados de una manera lógica para el receptor, no siempre podemos decir que los datos son información. se puede tener un montón de datos que solo son basura en el computador, así es que pasando a un nivel mas alto que solo el de datos, sino el de información, que se debe a una sintaxis, lógica etc. Claramente se puede deducir que: Al romper la seguridad de un hash hablando al nivel de datos, seria computacionalmente, por ahora, dificultoso romper su seguridad en un orden lógico ya que a simple vista se notaria que fue manipulado o modificado. Teniendo aun el resumen que el receptor quiso que el emisor reciba

De tal manera queda demostrado que el rompimiento de la seguridad de los algoritmos hash es muy poco probable, lo que nos brinda un grado alto de confianza en la firma digital.

4.1 INTRODUCCION

Hoy por hoy el contrato digital es conocido y utilizado en muchas partes del mundo, lo que hizo posible crear toda una estructura alrededor del tema, además de dar la oportunidad a estudiantes e investigadores de estudiarlo.

4.2 PARTES DEL CONTRATO ELECTRONICO

El contrato electrónico se divide en dos partes:

- Documento digital, es aquella parte la cual es diseñada entre el contratante y el contratado de manera que las dos partes tienen responsabilidades y obligaciones. El documento tiene que regirse a las leyes en el país o región que es elaborado, se sabe que las leyes a nivel mundial no son las mismas, en contraste la contratación electrónica permite derrumbar las fronteras. Por lo tanto el requerimiento al cual se sujeta el contrato es haber sido realizado digitalmente.
- La firma digital, es la encriptación del contrato digital dándole la seguridad necesaria para viajar a través de la autopista de la información

4.3 ELABORACION DEL DOCUMENTO DIGITAL

4.3.1 DEFINICION

El Código civil da del contrato una definición tomada de POTHIER: "El contrato es una convención por la cual una o más personas se obligan, hacia otra o varias más, a dar, a hacer o a no hacer, alguna cosa"

4.3.2 ASPECTOS LEGALES DEL DOCUMENTO

En el lenguaje corriente se emplean como sinónimos de contrato otros dos términos: acto jurídico y convención; pero, en el lenguaje del derecho, cada una de esas palabras posee, o debería poseer, un sentido técnico preciso.

El acto jurídico es toda manifestación de voluntad que tenga por fin producir un efecto jurídico, modificar una situación jurídica. Dicha manifestación de voluntad es unas veces unilateral (por ejemplo, el testamento): existe entonces un acto unilateral; otras veces consiste en un acuerdo: entonces hay convención.

La convención es; pues, una categoría particular de actos jurídicos. AUBRY y RAU la definieron: como "un acuerdo de dos o más voluntades sobre un objeto de interés jurídico"; es decir, un acuerdo que tenga por objeto modificar una situación jurídica: crear, extinguir o modificar un derecho.

El contrato es una convención generadora de derecho. El contrato es, por consiguiente, una especie particular de convención. La compraventa es un contrato, porque crea un derecho para el comprador y el vendedor. La remisión de una deuda, acto por el cual un acreedor dispensa del cumplimiento a su deudor, es una convención. La terminología no siempre se respeta rigurosamente, incluso en el Código civil, donde la palabra convención se utiliza con frecuencia como sinónimo de contrato.

4.3.2.1 EL CONSENSUALISMO Y EL EFECTO RELATIVO DEL CONTRATO

¿Cómo engendra el contrato un derecho personal, una obligación? Por el acuerdo de las voluntades. Pero no siempre ha sido así: en las civilizaciones arcaicas, la voluntad por sí sola era impotente para crear obligaciones; era preciso encajarla dentro de ciertas formas; la forma era la eficaz, no la voluntad. Hoy en día, por el contrario, y pese a un sensible retorno al formalismo, la creación de las obligaciones permanece regida por la regla "solus consensus obligat" (el solo consentimiento obliga).

El contrato no liga sino a las partes contratantes: no crea ninguna obligación con cargo a terceros. El principio del efecto relativo del contrato era conocido por los derechos formalistas, como lo es por los derechos consensualistas. Cuando la creación de obligaciones encontraba su origen en ciertos ritos, en formalidades, tan sólo se hallaban enlazadas las personas que se habían plegado a los ritos. Fundado sobre la voluntad, el contrato no puede tener además sino un efecto relativo; la obligación, por constituir un atentado contra la libertad individual, no pesa sobre el individuo más que

si ha consentido en ella, si la ha aceptado libremente. Las restricciones aportadas a la autonomía de la voluntad, como consecuencia de la evolución social, han llevado consigo múltiples excepciones al principio de la relatividad de los contratos; por ejemplo, la voluntad de algunas personas que fijan las condiciones de las convenciones colectivas de trabajo obligan a todos los miembros de la profesión.

4.3.2.2 EL DOBLE EFECTO DEL CONTRATO

Ha sido puntualizada la evolución que ha hecho del contrato puramente generador de obligaciones un acto susceptible de transmitir, por sí solo, los derechos reales. El Código civil afirma el doble efecto del contrato, "obligatorio" y "real. El aspecto "obligatorio" será el único examinado en la teoría general del contrato; el aspecto "real" del contrato será estudiado con los modos de adquirir la propiedad.

4.3.2.3 LAS OBLIGACIONES NACIDAS DEL CONTRATO

Numerosas son las obligaciones que unen a los hombres que viven en sociedad. Algunas son puramente morales; otras, solamente mundanas; ni las unas ni las otras ligan al individuo en el terreno jurídico. Los ingleses poseen un término para designar las convenciones que no crean obligaciones jurídicas, pero que se imponen no obstante en conciencia o en el plano de la corrección: gentlemen's agreement (acuerdo de caballeros). Semejantes obligaciones no nacen de un contrato. En efecto, el contrato crea obligaciones jurídicas, es decir, sancionadas por el derecho.

La frontera entre el contrato y el gentlemen's agreement resulta a veces difícil de determinar: entonces no puede precisarse más que averiguando la voluntad de las partes. Así, ¿el benévolo automovilista que cede a los requerimientos del que desea viajar en un auto particular concluye un contrato con ese pasajero? Se ha querido ver en ese gesto de cortesía un contrato innominado a título gratuito; pero parece que el automovilista no contrae obligación alguna; ¿la prueba no está en que tiene libertad para indicarle a su pasajero, en el curso del trayecto, su intención de modificar su itinerario, o incluso la de continuar solo el itinerario previsto? Esa cuestión presenta enorme interés práctico cuando se trata de precisar la responsabilidad del automovilista en caso de accidente; porque el contrato de transporte hace que nazca,

con cargo al transportista, una obligación de resultado, la de conducir al transportado sano y salvo a destino; la jurisprudencia, para evitarle al automovilista complaciente la aplicación de esa regla, se niega a ver en esa prestación de servicios gratuitos un verdadero contrato.

4.3.2.4 AMBITO DEL CONTRATO

Por tener necesariamente la obligación un aspecto pecuniario, el contrato que la crea posee también un carácter pecuniario predominante. Los actos jurídicos, tales como el matrimonio o la adopción, suponen desde luego un acuerdo de voluntades; pero no son verdaderos contratos; porque no crean, a título principal, más que derechos de la personalidad. Por el contrario, las convenciones que recaen sobre las consecuencias pecuniarias de los derechos de la personalidad son verdaderos contratos; así la convención matrimonial que fija el régimen de los bienes de los esposos es un verdadero contrato. Por consiguiente, el contrato penetra indirectamente en los derechos de familia.

4.3.2.5 LOS CONTRATOS ENTRE MIEMBROS DE UNA FAMILIA

Las convenciones que recaen sobre derechos pecuniarios no están prohibidas, en principio, entre miembros de una misma familia. El legislador ha debido intervenir a veces, sin embargo, para evitar el abuso que de su autoridad podría hacer uno de los miembros de la familia.

Los pactos sobre sucesiones futuras están prohibidos. Antes de .la rendición de cuentas de la tutela no. es válida ninguna convención entre el tutor y su pupilo. El Código civil prohíbe la compraventa entre esposos, porque es susceptible de disfrazar una donación que se convertiría así en irrevocable, cuando la donación entre cónyuges es revocable obligatoriamente "ad nutum". La jurisprudencia extendía esa prohibición a las sociedades entre esposos; pero los tribunales parecen resueltos a suprimir esta última prohibición que condenaba a las sociedades familiares, muy útiles socialmente; las resoluciones recientes se fundan sobre el carácter excepcional de la prohibición de la compra- venta entre cónyuges, derogación de la libertad de contratar, que no podría ser extendida.

4.3.2.6 EL DERECHO PÚBLICO Y EL CONTRATO: CRITERIO DE LA DISTINCION ENTRE LOS CONTRATOS" ADMINISTRATIVOS Y LOS CONTRATOS DE DERECHO PRIVADO

Por necesitar el contrato un acuerdo de voluntades libres, supone una cierta igualdad entre los contratantes, que no parece que pueda existir cuando la Administración trata con los particulares; la preeminencia del interés colectivo general sobre el interés particular parece excluir entonces la posibilidad de un verdadero contrato.

Sin embargo, resulta necesaria una distinción. Cuando la Administración contrata en las mismas condiciones que un particular, ya sea porque trata sobre su esfera privada, ya sea porque, aun actuando como persona pública, en el interés de un servicio público propiamente dicho, adopta las reglas contractuales del derecho privado (alquiler de un inmueble, por ejemplo), los contratos que celebra son contratos de derecho privado, sometidos a las reglas del Código civil y a la competencia de los tribunales judiciales.

El acto escapa, por el contrario, al derecho privado y a la competencia de los tribunales judiciales cuando se reúnen dos condiciones: se ha celebrado en el interés del servicio público; contiene cláusulas que rebasan la órbita del derecho común. En efecto, en los casos en que el servicio público funciona "con sus reglas propias y un carácter administrativo", utiliza procedimientos de derecho público; el acto celebrado con los particulares revela, por la adopción de cláusulas que rebasan la órbita del derecho común, la autoridad del servicio, que se impone al particular; no se está ya en presencia de un verdadero contrato, sino de un acto sometido a la fiscalización y a la dirección de la Administración, que puede ser modificado ulteriormente por ella, y donde se afirma la completa desigualdad de las partes. Se califica ese acto de contrato administrativo; pero no tiene ya de contrato sino el nombre.

4.3.3 LA FORMACION DE LOS CONTRATOS

Según la ley general del trabajo un contrato para ser legal tiene que seguir los siguientes pasos o cumplir las siguientes normas.

DEL CONTRATO DE TRABAJO

DISPOSICIONES GENERALES

Art. 5º El contrato individual de trabajo es aquél en virtud del cual una o más personas se obligan a prestar sus servicios manuales o intelectuales a otra u otras.

Art. 6º El contrato individual de trabajo constituye la ley de las partes, a reserva de que sus cláusulas no impliquen una renuncia del trabajador a cualquiera de los derechos que le son reconocidos por las disposiciones legales y por los contratos colectivos; a falta de estipulaciones expresas, será interpretado por los usos y costumbres de la localidad.

Art. 7º El contrato individual de trabajo deberá contener, por lo menos, las siguientes estipulaciones:

a) Nombres y apellidos paterno y materno o razón social de los contratantes;

b) Edad, nacionalidad, estado civil y domicilio del trabajador;

c) Naturaleza del servicio y el lugar donde será prestado;

d) Determinación de si el trabajo o servicio se efectuará por unidad de tiempo, de obra, por tarea o a destajo o por dos o más de estos sistemas;

e) Monto, forma y período de pago de la remuneración acordada;

f) Plazo de contrato;

g) Lugar y fecha del contrato;

h) Inscripción de sus herederos, con indicación de nombres y edad, para los efectos de las disposiciones concernientes a la reparación de riesgos profesionales.

Art. 8º Cuando fuere retirado el trabajador por causal ajena a su voluntad, el patrono estará obligado, independientemente del desahucio, a indemnizarle por tiempo de servicios, con la suma equivalente a un mes de sueldo o salario por cada ano de trabajo continuo; y si los servicios no alcanzaren a un año, en forma proporcional a los meses trabajados, descontando los tres primeros meses, que se reputan de prueba, excepto en los contratos de trabajo por tiempo determinado, que no sufrirán ningún descuento de tiempo. Se reputa como periodo de prueba sólo el que corresponde al inicial de los primeros tres meses más no a los subsiguientes que resulten en virtud de renovación o prorroga. Si el trabajador tuviera más de 15 años de servicios y el obrero más de 8 años percibirá la indicada indemnización aunque se retirase voluntariamente. Para los efectos de esta indemnización se computará el tiempo de servicios desde la promulgación de la ley que se reglamenta.

Art. 9º No habrá lugar a desahucio ni indemnización cuando exista una de las siguientes causales:

a) Perjuicio material causado con intención en las máquinas, productos o mercaderías;

b) Revelación de secretos industriales:

c) Omisiones e imprudencias que afecten a la higiene y seguridad industriales;

d) Inasistencia injustificada de más de tres días consecutivos o de más de seis en el curso de un mes;

e) Incumplimiento total o parcial del contrato de trabajo o del reglamento interno de la empresa;

f) Retiro voluntario del trabajador, antes de los términos fijados en el artículo 13 de la ley o en el del contrato;

g) Abuso de confianza, robo o hurto por el trabajador;

h) Vías de hecho, injurias o conducta inmoral en el trabajo;

i) Abandono en masa del trabajo, siempre que los trabajadores no obedecieran a la intimación de la autoridad competente.

Art. 10º En caso de conflicto colectivo de trabajo y siempre que se hubieran llenado las disposiciones contenidas en los capítulos pertinentes de la ley y de este Reglamento, se considerará que hay suspensión y no ruptura de contrato, para todos los fines del presente capítulo.

Art. 11º El cálculo de la indemnización se hará tomando en cuenta el promedio del salario, en los tres últimos meses, tratándose de salario mensual; y en los últimos 75 días hábiles de trabajo, tratándose de salario diario.

Art. 12º El tiempo de servicio para los efectos de indemnizaciones por retiro forzoso de los empleados, se computará desde el 21 de noviembre de 1924 o desde la fechas de promulgación de las leyes especiales que les concedieron tales beneficios.

Para los que recientemente son considerados como empleados por el artículo 2º de la ley que se reglamenta, así como para los obreros en general, el tiempo de servicios se computará desde el 8 de diciembre de 1942, fecha de su promulgación.

Art. 11º El trabajador conservará la propiedad de su empleo, sin derecho a remuneración, mientras cumpla el servicio militar obligatorio o forme parte de las reservas movilizadas.

Art. 14º El contrato de trabajo celebrado por escrito requiere, para alcanzar eficacia jurídica, ser refrenado por el Inspector de Trabajo o, en su defecto, por la autoridad administrativa superior del lugar.

Art. 15º Los contratos de trabajo se suscribirán en papel común, quedando exentos del uso de timbres, por tratarse de actos de servicio social.

Art. 16º A la terminación de todo contrato, y a solicitud verbal del trabajador, el patrono le otorgará en papel común, un certificado que exprese:

a) la fecha de ingreso

b) la de salida

c) la clase de trabajo ejecutado

d) la causa del retiro

e) la conducta observada.

DEL CONTRATO COLECTIVO

Art. 17º Contrato colectivo del trabajo es el convenio celebrado entre uno o más patronos y un sindicato, federación o confederación de sindicatos de trabajadores, con el objeto de determinar condiciones generales del trabajo o de reglamentarlo.

Art. 18º El contrato colectivo de trabajo deberá ser obligatoriamente celebrado por escrito y registrado ante el Inspector del trabajo.

Art. 19º Sólo los sindicatos, federaciones o confederaciones de sindicatos de trabajadores, con personería jurídica reconocida por el Supremo Gobierno y organizados del acuerdo a la Ley General del Trabajo y al presente Reglamento, podrán suscribir validamente contratos colectivos.

Art. 20º La representación de todo sindicato, federación o confederación de sindicatos de trabajadores será ejercida conforme a sus estatutos.

4.3.4 MODELO DE CONTRATO

Los contratos en Bolivia están regidos a un formato definido y constan de las siguientes partes:

MODELO DE CONTRATO DE COMPRA Y VENTA

PRIMERA.- (partes contratantes).- Intervienen como partes en la suscripción del siguiente contrato de compra venta:

1.1 Sr. _____, mayor de edad, con C.I. _____ vecino de _____, con domicilio en calle _____, de una parte, que será llamado COMPRADOR/VENDEDOR de aquí en adelante.

1.2 Sr. _____, mayor de edad, con C.I. _____ vecino de _____, con domicilio en calle _____, de otra parte, que será llamado VENDEDOR/COMPRADOR

SEGUNDA.- (objeto del contrato).- Sr, es propietario de un(a) _____, escriturada y libre de cargas y gravámenes, corriente al pago de contribuciones e impuestos (describir la posesión en cuestión, cuota de participación, inscripción y título).

TERCERA.- (conformidad).- En este acto, el comprador toma posesión de la vivienda, mercancía, adquirida por compraventa, libre de toda obligación, a su total satisfacción.

CUARTA.- (Precio del Contrato y Forma de Pago).- El precio estipulado del bien es de _____ bolivianos, que se deberá pagar en _____.

QUINTA.- (Obligaciones Tributarias).- las obligaciones tributarias partirá de acuerdo a lo concensuado entre las partes.

SEXTA.- (Responsabilidades y Obligaciones).- Por el presente el comprador se subroga en todos aquellos derechos que le corresponden al vendedor.

SEPTIMA.- (Causales de resolución del Contrato).- Serán causales de resolución del contrato, el incumplimiento de las partes de las obligaciones emergentes contenidas dentro del presente documento, con lo cual el contrato quedará resuelto y terminado a la fecha de aviso sin necesidad de requerimiento judicial ni extrajudicial.

Ambas partes podrán anunciar su voluntad unilateral de resolver el presente contrato en cualquier momento, notificando a la otra parte por escrito con 15 días calendario de antelación, durante estos días continúan vigentes las obligaciones contraídas.

OCTAVA.- (Conformidad y Aceptación).- En señal de conformidad y aceptación de todas y cada una de las cláusulas que componen el presente contrato, las partes lo suscriben en un original y una copia del mismo tenor en la ciudad de La Paz, el día _____ de _____ del año dos mil _____.

FIRMA DIGITAL DEL CONTRATADO	FIRMA DIGITAL DEL CONTRATANTE
CERTIFICADO DE AUTENTICIDAD	

CONTRATO DE PRESTACION DE SERVICIOS

Conste por el presente contrato de prestación de servicios, que entre las partes intervinientes se celebra, bajo el tenor de las cláusulas y estipulaciones siguientes:

PRIMERA.- (Partes Contratantes).- Intervienen como partes en la suscripción del presente contrato de prestación de servicios:

1.1 EL OFERERENTE, representado legalmente por su _____, según - _____, que en adelante y a efectos del presente contrato se denominarán simplemente EL OFERENTE.

1.2 El/La Sr(a). _____, mayor de edad, con Cédula de Identidad No _____. denominado en adelante simplemente EL/LA CONTRATADO/A.

SEGUNDA.- (Antecedentes).- EL OFERENTE requiere la contratación de un profesional consultor (caracteristicas); sujeto a Términos de Referencia específicos, que formarán parte integrante del presente contrato, aspecto por el cual se suscribe el mismo en el marco de LA LEY GRAL. DEL TRABAJO.

TERCERA.- (Objeto del Contrato).- La suscripción del presente contrato tiene por finalidad la prestación de servicios especializados por parte de EL/LA CONTRATADO/A, obligándose éste a la realización de trabajos específicos detallados en los Términos de Referencia que forman parte indisoluble del presente contrato.

Se deja establecido que el trabajo contratado quedará expresado en los resultados de los servicios prestados, que de acuerdo a la naturaleza de los servicios consisten en el

ejercicio de las funciones y responsabilidades detallados en los Términos de Referencia.

CUARTA.- (Duración del Contrato).- El presente contrato de prestación de servicios tendrá una duración fija de _____, computables a partir del día _____ de _____de _____., hasta el día _____ de _____ de _____.

A la finalización del término de duración estipulada en la presente cláusula y mientras las partes no acuerden lo contrario, no se producirá la tácita renovación del contrato y el mismo quedará concluido para ambas partes contratantes. Una vez que se haya extinguido la relación contractual no existirá ninguna relación de carácter jurídico ni contractual entre ambas partes.

La fuente de financiamiento para la cancelación de los honorarios, se realizarán mediante Recursos Específicos de la Institución.

QUINTA.- (Precio del Contrato y Forma de Pago).- En compensación por los servicios prestados, al OFERENTE cancelará a EL/LA CONTRATADO/A como honorario por sus servicios prestados, la suma global de Bs _____.- (_____00/100 BOLIVIANOS), monto de dinero que será cancelado de manera mensual y en _____ (_____) cuotas, la primera de Bs_____.- (_____ 00/100 BOLIVIANOS) y las dos siguientes cuotas de Bs_____.- (_____ 00/100 BOLIVIANOS) cada una. El monto global por la naturaleza del contrato no podrá ser reajustado ni indexado y será cancelado por mes vencido dentro los primeros cinco días hábiles de cada mes.

Como garantía de buena ejecución del contrato, el honorario correspondiente al último mes será cancelado luego de la aprobación del informe final por parte del Director Ejecutivo del RUAT y la máxima autoridad del Área Solicitante.

SEXTA.- (Obligaciones Tributarias).- Cualquier impuesto, tasa, gravamen u otros que pudiera afectar el costo del servicio estará a cargo de EL/LA CONTRATADO/A; quedando obligado al cumplimiento de las obligaciones tributarias emergentes del presente contrato, debiendo para tal efecto presentar el Número de Identificación Tributaria (N.I.T.).

SEPTIMA.- (Carácter del servicio).- Para fines consiguientes, se deja expresamente establecido que la prestación de estos servicios, por su naturaleza, no reconoce relación laboral de dependencia alguna entre El OFERENTE y EL/LA CONTRATADO/A o sus dependientes. En consecuencia, EL OFERENTE no estará obligado al pago de beneficios sociales o reconocer otros derechos emanados de la

Ley General del Trabajo, Código de la Seguridad Social u otras disposiciones conexas; la contratación de seguros de vida y accidentes, atención médica, corre por cuenta de EL/LA CONTRATADO/A, como trabajadora independiente.

OCTAVA.- (Responsabilidades y Obligaciones).- EL/LA CONTRATADO/A se obliga a prestar sus servicios en el lugar que se le señale con responsabilidad, capacidad y esfuerzo, acatando para ello las instrucciones y reglamentos que emanen de la Dirección Ejecutiva del RUAT, asumiendo total responsabilidad en la ejecución del trabajo encomendado, obligándose a preservar los equipos y materiales que se encuentran a su cargo, así como guardar estricta confidencialidad y reserva con relación a toda la información oral o escrita de las actividades propias del OFERENTE que llegase a conocer en el cumplimiento de las funciones asignadas; en consecuencia le está expresamente prohibido facilitar datos, cifras u otros informes a terceros sin previa autorización de los ejecutivos del RUAT. El quebrantamiento de la obligación contenida en la presente cláusula dará lugar a la imposición de procesos y sanciones que corresponda.

Asimismo, EL/LA CONTRATADO/A se obliga a prestar sus servicios con dedicación exclusiva respecto a los trabajos encomendados u otros afines o conexos, cumplir con todas sus obligaciones legales (civiles, tributarias, sociales, etc.), sin responsabilidad para el OFERENTE. EL/LA CONTRATADO/A no podrá subrogar, ceder o transferir, total o parcialmente el presente contrato a terceros sin el consentimiento del OFERENTE.

NOVENA.- (Propiedad de activos).- Los activos de propiedad del RUAT que se entregan a EL/LA CONTRATADO/A, equipos de computación y todo otro activo, tienen la calidad de herramientas de trabajo y en ningún caso constituyen propiedad de EL/LA CONTRATADO/A, quien a momento de la terminación del contrato y/o su eventual desvinculación contractual deberá entregarlos íntegramente y en la misma forma que los recibió.

Asimismo se deja establecido que los resultados del trabajo encomendado, documentales, informáticos u otros que obtenga y/o desarrolle EL/LA CONTRATADO/A emergente del presente contrato, serán de propiedad, uso y disposición exclusiva del OFERENTE.

DECIMA.- (Obligaciones del OFERENTE).- El OFERENTE, se obliga a pagar en forma puntual la remuneración convenida en la cláusula quinta y a dotar a EL/LA CONTRATADO/A de un ambiente adecuado para la prestación de sus servicios,

otorgar las facilidades necesarias para la ejecución del trabajo encomendado y que es objeto del presente contrato.

De acuerdo a los requerimientos de las tareas contratadas y cumplimiento de los objetivos institucionales, el OFERENTE se obliga a pagar a EL/LA CONTRATADO/A, los gastos necesarios de transporte aéreo o terrestre, así como los respectivos viáticos conforme a la escala vigente que se aplica en las entidades del sector público.

DECIMA PRIMERA.- (Documentos integrantes del Contrato).- Forman parte del presente contrato el Reglamento Interno de Consultores en lo que no sea oponible al presente contrato, los Términos de Referencia específicos, así como cualquier reglamentación, instructiva que apruebe el OFERENTE, relativo a la prosecución y/o cumplimiento del objeto del contrato.

DECIMA SEGUNDA.- (Causales de resolución del Contrato).- Serán causales de resolución del contrato, el incumplimiento de EL/LA CONTRATADO/A de las obligaciones emergentes contenidas dentro del presente documento, con lo cual el contrato quedará resuelto y terminado a la fecha de aviso sin necesidad de requerimiento judicial ni extrajudicial.

Ambas partes podrán anunciar su voluntad unilateral de resolver el presente contrato en cualquier momento, notificando a la otra parte por escrito con 15 días calendario de antelación, durante estos días continúan vigentes las obligaciones contraídas.

DECIMA TERCERA.- (Legislación aplicable al contrato). El presente contrato es un Contrato Administrativo, por lo que está sujeto a la normativa prevista en la Ley general del trabajo de Administración y Control Gubernamentales, en los aspectos de su ejecución y resultados.

DECIMA CUARTA.- (Solución de Controversias).- En caso de surgir controversias entre el OFERENTE y EL/LA CONTRATADO/A, que no puedan ser solucionadas por la vía de la concertación, las partes están facultadas para acudir a la vía judicial, bajo la jurisdicción coactivo fiscal.

DECIMA QUINTA .- (Conformidad y Aceptación).- En señal de conformidad y aceptación de todas y cada una de las cláusulas que componen el presente contrato, las partes lo suscriben en un original y una copia del mismo tenor en la ciudad de La Paz, el día _____ de _____ del año dos mil _____.

FIRMA DIGITAL DEL CONTRATADO	**FIRMA DIGITAL DEL CONTRATANTE**

Así entonces un documento digital pasa a ser un contrato legal, cumpliendo lo estipulado, ya explicado anteriormente.

4.4 CONSTRUCCION DE LA FIRMA DIGITAL

Se vio en la formación del contrato digital como en un documento son necesarias las firmas del contratante y del contratado para que el documento goce de legalidad, ahora en la propuesta la firma manuscrita es reemplazada por la firma digital

La elaboración de la firma digital de un documento es resumir el contenido del documento a través de un algoritmo hash en este caso el sha-1, dando como resultado una salida de 128n bits el cual se encripta para dar origen a una clave publica, que solo es decodificada por el usuario al cual esta dirigido el documento con la clave privada de encriptación.

4.4.1 DEFINICION

Firma electrónica o firma digital electrónica permite garantizar la identidad del firmante de un documento y la integridad del contenido de dicho documento.

Desde el punto de vista técnico la firma electrónica se basa en **algoritmos matemáticos de cifrado** más o menos complejos. Hoy en día la mayoría de los algoritmos están documentados y son de dominio público, para asegurar que la fuerza del algoritmo esté en la matemática que utiliza y no en la ocultación del proceso de cálculo.

Desde un punto de vista práctico, el procedimiento para firmar un documento es mucho más sencillo.

El emisor del documento debe tener al menos una clave de cifrado, que consiste a su vez en una **clave pública** y una **clave privada**.

La **clave privada es totalmente secreta** y sólo puede estar en manos del emisor, para garantizar la identidad de esa persona. Si la clave privada se pierde o cabe la posibilidad de que haya sido copiada o existen razones para pensar que está comprometida de alguna forma la seguridad de dicha clave, el propietario debe revocarla inmediatamente, para evitar que otras personas la utilicen suplantando su identidad.

La clave pública, como su nombre indica, puede (y debe) ser distribuida públicamente.

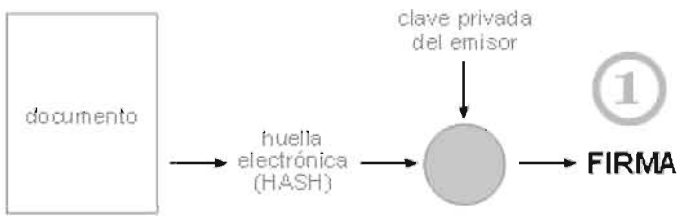
La idea básica del cifrado por llave (clave) asimétrica (pública + privada) es que lo que cierra una llave lo abre la otra.

La clave de cifrado se puede generar fácilmente mediante alguno de los programas de cifrado que existen en la actualidad. Esta clave es perfectamente válida para firmar documentos que van a ser intercambiados entre personas de confianza.

Entonces, una vez que el emisor tiene la clave de cifrado, ya sea generada por él mismo o proporcionada a través de su certificado digital personal:

4.4.2 FIRMAR EL DOCUMENTO

- Se genera en primer lugar una huella digital del documento mediante un **algoritmo de HASH**. Esta huella es una secuencia de unos y ceros de una determinada longitud. Un determinado documento sólo puede generar una huella. Si ese documento se modifica, aunque sólo sea en una coma, la huella será totalmente distinta. Esa huella que se ha generado a partir del documento se encripta con la clave privada del emisor del documento, y se obtiene la **firma digital de ese documento**.

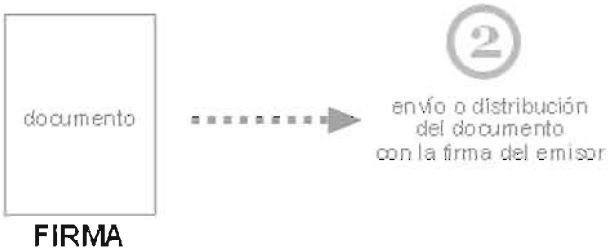


Elaboración propia

La firma digital obtenida garantiza:

- Que el documento ha sido firmado por el emisor. No es posible que haya sido firmado por otra persona a menos que haya robado la clave privada del emisor.
- Que el contenido del documento no ha sido manipulado desde la emisión hasta la recepción del mismo.

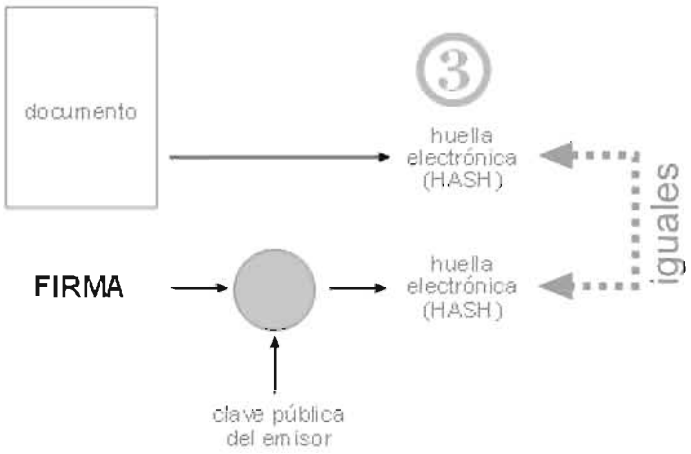
➢ Envío del documento firmado: Dependiendo del formato elegido, el documento y la firma pueden ir en el mismo fichero o en ficheros separados.



Elaboración propia

➢ Recepción del documento y comprobación: Cuando el documento llega al destinatario se lleva a cabo el proceso de comprobación, para asegurar que el documento no ha sido manipulado y para garantizar que efectivamente lo envía la persona real (y no alguien que suplanta su identidad).

En primer lugar se calcula la huella del documento utilizando el mismo algoritmo de HASH que utilizó el emisor.



Elaboración propia

Por otra parte se desencripta la huella digital original del documento (contenida en la firma). Para descifrar esta huella se utiliza la clave pública del emisor.

En el caso de los certificados digitales, la clave pública se obtiene a través de la entidad certificadora, que garantiza que pertenece precisamente a esa persona (emisor).

Una vez extraída la huella de la firma se la compara con la huella obtenida directamente del documento.

Si **las dos huellas son iguales** podemos garantizar que el documento no ha sido manipulado y que ha sido enviado por el emisor real.

El procedimiento de firma en origen y de comprobación en recepción lo realizan automáticamente las aplicaciones de cifrado. Es un proceso prácticamente transparente para el usuario.

4.5 AUTENTICACION DEL CONTRATO

4.5.1 AUTENTICACION

Para firmar documentos de una forma oficial y que tengan validez legal es necesario que esa clave esté certificada por una entidad en la que puedan confiar todos los usuarios. Esa entidad garantiza que efectivamente la persona que posee esa clave es quien dice ser.

Por lo tanto, un certificado digital no es más que una clave de cifrado, emitida por una entidad de certificación para una determinada persona física o jurídica, con la garantía que proporciona esa entidad de certificación con respecto a la identidad de la persona, y con una serie de mecanismos de gestión, mantenimiento y control.
El contrato es autenticado por una empresa externa a las partes que están negociando.

Hasta ahora se vio la forma de elaboración del documento digital y de la firma digital del documento, ahora se vera la forma de autenticación del contrato en si.
Los algoritmos de cifrado asimétrico se basan en el hecho de compartir una clave pública entre varios usuarios. En general, esta clave se comparte mediante un directorio electrónico, normalmente por una página Web.

Sin embargo, el modo de compartir presenta un inconveniente importante: nada garantiza que la clave pertenezca al usuario con el que está asociada. Un hacker puede corromper la clave pública que aparece en el directorio remplazándola con su propia clave pública. Por consiguiente, el hacker podrá descifrar todos los mensajes que se cifraron con la clave que aparece en el directorio.
Un certificado permite asociar una clave pública con una entidad (una persona, un equipo, etc.) para garantizar su validez. El certificado es como la tarjeta de identificación de la clave, emitida por una entidad llamada Entidad de certificación (que frecuentemente se abrevia CA, por sus siglas en inglés).
La entidad de certificación es responsable de emitir los certificados, de asignarles una fecha de validez (similar a la fecha de vencimiento de los alimentos) y de revocarlos antes de esta fecha en caso de que la clave (o su dueño) estén en una situación de riesgo.

4.5.2 ESTRUCTURA DE LOS CERTIFICADOS

Los certificados son pequeños archivos divididos en dos partes:

- La parte que contiene la información
- La parte que contiene la firma de la entidad de certificación

La estructura de los certificados está estandarizada por la norma X.509 (más precisamente, X.509v3) de la UIT, que define la información que contiene el certificado:

- La versión de X.509 a la que corresponde el certificado
- El número de serie del certificado;
- El algoritmo de cifrado utilizado para firmar el certificado;
- El nombre (DN, siglas en inglés de Nombre distinguido) de la entidad de certificación que lo emite;
- La fecha en que entra en vigencia el certificado;
- La fecha en que finaliza el período de validez del certificado;
- El objeto de utilización de la clave pública;
- La clave pública del dueño del certificado;
- La firma del emisor del certificado (huella digital).

La entidad de certificación firma toda esta información (información + clave pública del solicitante) lo que implica que una función hash crea una huella digital de esta información y luego este hash se cifra con la clave privada de la entidad de certificación. La clave pública se distribuye antes de tiempo para permitir a los usuarios verificar la firma de la entidad de certificación con su clave pública.
Cuando un usuario desea comunicarse con otra persona, sólo debe obtener el certificado del receptor. Este certificado contiene el nombre y la clave pública del receptor, y está firmado por la entidad de certificación. De esta forma, es posible verificar la validez del mensaje aplicando, primero, la función hash a la información

contenida en el certificado y, segundo, descifrando la firma de la entidad de certificación con la clave pública y comparando los dos resultados.

4.5.3 FIRMAS DEL CERTIFICADO

Existen varios tipos de certificados en función del nivel de sus firmas:

Los certificados firmados localmente son certificados de uso interno. Al estar firmados por un servidor local, este tipo de certificados permiten garantizar los intercambios confidenciales dentro de una organización, por ejemplo, en una Intranet. Los certificados firmados localmente se pueden usar para autentificar usuarios.

Los certificados firmados por una entidad de certificación son necesarios cuando se deben garantizar los intercambios seguros con usuarios anónimos, por ejemplo, en el caso de una página Web segura al que pueda acceder el público general. La certificación de un tercero garantiza al usuario que el certificado pertenece efectivamente a la organización a la que dice pertenecer.

Los certificados se utilizan principalmente en tres tipos de contextos:

Los certificados de cliente se almacenan en la estación de trabajo del usuario o se integran en un contenedor como una tarjeta inteligente, y permiten identificar a un usuario y asociarlo con ciertos privilegios. En la mayoría de los casos, se transmiten al servidor cuando se establece una conexión y el servidor asigna privilegios en función de la acreditación del usuario. Son verdaderas tarjetas de identificación digitales que usan un par de claves asimétricas con una longitud de 512 a 1024 bits.

Los certificados de servidor se instalan en un servidor Web y permiten conectar un servicio con el dueño del servicio. En el caso de página Web, permiten garantizar que la dirección URL de la página Web y especialmente su dominio pertenecen realmente a tal o cual compañía. También permiten proteger las transacciones con usuarios gracias al protocolo SSL.

Los certificados VPN (Red privada virtual) se instalan en un equipo de red y permiten cifrar flujos de comunicación de extremo a extremo entre dos puntos (por ejemplo, dos ubicaciones de una compañía). En este tipo de escenario, los usuarios tienen un

certificado cliente, los servidores aplican un certificado de servidor y el equipo de comunicación usa un certificado especial (generalmente un certificado IPSec).

Para que la propuesta sea realizable se debe crear un departamento privado o parte del gobierno el cual pueda fungir en Bolivia como la entidad que certifica las firmas digitales nacionales e internacionales, así de esta manera garantizar no solo la seguridad de los contratos electrónicos sino también de las transacciones hechas por la comunidad boliviana.

4.6 PROPUESTA

En la propuesta de la investigación tomaremos dos puntos; la propuesta de ley y la Entidad Certificadora

4.6.1 PROPUESTA DE LEY

Una vez conocida la forma de elaborar un contrato electrónico en sus dos partes, tanto el documento digital sujeto a las leyes y la firma digital, pasamos a la propuesta de ley.

OBJETIVO

La presente propuesta tiene como objetivo regular la contratación electrónica a través de la autenticación basada en una firma digital; otorgando y reconociendo seguridad, eficacia y valor jurídico a: la firma digital y contratación electrónica.

DEFINICIONES GENERALES

Acuse de recibo: Es el procedimiento por el cual se verifica, al momento de recepción por parte del destinatario, la integridad, autenticidad y origen de un mensaje de datos, y un aviso de recepción del mensaje de datos es enviado por el destinatario del mensaje.

Autenticación: Es el proceso a través del cual es posible verificar la identidad de un originador o destinatario de un mensaje de datos.

Datos personales: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de la propuesta.

Destinatario: Es la persona natural o jurídica a la cual el originador dirige el mensaje de datos.

Dispositivo electrónico: Instrumento físico o lógico utilizado independientemente para iniciar o responder mensajes de datos, sin intervención de una persona al momento de dicho inicio o respuesta.

Documento Digital: Todo mensaje de datos que se encuentra en archivos o registros electrónicos.

Estándares o Formatos Normalizadores: Son las reglas para el intercambio electrónico de datos para administración, comercio y transporte, que comprenden una serie de formatos, directorios, instrucciones y códigos calificadores para el intercambio electrónico estructurado de datos. Para el intercambio vinculado al comercio de bienes y servicios, entre sistemas de información.

Firma Digital: La firma digital es el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a un mensaje de datos, utilizada como método de identificación del firmante, con la intención de vincularse con el contenido de dicho mensaje de datos. Habiendo sido apropiadamente tratada para su seguridad.

Intercambio electrónico de datos: Cualquier transferencia electrónica de información efectuada de un sistema de información a otro, mediante estándares o formatos normalizados ó conforme a alguna norma técnica convenida al efecto.

Intermediario: Es toda persona que actuando por cuenta de otra, envíe, reciba o archive un mensaje da datos o preste algún otro servicio con respecto a él.

Mensaje de datos: Es la información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que es intercambiada por cualquier medio, entendiéndose por; generada y procesada al procedimiento realizado para su respectiva seguridad.

Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes: el intercambio electrónico de datos, el correo electrónico.

Originador: Es toda persona que, a tenor del mensaje, haya actuado por cuenta o en cuyo nombre se haya actuado para enviar o generar ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de intermediario.

Sellado de Tiempo: Anotación electrónica firmada electrónicamente y agregada a un mensaje de datos donde conste como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación.

Sistema de información: Es aquel que permite generar, procesar, transmitir, recibir o archivar documentos electrónicos y todo tipo de mensajes de datos.

Validación de Integridad: Medio o procedimiento a través del cual un originador o destinatario de mensajes de datos verifica que el mensaje está completo y no ha sufrido alteraciones.

Validación de autenticidad: Medio o procedimiento a través del cual un originador o destinatario de mensajes de datos verifica que el la firma digital pertenece al originador real.

Artículo 1

Principios Generales

I. Las actividades reguladas por esta propuesta se someterán a los principios de:

a) Autonomía de la voluntad, por el que se deja librada a la voluntad de las partes, la forma y utilización de medios electrónicos para la concreción de los negocios o actos jurídicos que celebren, observando en cada caso los requisitos y solemnidades exigibles, siempre y cuando no contravengan el ordenamiento jurídico.

b) Neutralidad normativa, por el cual, el Estado no debe favorecer ni restringir mediante la adopción de disposiciones legales, el uso de determinadas tecnologías de información, de tal manera que vaya en contra de la evolución tecnológica, salvo que se vulneren derechos y garantías constitucionales.

c) Asimilación jurídica, por el que todos los actos jurídicos celebrados por medios electrónicos, gozarán de la misma validez que la reconocida jurídicamente para los medios convencionales vigentes.

d) Equivalencia funcional, por el que se reconoce a la documentación consignada por medios electrónicos un grado de seguridad equivalente al de los documentos físicos, reconociéndoles su autenticidad, validez o eficacia probatoria, salvo prueba o mandato legal en contrario.

e) Confidencialidad y reserva regirá para los mensajes de datos, cualquiera sea su forma, medio o destino.

f) Compatibilidad internacional, por la que se observa la concordancia y complementariedad de las distintas normas y principios del derecho internacional en materia de comunicación electrónica de datos, contratación y firmas electrónicas.

II. En la interpretación de la presente Ley se tomará en consideración la voluntad de los participantes en una comunicación, de acuerdo al principio de autonomía de la voluntad. Las cuestiones relativas a materias que se rijan por la presente propuesta y que no están expresamente resueltas en ella, serán dirimidas de conformidad con los principios generales en que ella se inspiran y al ordenamiento jurídico vigente.

Artículo 2

Protección de datos

I. La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución política del Estado y esta propuesta, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.

II. No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, ni cuando se recojan para el ejercicio de las funciones propias de Administración Pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento de su relación contractual.

Pero en ningún caso, la Administración Pública podrá publicitar la recopilación efectuada, salvo aquella publicación efectuada por motivo de un delito.

III. El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.

CONTRATACION ELECTRONICA

Artículo 3

Validez de los contratos electrónicos

I. Los contratos civiles, comerciales y de otra naturaleza previstos en normas generales y especiales nominados o innominados, podrán ser instrumentados mediante documentos electrónicos. No se negará efectos jurídicos, validez o fuerza obligatoria a un contrato, a las manifestaciones de voluntad u otras declaraciones por la sola razón de estar en forma de uno o más mensajes de datos.

II. Lo dispuesto en el presente Capítulo no será aplicable a contratos respecto de los cuales la Ley excluya la validez de comunicaciones electrónicas expresamente.

III. Aquellos contratos a los que se exijan formalidades y solemnidades para su perfeccionamiento deberán cumplir con los mismos para surtir sus plenos efectos.

Artículo 4

Formación de un contrato electrónico

En la formación de un contrato electrónico, de no convenirse otra cosa por las partes, la oferta, contraoferta y su aceptación podrán ser expresadas por medio de mensajes de datos debidamente autenticados.

Artículo 5

Perfeccionamiento del contrato electrónico

I. La manifestación del consentimiento en los actos jurídicos se producirá cuando el originador reciba la aceptación del destinatario, mediante el envío del correspondiente mensaje de datos y se entenderá que el acto se ha perfeccionado en el lugar de la oferta o de la contraoferta y si hubiera acuerdo especial se tendrá como lugar de perfeccionamiento el que acordaren las partes con el sellado de tiempo.

II. Reglamentariamente se podrá establecer que en determinados casos el perfeccionamiento de los contratos electrónicos se producirá cuando el destinatario reciba del originador el acuse de recibo sobre la aceptación que le fue enviada al originador.

III. La simple recepción, confirmación de recepción, o apertura del mensaje de datos, no implica aceptación tácita del contrato electrónico, salvo acuerdo de las partes.

Artículo 6

Jurisdicción arbitral

I. En caso de controversias las partes se someterán de manera definitiva a la jurisdicción arbitral administrada por centros especializados dentro de Bolivia o fuera de ella, de acuerdo a lo convenido por las partes.

II. El caso de que las partes en cuestión o los prestadores de servicios de la sociedad de la información desearen establecer las condiciones del arbitraje, el convenio arbitral se sustanciará de manera escrita, a través de mensajes de datos intercambiados entre las partes, cláusulas dentro de los contratos o previsiones informadas a las partes por los administradores al momento de acceder a sus recursos.

FIRMA DIGITAL

Artículo 7

De los requisitos de la firma digital

I. La firma digital es aquella que cumple con los siguientes requisitos:

a) Estar debidamente acreditada, registrada y vigente.
b) Estar vinculada única y exclusivamente a su titular
c) Verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos de comprobación establecidos por la Ley y los reglamentos.
d) Que el método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual generado y/o comunicado, y;
e) Que los datos de creación de la firma estén, al momento de la firma bajo el control exclusivo del originador.

f) Que en caso de que uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, sea posible detectar cualquier alteración de esa información hecha después del momento de la firma.

Artículo 8

Efectos

I. La firma digital tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos.

II. No se negarán efectos jurídicos a una firma digital que no reúna los requisitos de firma digital en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica, debiendo valorársela de acuerdo a los criterios de la sana crítica.

Artículo 9

Presunciones

La firma digital que cumpla con los recaudos y exigencias que esta Ley y su reglamentación disponen, genera las siguientes presunciones, salvo prueba en contrario:

a) Que toda firma digital pertenece al titular de la misma.
b) Que el documento electrónico no ha sido modificado desde el momento de su firma electrónica, si el resultado del procedimiento de verificación así lo indica.

Artículo 10

Obligaciones del titular

I. El titular de la firma digital deberá cumplir con las obligaciones derivadas del uso de la firma digital, actuando con la debida diligencia y tomando las medidas de seguridad necesarias, para mantener la firma digital bajo su estricto control y evitar toda utilización no autorizada, debiendo cumplir las obligaciones establecidas en la presente propuesta y sus reglamentos.

Artículo 11

Extinción

I. La facultad de firmar digitalmente mediante el empleo de determinados dispositivos o datos de creación de firma se extinguirá por las causales que se establecen a continuación:

a) Muerte del titular en caso de ser una persona natural.

b) Extinción de la persona jurídica.
c) Por declaratoria judicial de quiebra.
d) Por sanción administrativa de acuerdo a lo previsto en los reglamentos.
e) Por prescripción.
f) Otras causales establecidas en los reglamentos.

II. La extinción de la facultad mencionada en el párrafo anterior no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

Artículo 12

Administraciones Públicas

I. Esta propuesta se aplicará al uso de la firma digital en el seno de las Entidades de la Administración Pública, sus organismos públicos y las entidades, dependientes o vinculadas a las mismas y en las relaciones que mantengan aquéllas y éstos entre sí o con los particulares.

II. Entidades de la Administración Pública, con el objeto de salvaguardar las garantías de cada procedimiento, podrán establecer condiciones adicionales a la utilización de la firma digital en sus procedimientos.

III. La utilización de la firma digital en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa nacional se regirá por normativa específica.

Observación

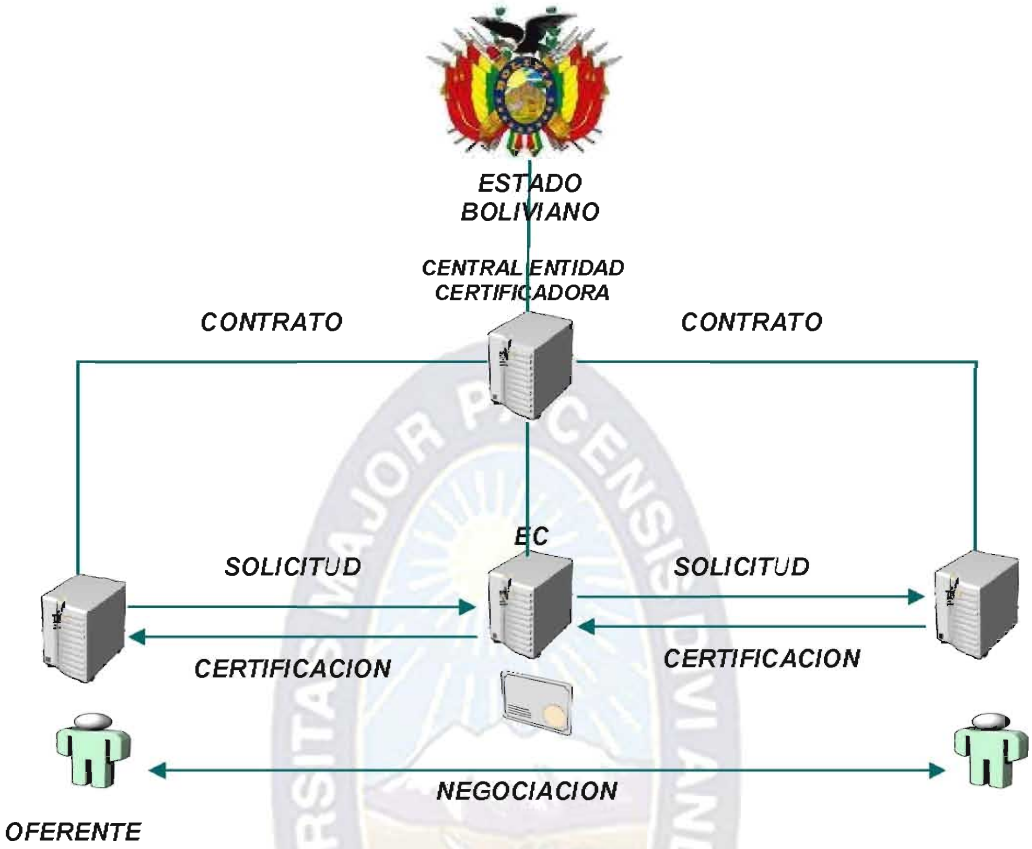
La propuesta se regirá a los procedimientos expuestos y desarrollados en el trabajo de investigación ya que los conceptos y procedimientos citados en la propuesta tienen su origen conceptual y practico en la tesis

4.6.2 PROUESTA DE ENTIDAD CERTIFICADORA

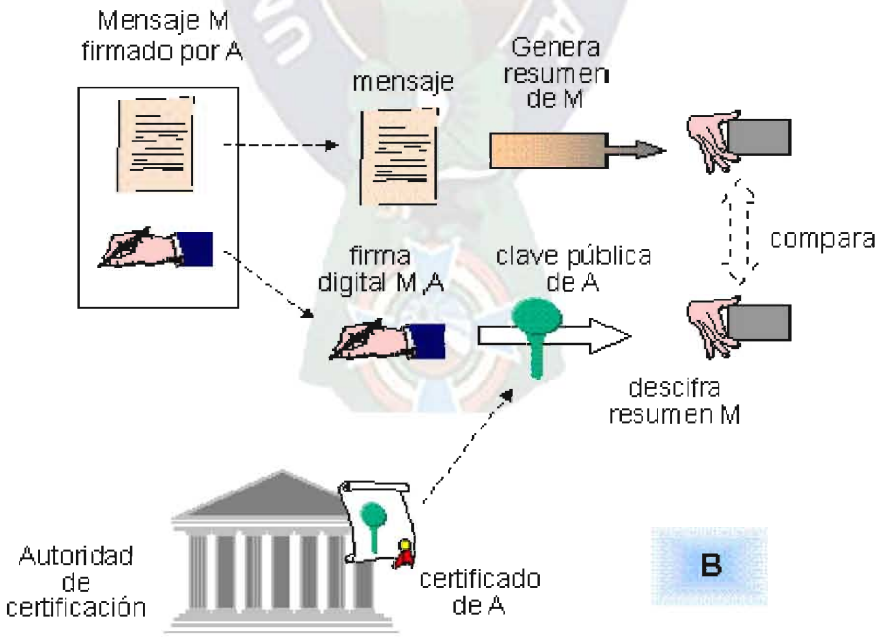
La única manera de garantizar que los proyectos nuevos, basados en tecnología, sean introducidos en la sociedad, es logrando que el Estado forme parte de el cambio.

La propuesta de la investigación sugiere que la Entidad Certificadora se un departamento estatal, la entidad manejara información confidencial, por esta razón es pertinente que ella sea parte del Estado. Así el Estado dará el pleno respaldo al encaminamiento de la realidad de firma digital en Bolivia.

En el siguiente grafico se muestra la forma de funcionalidad de la Entidad Certificadora



Fuente: elaboración propia



http://www.internautas.org/documentos/image8.gif

5.1 ESTADO FINAL DEL TRABAJO

La seguridad que presenta un contrato electrónico a través de la encriptación ha sido probada, la firma manuscrita es usada hoy en día en Bolivia aunque no es tan segura como la firma digital, en el nuevo mundo virtual, abierto para el desarrollo de la humanidad es necesario evolucionar junto con la tecnología, la sociedad boliviana ahora tiene un precedente en cuando a los contratos electrónicos no solo hecho de manera legal sino también de manera técnica, desde un punto de vista legal y también afrontado técnicamente enriqueciendo así la investigación conjunta de dos carreras, las cuales forman hoy en día pilares fundamentales dentro del desarrollo de Bolivia. La conjunción de dos ciencias, la informática y el derecho dan lugar a un campo de investigación poco explorado. La tesis realizada para la demostración de la seguridad de contratos electrónicos es solo el primer paso para la exploración conjunta en el campo de la tecnología legal.

5.2 CONCLUSIONES

La introducción del concepto de contratos electrónicos en la sociedad es de vital importancia, tan importante como abrir mercados internacionales, la tesis SEGURIDAD DE FIRMA Y CONTRATOS DIGITALES EN BOLIVIA, primero, empieza a dar alternativas a la sociedad acerca de que la tecnología, no es algo a lo cual temerle, sino que es una herramienta de progreso. Segundo, al promover la seguridad el mercado para profesionales, importadores, exportadores es abierto de manera que la distancia ya no es un impedimento.

A lo largo del periodo de investigación se probo la seguridad de los contratos electrónicos, en sus dos partes; legalmente, técnicamente. Además de proponer una ley basamentada en el punto de vista técnico, y un mecanismo de administración de la entidad certificadora. Como resultado podemos afirmar que; los contratos electrónicos son mucho mas seguros que los contratos con firma manuscrita, y pueden remplazarlos.

Todavía hay un camino muy largo por recorrer debido a que la cultura en Bolivia esta acostumbrada a estar retrasa en cuanto a países desarrollados. El solo hecho de ser llamados un país tercer mundista es un problema para el desarrollo en Bolivia. Así que es muy importante que despertemos en la sociedad la idea de tecnología y no dejar

que la tecnología nos atropelle para enseñarnos, el aporte logrado hasta aquí es sustancial. El desarrollo de la sociedad en cuanto a lo nuevo es normalmente lenta por tal motivo debemos como profesionales estimular el crecimiento y desarrollo en la sociedad boliviana.

5.3 RECOMENDACIONES

Al lo largo del desarrollo de la investigación se ha tropezado con varios problemas
La falta de conocimiento, en la carrera de derecho, la poca información en el contexto boliviano acerca de contratos electrónicos. Se recomienda que la materia "Derecho informático", en la carrera de derecho tenga un contenido más técnico y enfocado al avance tecnológico contemporáneo. Por otro lado, en la malla curricular de la carrera de informática, no existe una metería que introduzca al alumno, al apasionante mundo del Derecho Informático. Por lo tanto es necesario implementar la materia de Derecho Informático. Además de crear espacios de trabajo en los institutos de investigación de ambas carreras, tratando temas de interés para ambos De tal manera se preparará a Abogados e Informáticos, para la interactuación.
Todos los esfuerzos serian vanos si es que no se cuenta con el respaldo del Estado boliviano. El Estado boliviano debe ser el gestor más importante en contribuir a este proceso.

5.4 PROYECCIONES DE LA TESIS

Promoviendo un trabajo conjunto se estimulara la realización de un proyecto de ley que pueda ser presentado ante el congreso de la republica siendo un trabajo de investigación conjunta partiendo del buen nombre ganado por la Universidad Mayor De San Andrés, entendiendo que es una obligación de cada ciudadano contribuir en alguna manera con su sociedad. Otra proyección es incentivar la creación de carreras de especialidad como en seguridad informática dentro del pensum académico de la carrera de informática. Diseñar un plan de estudios para la carrera de derecho en cuanto al contenido de la metería de derecho informático, ya que a lo largo de la investigación se pudo ver que existen serias deficiencias en las aulas de la facultad de derecho en cuanto al tema

Así es como el contrato digital es urgentemente necesario para empezar el cambio hacia un mundo donde la tecnología se ha adelantado y ha dejado atrás a países desarrollados. La llave para abrir el mercado y la economía mundial es el contrato electrónico

REFERENCIAS BIBLIOGRAFICAS

ISO 17000

MAZEAUD, Henri y Léon; MAZEAUD, Jean. Tr. Luis Alcalá – Zamora y Castillo, Lecciones de Derecho Civil, Parte Segunda, Volumen I Obligaciones: El Contrato, La Promesa Unilateral. Año 1969, Buenos Aires – Argentina

Carlino, Bernardo P. *"Firma digital y Derecho Societario Electrónico*". Rubinzal – Culzoni Editores. Argentina, 1998.

Delpiazzo, Carlos E. "Relevancia jurídica de la encriptación y la firma electrónica en el comercio actual".

Memorias del VIII congreso Iberoamericano de Derecho e Informática México, noviembre 2000..

Horna, Pierre M. "Análisis legislativo de la Firma digital" Memorias del VIII congreso Iberoamericano de

Derecho e Informática México, noviembre 2000. Pág. 7.

Jijena Leiva, Renato. *"Firma digital y Proveedores de Servicios de Certificación*".

Memorias del VII congreso Iberoamericano de Derecho e Informática. Perú, abril 2000.

INTERNET

download.microsoft.com/download/b/b/9/bb95c403-ade1-4857-9245-e8a5d0dfc74c/TechNet_Seguridad_2003.ppt

www.auditoria.gov.co/9_documentos/6_2_8_lucio_molina_focazzio.ppt

jemarinoi.googlepages.com/8.-SeguridadInformatica.ppt

download.microsoft.com/download/b/b/9/bb95c403-ade1-4857-9245-e8a5d0dfc74c/TechNet_Seguridad_2003.ppt

www.sr-hadden.com.ar/documentos/seguridad_de_la_informacion.ppt

www.udistrital.edu.co/comunidad/grupos/ege/cti3/files/Bibliografia/Seguridad%20Informatica/SItema03.ppt

http://news.bbc.co.uk/hi/spanish/science/newsid_2431000/2431467.stm

http://www.cincodias.com/articulo/gestion/Servicios/banca/seguros/afectados/ataques/informaticos/cdscdi/20030908cdscdiges_1/Tes/

http://www.monografias.com/trabajos6/delin/delin.shtml

http://www.iworld.com.mx/iw_Opinions_read.asp?iwID=79

http://cxo_ommunity.com.ar/index.php?option=com_content&task=view&id=74&lang=es&Itemid=52
http://www.elpais.com/articulo/red/ataques/informaticos/Espana/subieron/42/ano/pasado/elpeputec/20030123elpcibenr_4/Tes
http://tecnologia.infobaeprofesional.com/notas/57711-Los-ataques-informaticos-ahora-se-concentran-en-los-equipos-con-conectividad.html?cookie
http://xbash.wordpress.com/2008/04/09/crecen-los-ataques-informaticos-desde-portales-sociales/
http://www.geocities.com/CapeCanaveral/2566/encrip/encrip.html 16:44 domingo 28 de septiembre
http://www.geocities.com/CapeCanaveral/2566/encrip/criptologia.html
http://www.geocities.com/CapeCanaveral/2566/encrip/criptogr.html
http://www.geocities.com/CapeCanaveral/2566/encrip/digital.htm
http://www.textoscientificos.com/criptografia/privada
http://es.wikipedia.org/wiki/Criptograf%C3%ADa
http://www.kriptopolis.org/algoritmos-de-encriptacion
http://es.wikipedia.org/wiki/Criptograf%C3%ADa_sim%C3%A9trica
http://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica
http://vexpert.mvps.org/articles/vbEncrypt.htm
http://es.wikipedia.org/wiki/Criptograf%C3%ADa_sim%C3%A9trica
http://www.alegsa.com.ar/Dic/c.htm
http://www.osmosislatina.com/aplicaciones/seguridad.htm
http://es.wikipedia.org/wiki/Firma_digital#Formato_de_la_firma_electr.C3.B3nica
http://www.uoc.edu/web/esp/launiversidad/inaugural01/encriptacion.html
http://intranet.logiconline.org.ve/articulos/encriptacion.html
http://www.uoc.edu/web/esp/launiversidad/inaugural01/encriptacion.html
http://www.google.com.bo/search?hl=es&q=metodos+de+encriptacion&revid=1618780168&sa=X&oi=revisions_inline&resnum=0&ct=top-revision&cd=1
http://es.wikipedia.org/wiki/Firma_digital#La_Ley_de_Firma_digital_en_el_Per.C3.BA
http://es.wikipedia.org/wiki/Firma_electr%C3%B3nica_escrita
http://es.wikipedia.org/wiki/Firma
http://es.wikipedia.org/wiki/@firma
http://es.wikipedia.org/wiki/Certificado_digital
http://es.wikipedia.org/wiki/Infraestructura_de_clave_p%C3%BAblica

http://es.wikipedia.org/wiki/Firma_digital
http://es.wikipedia.org/wiki/Firma_digital#La_Ley_de_Firma_digital_en_el_Per.C3.BA
http://es.wikipedia.org/wiki/Firma
http://es.wikipedia.org/wiki/Graf%C3%B3logo
http://es.wikipedia.org/wiki/Certificado_digital
http://es.wikipedia.org/wiki/X.509
http://es.wikipedia.org/wiki/Infraestructura_de_clave_p%C3%BAblica
http://www.portaldeabogados.com.ar/derechoinformatico/firmadigperu.htm
http://decsai.ugr.es/~jfv/ed1/tedi/cdrom/docs/
http://foro.elhacker.net/criptografia/funciones_de_hash-t100025.0.html
http://es.wikipedia.org/wiki/Hash
http://www.espaciosjuridicos.com.ar/datos/AREAS%20TEMATICAS/ECONOMICO/firmadigital.htm
http://www.conicit.go.cr/boletin/boletin4/marco.html
http://www.perspectivaciudadana.com/contenido.php?itemid=5097
http://www.elmundo.es/navegante/2008/04/15/tecnologia/1208245259.html
http://www.legistdf.gov.ar/site/documentos/firmadigital/Conferencia%20ONTI%20Profesionales.pdf
http://www.perspectivaciudadana.com/contenido.php?itemid=5097
http://www.pki.gob.ar/index.php?option=com_content&task=view&id=350&Itemid=180
http://linuxreflejo.wordpress.com/2008/07/25/conceptos-de-criptografia-y-firma-digital/
http://www.marketingycomercio.com/numero14/00abr_firmadigital.htm
http://blog.segu-info.com.ar/2006/08/luz-verde-para-la-firma-digital-en.html
http://www.monografias.com/trabajos44/normativa-firma-digital/normativa-firma-digital.shtml
http://www.pki.gob.ar/index.php?option=com_content&task=view&id=363&Itemid=180
http://www.pki.gob.ar/index.php?option=com_content&task=view&id=343&Itemid=180
http://www.pki.gob.ar/index.php?option=com_content&task=view&id=353&Itemid=180

LEY Nº 1632

LEY DE 05 DE JULIO DE 1995

GONZALO SÁNCHEZ DE LOZADA

PRESIDENTE CONSTITUCIONAL DE LA REPUBLICA

Por cuanto, el Honorable Congreso Nacional, ha sancionado la siguiente Ley:

LEY DE TELECOMUNICACIONES.-

EL HONORABLE CONGRESO NACIONAL,

DECRETA:

LEY DE TELECOMUNICACIONES

ARTICULO 7º.- CONTRATOS DE CONCESION. Los contratos de concesión, además de los requisitos generales establecidos por ley, deberán contener cláusulas sobre los aspectos que se señalan a continuación, en la medida en que la naturaleza y la extensión de los servicios así lo requieran:

a) Objeto, plazo y términos de caducidad;
b) Cláusulas reglamentarias y convencionales;
c) Instalaciones, tipos y áreas de servicios prestados y frecuencias otorgadas;
d) Derechos y protección del usuario;
e) Regulación de tarifas e interconexión;
f) Requerimientos de modernización, expansión y desarrollo de la Red;
g) Obligaciones respecto a servicios rurales;
h) Requisitos para la presentación de informes contables, operativos, de auditoría e inspecciones;
i) Tasas y derechos;
j) Obligaciones en casos de emergencia;
k) Sanciones;
1) Sistema de facturación;
m) Fianzas y otras garantías;
n) Separación contable y estructural de las operaciones;
o) Obligaciones respecto a rutas directas internacionales; y
p) Otras que la Superintendencia de Telecomunicaciones considere necesarias, dentro del marco de la ley.

ARTICULO 8º.- TRANSFERENCIA AL NUEVO TITULAR. Al vencimiento del plazo o declaratoria de caducidad de la concesión, se efectuará una licitación pública con el fin de otorgar una concesión, mediante un nuevo contrato de concesión y transferir al nuevo titular todas las instalaciones, equipos, obras y derechos del titular cesante. Este último tiene la obligación de cooperar durante todo el proceso de licitación y transferencia, no pudiendo sus acreedores oponerse a la misma. En el caso de vencimiento de plazo, el titular cesante podrá participar en la licitación para el otorgamiento de una nueva Concesión. Las disposiciones establecidas en el presente artículo se aplican únicamente a los Proveedores de Servicios Básicos de Telecomunicaciones, incluyendo Local, Móviles y Larga Distancia.

El Contrato de Concesión de los Servicios autorizará a la Superintendencia de Telecomunicaciones a efectuar, en ambos casos, la indicada licitación. El monto del pago que recibirá el titular cesante por los bienes afectados a la concesión será el valor de libros o el de licitación, el que fuera menor; deduciendo en ambos casos, los gastos incurridos en el proceso de licitación, multas y/u otros pagos pendientes.

Toda diferencia mayor que no se deba pagar al titular cesante, se depositará en una cuenta del Fondo Nacional de Desarrollo Regional para los efectos establecidos en el Art. 28º de la presente ley.

Remítase al Poder Ejecutivo para fines constitucionales.

Sala de sesiones del H. Congreso Nacional.

La Paz, 5 de julio de 1995.

Fdo. H. Juan Carlos Durán Saucedo, Presidente H. Senado Nacional; H. Javier Campero Paz, Presidente H. Cámara de Diputados; H. Walter Zuleta Roncal, Senador Secretario; H. Freddy Tejerina Ribera, Senador Secretario; H. Carlos Suárez Mendoza, Diputado Secretario; H. Yerko Kukoc del Capio, Diputado Secretario.

Por tanto, la promulgo para que se tenga y cumpla como Ley de la República.

Palacio de Gobierno de la ciudad de La Paz, a los cinco días del mes de julio de mil novecientos noventa y cinco años.

FDO. GONZALO SÁNCHEZ DE LOZADA, Alfonso Revollo Thenier, Ministro de Capitalización; Dr. Jaime Villalobos, Ministro de Desarrollo Económico; José Guillermo Justiniano Sandoval, Ministro de la Presidencia de la República.

MODIFICACION DE LOS ARTICULOS

2°, 4°, 11°, 21° TITULO VII Y 28 DE LA

LEY 1632.

LEY N ° 2342

LEY DE 25 DE ABRIL DE 2002

JORGE QUIROGA RAMIREZ

PRESIDENTE CONSTITUCIONAL DE LA REPUBLICA

Por cuanto, el Honorable Congreso Nacional, ha sancionado la siguiente Ley:

EL HONORABLE CONGRESO NACIONAL,

DECRETA:

LEY DE MODIFICACIONES A LA LEY DE TELECOMUNICACIONES, N ° 1632 DE 5 DE JULIO DE 1995 Y DE OTROS ASPECTOS COMPLENTARIOS DEL SECTOR DE TELECOMUNICACIONES

PARA LA PROMOCION DE LA COMPETENCIA.

Es dada en la Sala de Sesiones del Honorable Congreso Nacional, a los veintitrés días del mes de abril de dos mil dos años.

Fdo. Freddy Teodovich Ortíz, Luis Angel Vásquez Villamor, Wilson Lora Espada, Rubén E. Poma Rojas, Fernand6 Rodríguez Calvo, Nestor Guzmán Villarroel.

Por tanto la promulgo para que se tenga y cumpla como Ley de la República.

Palacio de Gobierno de la ciudad de La Paz, a los veinticinco días del mes de abril de dos mil dos años.

FDO. JORGE QUIROGA RAMIREZ, Alberto Leytón Avilés,

Jacques Trigo Loubiere, Carlos Kempff Bruno.