UAEM | Universidad Autónoma del Estado de México

CENTRO UNIVERSITARIO XICO VALLE DE CHALCO

C.U. Valle de Chalco

GENERACIÓN DE UN PROTOCOLO CRIPTOGRÁFICO PARA LA CERTIFICACIÓN CONJUNTA DE DOCUMENTOS OFICIALES

T E S I S

QUE PARA OBTENER EL GRADO DE

MAESTRA EN CIENCIAS DE LA COMPUTACIÓN

P R E S E N T A

ERIKA ZULEIMA PEREZ MENDEZ

TUTORA ACADÉMICA
DRA. MARÍA DE LOURDES LÓPEZ GARCÍA

TUTOR ADJUNTO
DR. MANUEL ÁVILA AOKI
TUTOR ADJUNTO
DR. SAMUEL OLMOS PEÑA

VALLE DE CHALCO SOLIDARIDAD, MÉXICO OCTUBRE 2017.

Universidad Autónoma del Estado de México
Centro Universitario Valle de Chalco

Valle de Chalco Solidaridad, Edo de Méx. a lunes, 16 de octubre de 2017

DR. EN C. JUVENAL RUEDA PAZ
COORDINADOR DE LA MAESTRÍA CIENCIAS DE LA COMPUTACIÓN
DEL CENTRO UNIVERSITARIO *UAEM* VALLE DE CHALCO.

P R E S E N T E.

Por este medio le comunico a usted que la comisión revisora designada para realizar la tesis denominada: **"Generación de un protocolo criptográfico para la certificación conjunta de documentos oficiales"**, como parte de los requisitos para obtener el grado académico de Maestría en **Ciencias de la Computación** presenta **Erika Zuleima Perez Mendez**, con número de cuenta **0922807** para sustentar el acto de evaluación de grado, ha dictaminado que dicho trabajo reúne las características de contenido para proceder a la impresión del mismo

A T E N T A M E N T E

Tutor adjunto	**Tutora Académica**	**Tutor Adjunto**
Dr. Manuel Ávila Aoki	**Dra. María de Lourdes López García**	**Dr. Samuel Olmos Peña**

Av. Hermenegildo Galeana Num 3
Col. María Isabel CP.56615
Tel. 55) 59714940 Ext.115
http://titulacioncuvalledechalco.weebly.com/

Universidad Autónoma del Estado de México
Centro Universitario Valle de Chalco

Valle de Chalco Solidaridad, Estado de México lunes, 16 de octubre de 2017

ERIKA ZULEIMA PEREZ MENDEZ
CANDIDATA A GRADO DE MAESTRÍA EN CIENCIAS DE LA COMPUTACIÓN
CENTRO UNIVERSITARIO UAEM VALLE DE CHALCO

Presente

De acuerdo con el Reglamento de Estudios Avanzados de la Universidad Autónoma del Estado de México y habiendo cumplido con todas las indicaciones que la Comisión Revisora realizó con respecto a su trabajo **Tesis** titulado **"GENERACIÓN DE UN PROTOCOLO CRIPTOGRÁFICO PARA LA CERTIFICACIÓN CONJUNTA DE DOCUMENTOS OFICIALES"** la Coordinación de la Maestría en **Ciencias de la Computación** del Centro Universitario UAEM Valle de Chalco concede la autorización para que proceda a la impresión de la misma.

Sin más por el momento, le reitero la seguridad de mi especial consideración y estima.

CENTRO UNIVERSITARIO UAEM VALLE DE CHALCO MAESTRÍA EN CIENCIAS DE LA COMPUTACIÓN

DR. EN C. JUVENAL RUEDA PAZ
COORDINADOR DE LA MAESTRÍA CIENCIAS DE LA COMPUTACIÓN
CENTRO UNIVERSITARIO UAEM
VALLE DE CHALCO

Universidad Autónoma del Estado de México
Centro Universitario Valle de Chalco

CARTA DE CESIÓN DE DERECHOS DE AUTOR

El que suscribe **Erika Zuleima Perez Mendez** Autor del trabajo escrito de evaluación profesional en la opción de Trabajo terminal de Grado con el título Generación de un protocolo criptográfico para la certificación conjunta de documentos oficiales, por medio de la presente con fundamento en lo dispuesto en los artículos 5, 18, 24, 25, 27, 30, 32 y 148 de la Ley Federal de Derechos de Autor, así como los artículos 35 y 36 fracción II de la Ley de la Universidad Autónoma del Estado de México; manifiesto mi autoría y originalidad de la obra mencionada que se presentó en el **Centro Universitario UAEM Valle de Chalco** para ser evaluada con el fin de obtener el Grado de Maestra en Ciencias de la Computación.

Así mismo expreso mi conformidad de ceder los derechos de reproducción, difusión y circulación de esta obra, en forma NO EXCLUSIVA, a la Universidad Autónoma del Estado de México; se podrá realizar a nivel nacional e internacional, de manera parcial o total a través de cualquier medio de información que sea susceptible para ello, en una o varias ocasiones, así como en cualquier soporte documental, todo ello siempre y cuando sus fines sean académicos, humanísticos, tecnológicos, históricos, artísticos, sociales, científicos u otra manifestación de la cultura.

Entendiendo que dicha cesión no genera obligación alguna para la Universidad Autónoma del Estado de México y que podrá o no ejercer los derechos cedidos.

Por lo que el autor da su consentimiento para la publicación de su trabajo escrito de evaluación profesional.

Se firma la presente en la ciudad de Valle de Chalco, a los 16 días del mes de Octubre de 2017.

Lic. Erika Zuleima Perez Mendez

Dedicatoria

Cuando miro hacia atrás puedo ver que hubo personas que para nada me desearon lo mejor, recibía críticas, palabras de desaliento diciéndome que no podía estudiar y terminar una maestría, qué con lo que hacía nada lograría. Otras apostando porque jamás llegaría a ninguna parte por el simple hecho de no estar a nivel de un Ingeniero, por ser solo una Licenciada, por lo que me pertenecía otro mundo y no el de las Ciencias en Computación. Pero lo que esas personas no saben, es que las metas no solo se realizan para obtener y merecer éxito, al contrario se hacen por gusto, por deseo, porque están en tu corazón y porque ese esfuerzo de hoy, el día de mañana nos hará feliz y valdrá la pena. Así que dedico esta tesis, a esas personas que esperaban mi fracaso en cada paso que daba hacia la culminación de esta “meta alcanzada". Gracias por sus magníficas opiniones.

Agradecimientos

A ti Dios, gracias por la sabiduría que me diste, por haberme regalado el don de la perseverancia, porque gracias a eso, soy una persona que no sabe rendirse, al contrario, busco siempre lo mejor de manera insistente para finalizar mis metas y sueños. Deposite toda mi fe en ti para este logro. Por lo que, este agradecimiento es mínimo en comparación con todo lo que me has regalado, te agradezco mis buenos y malos momentos que se presentaron en el trayecto de esta ilusión porque de ello me enseñaste a valorar esfuerzos y sacrificios.

A mi madre Olga por acompañarme en esta locura, por ser mi mejor amiga, por no haberme dejado sola en mis desvelos, siempre estuviste ahí conmigo, dándome ánimos y palabras de aliento para seguir con mi sueño. La que confía más en mí, la que me brinda su amor, apoyo incondicional, que no haría sin ti, sin tus consejos, sin tu complicidad, gracias por tu protección. Espero que este logro sea la compensación a tus desvelos y dedicación. Te amo mamita.

A mi padre Raúl, sin dudarlo este logro también es tuyo, porque eres esa persona que me apoya y confía en mí. Siempre me has permitido cumplir mis sueños, jamás me has negado la posibilidad de crecer como hija y profesionalmente. Tu esfuerzo que has realizado todo este tiempo ha dado frutos, gracias por darme la oportunidad de hacer realidad este sueño y sobre todo por tu cariño que me regalas día a día. Te adoro papá.

A mis dos hermanas Alexa y Mónica, sin querer también forman parte de mis sueños. Ustedes me han regalado momentos agradables, momentos que me han ayudado para ser feliz. Su interés que ponen en mí, me da ánimo para seguir adelante, así que no dejen de darme lata. Las quiero mucho.

A mi Tutora de tesis a la Dra. María de Lourdes López García le agradezco primordialmente por la paciencia que me tuvo cuando no entendía los temas o cuando se me olvidaba alguna indicación. Su manera estricta hizo que me pusiera las pilas para concluir este trabajo. Su esfuerzo y dedicación, me ayudaron a desempeñar de manera correcta cada una de mis actividades. Gracias por los conocimientos que me brindó y por todo el tiempo que me otorgó, sin usted no se habría logrado todo esto.

A mis tutores de tesis al Dr. Manuel Ávila Aoki y el Dr. Samuel Olmos Peña gracias por su tiempo y por sus aportaciones a mi trabajo de tesis. A los sinodales gracias por estudiar mi tesis y por su aportación de ideas y conocimientos.

Agradezco al Consejo Nacional de Ciencia y Tecnología (CONACyT) y a la Beca de Escolaridad para estudios de posgrado (UAEM) su apoyo económico permitió que continuara con mis estudios de maestría. Gracias a la contribución de estas instituciones, se puede lograr que las cosas salgan bien, y se alcance la conclusión de esta tesis en tiempo y forma.

Y por supuesto también estoy muy agradecida con el Centro Universitario Valle de Chalco (UAEM), por el apoyo brindado durante el tiempo en que fui su alumna. La dedicación que cada profesor me brindo, permitió un mejor desarrollo en mi profesión. Gracias por sus conocimientos.

Resumen

Actualmente, los procesos automatizados han tomado gran importancia en las tecnologías de la información y comunicación por el reemplazo de procesos manuales a electrónicos.

Los documentos con más de una firma son procesos que no tienen una versión automatizada. En este sentido, es importante notar que un documento con múltiples firmas no es protegido, debido a que es inusual la versión digital. Sin embargo, este tipo de documentos son susceptibles a la fabricación de una versión falsa utilizando aplicaciones especiales.

En este trabajo, se propone un esquema de certificación para un documento con tres firmas. El esquema de certificación usa dos herramientas criptográficas especiales, denominadas, *firmas agregadas* y *estampa de tiempo*, ambos basados en RSA. El proceso de certificación es realizado en orden jerárquico, garantizando que cada firmante verifica el documento antes de emitir su firma. El resultado es un documento con una firma digital que contiene dos agregaciones, que puede ser verificada por cualquier entidad.

La propuesta protege el documento de falsificaciones, gracias a la seguridad de RSA y es más eficiente que la versión manual.

Abstract

Nowadays, the process automation has taken an important point in the information technology and communication, due to, the replacement from manual to automated process.

The documents with more than one signature are process that usually are realized in a manual version. In this contexts, it is important to note that a document with multiply signatures is not protected, because they are unusual in an electronic version. However this kind of documents are susceptible to fabrication of a fake version using special applications.

In this work, a certification scheme for a document with three signatures is proposed. The certification scheme uses two special cryptography tools called *aggregate signatures*, and *time stamp*, both based on RSA. The process of certifications is realized in hierarchical order, guaranteing that the each signer verifies the document before emits the signature. The result is a document with one digital signature that contains two aggregate signatures, that can be verified by any entity.

The proposal protects the document of forgeries, thanks the security of the RSA signature, and it is more efficient than the manual version.

Índice general

Índice de figuras

Índice de tablas

1. Introducción

El uso de Internet se ha convertido en una herramienta importante entre las personas, para tareas como la transferencia de documentos digitales. Sin embargo, existen procesos que aún se realizan de manera manual, ejemplo de esto, son los documentos oficiales que contienen más de una firma.

A este tipo de documentos se les confiere una mala seguridad en sus datos, por lo que están expuestos a la modificación y a la falsificación. Esto presenta una dificultad, al querer asociar un documento con la firma autógrafa de un usuario, de tal manera que, este inconveniente produce que el intercambio de información se transforme en una acción dudosa para el usuario porque no existe una seguridad de la identidad de quién remite la firma, ni mucho menos una garantía de que los datos de ese documento oficial no fueron alterados manualmente.Ya que puede suceder que un tercero usurpe al emisor colocando una firma parecida a la original o modifique el texto sin que se encuentre la forma de hacer válida la integridad de los datos.

Lo anterior, obliga a establecer medidas de integridad y autenticación, con el fin de asegurar que los datos no sean manipulados o que alguna persona adquiera de manera maliciosa la identidad de otra. En este sentido, la criptografía es una herramienta que ayuda a contrarrestar posibles amenazas, a través de servicios de seguridad como se definen en (Maiorano, 2009).

- **Confidencialidad**, la información sólo puede ser leída por las partes autorizadas, es decir, que tengan el derecho a usarla de manera cifrada.
- **Integridad de los datos**, se refiere a que la información no haya sido alterada

en el transcurso del origen hacia el destino.

- **Autenticación**, verifica que el mensaje enviado es de quién dice ser.
- **No repudio**, permite asegurar que cualquier parte que envía o recibe información no pueda rechazar ante terceros que la envió o recibió.

Una solución a esta situación, la brinda la criptografía de llave pública (Diffie y Hellman, 1976), en específico la firma digital (Rivest y Adleman, 1978). En este contexto, la firma digital se presenta como una salvación para la seguridad de dichos documentos, dando más firmeza a la certificación de un documento oficial. Es importante mencionar, que se ha demostrado que los esquemas criptográficos son altamente seguros, por lo cual, son utilizados como herramientas primarias para la seguridad y la confianza en las comunicaciones electrónicas.

1.1. Planteamiento del problema

En la actualidad la expedición de documentos oficiales con más de una firma, por ejemplo, las solicitudes de becas, solicitudes de servicios a dependencias gubernamentales o entidades privadas, constancias, permisos que otorga un director, subdirector, jefe o administrativo, el de comisiones y económicos, entre otros, cuentan con información impresa y firmas autógrafas.

Al digitalizar este tipo de documentos, pueden estar expuestos a falsificación usando editores como Adobe, Photoshop, Paint, etc. Esto obliga a establecer medidas de identificación y autenticación con el fin de asegurar que ninguna otra persona acceda a datos ajenos o privados y a la modificación de éstos. Es por ello que se requieren otras técnicas que resuelvan dicho problema, como el uso de diferentes protocolos de seguridad que existen, basados en información confidencial, pero acaso ¿existirá un protocolo que ayude a contrarrestar la falsificación de documentos?, para ayudar a dicha problemática se pretende saber ¿qué tipo de técnicas ayudarán al usuario a identificar sin ningún tipo de dudas la falsificación de un documento?.

Por tanto, es de suma importancia un proceso de certificación digital, basándose en diferentes rasgos de una firma, porque es cierto que manualmente cada quién tiene diferentes formas de firmar y para la verificación de éstas se necesita sólo realizar una comparación visual, susceptible a la confusión. Es por eso, que se requiere investigar ¿de qué manera será posible la autenticación de la firma de un usuario?, ¿de qué manera ayuda desarrollar un protocolo criptográfico para la certificación de un documento?, ¿cómo se puede comprobar la identidad de un usuario antes de emitir una certificación?. De tal forma que sea posible identificar claramente si un documento es genuino o no.

1.2. Hipótesis

Sí se genera un protocolo criptográfico de llave pública para la autenticación de documentos oficiales entonces éstos pueden estar protegidos bajo ciertos parámetros de seguridad contra los ataques de falsificación, usurpación y modificación de sus datos.

1.3. Objetivos

General

Desarrollar un protocolo criptográfico que proteja un documento digital que contiene más de una firma ante ataques de falsificación, modificación y usurpación.

Específicos

1. Estudiar los conceptos básicos sobre los protocolos de autenticación e integridad de los datos.
2. Proponer un protocolo criptográfico para la certificación de documentos oficiales.
3. Automatizar el proceso de certificación de los documentos oficiales impresos.
4. Probar que la certificación de un documento sea de forma segura y eficiente.

5. Realizar un análisis de seguridad sobre el protocolo propuesto.

6. Comprobar la eficiencia del protocolo propuesto a través de una prueba piloto.

1.4. Alcances de la investigación

Esta investigación tomará en cuenta el estudio y análisis de la información referente al problema de la inseguridad de los datos y la falsificación de un documento oficial que contenga más de dos firmas, tomando en cuenta aquellos elementos que aporten criterios con los cuales se pueda validar la información del protocolo y que permita de alguna manera realizar pruebas de validación.

1.5. Metodología

La investigación básica de tipo documental permitirá identificar las herramientas correctas para la generación del protocolo propuesto. Debido al desarrollo de un protocolo criptográfico para certificar documentos que requieren más de dos firmas, también la investigación es de tipo aplicada, gracias a la realización de pruebas que se implementan para el cumplimiento de los objetivos de este trabajo.

Para la realización de esta investigación se usa una metametodología porque se desarrolla un nuevo método para certificar documentos oficiales con más de una firma. De acuerdo a la Figura 1.1, se analiza el modelo de capas del esquema de certificación basado en firmas digitales y agregadas.

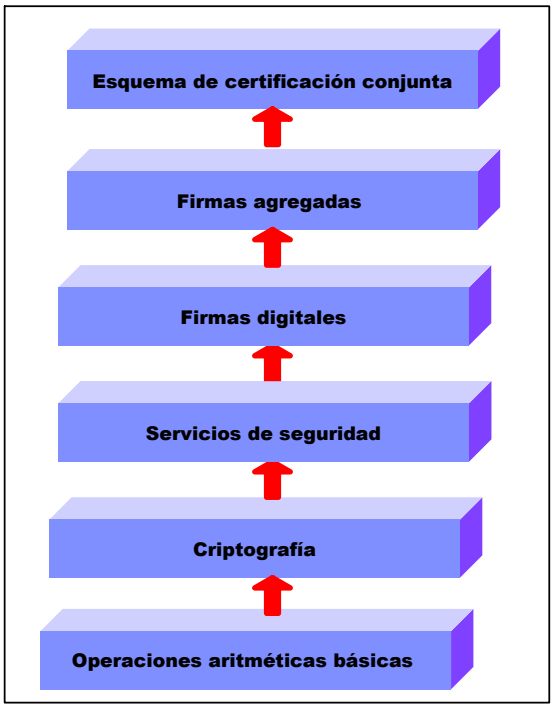


Figura 1.1: Modelo de capas de un esquema de certificación conjunta. (Elaboración propia, 2017)

El modelo anterior exige el conocimiento de las capas previas, de tal forma que es necesario estudiar desde las operaciones aritméticas básicas de la criptografía hasta las firmas agregadas para generar un esquema de certificación conjunta.

1.6. Organización de la tesis

El contenido de la tesis se organiza como sigue. En el capítulo 2, se presentan los fundamentos criptográficos de las herramientas que son utilizadas por el esquema propuesto. En el capítulo 3 se realiza un análisis de la certificación conjunta de los documentos no digitales. Por lo tanto, en el capítulo 4 se muestra la funcionalidad del esquema propuesto, considerando los pasos que el proceso manual debe realizar, con presentación del flujo de datos entre las entidades participantes y un análisis de seguridad y eficiencia. La comprobación e implementación del protocolo se presenta en el capítulo 5. Por último, en el capítulo 6, se listan las conclusiones de este trabajo.

2. Principios criptográficos

Este capítulo introduce los conceptos básicos que engloban el tema de la criptografía, donde se presenta su definición, los servicios que ofrece para proteger la información, el tipo de clasificación para saber los distintos métodos propuestos y que hasta la actualidad se han encargado de garantizar la seguridad de los datos. Por otro lado, se presentan las herramientas criptográficas que fueron empleadas para la elaboración del protocolo propuesto.

2.1. Criptografía

La palabra *criptografía* proviene del griego *kryptos*, que significa ocultar y *graphos* que es escritura, es decir, escritura escondida, ha sido usada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo las personas autorizadas tengan acceso al mensaje. También, es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hace posible que la transferencia de información sea segura y que sólo pueda ser leída por las personas a quienes va dirigida (García, 2011).

A lo que se le llama cifrar es al proceso de ocultar información confidencial aplicando técnicas criptográficas para esconder el mensaje, mientras se manda el mensaje por una línea de comunicación que se supone es insegura y después sólo el receptor autorizado puede obtener el mensaje escondido, a esto se le conoce como descifrar.

En su clasificación dentro de las ciencias, la criptografía proviene de una rama de las matemáticas, que fue iniciada por el matemático Claude Elwood Shannon en

1948, denominada: Teoría de la Información. Esta rama de las ciencias se divide en: Teoría de Códigos y en Criptología, a su vez la Criptología se divide en Criptoanálisis y Criptografía (Paredes, 2006). Formalmente hablando, se define como: (Menezes, Van Oorschot, y Vanstone, 2001):

Definición 2.1.1 *La criptografía es la disciplina que estudia las técnicas matemáticas relacionadas a la seguridad de la información, que provee los servicios de confidencialidad, integridad de los datos, autenticación y no rechazo.*

La criptografía se clasifica históricamente en dos: clásica y moderna. La primera es aquella que se utilizó antes de la era computacional, es decir, a mitad del siglo XX. También puede entenderse como la criptografía no computarizada o mejor dicho no digitalizada. Los métodos utilizados eran variados, algunos muy simples y otros muy complicados de criptoanalizar para su época. Las técnicas criptográficas eran muy perspicaces para enviar mensajes secretos entre las personas que tenían el poder o en época de guerra para enviar instrucciones. A diferencia de la criptografía moderna, el algoritmo del sistema criptográfico se mantenía en secreto.

Esta criptografía también incluye la construcción de máquinas, que mediante mecanismos, comúnmente engranes o aspas, transformaban un mensaje en claro a un mensaje cifrado, como la máquina Enigma usada en la Segunda Guerra Mundial. Esta criptografía emplea los cifradores por transposición y por sustitución. Los primeros cifradores utilizaban la técnica de permutación de forma que los caracteres del texto se reordenan mediante un algoritmo específico.

Los cifradores por sustitución utilizan la técnica de modificación de cada carácter del texto en claro por otro correspondiente al alfabeto de cifrado. Si el alfabeto de cifrado es el mismo que el del mensaje o bien el único, hablamos entonces de cifradores monoalfabéticos; es decir, existe un único alfabeto en la operación de transformación del mensaje en criptograma. Por el contrario, si en dicha operación intervienen más de un alfabeto, se dice que el cifrador es polialfabético, como ejemplo de estas técnicas es la escítala, esta usa un cifrado de transposición de grupos y el cifrado César usa el de sustitución monoalfabética (Paredes, 2006).

En el caso de la criptografía moderna se clasifica en dos grupos, en criptografía de llave secreta o simétrica y en criptografía de llave pública o asimétrica.

2.1.1. Criptografía de llave secreta

En un escenario básico de comunicación, como se puede apreciar en la Figura 2.1 existen dos entidades, *Alicia* y *Beto* quienes desean establecer una comunicación segura en contra de un oponente denominado *Carlos* que quiere interceptar y conocer la información transmitida entre ellos. La información que Alicia transmite a Beto tiene un proceso de transformación del texto original m denominado texto en claro por medio de una función de cifrado E parametrizada por una llave k para producir un texto nuevo c que se conoce como texto cifrado, el cual asegurará la información evitando que sea expuesta ante Carlos. La información es recibida por Beto quien toma c y k como parámetros de entrada de la función de descifrado D para obtener m.

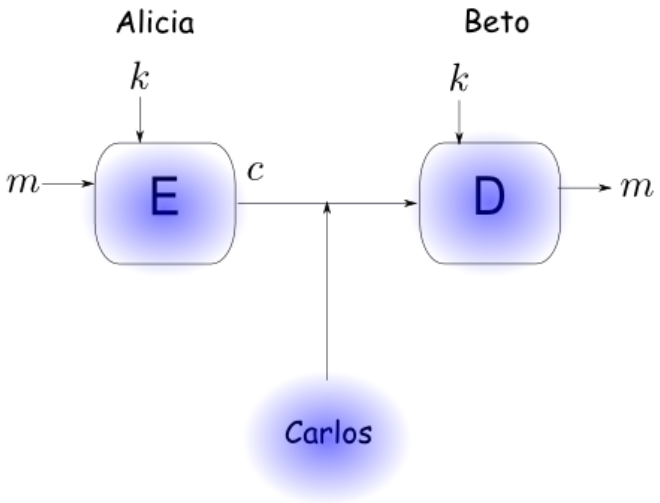


Figura 2.1: Cifrado y descifrado, criptografía de llave secreta. (Elaboración propia, 2017)

Formalmente hablando, la criptografía de llave secreta es definida como sigue (Rodríguez-Henríquez, Saqip, Díaz-Pérez, y Kaya, 2006):

Definición 2.1.2 Sea $\mathcal{P}$ el conjunto finito de textos en claro, $\mathcal{C}$ el conjunto finito de

textos cifrados, $\mathcal{K}$ el conjunto finito de llaves secretas. La Criptografía de Llave Secreta consiste en la tupla $(\mathcal{P}, \mathcal{C}, \mathcal{K}, E, D)$ donde $E : \mathcal{K} \times \mathcal{P} \to \mathcal{C}$ y $D : \mathcal{K} \times \mathcal{C} \to \mathcal{P}$, tal que para cada $k \in \mathcal{K}$ y $m \in \mathcal{P}$, se cumple que $D(k, E(k, m)) = m$.

Un *esquema de cifrado* consta de tres algoritmos (Gen, E, D) tales que,

i. *Gen* es el algoritmo de generación de llaves. Requiere de una comunicación previa (tal vez insegura) entre las partes, con la finalidad de compartir la llave secreta.

ii. *E* es el algoritmo de cifrado. Tiene como entrada la llave secreta $k \in \mathcal{K}$ y un texto en claro $m \in \mathcal{P}$ y como salida el texto cifrado $c \in \mathcal{C}$.

iii. *D* es el algoritmo de descifrado. Tiene como entrada la misma llave secreta de E y el texto cifrado $c \in \mathcal{C}$ y obtiene como salida el texto en claro $m \in \mathcal{P}$.

A pesar de que los esquemas de cifrado ofrecen alta seguridad y eficiencia computacional, su principal restricción es la distribución de la llave. Dado que tanto el cifrado como el descifrado usan la misma k, ambas partes en la comunicación deben acordar un mecanismo que les permita obtener la llave secreta de tal manera que no se exponga ante alguna entidad maliciosa.

2.1.2. Criptografía de llave pública

La criptografía de llave pública fue desarrollada para resolver el problema de intercambio de llaves (Diffie y Hellman, 1976), a través de *funciones de sólo ida* e *información secreta*, definidas a continuación:

Definición 2.1.3 Una función $f : \{0,1\}^* \to \{0,1\}^*$ es de *sólo ida*, si se satisfacen las siguientes condiciones:

$i)$ f *es fácil*, es decir, existe un algoritmo $\mathcal{A}$ de tiempo polinomial que calcula eficientemente $f(x)$ para todo x.

ii) f^{-1} ***es difícil***, es decir, para cada algoritmo $\mathcal{A}$ de tiempo polinomial, existe la probabilidad desdeñable de que dada la imagen $f(x)$ obtenga x.

La información secreta es información esencial que permite calcular el inverso de la función de sólo ida. Los esquemas de llave pública usan una llave pública y una llave privada, ambas asignadas a cada usuario del sistema. La llave privada es conocida sólo por su propietario y la llave pública como su nombre lo indica es de dominio público. Esta última se calcula usando una función de sólo ida y la llave privada es la información secreta para resolverla.

Los esquemas de cifrado de llave púlbica constan de tres algoritmos principales: generador de llaves, cifrado y descifrado; y un algoritmo adicional que también suele incluirse denominado generador de parámetros de dominio. La generación de llaves es invariable en los esquemas de llave pública. El objetivo es generar la llave privada denotada como ks_x y obtener la llave pública (kv_x) para una entidad x. El cifrado es la operación pública, donde *Alicia* que desea cifrar el mensaje m, usa la llave pública de *Beto*, de la forma $E_{kv_B}(m) = c$. El descifrado es la operación privada, donde B al recibir el mensaje cifrado, obtiene m usando su llave privada, $D_{ks_B}(c) = m$. La Figura 2.2 muestra el procedimiento.

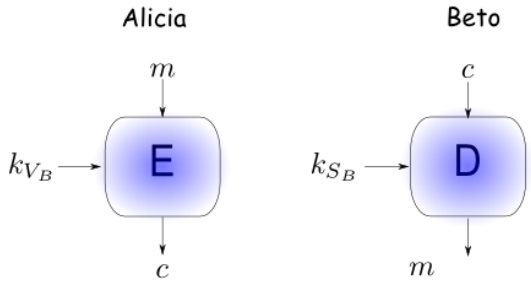


Figura 2.2: Cifrado y descifrado, criptografía de llave pública. (Elaboración propia, 2017)

2.1.3. Esquemas de firma digital

En la criptografía moderna, los esquemas de llave pública son ampliamente usados para generar firmas digitales. Una firma digital es una firma autógrafa, pero tiene el

servicio adicional de proteger la información de alteraciones intencionales de alguna entidad maliciosa. La llave privada del usuario es requerida por el firmante para generar una única e infalsificable firma digital para un documento dado, mientras que la llave pública debe ser conocida por el verificador de la firma, para decidir si la firma del documento es válida o no. Una firma digital consta de los siguientes elementos:

- $\diamond$ $\mathcal{M}$ representa el conjunto de todos los mensajes que pueden ser firmados.
- $\diamond$ $\mathcal{S}$ representa el conjunto de todas las firmas que pueden ser generadas, usualmente con una longitud fija.
- $\diamond$ $\mathcal{K}_{\mathcal{S}}$ representa el conjunto de llaves privadas.
- $\diamond$ $\mathcal{K}_{\mathcal{V}}$ representa el conjunto de llave públicas.
- $\diamond$ $\mathcal{S}_{\mathcal{E}} : \mathcal{M} \times \mathcal{K}_{\mathcal{S}} \rightarrow \mathcal{S}$ representa las reglas de transformación para que la entidad $\mathcal{E}$ produzca una firma.
- $\diamond$ $\mathcal{V}_{\mathcal{E}} : \mathcal{M} \times \mathcal{K}_{\mathcal{V}} \rightarrow \{verdadero, falso\}$ representa las reglas de verificación de la transformación para una firma producida por $\mathcal{E}$. Estas reglas son usadas por las entidades que requieran la verificación de la firma.

Una firma digital se define como (Rodríguez-Henríquez y cols., 2006):

Definición 2.1.4 Un esquema de firma digital es la tripleta de algoritmos (*Genera,Firma,Verifica*) tales que,

i. *Genera* es el algoritmo de generación de llaves. Tiene como entrada el parámetro de seguridad ℓ y como salida el par $(k_{\mathcal{S}}, k_{\mathcal{V}}) \in \mathcal{K}_{\mathcal{S}} \times \mathcal{K}_{\mathcal{V}}$, correspondiente a la llave privada y pública, respectivamente.

ii. *Firma* es el algoritmo de firma. Tiene como entrada $(m, k_{\mathcal{S}}) \in \mathcal{M} \times \mathcal{K}_{\mathcal{S}}$ y como salida un elemento $\sigma \in \mathcal{S}$, el cual es la firma del mensaje m, producida con la llave privada $k_{\mathcal{S}}$.

iii. *Verifica* es el algoritmo de verificación. Tiene como entrada $(m, \sigma, k_{\mathcal{V}}) \in \mathcal{M} \times \mathcal{S} \times \mathcal{K}_{\mathcal{V}}$ y como salida un valor *verdadero* para indicar una firma válida o un valor *falso* en caso contrario. Se dice que una firma es válida si

$$\textit{Verifica}(m, Firma(m, k_{\mathcal{S}}), k_{\mathcal{V}}) = verdadero$$

se cumple para cada $(k_{\mathcal{S}}, k_{\mathcal{V}})$ obtenido del algoritmo *Genera* y para cada $m \in \mathcal{M}$.

2.1.4. Funciones Hash (picadillo)

Una función picadillo es una función de sólo ida que toma una cadena de longitud arbitraria y la comprime en una cadena de longitud fija. Formalmente, se define como sigue:

Definición 2.1.5 *Una función picadillo $H : \{0,1\}^* \to \{0,1\}^n$ es una función de sólo ida que proyecta una cadena binaria de longitud arbitraria a una cadena binaria de longitud fija. Se dice que, $H(x)$ es el digesto de $x \in \{0,1\}^*$, de longitud n.*

Una función picadillo H se considera segura, si los tres siguientes problemas son difíciles de resolver (Stinson, 2006).

1. *Transformación mezclada*: un cambio a la entrada de incluso 1 bit, produce una salida diferente.
2. *Preimagen*: Dado $y \in \{0,1\}^n$, encontrar $x \in \{0,1\}^*$ tal que $H(x) = y$.
3. *Colisión*: Dado $x \in \{0,1\}^*$, encontrar $x' \in \{0,1\}^*$ tal que $x \neq x'$ y $H(x) = H(x')$.

Las funciones picadillo son utilizadas en los esquemas de firma digital y en la verificación de la integridad de los datos, en donde se pueden tener dos escenarios. El primero de ellos, cuando los datos son transmitidos y el canal de comunicación introduce errores en ellos. El segundo, cuando una entidad cambia maliciosamente los datos antes de que lleguen al destino. En ambos casos, la función picadillo garantiza

que cualquier modificación realizada a los datos originales, modificará el picadillo de los mismos.

En las firmas digitales, una función *hash* es un algoritmo que se utiliza para amparar a un documento digital de integridad, esto es, detectar cualquier alteración posterior a su certificación. Por lo que, este algoritmo produce una cadena en función del documento. El largo de la cadena depende de la versión del algoritmo de la función *hash* utilizada y si el algoritmo se aplica siempre al mismo documento produce la misma cadena en cuestión, pero si el documento varía en tan sólo un bit de información, la cadena producida va a diferir completamente a la anterior. La cadena creada por este algoritmo determina al documento en forma unívoca (Flores, 2005).

La función *hash* se encuentra categorizada dentro de una clase de funciones que se conocen como funciones de una sóla ida, es decir, que dado un documento es posible obtener siempre su resumen pero, por el contrario, es prácticamente imposible deducir el documento original a partir del resumen. Esto permite garantizar la unicidad e integridad del documento que se esta por firmar. Cabe destacar que, una función *hash* debe calcularse de manera eficiente y además debe asegurar que el cambio de incluso en un bit en *x*, producirá un digesto diferente.

2.1.5. Estampa de tiempo

Una estampa de tiempo provee una prueba de la existencia de un dato o un documento en un instante de tiempo. Consiste en agregar la fecha y la hora a la información deseada, con lo cuál se previene la corrupción del tiempo, al momento de ser creada dicha información. Para que el estampado sea seguro se debe garantizar la integridad, es decir, que el cambio del documento o de la estampa debe ser detectado.

En el caso de un documento firmado digitalmente es importante conocer el estado del documento electrónico en el preciso momento en el que es generada la firma, por lo que es indispensable aplicarla, el cual permite garantizar que la información contenida en el mismo no se ha modificado desde el momento que se generó la estampa.

Esta estampa de tiempo se genera con la función $hash$, la fecha y con la hora

de una fuente fiable de tiempo, y su respectiva firma digital, después la Autoridad de Sellado de Tiempo (TSA) proporciona el sello al solicitante y este lo adjunta a la información para verificar y garantizar a la vez la integridad del tiempo. Esta herramienta se utiliza para almacenar de manera segura los documentos electrónicos.

Para realizar este tipo de estampa, primero se solicita a una (TSA) para que habilite los servicios y se pueda realizar el proceso de sellado, para este requisito se necesita comprobar que la firma y el certificado sean válidos. Según (Hernández y Ramos, 2007), se tiene que tomar en cuenta que existe una diferencia de tiempo entre el momento real de la generación de la firma por parte del firmante y el momento en que la autoridad de validación (VA) valida la firma, por lo tanto, aconseja que la diferencia de tiempo sea la menor posible, para que se otorgue la máxima fiabilidad a las firmas electrónicas.

2.2. Infraestructura de llave pública *PKI*

PKI (por sus siglas en inglés, Public Key Infrastructure), es una combinación de software, hardware, tecnologías de cifrado y servicios que permiten proteger la información en su transmisión.
Específicamente hablando, *PKI* es un sistema para la gestión de certificados digitales y aplicaciones de firma digital, es la integración de criptografía simétrica, asimétrica y funciones $hash$ que ofrece a cada uno de los usuarios un conjunto de servicios relacionados con la identificación y el control de acceso como:

- Crear certificados que asocian la identidad de un usuario con una llave pública.
- Dar a conocer certificados desde una base de datos.
- Agregar credibilidad a la autenticidad del certificado.
- Confirmar o negar que el certificado sea válido.

- Invalidar certificados para los usuarios que no tengan acceso permitido o si la llave privada ha sido expuesta.

Por tanto, una *PKI* debe garantizar los siguientes servicios de seguridad de integridad, confidencialidad, autenticación y no repudio. A menudo *PKI*, es considerado un estándar, por ser un conjunto de políticas, productos y procedimientos, que se dejan a la interpretación sin tener un sentido estricto, los procedimientos dictan como las llaves deberían ser generadas, manejadas y usadas. Finalmente, los productos en realidad ponen en práctica las políticas y ellas generan, almacenan y manejan las llaves.

El proceso para construir una *PKI* deberá siempre partir de la definición de las políticas operativas y contempla como requerimiento esencial asegurar la calidad y seguridad de las operaciones que los usuarios finales realizan con sus llaves privadas. La infraestructura de llave pública se constituye de cinco elementos según (Cruz, 2009):

1. Autoridades de Certificación (AC): fuente de confianza de una infraestructura de llave pública, que emiten los certificados digitales y los firman con su llave privada. Entre las actividades que realizan se encuentran el almacenamiento de los certificados en un repositorio público, la certificación del vínculo entre la llave pública y un usuario final, la gestión de la validez del certificado por expiración o por renovación.

2. Autoridades de Registro (AR): entidades que realizan el proceso de registro de los usuarios, validando los datos del solicitante, verificando el enlace entre la entidad titular y su llave pública, y generando el par de llaves de la entidad solicitante.

3. Repositorios: lugares donde la información de los certificados y las listas de revocación son almacenados.

4. Listas de revocación de certificados: listas de los certificados que han dejado de ser válidos por algún motivo y por tanto, en los que no se puede confiar. Se pueden revocar en casos como: la llave privada ha sido comprometida, hayan cambiado los datos del certificado, o la llave privada ha expirado.

5. Aplicaciones: software capaz de operar con los certificados digitales, que hace posible, por poner algún ejemplo, el uso de cifrado y firma digital en documentos o

correo electrónico.

Es importante destacar que el principal objetivo de un sistema PKI es la gestión y distribución de llaves públicas, la cual es llevada a cabo por una Autoridad Certificadora (AC). La PKI en sentido general se basa en un modelo de confianza, en el cual, los usuarios confían que las llaves públicas gestionadas por dicha PKI son auténticas (Adams y Lloyd, 2002).

Una *PKI* se compone de muchas Autoridades Certificadoras (ACs) vinculadas a rutas de confianza. Una ruta de confianza conecta a un componente confiable con una o más terceras partes confiables, de tal forma que todas las partes tengan confianza en la validez de un certificado. Es importante resaltar que, los usuarios finales deben confiar en las ACs porque son las que confirman plenamente la identidad del suscriptor con sus respectivos documentos de identidad.

2.3. Herramientas criptográficas

Existe una gran variedad de algoritmos o esquemas criptográficos, en este proyecto se utilizan dos esquemas de firma digital. Es importante considerar que la firma manuscrita tiene reconocimiento legal elevado a pesar de que pueda ser falsificada, pero tiene características que la hacen sencilla de elaborar, de comprobar y de relacionar a quién la crea, según (Peñaranda, 2011) porque la verdadera firma manuscrita sólo puede ser realizada por una persona y puede ser comprobada por cualquiera con la ayuda de una muestra.

En materia de firma digital, para intentar conseguir los mismos efectos legales que la firma manuscrita, se requiere el uso de la criptografía y el empleo de algoritmos matemáticos. El fin que persigue la firma digital es el mismo que el de la firma manuscrita, es decir, dar asentamiento y compromiso con el documento firmado, lo que trae como consecuencia positiva facilitar la autentificación a distancia entre partes que no necesariamente se conocen, proveyendo seguridad y confianza en las redes abiertas. Las características deseables de una firma digital son las siguientes (Abbas, 2004):

- Única.
- Verificable.
- Bajo control exclusivo del firmante.
- Ligada a la información del mensaje.
- Acorde con la reglamentación.

La firma digital de un mensaje electrónico está asociado a un proceso coordinado, organizado y secuencial para permitir que sea seguro, por lo tanto, se debe cumplir lo siguiente según (Rojas y Meneses, 2011):

1. El emisor crea un mensaje determinado.
2. El emisor aplica al mensaje una función $hash$ y así obtiene un resumen del mensaje.
3. El emisor cifra el mensaje utilizando su llave privada.
4. El emisor le envía al receptor una notificación con los siguientes elementos:
    - El cuerpo del mensaje (sin cifrar o cifrado, por medio de la llave pública del receptor).
    - La firma del mensaje, que se compone de: el $hash$ o mensaje cifrado con la llave privada del emisor y el certificado digital del emisor con todos sus datos y que está cifrado con la llave privada del prestador de servicios de certificación.

Para que una firma digital producida sea válida debe cumplir:

- Vigencia: haber sido creada durante el periodo de vigencia del certificado digital válido del firmante.

- Verificación: ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente.
- Emisión: ser validada con un certificado que haya sido emitido o reconocido por un certificador.

Las propuestas desarrolladas de esquemas de firma digital han sido variadas, sin embargo, el primer esquema propuesto fue la firma digital RSA.

2.3.1. Firma digital RSA

El esquema de firma digital RSA, es el esquema más utilizado en la actualidad por su simplicidad. La generación de llaves, la generación de la firma y la verificación son como sigue (Rivest y Adleman, 1978):

Generación de llaves: el usuario genera un par de llaves de la forma (N, e) para la llave pública y (N, d) para la llave privada, de acuerdo al algoritmo de generación de llaves de RSA:

1. Elige aleatoriamente dos números primos p y q, de $\ell/2$ bits de longitud, con ℓ definido de acuerdo al nivel de seguridad deseado.
2. Elige aleatoriamente un número pequeño e (normalmente $e = 2^{16} + 1$).
3. Calcula $N = p * q$.
4. Calcula $\phi(N) = (p-1)(q-1)$, con $mcd(e, \phi(N)) = 1$.
5. Obtiene d tal que $d \equiv e^{-1} \, mod \, \phi(N)$.

Generación de la firma: el usuario usa su llave privada (N, d) para generar la firma del mensaje M de la siguiente manera:

1. Obtiene el picadillo $h = H((M)$, con la función hash H elegida.
2. Calcula $\sigma = h^d \, mod \, N$, donde σ es la firma digital del mensaje.

Verificación de la firma: al verificador se le entrega la firma σ, el mensaje M y la llave pública del firmante (N, e) y procede como sigue:

1. Verifica la validez de la llave pública con el certificado digital.
2. Calcula $y = \sigma^e \, mod \, N$.
3. Obtiene el picadillo $h = H(M)$.
4. Compara si y es igual a h entonces la firma es válida, o inválida en otro caso.

La seguridad de la firma digital RSA se basa en el problema de factorización de números grandes. En la firma digital RSA, el módulo es un número compuesto por la multiplación de dos números primos grandes. La longitud de los primos debe ser mínimo de 512 bits para garantizar que el problema de factorizar el producto sea intratable computacionalmente. Así, el módulo N (producto de los primos p y q) tendrá una longitud de 1024 bits, consiguiendo con esto, una seguridad de 80 bits, es decir, se requieren como mínimo 2^{80} operaciones para vulnerar el esquema. Bajo este escenario, el esquema de firma digital RSA se considera seguro.

2.3.2. Firma agregada basada en RSA

Es un tipo de firma digital que soporta la agregación. En (Boneh y Shacham, 2003) se define de la siguiente manera:

Definición 2.3.1 *Dado n firmas de n distintos mensajes provenientes de n distintos usuarios, es posible agregar todas esas firmas en una sola. La verificación de la firma resultante bastará para que se valide que los n usuarios participantes firmaron los n mensajes. Por tanto, un esquema de firma agregada permite que n firmantes, reduzcan el tiempo de las n firmas individuales. En este esquema, la firma de agregación sólo puede hacerse durante el proceso de la firma. Cada firmante a su vez añade su firma al agregado actual.*

Las propiedades que debe cumplir son las de una firma digital:

- Infalsificable: el firmante actual no podrá modificar la información de los firmantes anteriores, de lo contrario se invalidaría toda la firma.
- Verificable: para verificar la firma agregada basta con verificar la firma del último firmante.

Las firmas agregadas son una generalización de multifirmas, en el que las firmas son realizadas por varios usuarios, en varios mensajes distintos que se pueden combinar en un agregado cuya longitud es la misma que la de una sola firma. El uso de una firma agregada es en lugar de varias firmas individuales para mejorar el rendimiento y el ahorro de espacio (Brogle y Reyzin, 2014).

Existen variaciones de las firmas agregadas como la propuesta en (Lysyanskaya y Shacham, 2004), donde la firma agregada está basada en RSA y se genera de forma secuencial en tres fases:

Fase 1. Generación de llaves: cada usuario i genera un par de llaves de la forma (N_i, e_i) para la llave pública y (N_i, d_i) para la llave privada, de acuerdo al algoritmo de generación de llaves de RSA:

1. Elige aleatoriamente dos números primos p y q, de $\ell/2$ bits de longitud, con ℓ definido de acuerdo al nivel de seguridad deseado.
2. Elige aleatoriamente un número pequeño e (normalmente $e = 2^{16} + 1$).
3. Calcula $N = p * q$.
4. Calcula $\phi(N) = (p-1)(q-1)$, con $mcd(e, \phi(N)) = 1$.
5. Obtiene d tal que $d \equiv e^{-1} \, mod \, \phi(N)$.

Fase 2. Generación de la firma: al usuario i se le entrega una firma agregada σ', los mensajes $M_1, ..., M_{i-1}$ y sus correspondientes llaves públicas $(N_1, e_1), ..., (N_{i-1}, e_{i-1})$.

El usuario i verifica la firma σ', usando el procedimiento de verificación mostrado en la fase 3. Si la firma es válida entonces:

1. Calcula el digesto $h_i = H((M_1, ..., M_i), ((N_1, e_1), ..., (N_i, e_i)))$, con la función hash H elegida.
2. Obtiene $y = h_i + \sigma'$.
3. Calcula $\sigma = y^{d_i} \, mod \, N_i$, donde σ es la firma agregada secuencialmente.

Fase 3. Verificación de la firma: al verificador se le entrega una firma agregada σ, los mensajes $M_1, ..., M_i$, las correspondientes llaves públicas $(N_1, e_i), ..., (N_i, e_i)$ y procede como sigue:

1. Verifica que no haya duplicidad en alguna llave pública.
2. Calcula $y = \sigma^{e_i} \, mod \, N_i$.
3. Obtiene el digesto $h_i = H((M_1, ..., M_i), ((N_1, e_1), ..., (N_i, e_i)))$.
4. Calcula $\sigma' = y - h_i \, mod \, N_i$.
5. La verificación es recursiva hasta que $\sigma = 0$.

Este esquema ofrece la facilidad de generar una firma agregada adicionando de manera secuencial cada firma. Lo que le permite trabajar en un escenario donde la jerarquía es importante.

2.3.3. Certificado digital

Un certificado digital, tiene una similitud con la licencia de conducir, misma que admite el derecho de viajar por las carreteras, mientras que un certificado digital permite navegar por la red de Internet, la principal característica es que otorga identidad al usuario y puede navegar con seguridad. De igual forma una licencia de conducir le asigna identidad a quien la porta en ciertos casos, el certificado digital ofrece lo mismo pero a

una llave pública que puede comportarse como una persona en el espacio cibernético (Ford y Baum, 1997) (Feghhi y Williams, 1999).

El nacimiento del certificado digital fue a raíz de resolver el problema de administrar las llaves públicas y que la identidad del dueño pudiera ser falsa. La idea es que una tercera entidad intervenga en la administración de las llaves públicas y asegure que éstas tengan asociado un usuario claramente identificado. Esto fue inicialmente planteado por Kohnfelder en su tesis de licenciatura (Kohnfelder, 1978).
Las tres partes más importantes de un certificado digital son:

1. Una llave pública.
2. La identidad del implicado: nombre y datos generales.
3. La firma de una tercera entidad llamada autoridad certificadora que todos reconocen como tal y que válida la asociación de la llave pública en cuestión con la persona que dice ser.

Un certificado es seguro por lo siguiente:

- La autoridad certificadora firma digitalmente el certificado calculando su valor $hash$ y lo firma con su llave privada.
- La generación del certificado involucra algoritmos criptográficos para firmas digitales.

Esto dificulta la falsificación, ya que el adversario necesita conocer la llave privada de la autoridad certificadora. Si un atacante modifica el certificado, el valor $hash$ cambia y no coincidirá con la firma que la autoridad certificadora generó.

Por estos motivos, un certificado digital de llave pública permite asegurar que la llave pertenece a la entidad certificada y que dicha entidad posee la correspondiente llave privada.
El proceso para obtener un certificado digital es el siguiente propuesto por (García, 2011):

1. El solicitante se dirige a una empresa o entidad que tenga el carácter de Prestador de Servicios de Certificación y solicita de ellos las llaves y el certificado digital correspondiente a las mismas. Este trámite generalmente se puede realizar presencialmente, acudiendo a dicha entidad o virtualmente, por medio de Internet, utilizando la página Web del Prestador de Servicios de Certificación.

2. El prestador de Servicios de Certificación comprobará la identidad del solicitante, bien sea directamente o por medio de entidades colaboradoras (Autoridades Locales de Registro), para lo cual se deberá mostrar el Documento Nacional de Identidad (DNI) y si se trata de un representante de una sociedad (administrador, apoderado, etc.) o de cualquier otra persona jurídica, deberá acreditar documentalmente el cargo y las facultades del mismo (vigencia de poderes).

3. El prestador de Servicios de Certificación mediante los dispositivos técnicos adecuados crea las llaves pública y privada que le corresponde al solicitante, y genera el certificado digital correspondiente a dichas llaves.

Los estándares para los certificados facilitan el desarrollo y compatibilidad de una infraestructura de certificados, definen los mecanismos de seguridad, mensajes, estructura de los datos y los procedimientos del manejo de la información para firmas y certificados digitales. A continuacion se presentan los elementos que se han estandarizado según (Cruz, 2009) son:

- X.509: Formato de certificados.

- PKCS#10: Solicitudes de certificación. Describe la sintaxis para solicitudes de certificación. Una solicitud consiste en un nombre y la llave pública.

- PKCS#7: Formato para enviar el certificado al solicitante. Define y especifica el mecanismo de propósito general para la creación de una especie de sobre firmado digitalmente.

- PKCS#12: Formato para transferir y almacenar certificados junto con sus llaves privadas. Especifica el formato de intercambio diseñado para transferir los certificados, rutas de certificación y las llaves privadas entre las computadoras.

Los certificados X.509, tienen un periodo de validez, desde pocos meses hasta algunos años. Una vez que caduca el certificado, se convierte en no válido, es inseguro seguir confiando en él. Un certificado deja de ser vigente cuando vence el periodo de validez, en este caso la autoridad certificadora revoca el certificado.

3. Análisis de la certificación conjunta de documentos no digitales

En este apartado se analiza la problemática actual de los documentos oficiales con más de una firma, que hasta el momento son elaborados de manera manual y a su vez también carecen de seguridad y validez, por lo que se descubrió que gracias a la falta de interés en cuanto a su protección respecta, son vulnerables en la pérdida o robo de información confidencial, por lo tanto, se exponen a diferentes peligros informáticos.

3.1. Escenario manual

En la actualidad, la información tradicional a papel es más fácil que sufra alteraciones o modificaciones que la información digital protegida por protocolos de seguridad. A consecuencia de los cambios tecnológicos, los más afectados son los documentos oficiales pero que como principal característica poseen más de una firma, éstos hasta la fecha, se manejan aún de forma escrita, fotocopiada o impresa.

Es verdad que lo importante en un documento en papel es el mensaje transmitido o el contenido, pero también debe interesar la protección, el valor y la certificación a la información incluida en el documento.

Aparte de su valor, hoy en día, la información para todo tipo de organización o institución es muy valiosa, porque la crean, administran y distribuyen. Sin embargo, muchas de ellas no la protegen de forma correcta.

Cuando un documento se convierte en un formato digital y accesible en la red, la

información que contiene se enfrenta a riesgos de pérdida o modificación. Como resultado de esto, el escenario manual se ha vuelto más vulnerable ya que está expuesto a una mayor variedad de amenazas existentes cuando se digitaliza el documento.

Por ello, es importante contar con herramientas criptográficas que aporten soluciones de seguridad documental, para evitar la pérdida o robo de información confidencial. Esto hace a su vez que surjan nuevos protocolos para escudar la seguridad de la información, por lo que el protocolo de certificación pretende abarcar y disminuir estas inseguridades.

3.2. Técnica de certificación manual

Existen muchas organizaciones e instituciones que no custodian sus documentos o no les brindan protección. Pensar en el nivel de comportamiento de éstas, hace referencia a que muchas de ellas, desconocen las amenazas de seguridad de documentos entre su propia comisión directiva y administrativa.

Una principal amenaza proviene de las personas que manejan los documentos, llámese directivo, administrativo o empleado, este tipo de personas algunas veces llegan a romper los esquemas de seguridad, en el contenido del documento, sin ser conscientes de ello, es decir, la vulnerabilidad puede realizarse sin importar, si lo cometido fue de manera intencionada o no.

Para ejemplo de esto, se explica lo siguiente. De manera manual, una persona tiene en su poder un documento (realizado y firmado manualmente por otra persona), revisa el contenido y se percata que alguna parte del documento está mal escrito, y quiere cambiarlo, pero la única manera para hacerlo, es de forma digital. Por lo tanto, lo escanea y en su formato digital comienza a modificarlo. Concluye su objetivo y lo imprime. El documento pasa a una segunda persona, ésta de manera visual no se percata de la modificación y lo toma como válido. Este caso en particular muestra que el problema del escenario manual es vulnerable, ya que, en la mente del falsificador, en realidad, sólo corrigió el documento, sin embargo, con mala intención o no, generó

un documento falso.

En el caso de un documento con más de una firma, este procedimiento suele ser más común. De tal forma, que si alguno de los firmantes se percata de un error u omisión en el documento, es para él más sencillo realizar una modificación (usando el software para ello), que invalidar el documento e iniciar nuevamente el procedimiento.

A continuación, se muestra el proceso para la generación de un documento que contiene tres firmas. Cabe destacar que la firma del documento normalmente no se realiza secuencialmente y en orden jerárquico, considerando que la entidad de mayor rango es quien primero firma y obviamente la de menor rango lo hace al final.

Proceso para la generación de un documento que contiene tres firmas

1. El primer paso es crear el documento, con estructura de encabezamiento, cuerpo, pie y en formato real impreso, como se observa en la Figura 3.1.

2. El segundo paso es la certificación del primer firmante, este revisa el contenido, si es correcto, plasma su firma, esto implica que se modifica el documento original y se obtiene una versión certificada, como se indica en la Figura 3.2.

3. El tercer paso es la puesta de la segunda firma. El segundo firmante revisa el contenido, si es correcto, plasma su firma, nuevamente, el contenido del documento es actualizado con el mismo texto pero ahora con dos firmas. La segunda certificación se muestra en la Figura 3.3.

4. Por último, con la colocación de la tercera firma, el último firmante verifica, comparando visualmente las firmas de los dos primeros firmantes. Si considera que son reales emite su firma, obteniendo un documento final certificado tres veces, como se indica en la Figura 3.4.

Como bien se sabe, cada entidad debe verificar, en su totalidad, de forma visual el contenido del documento en el que depositará su firma. Lo que implica que el primer firmante sólo verifica el texto, el segundo firmante, por su parte, inspecciona el texto y

México CDMX A 05 de junio de 2017

CARTA DE DESCUENTO

E S.A DE C.V
C.GERENTE GENERAL

Por medio de la presente me dirijo a usted para solicitarle de la manera más respetuosa tenga la amabilidad de considerar realizar 30% de descuento en el pedido de equipos comerciales que solicitamos para el próximo mes de julio, ya que es el doble de lo que compramos mensualmente y por tanto es una transacción bastante grande.

Espero que debido al monto de esta compra analice la situación que le expongo y otorgue a la empresa que represento el descuento que lo solicito.

Mucho le agradeceré la atención que se sirva prestar a la presente.

ATENTAMENTE

Juan Carlos López González
Gerente General

Mario Acosta Lozano
Jefe Administrativo

Nelson Banderas
Supervisor

Figura 3.1: Creación del documento impreso. (Elaboración propia, 2017)

México CDMX A 05 de junio de 2017

CARTA DE DESCUENTO

E S.A DE C.V
C.GERENTE GENERAL

Por medio de la presente me dirijo a usted para solicitarle de la manera más respetuosa tenga la amabilidad de considerar realizar 30% de descuento en el pedido de equipos comerciales que solicitamos para el próximo mes de julio, ya que es el doble de lo que compramos mensualmente y por tanto es una transacción bastante grande.

Espero que debido al monto de esta compra analice la situación que le expongo y otorgue a la empresa que represento el descuento que lo solicito.

Mucho le agradeceré la atención que se sirva prestar a la presente.

ATENTAMENTE

Juan Carlos López González
Gerente General

Mario Acosta Lozano
Jefe Administrativo

Nelson Banderas
Supervisor

Figura 3.2: Generación de la primer firma. (Elaboración propia, 2017)

México CDMX A 05 de junio de 2017

CARTA DE DESCUENTO

E S.A DE C.V
C.GERENTE GENERAL

Por medio de la presente me dirijo a usted para solicitarle de la manera más respetuosa tenga la amabilidad de considerar realizar 30% de descuento en el pedido de equipos comerciales que solicitamos para el próximo mes de julio, ya que es el doble de lo que compramos mensualmente y por tanto es una transacción bastante grande.

Espero que debido al monto de esta compra analice la situación que le expongo y otorgue a la empresa que represento el descuento que lo solicito.

Mucho le agradeceré la atención que se sirva prestar a la presente.

ATENTAMENTE

Juan Carlos López González
Gerente General

Mario Acosta Lozano
Jefe Administrativo

Nelson Banderas
Supervisor

Figura 3.3: Generación de la segunda firma. (Elaboración propia, 2017)


México CDMX A 05 de junio de 2017

CARTA DE DESCUENTO

E S.A DE C.V
C.GERENTE GENERAL

Por medio de la presente me dirijo a usted para solicitarle de la manera más respetuosa tenga la amabilidad de considerar realizar 30% de descuento en el pedido de equipos comerciales que solicitamos para el próximo mes de julio, ya que es el doble de lo que compramos mensualmente y por tanto es una transacción bastante grande.

Espero que debido al monto de esta compra analice la situación que le expongo y otorgue a la empresa que represento el descuento que lo solicito.

Mucho le agradeceré la atención que se sirva prestar a la presente.

ATENTAMENTE

Juan Carlos López González
Gerente General

Mario Acosta Lozano
Jefe Administrativo

Nelson Banderas
Supervisor

Figura 3.4: Generación de la tercer firma. (Elaboración propia, 2017)

la firma ya contenida en el documento. El tercer firmante, por tanto, deberá comprobar que el texto no ha sido alterado, y que las dos firmas que contiene se asemejen lo más posible a la entidades correspondientes.

3.3. Documentos oficiales

El tipo de documentos en el que se enfoca este trabajo, principalmente, son los documentos oficiales administrativos, porque contienen información de carácter oficial, aparte de que en muchos de ellos se encuentran plasmadas tres firmas.

Según (F. Sánchez, 2008), un documento administrativo es un escrito en el que constan datos fidedignos, que sirve de prueba o testimonio, o que proporciona una información, especialmente de carácter histórico, oficial o legal.

Dada la definición anterior, se dice que además de ser oficiales, también sirven de soporte y pueden ser utilizados como prueba o consulta. Para términos de compro-

bación se expondrán tres ejemplos de documentos en los que el protocolo propuesto, puede aplicar no sólo para dichos documentos, también para cualquier otro tipo de clasificación, solo que contengan más de una firma. Los documentos a tratar son los siguientes:

1. **Solicitud de permiso:** Es una carta de permiso laboral, se redacta para solicitar un permiso en el centro de trabajo o lugar donde labora la persona que realiza la solicitud. Por lo tanto, es un documento expedido por el departamento de control de personal, en el se expresa el deseo de pedir permiso a algún superior o jefe en beneficio del trabajador, de manera escrita con lenguaje formal, en este documento se señala el objetivo que puede ser:

   - Permiso Económico.
   - Vacaciones por Antigüedad.
   - Comisión.
   - Asistencia a eventos académicos y/o capacitación.
   - Otros.

   Una vez especificado el tipo de permiso se firma el documento de manera autógrafa por tres entidades, una vez que autoricen el permiso.

2. **Carta de descuento:** Es una petición para ahorrar costos, por una compra o una buena inversión en una empresa, solo se pide especificar el porcentaje de descuento que se considera pedir por la venta, su elaboración es de manera escrita y pide que se firme por tres tipos de personas en este caso, supervisor, jefe de departamento y gerente general.

3. **Acuse de la entrega de credencial institucional:** Este tipo de documento, lo emite un sistema de identificación personal y el proceso carece de seguridad. Para la realización de la notificación se pide que la persona mande escaneada su foto y su firma autógrafa. De manera automática, el sistema la toma y elabora

la credencial del trabajador, con los datos personales que se ingresaron. Por último, se envía el acuse de la nueva credencial al titular de la misma, con las firmas del trabajador y de autorización.

En los documentos oficiales se hace la presencia de tres elementos importantes según (A. Sánchez, 1995):

- **El autor:** Es la persona a cuyo nombre se expide el documento y que, mediante se plasme su firma, se responsabiliza de él.
- **El destinatario:** Es la persona a quien se dirige el documento, que puede ser o no, el interesado en el contenido de la información.
- **Autenticadores:** Son las firmas oficiales que certifican de manera autógrafa un documento, garantizando que la firma que aparece en el documento es realmente del firmante.

Como ya se ha mencionado, la certificación manual, cuenta con amenazas no deseadas, que pueden transformar a los documentos oficiales en inseguros. Entre ellas, se identifican las siguientes:

- La alteración de información haciendo uso de herramientas para editar documentos.
- La sustracción, consulta y divulgación del contenido del documento por parte de personas malintencionadas.
- La sustracción de datos personales para usos malintencionados.
- La extracción, modificación o eliminación de información valiosa o privada.
- La pérdida de la privacidad en los documentos con firmas integradas.
- La usurpación de identidad al hacer mal uso con las firmas autógrafas.

Dado lo anterior, los riesgos encontrados en este tipo de certificación manual tientan contra la seguridad de la información y con ayuda de un protocolo de seguridad es posible disminuir el porcentaje de esta problemática.

4. Protocolo de certificación propuesto

En este capítulo se presenta la propuesta y la importancia que tiene la certificación digital, añadiendo la presentación matemática del protocolo de certificación.

4.1. Técnica de certificación automatizada

El mundo digital, en la transición del papel a lo electrónico, ha sido el principal objetivo para transformar cualquier tipo de documento manual en formato digital, esto conlleva a otorgar una máxima seguridad en el contenido del mismo, por lo que, esta tesis se enfocará a certificar documentos oficiales con más de una firma para contrarrestar los efectos a la alteración, a la eliminación, a la generación de información no auténtica contraria de la información real del documento.

Al aplicar la certificación digital, a los documentos con más de una firma, ayudará a terminar con los delitos de falsedad documental. La tesis, propone esta tendencia, para proteger cualquier contenido electrónico de carácter documental. Para la automatización del procedimiento de certificación manual, considerando las características de secuencial y jerárquico, la propuesta de (Lysyanskaya y Shacham, 2004) sobre las firmas agregadas es muy útil.

La propuesta sobre la automatización se presenta en la Figura 4.1. Como puede observarse, la versión digital cumple con las propiedades requeridas en su contraparte manual. Cabe destacar, que el proceso se realiza secuencialmente y estrictamente en

forma jerárquica tomando en cuenta el tiempo de la realización de cada firma.

El firmante 1 usa su llave privada para realizar la primera firma del digesto $h1$ obtenido del mensaje original y el tiempo. Por su parte, el firmante 2 realiza el proceso de verificación de la firma 1, si es válida, genera un nuevo digesto $h2$ que corresponde a la unión del mensaje original con la firma 1 y el tiempo de realización. Toca el turno al firmante 3, que una vez verificada la firma 2, certifica el documento generando la firma 3 en el tiempo que le corresponda.

La última verificación, la realiza cualquier usuario que contenga las llaves públicas de los tres firmantes que participaron en la generación del documento certificado tres veces. Además, se puede considerar que la verificación sobre la integridad del mensaje y la fiabilidad de cada firma es más precisa. La razón es muy simple, mientras que en la forma manual, cada firmante sólo inspecciona de forma visual el *parecido* de la firma autógrafa con su dueño, en la versión digital, el proceso garantiza, matemáticamente hablando, la fiabilidad tanto de la firma como del mensaje.

4.2. Flujo de datos del protocolo propuesto

En la Tabla 4.1 se muestra el flujo de datos del esquema propuesto, el cual, está basado en la firma agregada de (Lysyanskaya y Shacham, 2004).

El esquema requiere de cuatro entidades como mínimo: tres entidades firmantes y un verificador general. Las tres primeras entidades son las encargadas de certificar el documento, mientras que el verificador general sólo tiene interés en comprobar que el documento certificado es válido. Tal procedimiento lo realiza verificando únicamente la última firma, el resultado sobre la automatización se presenta en la Figura 4.2.

Una diferencia que es importante destacar, es que el esquema de certificación propuesto sólo contiene un mensaje (que es el documento a certificar), mientras que la firma agregada original considera para cada entidad firmante un mensaje diferente. Esto permite que el flujo de información entre las entidades sea más corta, puesto que sólo se requiere enviar las firmas y las llaves públicas de los firmantes anteriores y

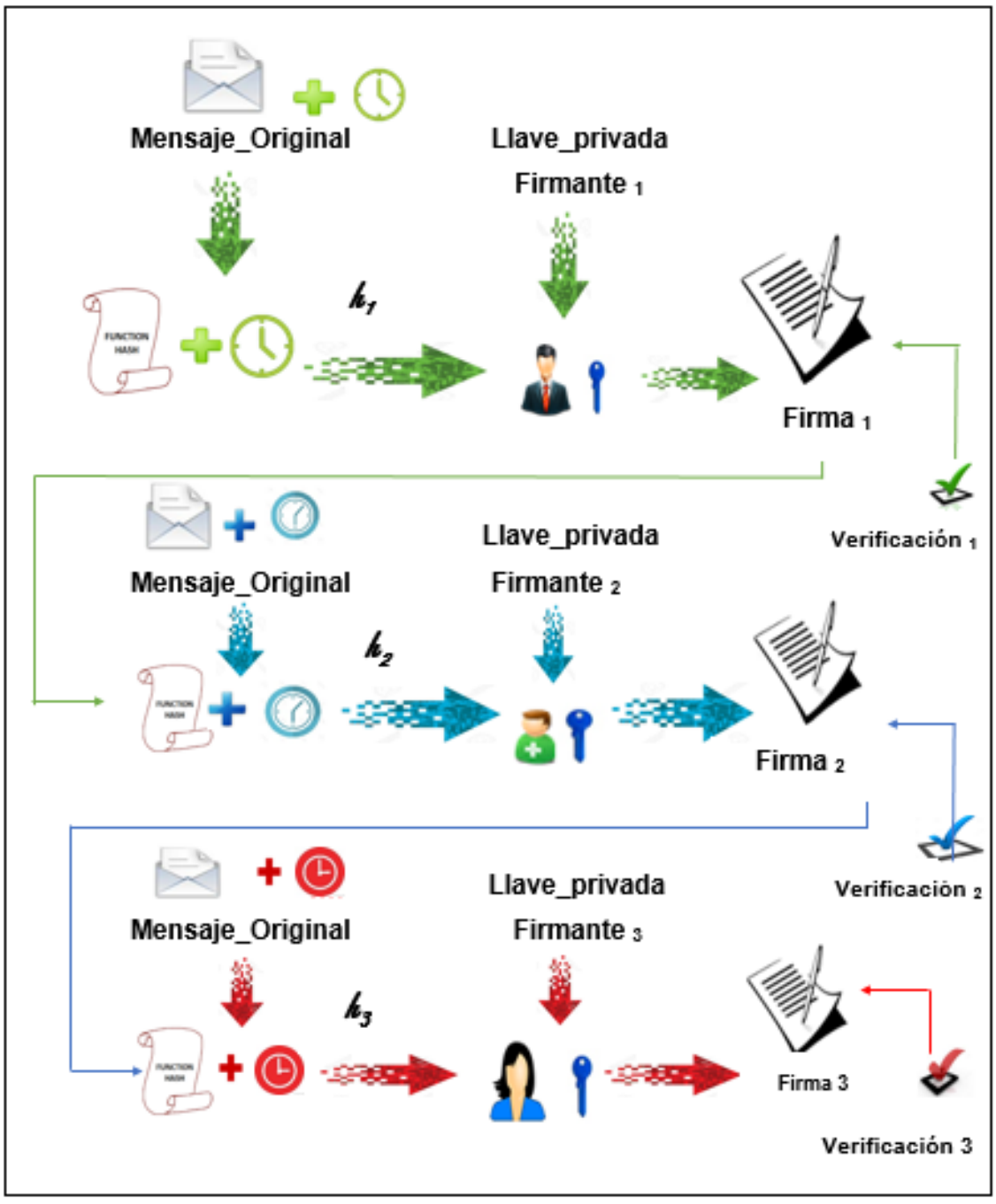


Figura 4.1: Proceso de automatización para la generación de un documento impreso con tres firmas. (Elaboración propia, 2017).

Tabla 4.1: Flujo de datos del esquema de certificación propuesto (Elaboración propia, 2017).

Notación
(N_X, e_X, d_X) corresponde al módulo, llave pública y llave privada RSA, del usuario X.
m es la versión digital (sin escanear) del contenido del documento a certificar.
t es el tiempo agregado a m.
σ_X es la firma generada por el usuario X.
$Hash(.)$ es la función $hash$ elegida.

Firmante 1 (N_1, e_1, d_1, t_1)

1. $h_1 = Hash(m, (N_1, e_1) + t_1)$
2. $\sigma_1 = h_1^{d_1} \, mod \, N_1$

$$\xrightarrow{3.\ m, \sigma_1, (N_1, e_1) + t_1}$$

Firmante 2 (N_2, e_2, d_2, t_2)

4. $y = \sigma_1^{e_1} \, mod \, N_1$
5. $h_1 = Hash(m, (N_1, e_1)) + t_1$
6. $\sigma' = y - h_1$
7. Si $\sigma' = 0$ entonces
   7.1 $y = Hash(m, (N_1, e_1) + t_1, (N_2, e_2) + t_2) + \sigma_1$
   7.2 $\sigma_2 = y^{d_2} \, mod \, N_2$

$$\xleftarrow{8.\ m, \sigma_1, \sigma_2, (N_1, e_1), (N_2, e_2) + t_2}$$

Firmante 3 (N_3, e_3, d_3, t_3)

09. $y = \sigma_2^{e_2} \, mod \, N_2$
10. $h_2 = Hash(m, (N_1, e_1) + t_1), (N_2, e_2) + t_2)$
11. $\sigma' = y - h_2$
12. Si $\sigma_1 = \sigma'$ entonces
   12.1 $y = Hash(m, (N_1, e_1) + t_1), (N_2, e_2) + t_2), (N_3, e_3) + t_3) + \sigma_2$
   12.2 $\sigma_3 = y^{d_3} \, mod \, N_3$

$$\xrightarrow{13.\ m, \sigma_1, \sigma_2, \sigma_3, (N_1, e_1) + t_1, (N_2, e_2) + t_2, (N_3, e_3) + t_3}$$

Verificador

14. $y = \sigma_3^{e_3} \, mod \, N_3$
15. $h_3 = Hash(m, (N_1, e_1) + t_1, (N_2, e_2) + t_2, (N_3, e_3) + t_3)$
16. $\sigma' = y - h_3$
17. Si $\sigma_2 = \sigma'$ entonces
   17.1 El documento es válido.

únicamente un mensaje.

4.3. Análisis de seguridad y eficiencia

En esta sección, se presenta un análisis tanto de la seguridad como de la eficiencia del esquema de certificación propuesto.

4.3.1. Seguridad

El esquema propuesto para la certificación de documentos de más de una firma basa su seguridad en la fiabilidad de la firma agregada de (Lysyanskaya y Shacham, 2004) y cumple los siguientes servicios de seguridad:

- Integridad. Cada firma es generada para el digesto del mensaje en turno, lo que garantiza que si cualquiera de los mensajes fue modificado aunque sea en un bit, el digesto resultante será totalmente distinto. Cada firmante, por tanto, está obligado a producir el digesto del mensaje original, de lo contrario, la firma resultará inválida.

- Autenticación. Cada firmante usa su llave privada para generar la firma. Una de las condiciones de las firmas digitales es que la llave privada sólo sea conocida por su dueño y que ésta sea el inverso matemático de su correspondiente llave pública, de tal manera que lo realizado por la llave privada pueda ser invertido por su contraparte pública, garantizando así que el único conocedor de la llave privada fue quien la usó para generar la firma.

Además de los servicios de seguridad, el esquema propuesto evita los siguientes ataques:

- Falsificación. La función picadillo evita que un atacante genere un mensaje malicioso al agregar o quitar información del mensaje original, por su resistencia a la preimagen y a la colisión.

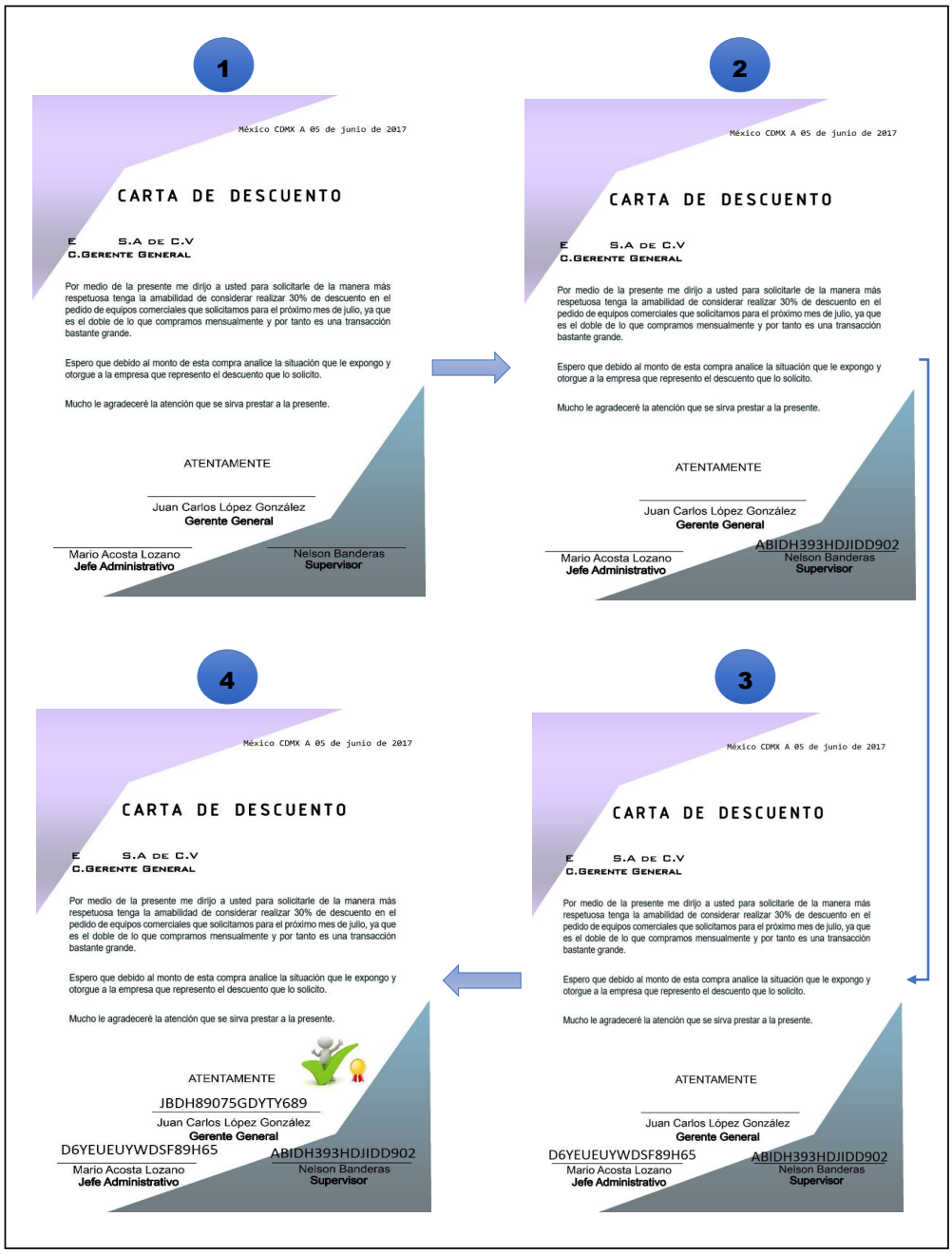


Figura 4.2: Presentación de la automatización de certificación. (Elaboración propia, 2017).

- Usurpación. La generación de llaves considera un par de llaves, sin embargo, puede haber usurpación si no se tiene un control en la relación entre la llave pública y la persona asociada a ella. Para evitarlo, el uso de los certificados digitales es necesario. Un certificado digital es una herramienta ampliamente usada para garantizar la vinculación entre el usuario y su llave pública (Tuecke y Thompson, 2004).

4.3.2. Eficiencia

El esquema propuesto está basado en la criptografía de llave pública, específicamente en el esquema de firma digital RSA, el cual, usa como operación principal la exponenciación modular. Es importante destacar que RSA tiene un nivel de seguridad de 80 bits, cuando su módulo es de longitud de al menos 1024 bits.

Haciendo una revisión en el algoritmo de generación de llaves, la llave privada d_i de cada firmante tiene una longitud de 1024 bits, de acuerdo al módulo N_i, mientras que la llave pública, para mayor eficiencia es de 16 bits. Lo anterior implica que la operación que usa la llave privada (operación privada) es de mayor costo que su contraparte pública (operación pública).

En la Tabla 4.2, se listan las operaciones privadas y públicas que cada entidad realiza. Como puede observarse, las entidades firmantes 2 y 3, realizan dos operaciones, mientras que el firmante 1 y el verificador general sólo una. Esto indica, que las entidades intermedias usan más recursos al tener que verificar y firmar en cada participación. Por su parte, el firmante 1, sólo produce la firma para el mensaje original, por ser el primero, no tiene una firma antecesora que deba verificar. Por último, cualquier entidad puede verificar la firma agregada, es decir, la última generada, lo que significa que únicamente realiza una operación pública, así, esta entidad es la que menos recursos requiere.

De tal forma se realizan 3 operaciones privadas, que son las más costosas, y se cal-

Tabla 4.2: Número de operaciones modulares realizadas por el esquema propuesto. (Elaboración propia, 2017).

Usuario	Operación privada	Operación pública
Firmante 1	1	0
Firmante 2	1	1
Firmante 3	1	1
Verificador general	0	1

culan de forma separada, específicamente, una por cada entidad. Lo que quiere decir, que el máximo consumo de recursos es una exponenciación modular con 1024 bits de longitud en el módulo por entidad. Haciendo significativamente eficiente el protocolo propuesto.

5. Aplicación y comprobación del protocolo de certificación en un escenario real

En este capítulo se presenta el diseño e implementación del sistema nombrado *ICA*, nombre que se refiere a los tres servicios de seguridad que ofrece el mismo: integridad, confidencialidad y autenticidad, este fue realizado únicamente para comprobar la funcionalidad del protocolo de certificación en los documentos oficiales.

5.1. Caso de estudio

Cabe destacar que el sistema *ICA* solo comprueba la funcionalidad del protocolo propuesto y toma como prueba el documento llamado *carta de descuento*, en el que se le aplica la técnica automatizada.

Para identificar plenamente la aplicación del protocolo propuesto, se presentan los diagramas de casos de uso del sistema de certificación para la emisión de la carta de descuento, el diseño de los diagramas y las tablas de caso de uso, tomando en cuenta el modelado de software UML (Fontela, 2011).

El diagrama de caso de uso general del sistema ICA, mostrado en la Figura 5.1, indica cómo debe interactuar el sistema con el usuario y específica 3 características

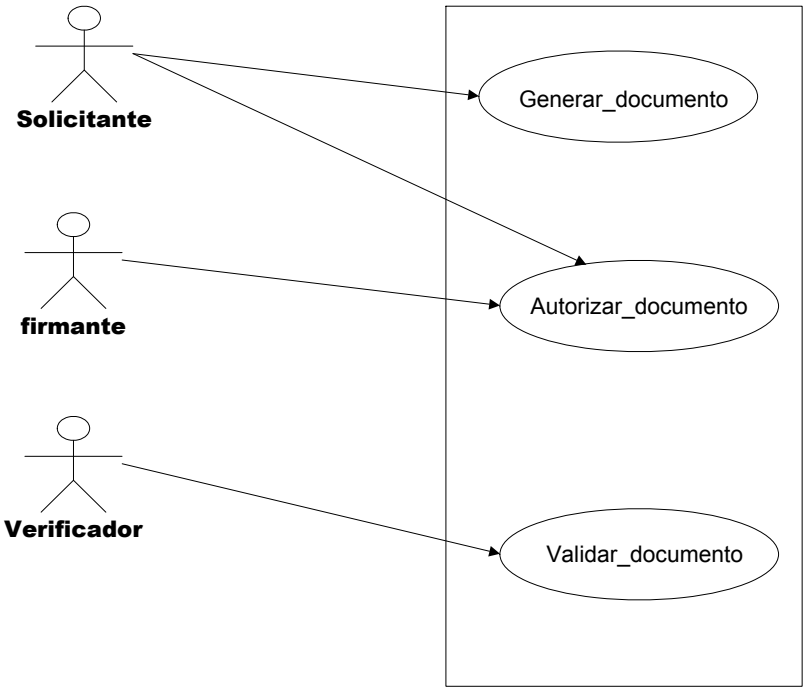


Figura 5.1: Caso de uso general del sistema. (Elaboración propia, 2017).

principales que se tomarán en cuenta para describir el comportamiento del software.

- *Generar documento:* La necesidad de crear un nuevo documento surge cuando el supervidor requiere solicitar un descuento y agrega los datos que respecte al documento.
- *Autorizar documento:* El sistema automáticamente identifica al jefe del área o gerente que debe plasmar su respectiva firma.
- *Validar documento:* El sistema valida la identidad de los firmantes autorizados en el documento final.

La Figura 5.2. describe el caso de uso de la generación y autorización del documento, especificando las tareas que realizará cada actor en el sistema de la siguiente manera:

- *Solicitante:* Creará un nuevo documento de la forma que respecte, además, debe plasmar la primera firma.

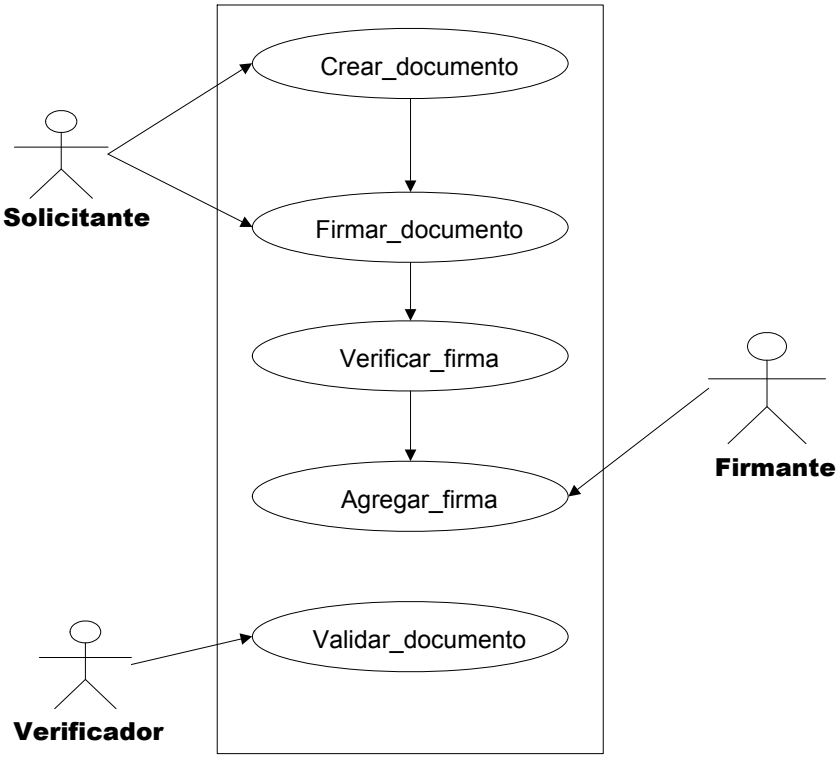


Figura 5.2: Caso de uso específico del sistema ICA. (Elaboración propia, 2017).

- *Firmante:* Cumplirá con dos tareas, como primera tiene que comprobar la firma anterior, usando la llave pública del solicitante. Una vez validada la identidad del mismo, se agrega la firma siguiente.
- *Verificador:* Validará la identidad del último firmante, con su respectiva llave pública.

Una vez entendido, cada una de las tareas de los actores, a continuación se explica detalladamente las actividades del sistema según sus casos de uso, indicados de la Figura 5.3 a la Figura 5.7.

Nombre	**Crear_documento**
Actor	Solicitante.
Descripción	Permite crear documentos con formato oficial.
Disparador	Con un solo click en la casilla de crear documento.
Precondiciones	La sesión del usuario debe estar iniciada.
Postcondiciones	Ninguna.
Flujo normal	1. El solicitante solicita crear documento. 2. El sistema muestra el documento para poder ingresar los datos *a.Fecha (*)* *b.Dirigido a: (*)* *c.Tipo de documento (*)* *d.Nombre del solicitante (*)* *e.Puesto del solicitante (*)* *f.Motivo del documento (*)* *3. El solicitante llena los campos.(S1)* 4. El sistema valida los datos. (S2) 5. El sistema permite guardar la información en un documento, con el formato oficial requerido. 6. Iniciar caso de uso Firmar_documento. 7. Finaliza el caso de uso.
Flujos alternativos	S1. El solicitante puede abandonar el llenado del documento sin terminar antes del paso 4 del flujo normal. *S1.1. El sistema preguntara al solicitante si desea abandonar.* *S1.2. Si la respuesta del solicitante es "sí", el sistema guardara el registro del nombre del usuario en la sección de "pendientes".* *S1.3. Finaliza el caso de uso.* S2. El sistema preguntara al solicitante si desea enviar para que valide los datos. *S2.1. Si los datos no son correctos* *S2.1.1. El sistema muestra el mensaje de "error" y se regresa al paso 2.* *S2.2. Si no hay error* *S2.2.1. El sistema muestra el mensaje de "confirmación".* *S2.3. Finaliza el caso de uso.*
Excepciones	E1. No se cargaron todos los datos requeridos. E1.1. El sistema indica que existen datos requeridos no cargados. E1.2 Vuelve al flujo principal, paso 3. E2. El sistema indica que los datos ingresados no son válidos. E2.1. Vuelve al flujo principal, paso 3.
Prioridad	Alta.
Frecuencia de uso	Alta.
Reglas de negocio	Ninguna.
Requerimientos especiales	Ninguno.
Suposiciones	*: el dato es obligatorio.
Notas y preguntas	Ninguna.

Figura 5.3: Caso de uso para crear un documento. (Elaboración propia, 2017).

Nombre	**Firmar_documento**
Actores	Solicitante. Caso de uso "Crear_documento".
Descripción	Permite seleccionar el documento para firmarlo.
Disparador	La finalización del caso de uso "Crear_documento".
Precondiciones	1. El primer firmante debe haber creado el documento.
Postcondiciones	Ninguna.
Flujo normal	1. El firmante da click en la opción de firmar documento. 2. El sistema muestra la pantalla del documento a firmar. 3. El firmante da click en la opción firmar. 4. El sistema solicita la llave privada del firmante (S1). 5. El sistema genera la firma. 6. El sistema genera el documento firmado en formato pdf. 7. Finaliza el caso de uso.
Flujos alternativos	S1. El sistema verificara si la llave ya caduco. *S1.1. Si la llave caduco el sistema lanzará un error y el firmante deberá volver a repetir el proceso.* *S1.2. El sistema validará la llave privada del firmante.* *S1.2.1. Si la llave es incorrecta, el sistema enviará el siguiente error "La llave no es correcta, por favor intente de nuevo".* *S1.2.2. Si la llave es correcta, el sistema enviará mensaje de "confirmación".* *S1.2.3. Finaliza el caso de uso.*
Excepciones	E1. El sistema indica que la llave no es válida. E2. El sistema no podrá generar la firma si no son válidas las llaves privadas de los firmantes.
Prioridad	Alta.
Frecuencia de uso	Alta.
Reglas de negocio	Al firmar, esto siempre queda en estado activo.
Requerimientos especiales	Ninguno.
Suposiciones	Ninguna.
Notas y preguntas	Ninguna.

Figura 5.4: Caso de uso para firmar un documento. (Elaboración propia, 2017).

Nombre	**Agregar_firma**
Actor	Firmante.
Descripción	Agrega firma.
Disparador	Permite visualizar más de una firma en un documento.
Precondiciones	1. Contar con el documento seleccionado. 2. Que el documento seleccionado se encuentre firmado digitalmente.
Postcondiciones	Ninguna.
Flujo normal	1. El sistema solicita la firma digital de cada firmante. 2. El sistema aplica la *hash* a las firmas. 3. Se realiza el agregado de firma una vez obtenida la *hash* de cada firma digital con su respectiva operación matemática. (S1) 4. Finaliza el caso de uso.
Flujos alternativos	S1. El sistema no podra agregar las firmas hasta que verifique la *hash de cada una.* *S1.1. Finaliza el caso de uso.*
Excepciones	Ninguna.
Prioridad	Alta.
Frecuencia de uso	Alta.
Reglas de negocio	Si la *hash* es válida, se agrega la firma.
Requerimientos especiales	Ninguno.
Suposiciones	Ninguna.
Notas y preguntas	Ninguna.

Figura 5.5: Caso de uso para agregar una firma. (Elaboración propia, 2017).

Nombre	**Verificar_firma**
Actor	Caso de uso "Agregar_firma".
Descripción	Permite validar la autenticidad e integridad de los datos a través de las firmas en el documento.
Disparador	Llamada proveniente del caso de uso "Agregar_firma".
Precondiciones	Que el documento seleccionado se encuentre firmado.
Postcondiciones	Ninguna.
Flujo normal	1. El sistema solicita la llave pública del firmante anterior (S1). 2. El sistema verifica la firma (S2). 3. Finaliza el caso de uso.
Flujos alternativos	S1. Al solicitar la llave pública el sistema deberá checar lo siguiente: *S1.1. Que la llave pública sea válida.* *S1.2. Que la llave pública no haya caducado.* *S1.3. Si todo es correcto, pasa al paso 2, de lo contrario vuelve al flujo principal, paso 1.* S2. El sistema pregunta al solicitante si desea verificar la firma. *S2.1. Si la respuesta del firmante es positiva, el sistema verificara si la firma es válida, si es correcto, el sistema mostrara un mensaje de confirmación.* *S2.2. Si la firma es inválida, el sistema mostrara un mensaje de que "la firma no es válida".* *S2.3. Finaliza el caso de uso.*
Excepciones	E1. El sistema no podrá validar las firmas hasta que verifique que las llaves de cada firmante son correctas.
Prioridad	Alta.
Frecuencia de uso	Alta.
Reglas de negocio	Si las llaves coinciden, se validan las firmas.
Requerimientos especiales	Ninguno.
Suposiciones	Ninguna.
Notas y preguntas	Ninguna.

Figura 5.6: Caso de uso para verificar una firma. (Elaboración propia, 2017).

Nombre	**Validar_documento**
Actor	Caso de uso "Verificar_firma".
Descripción	Validación del documento firmado.
Disparador	Garantiza la autenticidad, no repudio e integridad del documento, otorgando seguridad al contenido.
Precondiciones	1. Que el documento cuente con la agregación de las firmas.
Postcondiciones	Ninguna.
Flujo normal	1. El sistema verificará que el contenido no haya sido modificado. (S1) 2. El sistema dará por concluido el documento. 3. Finaliza el caso de uso.
Flujos alternativos	S1. El sistema pregunta al usuario si desea verificar el documento. *S1.1.Si la respuesta del usuario es positiva, el sistema válida si es correcto, si lo es muestra mensaje de confirmación.* *S1.2. De lo contrario, mostrará mensaje de "documento no válido".* *S1.3. Finaliza el caso de uso.*
Excepciones	E1. El mensaje, la *hash* de las firmas digitales y las llaves privadas y públicas no son válidos. E2. El sistema no podrá validar todo el documento, si encuentra modificación o alteración del mismo. *E2.1. Vuelve al flujo principal, paso 1.*
Prioridad	Alta.
Frecuencia de uso	Alta.
Reglas de negocio	Si todo el contenido del documento es válido, podrá valerse como certificado.
Requerimientos especiales	Ninguno.
Suposiciones	Ninguna.
Notas y preguntas	Ninguna.

Figura 5.7: Caso de uso para validar un documento. (Elaboración propia, 2017).

El *diagrama de clases* para crear un documento se muestra en la Figura 5.8 y el agregado de las firmas se visualiza en la Figura 5.9. Como puede observarse, se componen de dos clases con sus respectivos métodos. A partir de esto, la aplicación permite realizar el proceso de certificación.

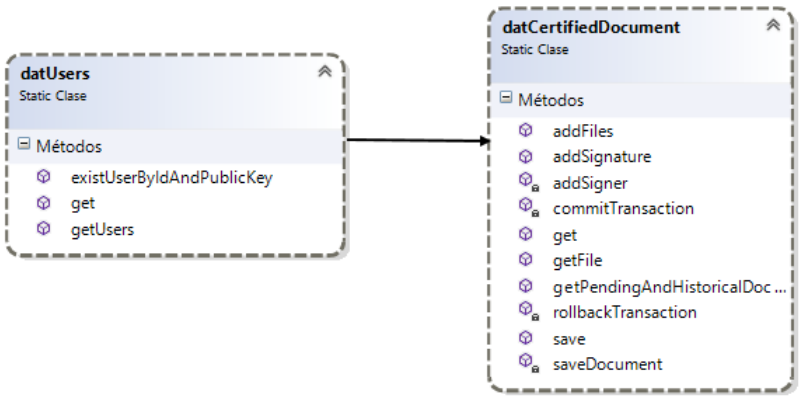


Figura 5.8: Diagrama de clases para crear un documento. (Elaboración propia, 2017).

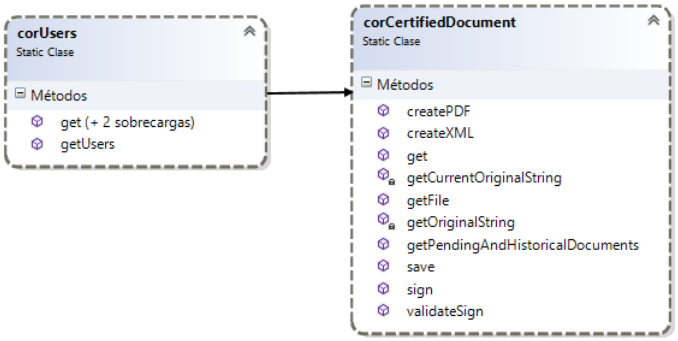


Figura 5.9: Diagrama de clases para agregar una firma. (Elaboración propia, 2017).

Una vez obtenidos los diagramas de clases, es posible generar los diagramas de secuencia. La Figura 5.10 muestra la relación de las clases para la creación del documento y la generación de la primera firma. La Figura 5.11 presenta el diagrama de secuencia de la agregación de la firma. Este proceso lo realiza una entidad con jerarquía mayor a la del solicitante del permiso.

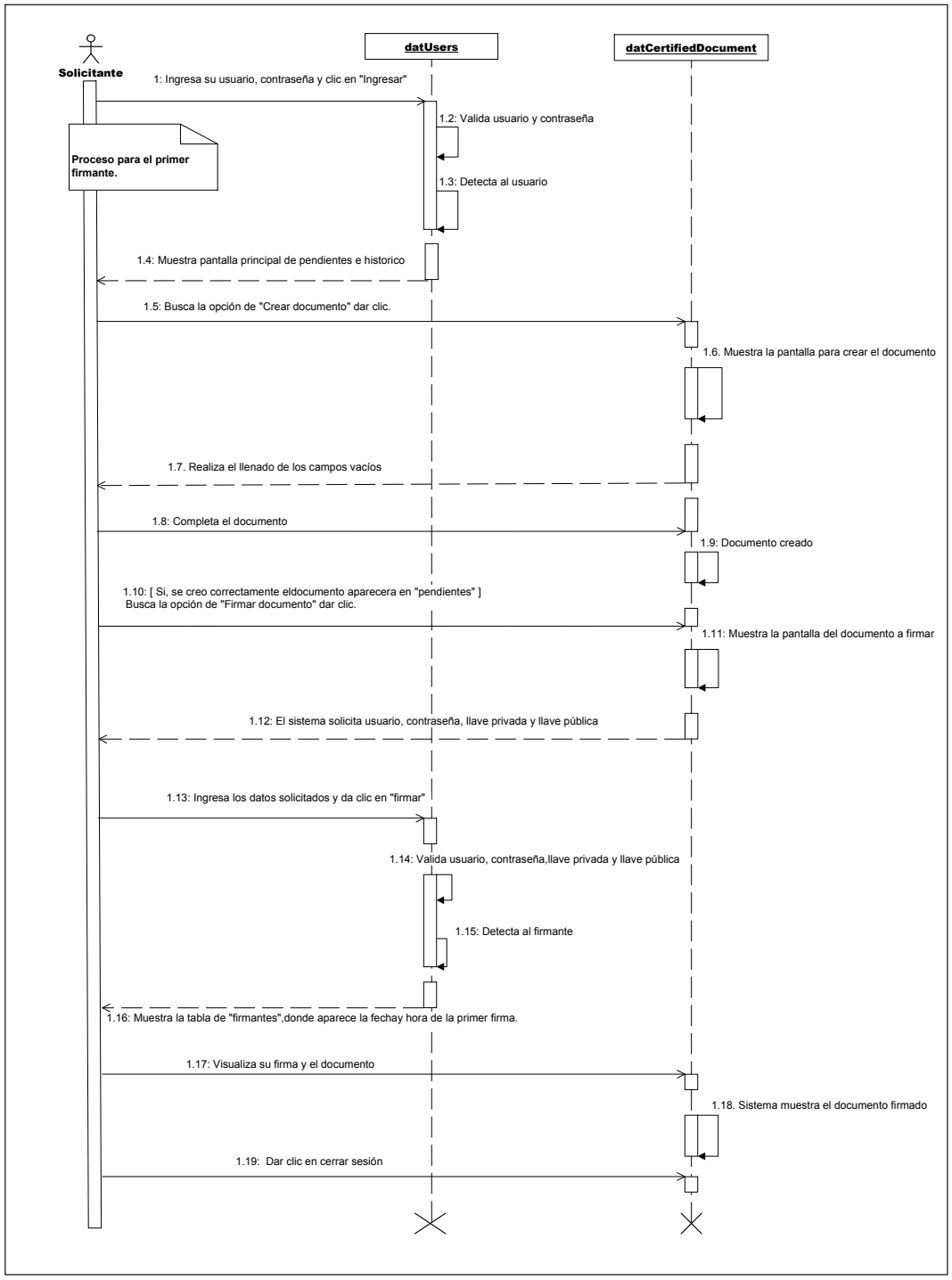


Figura 5.10: Diagrama de secuencia para el caso de uso *crear documento*. (Elaboración propia, 2017).

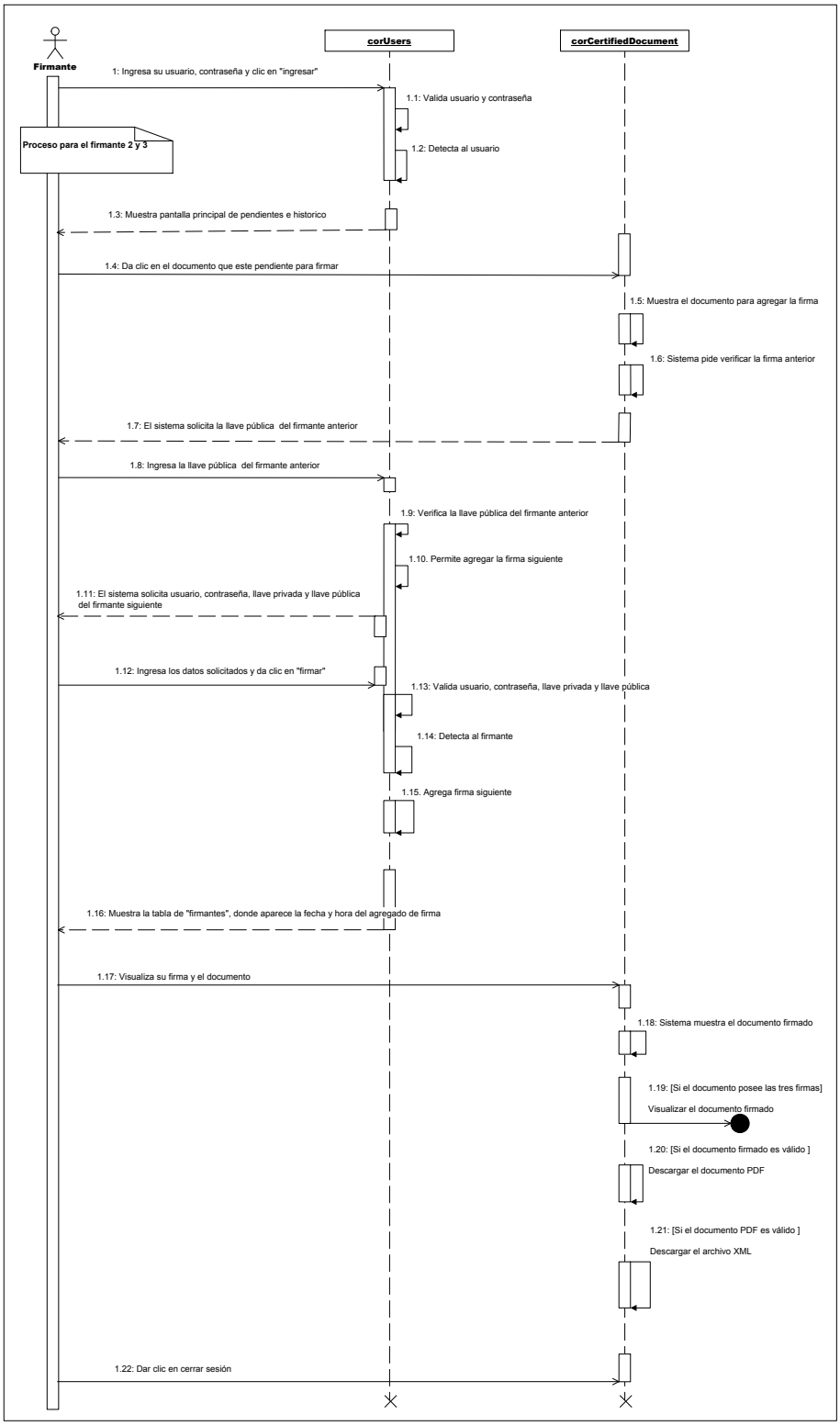


Figura 5.11: Diagrama de secuencia para el caso de uso *agregar una firma*. (Elaboración propia, 2017).

Es importante recordar que el proceso es jerárquico, por lo que, la entidad con menor rango es la primera que firma. La segunda firma se emite una vez que se ha verificado la autenticación de la primera entidad, lo que produce la certificación de la entidad con rango medio. En el último paso, el documento y las dos firmas son revisadas y certificadas por la autoridad de mayor rango.

Por lo anterior, este proceso es altamente importante, puesto que, la agregación es realizada una vez que la verificación de autenticación e integridad del documento se confirman, por la autoridad calificada para ello. El sistema ICA garantiza que dependiendo del perfil del firmante, éste se encuentre autorizado para emitir su firma ya sea en la solicitud o en alguna de las certificaciones, gracias al protocolo propuesto se cumple con la agregación secuencial y jerárquica.

Por último, se presentan los diagramas de actividades de la aplicación. Estos diagramas detallan las actividades que se realizan en cada caso de uso. A continuación, se explica de manera congruente cómo se llevan a cabo las funciones del sistema ICA, así como sus respectivas sentencias.

En la Figura 5.12 se muestra el diagrama de actividades para crear un documento nuevo. Como puede observarse, se especifica cada uno de los pasos requeridos para crear un documento, considerando el inicio de sesión para identificar el perfil del usuario. Este diagrama concluye con la elaboración del documento sin firmar.

En la Figura 5.13 se describe el diagrama de actividades para firmar un documento elaborado. La actividad principal de este diagrama es la emisión de la primera firma, por lo cual, se solicita la información de seguridad, como la llave privada del primer firmante.

Por último, en las Figuras 5.14 y 5.15 presentan el diagrama de actividades para agregar la segunda y tercera firma al documento. Es importante notar, que se realiza la autenticación de la primera firma y una vez que ha sido validada, la firma de la autoridad con rango medio, deposita la firma. Para el caso de la tercera y última firma, el proceso es similar, considerando que se agrega la estampa de tiempo, para garantizar la secuencia y la jerarquía correcta de las firmas.

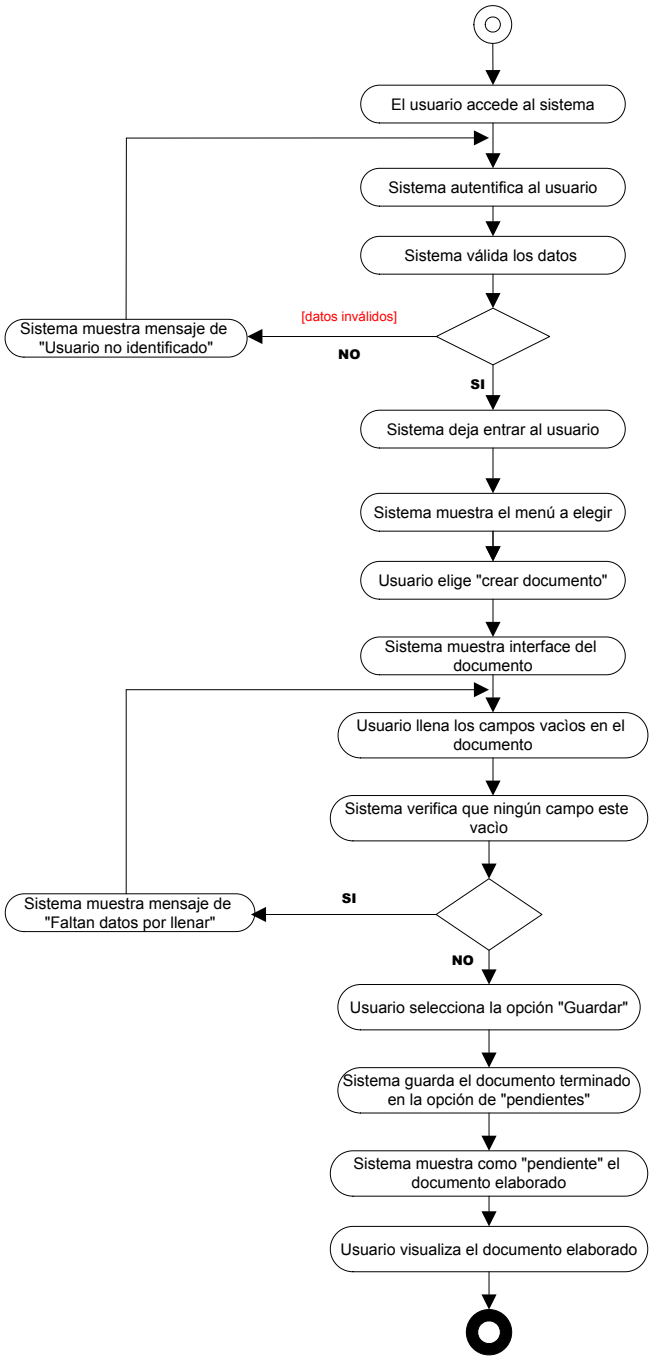


Figura 5.12: Diagrama de actividades para crear un documento. (Elaboración propia, 2017).

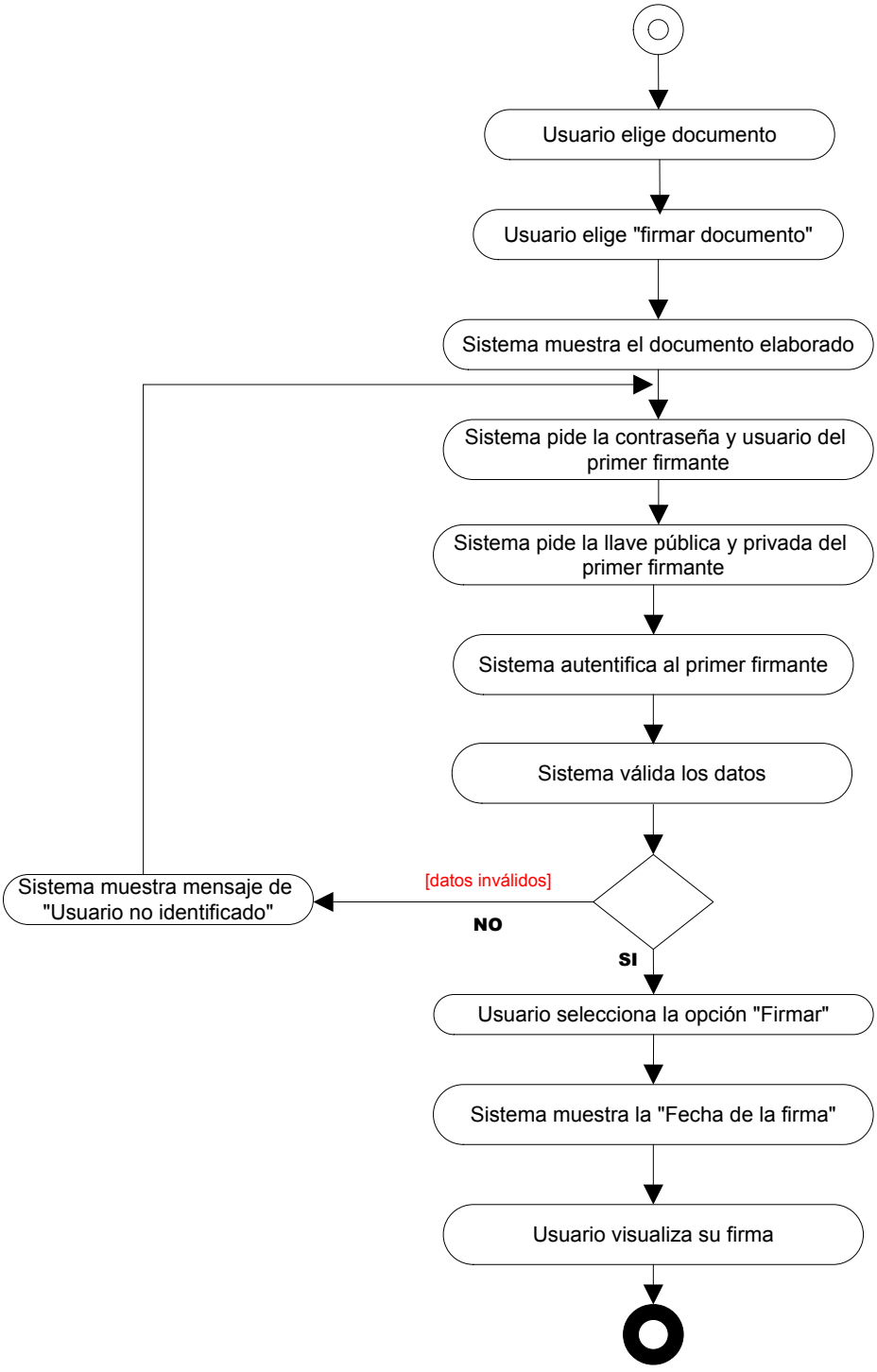


Figura 5.13: Diagrama de actividades para firmar un documento. (Elaboración propia, 2017).

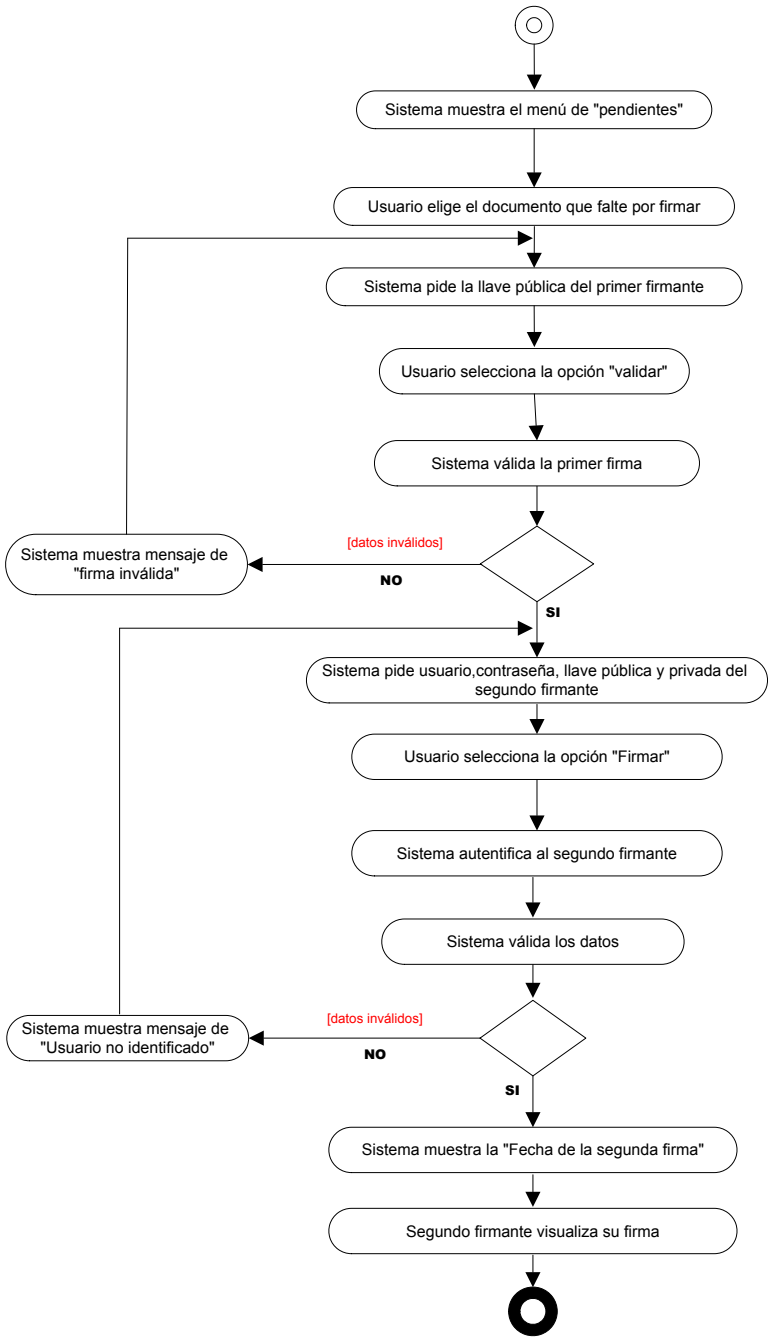


Figura 5.14: Diagrama de actividades para agregar la segunda firma. (Elaboración propia, 2017).

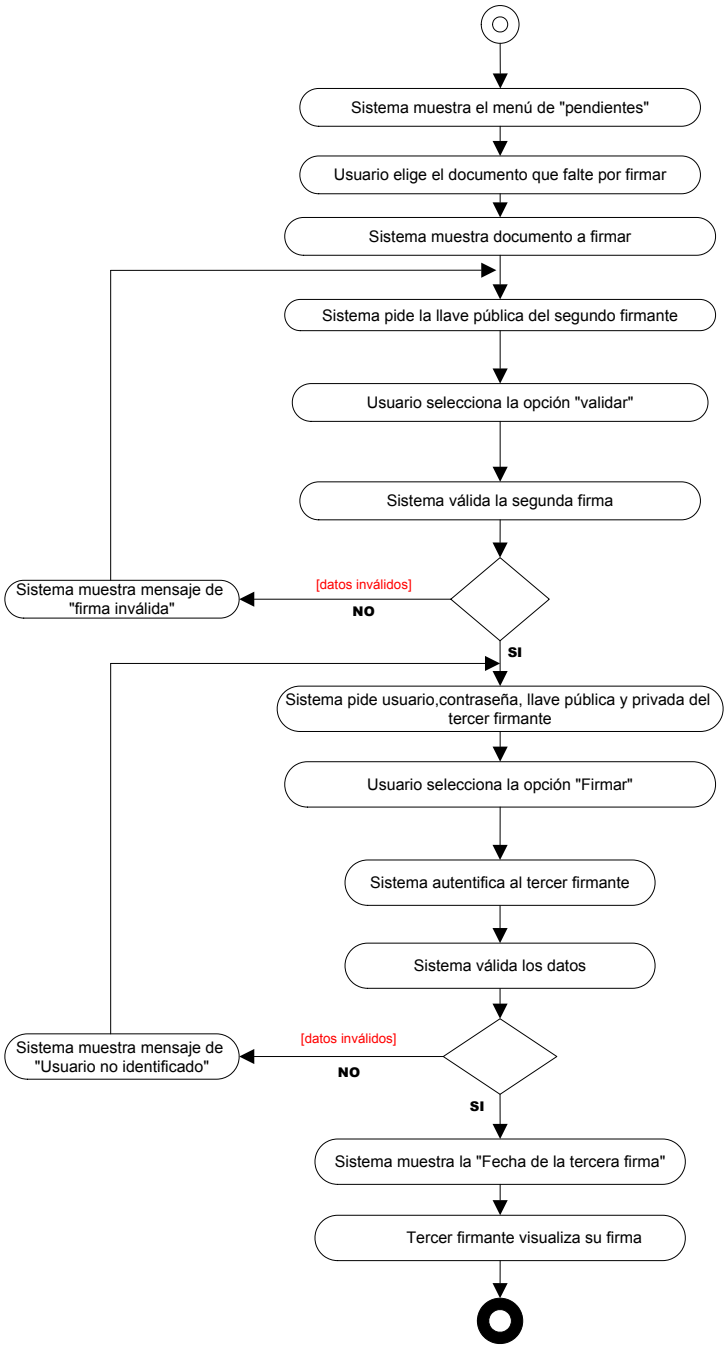


Figura 5.15: Diagrama de actividades para agregar la tercer firma. (Elaboración propia, 2017).

5.2. Implementación

El sistema ICA fue programado en lenguaje C#, haciendo uso de bibliotecas especiales para trabajar con la criptografía y concluir con la implementación del protocolo. La Figura 5.16 presenta las 3 principales características sobresalientes de la interfaz del sistema. Su proceso se determina de la siguiente manera, en el punto uno cualquier usuario dado de alta en el sistema, tiene permiso de crear un documento y de determinar el orden de los tres firmantes. En el punto dos, el sistema verificará el orden y el turno de los firmantes para plasmar su respectiva firma. Por último, en el punto tres, el sistema se encargará de verificar y validar la información del documento, incluyendo sus firmas.

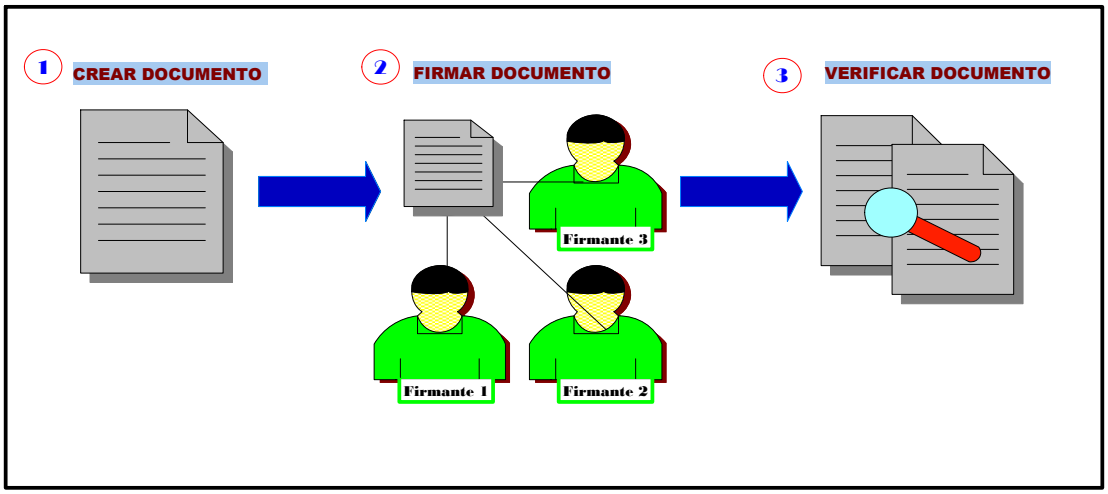


Figura 5.16: Características principales del sistema ICA. (Elaboración propia, 2017).

A continuación, se presenta la interfaz del sistema ICA, la cual, permite a distintos usuarios realizar las opciones de identificación, de contenido y de certificación, para obtener un documento oficial digital.

- Acceso: El sistema, le solicita a cada usuario ingresar su *usuario* y *contraseña*, tal como lo muestra la Figura 5.17.

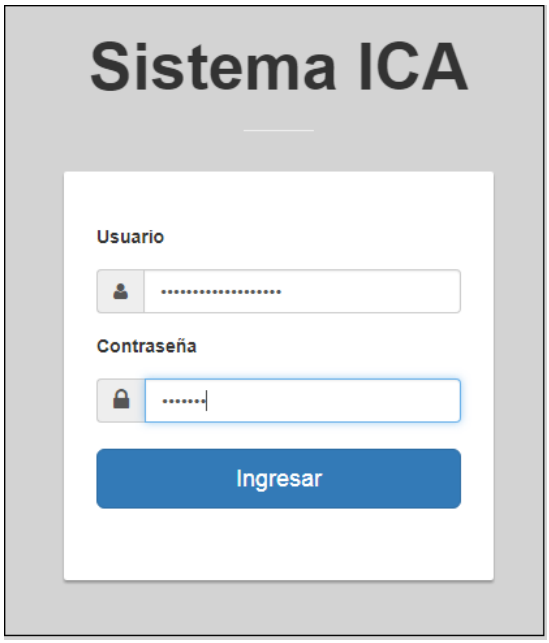


Figura 5.17: Acceso al sistema. (Elaboración propia, 2017).

- Menú: Inicializada la sesión correctamente, se mostrará la página principal. Donde el usuario podrá observar que en la parte superior del lado derecho, se muestra un menú con las opciones, de crear documento, firmar documento y cerrar sesión según lo elija el usuario, como se indica en la Figura 5.18.

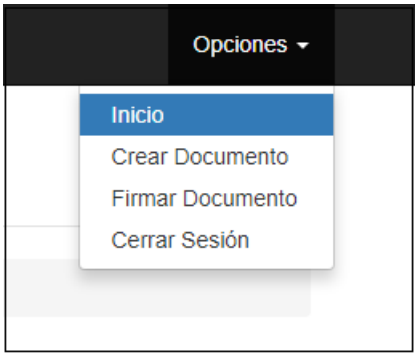


Figura 5.18: Pantalla de inicio. (Elaboración propia, 2017).

- Pendientes: Este apartado le notifica al usuario que tiene un documento pendiente por firmar. Como se observa en la Figura5.19, se le informa al usuario la fecha de creación y la entidad pendiente por firmar.

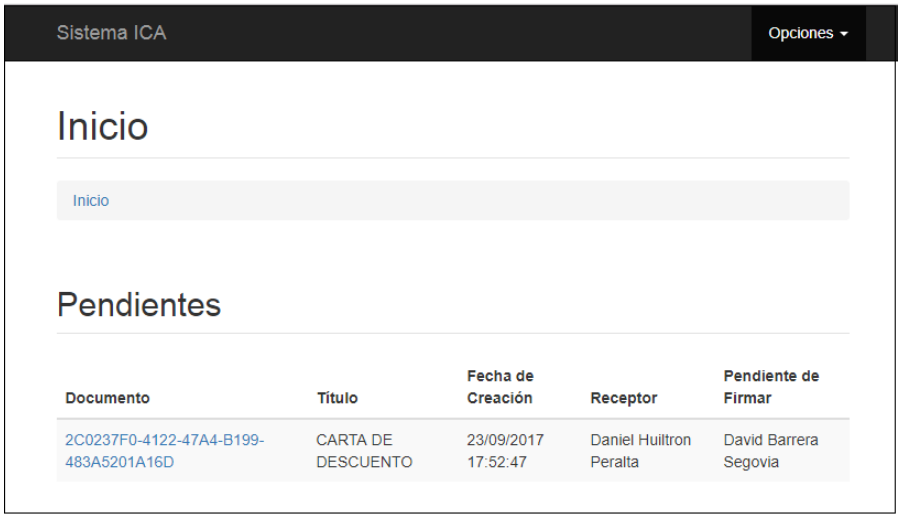


Figura 5.19: Pantalla de pendientes. (Elaboración propia, 2017).

- Histórico: En este apartado se visualizan los documentos que ya fueron firmados en fechas anteriores. La información relevante es la fecha de emisión de la última firma realizada. La Figura 5.20 muestra un listado ejemplo.

Figura 5.20: Pantalla de Histórico. (Elaboración propia, 2017).

- Crear documento: El sistema mostrará la pantalla para llenar el documento correspondiente que el usuario asigne, por lo tanto, pedirá los siguientes datos,

como se muestra en la Figura 5.21.

$a)$ Lugar de emisión: Asignar un lugar, únicamente indicar la ciudad, sin necesidad de especificar la calle y el número del lugar.

$b)$ Fecha: Especificar la fecha de creación del documento *dd/mm/aaaa*.

$c)$ Título: Especificar el nombre del documento.

$d)$ Mensaje: Redactar el cuerpo del documento.

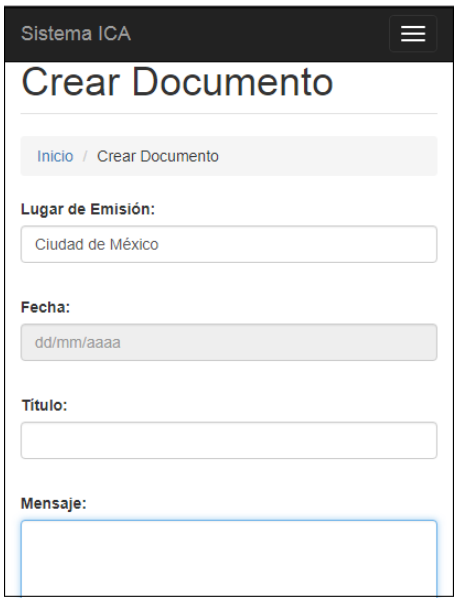


Figura 5.21: Pantalla para crear un documento. (Elaboración propia, 2017).

- Agregar firmantes: El sistema solicita la información del certificador. Dependiendo del número de firmas que se han emitido para el documento, el sistema despliega la lista de los posibles firmantes. De acuerdo a la Figura 5.22, la información solicitada es la siguiente:

  $a)$ Firmante: Se indica el nombre respectivo de cada firmante y se agrega. Cabe destacar que en el documento solo se agregará a tres firmantes y a un verificador general.

b) Puesto: Campo correspondiente a la información laboral del empleado como es el área a la que pertenece.

c) Receptor: Se específica el nombre del firmante a quien está dirigido el documento.

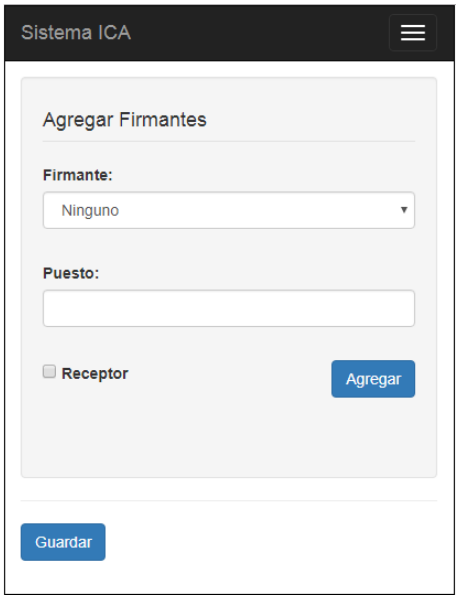


Figura 5.22: Pantalla para agregar firmantes. (Elaboración propia, 2017).

Nota: Al ser guardado el documento, el sistema visualizará el número de folio del documento que fue creado. El mensaje se muestra en la Figura 5.23.

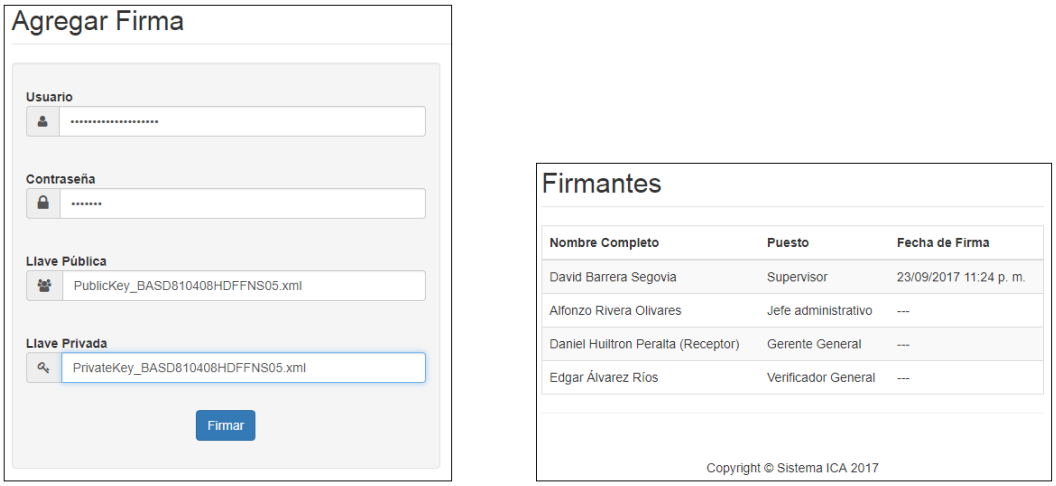
Figura 5.23: Folio asignado por el sistema. (Elaboración propia, 2017).

- Visualización del documento creado: En la parte de **"pendientes"**, se puede obtener el documento creado. Dar clic en el número de folio para visualizarlo. La pantalla muestra el documento como lo indica la Figura 5.24.

Figura 5.24: Vista de un documento creado. (Elaboración propia, 2017).

- Firmar documento: El requisito que pide el sistema para que un usuario pueda firmar, son las dos llaves privada y pública que se le asignó a cada usuario, además, de la información de inicio de sesión, para confirmar la identidad del usuario (Figura 5.25) parte a. Cada usuario, al momento de firmar, observará que su firma se emitió, indicándole la fecha y hora de la realización del proceso. Un ejemplo de ello se presenta en la Figura 5.25 parte b.

- Agregar la segunda firma: Antes de firmar por segunda vez, el sistema valida la primera firma, por lo tanto, pide la llave pública del primer firmante. Una vez que el sistema realizó la primera validación, nuevamente, se pide la información de seguridad para emitir la segunda firma. Después de certificar, en automático



(a) Solicitud de información segura

(b) Emisión de las firmas

Figura 5.25: Proceso para la primera firma. (Elaboración propia, 2017).

aparecerá la pantalla indicando la fecha de la segunda firma.

- Agregar la tercera firma: El proceso es el mismo que el anterior, la única diferencia es la información de inicio de sesión, la llave pública y la llave privada del firmante, que en esta fase pertenece a la entidad de mayor rango. La Figura 5.26 muestra el listado de las tres firmas emitidas y las fechas de generación.

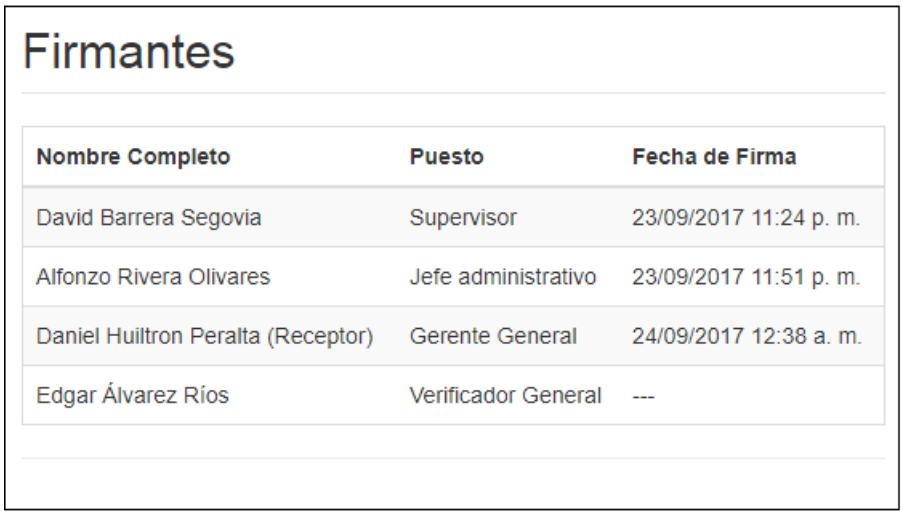


Figura 5.26: Información de las firmas emitidas. (Elaboración propia, 2017).

- Verificador general: Existe un verificador que se encarga de obtener las llaves públicas de los usuarios y ocuparlas para verificar la última firma emitida. En esta ocasión, el sistema solicita la llave pública del último firmante, con la cual, la entidad *verificador* validará el documento. La Figura 5.27 muestra la ventana del sistema que indica el proceso completo para la carta de descuento firmada por el solicitante, certificada por dos entidades de mayor rango y validada por la entidad *verificador*. Es importante notar que una vez concluido el proceso de los firmantes, en el sistema cada entidad tiene la opción de **Descargar PDF o Descargar XML** según se solicite.

Figura 5.27: Proceso completo para solicitar una carta de descuento. (Elaboración propia, 2017).

- Visualización del documento firmado: Cuando el sistema detecte que los tres firmantes concluyeron el proceso satisfactoriamente, cada usuario podrá obtener de manera digital el documento en pdf, un ejemplo se aprecia en la Figura 5.28.

Folio: 2C0237F0-4122-47A4-B199-483A5201A16D

Ciudad de México, a 23 de Septiembre de 2017

CARTA DE DESCUENTO

Daniel Huiltron Peralta
Gerente General

P R E S E N T E:

Por medio de la presente me dirijo a usted para solicitarle de manera respetuosa tenga la amabilidad de considerar realizar el 15% de descuento en el pedido de equipos comerciales que solicitamos para el próximo mes de Octubre, ya que es el doble de lo que compramos mensualmente y por lo tanto es una transacción bastante grande.

Espero que debido al monto de esta compra analice la situación que le expongo y otorgue a la empresa que represento el descuento que le solicito.

Mucho le agradeceré la atención que se sirva prestar a la presente.

David Barrera Segovia (BASD810408HDFFNS05)	
Puesto:	Supervisor
Cadena Original:	2C0237F0-4122-47A4-B199-483A5201A16D@|@BASD810408HDFFNS05@|@David Barrera Segovia@|@Supervisor@|@1@|@No Receptor@|@2017-09-23T23:24:47Z@|@2017-09-23T17:52:47Z@|@2017-09-23T00:00:00Z@|@Ciudad de México@|@CARTA DE DESCUENTO@|@Por medio de la presente me dirijo a usted para solicitarle de manera respetuosa tenga la amabilidad de considerar realizar el 15% de descuento en el pedido de equipos comerciales que solicitamos para el próximo mes de Octubre, ya que es el doble de lo que compramos mensualmente y por lo tanto es una transacción bastante grande.Espero que debido al monto de esta compra analice la situación que le expongo y otorgue a la empresa que represento el descuento que le solicito.Mucho le agradeceré la atención que se sirva prestar a la presente.@|@189C1803F232D4389251EFE25C951CF5A884062F41DE0E2CA8DE82E1ED7ED298
Fecha y Hora de Firma #1:	23/09/2017 11:24 p. m.
Firma #1:	[illegible]

Figura 5.28: Documento digital firmado. (Elaboración propia, 2017).

5.3. Experimentación

En esta sección se realizan ataques al sistema que atentan contra la integridad y la autenticación. La Figura 5.29 asimila el proceso que realizó cada firmante para certificar un documento, este proceso se tomó en cuenta para realizar las pruebas de vulnerabilidades en el sistema ICA. A continuación, se explica el proceso que ayudó a detectar vulnerabilidades, de acuerdo a los números que señala.

1. **Crear documento:** Cualquier usuario dado de alta en el sistema, tuvo autoriza-

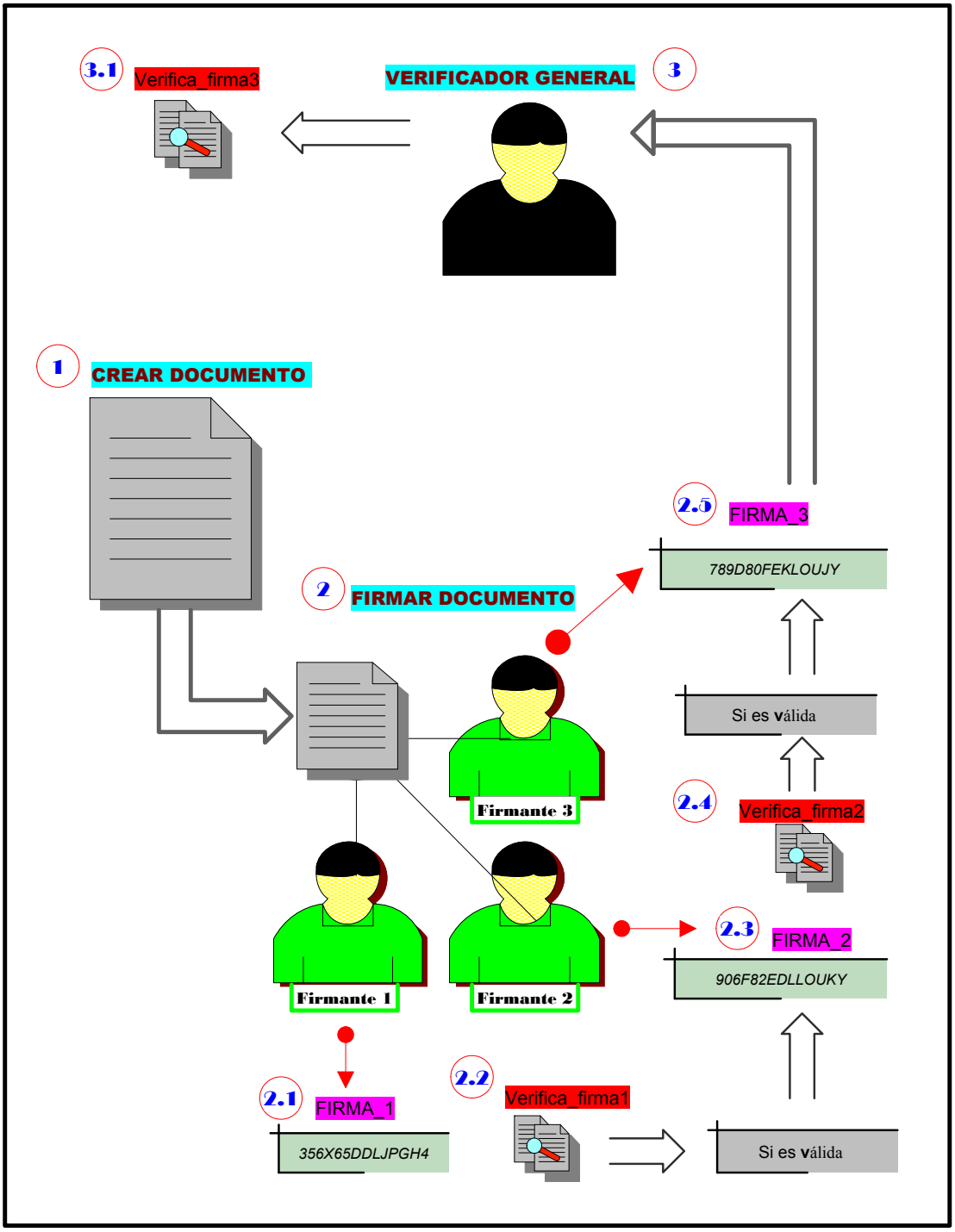


Figura 5.29: Proceso de simulación de ataque. (Elaboración propia, 2017).

ción para crear un documento. Pero también, tuvo la oportunidad de realizar acciones malintencionadas al documento. Por ejemplo, modificar el folio que asigna el sistema o alterar cualquier dato de la información.

2. **Firmar documento:** El documento fue firmado por tres usuarios.

   a) El primer firmante colocó su firma (2.1).

   b) El segundo firmante le tocó validar la firma del primero (2.2), pero ahora el caso es diferente, la llave pública que uso para la validación, no le pertenecía al primer firmante, por lo que tuvo que pedir la llave original para emitir su segunda firma (2.3).

   c) Ahora, el turno del tercer firmante, concluyó la validación sin problema (2.4). Pero a la hora de firmar, el sistema detectó que el archivo PublicKey.xml era falso. Así que después de lo sucedido, de manera correcta obtuvo su llave privada y el sistema permitió la emisión de su firma (2.5).

3. **Verificador general:** Como la última firma fue válida (3.1), el sistema automáticamente permite a cada firmante descargar el documento en PDF.

La prueba de seguridad se realizó en 30 documentos para descubrir si el sistema ICA ayuda a eliminar las vulnerabilidades del escenario manual. Cabe mencionar que el símbolo x en las tablas, señala el documento con su respectivo ataque y específica que el sistema no fue vulnerado.

La Tabla 5.1 señala el número de documentos y el nombre de cada ataque aplicado. Se específican 15 documentos y 15 vulnerabilidades que el sistema detectó y no las permitió realizar. Un ejemplo de consulta del primer documento se lee de la siguiente manera: un usuario intentó acceder al sistema usando el nombre del usuario y contraseña erróneas, el sistema lo detectó y no permitió acceder al sistema. El usuario tuvo que introducir nuevamente los datos correctos para elaborar el documento.

Tabla 5.1: Pruebas, parte 1. (Elaboración propia, 2017).

NUMERO DE DOCUMENTO															
ATAQUE	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Usuario no identificado	x														x
Contraseña errònea	x														x
Modificar el folio del documento		x													x
Modificar el lugar de emisiòn															x
Modificar la fecha			x												x
Modificar el titulo				x											x
Modificar el mensaje					x										x
Modificar el nombre del firmante						x									x
Modificar el puesto del firmante							x								x
Modificar el nombre del receptor								x							x
Modificar la fecha de creaciòn del documento									x						x
Cambiar el nombre del firmante que se encuentre pendiente de firmar										x					x
Obtener llave privada errònea											x				x
Obtener llave pùblica errònea												x	x		
Subir archivo PublicKey.xml falso													x	x	x
Tiempo total en segundos del Proceso	**1.78**	**3.35**	**3.27**	**4.41**	**5.66**	**7.10**	**8.74**	**10.84**	**11.69**	**12.55**	**13.21**	**14.26**	**15.25**	**16.95**	**20.10**

Los documentos restantes se visualizan en la Tabla 5.2, con 12 vulnerabilidades detectadas en el sistema. Un ejemplo de consulta del documento 17 se lee de la siguiente manera: el firmante dos, intentó modificar la hora de la creación de la primera firma. El sistema no deja realizar ninguna alteración de ese tipo, por lo que tampoco fue posible modificar la fecha y hora de la segunda firma. Al subir el archivo de la llave pública del primer firmante, el sistema le indicó que era falsa, así que no le permitió firmar hasta que la validación de la firma uno fuera correcta.

Tabla 5.2: Pruebas parte 2. (Elaboración propia, 2017).

NUMERO DE DOCUMENTO															
ATAQUE	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**
Subir archivo Privatekey.xml falso	x														x
Modificar la fecha de la creacion de la firma 1															x
Modificar la hora de la creacion de la firma 1		x			x										x x
Subir archivo Publickey.xml del firmante 1 equivocado		x	x												x x
Modificar la fecha de la creacion de la firma 2		x		x											x
Modificar la hora de la creacion de la firma 2		x													x
Subir archivo Publickey.xml del firmante 2 equivocado						x					x				x x
Modificar la fecha de la creacion de la firma 3							x								x
Modificar la hora de la creacion de la firma 3								x		x				x	x
Subir archivo Publickey.xml del firmante 3 equivocado									x	x	x				x
Modificar el documento PDF										x		x	x		x
Modificar el documento XML													x	x	x
Tiempo total en segundos del Proceso	**1.78**	**3.35**	**3.27**	**4.41**	**5.66**	**7.10**	**8.74**	**10.84**	**11.69**	**12.55**	**13.21**	**14.26**	**15.25**	**16.95**	**20.10**

El resultado que se obtuvo fue satisfactorio porque el sistema protege al documento digital de distintas formas, se concluye que para cualquier tipo de modificación o alteración indicada en las Tablas 5.1 y 5.2, el sistema no se presta para proceder con tales ilícitos. Por lo tanto, el protocolo de certificación que se propuso en este tema de tesis es altamente invulnerable y seguro porque tiene la capacidad de resguardar a un documento digital de personas maliciosas.

6. Conclusiones

En este proyecto de tesis se presenta un esquema de certificación conjunta para documentos que contienen tres firmas. La propuesta planteada toma en cuenta los esquemas de firma digital y firma agregada. Añadiendo funciones hash y la estampa de tiempo como garantía de que la información es mas segura y confiable en el proceso digital que en el manual.

Gracias a la certificación digital, es posible aplicar algoritmos criptográficos que están basados en problemas matemáticos difíciles que garantizan tanto la integridad del documento como la autenticación de las entidades. Dando como resultado un proceso más confiable. Con la finalidad de comprobar la fiabilidad del protocolo propuesto, se realizó un sistema llamado ICA que certifica documentos con más de una firma. Verificando el proceso de cada firmante para proteger la certificación individual. Para su desarrollo se utilizaron un par de llaves para cada entidad que permite a cada firmante garantizar la integridad del documento. Utilizando la llave privada para emitir su firma y la llave pública para verificarla. La aplicación que se realizó para comprobar la eficacia del protocolo ayuda a corroborar que el contenido de un documento no fue alterado y que el documento creado mantiene su estado original libre de tentativas de ataque.

Con el desarrollo de este proyecto se concluye que la certificación en los documentos manuales es de suma importancia, en especial, los que contienen más de una firma. El protocolo propuesto convirtió a un documento digital en seguro. Lo que ayudo para salvaguardarlos de acontecimientos ilícitos, como la modificación o la falsificación del contenido verdadero después de concluido y firmado.

Por otra parte, se evita que las firmas no sean usurpadas por terceras personas.

Al obtener una firma escaneada, la persona malintencionada sin autorización emite una firma falsa sin consentimiento de la persona que resulte afectada, la altera para cometer fraudes, comprometer bienes o por el simple hecho de causar un mal a la sociedad o a un tercero. El protocolo que se propuso permite certificar documentos y verificar que no hayan sido expuestos a los sucesos anteriores. Haciendo que la propuesta sea una herramienta útil, eficiente y segura para un proceso que requiera la generación de un documento que cumpla con la característica de tener más de una firma en su contenido.

6.1. Trabajo futuro

El protocolo de certificación satisface los requerimientos que se consideraron importantes en un documento oficial como es la integridad, la autenticación y el no repudio. Por lo que se consideran dos puntos como trabajo futuro:

- Dado que la implementación del sistema se llevo a cabo solo para tres firmantes, se propone que se involucren a n firmantes, para hacerlo más general y aprovechar la seguridad que el protocolo brinda.
- Para proteger aún más la información de un documento, no se descarta, la posibilidad de agregar más servicios de seguridad que la criptografía ofrece, como lo es, la confidencialidad del contenido del mensaje.

Referencias

Abbas, N. (2004). Implementación eficiente de algoritmos criptográficos en dispositivos de hardware reconfigurable. En *Tesis de doctorado en ciencias de la computación.* (pp. 1–173).

Adams, C., y Lloyd, S. (2002). *Understanding pki: Concepts, standards, and deployment considerations.* USA: Addison Wesley.

Boneh, G. C. L. B., D., y Shacham, H. (2003). Aggregate and verifiably encrypted signatures from bilinear maps. advances in cryptology — eurocrypt 2003. *International Conference on the Theory and Applications of Cryptographic Techniques*, *4*(8), 416–432.

Brogle, G. S., K., y Reyzin, L. (2014). Sequencial aggregate signatures with lazy verification from trapdoor permutations. *Information and computation.*, *239*(1), 356–376.

Cruz, E. (2009). Criptografía asimétrica con la implementación de cifrado y firma digital en correo electrónico en la comisión nacional bancaria y de valores. En *Tesis de licenciatura en informática.* (pp. 1–162).

Diffie, W., y Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654.

Feghhi, J., y Williams, P. (1999). *Digital certificates applied internet security.* USA: Addison Wesley.

Flores, M. (2005). Firma digital. En *Tesis de licenciatura en ingeniería informática.* (pp. 1–95).

Fontela, C. (2011). *Uml: modelado de software para profesionales.* Buenos Aires:

Alfaomega Grupo Editor.

Ford, W., y Baum, M. (1997). *Secure electronic commerce: Building the infrastructure for digital signature and encryption.* Prentice-Hall.

García, W. (2011). Implementación de firma digital en una plataforma de comercio electrónico. En *Tesis de licenciatura en ingeniería informática.* (pp. 1–102).

Hernández, G. A., J., y Ramos, B. (2007). Repudiation of electronic signatures in infrastructures of key publishes. *Department of Industry, Tourism and Trade of Spain.*, 4–9.

Kohnfelder, L. (1978). *Toward a practical public-key cryptosystem.* MIT Department of Electrical Engineering.

Lysyanskaya, M. S. R. L., A., y Shacham, H. (2004). Sequential aggregate signatures from trapdoor permutations. advances in cryptology - eurocrypt 2004. *International Conference on the Theory and Applications of Cryptographic Techniques.*, *2*(6), 74–90.

Maiorano, A. (2009). *Criptografía: técnicas de desarrollo para profesionales*. Buenos Aires: Alfaomega.

Menezes, A., Van Oorschot, P., y Vanstone, S. (2001). *Handbook of Applied Cryptography*. CRC Press.

Paredes, G. (2006). Introduction to the criptography. *Revista Digital Universitaria*, *7*(7), 1-17.

Peñaranda, H. (2011). La firma electrónica digital en venezuela. *Nómadas.*(29), 7–14.

Rivest, S. A., R., y Adleman, L. (1978). A method for obtaining digital signatures and public key cryptosystems. *Commucation ACM*, *21*(2), 120–126.

Rodríguez-Henríquez, F., Saqip, N., Díaz-Pérez, A., y Kaya, K. (2006). *Cryptographic Algorithms on Reconfigurable Hardware (Signals and Communication Technology)*. Springer-Verlag New York, Inc.

Rojas, S. D., M., y Meneses, C. (2011). Digital signature: Information transmisión instrument for financial enterprises. *Revista Avances en Sistemas e Informática.*, *8*(1), 1–9.

Sánchez, A. (1995). Documentos administrativos: un ensayo de diplomática contemporánea. *Revista Científica Compluetense Documentación de las Ciencias de la Información*, *18*(1), 193–210.

Sánchez, F. (2008). *Redacción de documentos administrativos*. Escuela de Administración Pública, Comunidad Autónoma de la Región de Murcía.

Stinson, D. R. (2006). *Cryptography: Theory and Practice*. Chapman and Hall/CRC.

Tuecke, W. V. E. D. P. L., S., y Thompson, M. (2004). Internet x.509 public key infrastructure (pki) proxy certificate profile. rfc 3820 (proposed standard). *Internet Engineering Task Force*, *3820*(1), 1–37.